*Quaderni di* C.R.S.T.

Centro di Ricerca sulla Sicurezza ed il Terrorismo

Centro Ricerca Sicurezza e Terrorismo

Direttore Ranieri Razzante

Michele Punzi

# Analisi comparativa delle direttive NIS1 e NIS2

Pacini Giuridica

*Quaderni di*

C.R.S.T.

Centro di Ricerca sulla Sicurezza ed il Terrorismo

1. Dante Gatta, *Africa occidentale e Sahel: problematiche locali dalla valenza globale*
2. Miriam Ferrara e Dante Gatta, *Lineamenti di counter-terrorism comparato*
3. Alessandro Lentini, *Selected Issues in Counter-terrorism: special investigative techniques and the international judicial cooperation Focus on the European Union*
4. Michele Turzi, *The effects of Private Military and Security Companies on local populations in Afghanistan*
5. Ilaria Stivala, *Hezbollah: un modello di resistenza islamica multidimensionale*
6. Alessandro Anselmi, *Onion routing, cripto-valute e crimine organizzato*
7. Fabio Giannini, *La mafia e gli aspetti criminologici*
8. Giuseppe Lana, *Si Vis Pacem Para Ludum. Ping Pong Diplomacy: When Sport Breaks Walls*
9. Costanza Pestarino, *Permanent Structured Cooperation (PESCO). Opportunities and Risks for the italian military Sector*
10. Fabio Giannini, *Terrorismo internazionale. Aspetti criminologici e normativi*
11. Alessandro Anselmi, *Polizia e popolo. Dall'assolutismo allo stato di diritto tra il XVIII e il XIX secolo*
12. Antonio Rosato, *Profili penali delle criptovalute*
13. Giuliana Milone, *Recupero e valorizzazione dei beni confiscati alla criminalità organizzata*
14. Alessia Pietrantuono, *Sanzioni internazionali individuali e compliance come strumento di lotta al terrorismo*
15. Elena Canopoli, *Il coraggio di opporsi. Tutela e protezione nei confronti di chi denuncia la criminalità organizzata*
16. Sara Nazzaro, *Il valore educativo dei beni confiscati alla mafia*
17. Ken Terranova, *L'infiltrazione mafiosa nelle crisi: il caso dell'emergenza Coronavirus*
18. Bruno Mattia Balletti, *L'antiriciclaggio ai tempi dell'emergenza da Covid-19*
19. Sofia Mazzei, *The financing of Terrorism*
20. Mariagrazia Mazzaraco, *L'Intelligence economica nel dark web*
21. Michele Punzi, *Analisi comparativa delle direttive NIS1 e NIS2*



*Realizzazione editoriale*

Pacini Editore

Via A. Gherardesca
56121 Pisa

*Responsabile di redazione*
Gloria Giacomelli

## SOMMARIO

Nel processo di trasformazione digitale contemporanea, la cybersicurezza rappresenta uno snodo cruciale per la tutela delle infrastrutture critiche, dei dati personali e della fiducia nei servizi digitali da parte di tutti i cittadini europei.

L'elaborato analizza il percorso normativo dell'Unione Europea in materia di sicurezza informatica, con un *focus* comparativo sulle direttive NIS1 (Direttiva UE 2016/1148) e NIS2 (Direttiva UE 2022/2555).

Dopo aver contestualizzato l'evoluzione del quadro giuridico e le motivazioni strategiche alla base dell'intervento da parte del legislatore europeo, vengono esaminati i limiti incontrati nell'applicazione della NIS1 – quali la frammentarietà e l'eterogeneità di recepimento degli Stati membri – e le considerevoli innovazioni introdotte dalla NIS2, tra cui: ampliamento del campo di applicazione su soggetti prima esclusi, rafforzamento degli obblighi e dei requisiti di sicurezza, rigoroso coinvolgimento nelle responsabilità del settore per i vertici aziendali, nuovi e più rigidi meccanismi sanzionatori e un più articolato impianto di governance e cooperazione tra Stati membri.

Attraverso l'analisi sistematica dei testi normativi e il confronto con fonti dottrinali e istituzionali, il lavoro indaga le implicazioni operative ed economiche della nuova normativa per soggetti pubblici e privati, considerando soprattutto il settore delle piccole e medie imprese.

L'inclusione di un autorevole contributo del Prof. Ranieri Razzante, consulente istituzionale in materia di cybersecurity e tra i massimi esperti italiani nel settore

della sicurezza cibernetica e delle politiche di contrasto alle minacce digitali, arricchisce il lavoro offrendo una prospettiva critica e applicata alle sfide e le prospettive della cybersicurezza europea.

L'elaborato si propone così di fornire un contributo teorico e pratico alla comprensione del nuovo assetto regolatorio europeo, sottolineando l'urgenza di proseguire sulla strada legislativa intrapresa attraverso l'utilizzo di strumenti giuridici coerenti, attuali ed in grado di affrontare minacce transnazionali in uno scenario di sfide digitali sempre più complesse.

## INDICE

# INTRODUZIONE

Nel contesto dell'evoluzione digitale contemporanea, la sicurezza delle reti e dei sistemi informativi è diventata una priorità imprescindibile per le istituzioni pubbliche, le imprese e l'intera società.

La trasformazione digitale in atto ha investito i processi economici, amministrativi e sociali a partire sin dal primo decennio del XXI secolo ed ha generato opportunità straordinarie in termini di efficienza, innovazione e connettività, allo stesso tempo, tuttavia, ha esposto i citati processi a rischi digitali crescenti.

Gli attacchi informatici, sempre più sofisticati e frequenti, rappresentano senza dubbio le minacce più rilevanti alla stabilità delle infrastrutture critiche, alla tutela e sicurezza dei dati personali e, in ambito sociale, alla fiducia dei cittadini nell'utilizzo dei servizi digitali. Tali minacce non conoscono confini nazionali e si sviluppano con modalità transfrontaliere e con finalità eterogenee: dal *cybercrime* ai *ransomware*, dallo spionaggio industriale agli attacchi di matrice geopolitica.

Lo scenario del *cyberspazio* è divenuto il terreno di confronto, conflitto e vulnerabilità sistemica globale. È in questo scenario che gli Organi dell'Unione Europea hanno maturato la consapevolezza della necessità di dotarsi di un quadro normativo organico e coerente per garantire un adeguato livello comune di cybersicurezza in tutti gli Stati membri. Già a partire dal 2016, con l'adozione della Direttiva (UE) 2016/1148, nota come Direttiva NIS (Network and Information Security), di seguito identificata come Direttiva NIS1 per semplificazione, l'Unione Europea ha compiuto un primo passo verso l'armonizzazione delle politiche di sicurezza informatica, imponendo agli Stati membri obblighi minimi in termini di strategia nazionale, cooperazione istituzionale e misure di sicurezza per gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD). Tuttavia, la natura di *"armonizzazione minima"* contemplata dalla NIS1 ed il suo

recepimento e conseguente attuazione disomogenea nei diversi ordinamenti nazionali hanno presto mostrato sia il limite di un approccio frammentario sia quello della natura poco vincolante dell'atto giuridico europeo utilizzato in un settore già di per sé molto tecnico.

La rapida evoluzione delle minacce, il moltiplicarsi degli attori coinvolti, l'interconnessione sempre più spinta tra settori e Paesi e la pressione esercitata da eventi globali recenti – tra cui la pandemia *COVID-19* ed il conflitto in Ucraina – hanno evidenziato l'urgenza di un rafforzamento del quadro normativo e sua conseguente revisione. In risposta a tale esigenza, nel dicembre 2022 è stata adottata la Direttiva (UE) 2022/2555, conosciuta come Direttiva NIS2, che è entrata in vigore nel gennaio 2023 ed è stata recepita in Italia con il Decreto legislativo n. 138/2024, entrato in vigore il 18 ottobre 2024.

La NIS2 si propone l'obiettivo di superare le criticità emerse con la precedente direttiva attraverso una serie di interventi e modifiche dell'impianto normativo preesistente ampliando il campo di applicazione, rafforzando i requisiti di sicurezza richiesti alle organizzazioni, potenziando e coinvolgendo maggiormente i meccanismi di governance ed introducendo un sistema sanzionatorio più rigido ed incisivo.

L'elaborato si propone di analizzare in maniera comparativa le due direttive, con l'obiettivo di mettere in luce i principali elementi di continuità e discontinuità, le criticità riscontrate nell'attuazione della NIS1, le novità normative introdotte dalla NIS2 cercando di cogliere le implicazioni operative per i soggetti pubblici e privati che ricadono nel suo perimetro di azione. Attraverso un'analisi sistematica del testo normativo, supportata da fonti dottrinali, report tecnici e documenti istituzionali (in particolare modo quelli prodotti da ENISA, ACN e la Commissione Europea), si intende valutare l'impatto della nuova disciplina in termini di efficacia, proporzionalità, sostenibilità e armonizzazione a livello europeo.

Il primo capitolo contestualizza il tema della sicurezza informatica nel panorama europeo, illustrando il quadro normativo generale e soffermandosi sugli obiettivi strategici delle direttive NIS e NIS2. Si pone l'accento sulle esigenze che hanno portato l'Unione Europea ad intervenire in maniera sistematica, focalizzando il legame tra cybersicurezza, digitalizzazione e resilienza delle infrastrutture critiche.

Il secondo capitolo è dedicato all'analisi della direttiva NIS come *opera prima* nel settore, esaminando i suoi obiettivi principali, l'ambito di applicazione, il ruolo degli *operatori di servizi essenziali* (OSE) e dei *fornitori di servizi digitali* (FSD), nonché le principali criticità che gli Stati membri hanno riscontrato nell'implementazione della norma durante l'*iter* applicativo e che hanno reso necessaria una robusta revisione normativa.

Il terzo capitolo affronta la nuova direttiva NIS2, mettendo in luce le principali e determinanti novità rispetto alla precedente, analizzando l'ampliamento del campo di applicazione, il rafforzamento degli obblighi di sicurezza e dei meccanismi sanzionatori, le nuove sfide organizzative per gli enti coinvolti e le *best practices* per l'adeguamento normativo.

Nel quarto ed ultimo capitolo, l'analisi comparativa tra le due direttive si concentra sulla ridefinizione delle responsabilità della *governance* delle organizzazioni, sulla gestione del rischio e sulla cooperazione istituzionale a livello europeo, vero fattore innovativo nella costruzione di un sistema normativo più coerente, armonizzato e capace di affrontare le minacce cibernetiche transfrontaliere e multilivello.

Nelle conclusioni, infine, si pone l'accento sulla evoluzione strutturale della normativa europea nella cybersicurezza, ampliando il numero di soggetti coinvolti, rafforzando gli obblighi di sicurezza e attribuendo maggiore responsabilità ai vertici aziendali. Le principali sfide di questo nuovo approccio includeranno l'adeguamento organizzativo e tecnologico delle PMI, la necessità

di un'applicazione nazionale efficace ed uniforme, il coordinamento tra normative sovrapposte e la gestione della crescente complessità del contesto geopolitico e digitale. Per affrontarle, serviranno supporto istituzionale, cooperazione multilivello e una strategia condivisa tra tutti gli attori coinvolti.

Nel complesso, la tesi intende offrire un contributo teorico e operativo alla comprensione del nuovo assetto regolatorio europeo in tema di cybersicurezza, evidenziandone il potenziale normativo ma anche le criticità applicative del citato nuovo assetto. In un'epoca in cui la sicurezza informatica non è più un tema settoriale ma una dimensione trasversale che coinvolge tutte le strutture economiche, amministrative e sociali, è essenziale dotarsi di strumenti normativi coerenti, aggiornati e capaci di affrontare le minacce in modo sistemico e multilivello. La Direttiva NIS2 rappresenta, in questo senso, un passo decisivo verso una cybersicurezza europea più solida, integrata e condivisa.

Nell'ambito dell'elaborato è stato ritenuto opportuno integrare un contributo autorevole volto ad approfondire gli aspetti evolutivi e applicativi del nuovo quadro normativo europeo in materia di sicurezza informatica, coinvolgendo il Prof. Ranieri Razzante in un'intervista riportata in allegato. Avvocato, dottore commercialista e revisore dei conti, il docente è esperto in materie legate alla sicurezza cibernetica, al *cybercrime* e alla gestione dei rischi di riciclaggio in diverse prestigiose sedi accademiche italiane ed Istituti militari, consulente istituzionale in materia di cybersecurity ed è tra i massimi esperti italiani nel settore della sicurezza cibernetica e delle politiche di contrasto alle minacce digitali. Ricopre importanti incarichi istituzionali ed ha svolto ruoli di consulenza per la Commissione Parlamentare Antimafia e per il Governo, contribuendo anche alla strategia nazionale sull'intelligenza artificiale.

L'intervista affronta tematiche centrali relative al passaggio dalla NIS1 alla NIS2, con particolare attenzione agli elementi innovativi della direttiva, alle sfide operative per gli Stati membri e alle prospettive evolutive del diritto europeo in questo ambito strategico. Il contributo del Prof. Razzante si configura come un

prezioso complemento alla trattazione teorica, offrendo uno sguardo critico e qualificato sull'effettiva portata della NIS2 e sul futuro della *governance* della cybersicurezza nell'Unione Europea.

# 1. LA SICUREZZA INFORMATICA

## 1.1 Contesto normativo nell'Unione Europea

Il processo di digitalizzazione globale è entrato prepotentemente nell'evoluzione delle società contemporanee e la sicurezza informatica ha scalato le priorità delle politiche pubbliche assumendo un ruolo centrale e fondamentale nella programmazione delle agende politiche dei membri dell'Unione Europea e di conseguenza di quelle nazionali. Consapevole della dimensione transnazionale e della complessità sistemica delle minacce cibernetiche, l'UE ha intrapreso, nell'ultimo decennio, un percorso di progressiva definizione e rafforzamento del proprio assetto normativo, con l'obiettivo di assicurare un livello uniforme e adeguato di protezione delle reti e dei sistemi informativi all'interno dei confini dell'Unione.

Il primo importante intervento normativo a livello europeo in tale contesto è rappresentato dalla Direttiva (UE) 2016/1148, nota come Direttiva NIS (Network and Information Security), la quale ha introdotto per la prima volta obblighi vincolanti per gli Stati membri in materia di sicurezza cibernetica[1]. Il provvedimento impone, in buona sostanza, l'adozione di strategie nazionali di cybersicurezza, la designazione di autorità competenti, nonché l'identificazione degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD), imponendo a tali soggetti l'obbligo di adottare misure tecniche e organizzative adeguate alla gestione del rischio e alla prevenzione degli incidenti informatici.

Alla luce delle crescenti criticità emerse negli anni successivi ed il mutato panorama geopolitico globale dovuto a diverse cause, l'Unione Europea ha adottato la Direttiva (UE) 2022/2555 (NIS2), che amplia la portata della normativa

[1] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, relativa a misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione recepita in Italia con il Decreto legislativo n. 65 del 18 maggio 2018, entrato in vigore il 26 giugno 2018.

originaria[2], estendendo gli obblighi a nuovi settori e soggetti, rafforzando i meccanismi di governance e introducendo un sistema armonizzato di sanzioni. La NIS2 rappresenta, come vedremo, una tappa fondamentale nella costruzione di un ecosistema normativo europeo, in rapida evoluzione, in grado di affrontare nuove e più complesse minacce.

Accanto alle normative NIS, succedutesi nel tempo, un ruolo rilevante è rappresentato dal Cybersecurity Act (Regolamento (UE) 2019/881), che pone il mandato permanente all'Agenzia dell'Unione europea per la cybersicurezza (ENISA) al centro dell'azione settoriale, rafforzandone le competenze in materia di assistenza agli Stati membri, analisi delle minacce e supporto tecnico[3]. Il regolamento ha inoltre istituito un quadro europeo per la certificazione della cybersicurezza, finalizzato a garantire standard comuni per la sicurezza dei prodotti, servizi e processi digitali all'interno del mercato unico.

Un ulteriore pilastro normativo è costituito dal Regolamento generale sulla protezione dei dati (GDPR – Regolamento (UE) 2016/679), che, pur non essendo orientato esclusivamente sulla cybersicurezza, impone alle organizzazioni l'obbligo di adottare misure adeguate alla protezione dei dati personali, incluse quelle di natura tecnico-organizzativa[4]. In particolare, l'obbligo di notifica delle violazioni di dati personali (*data breach*) costituisce un importante strumento di trasparenza e *accountability* nel contesto della sicurezza informatica.

---

[2] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recepita in Italia con il Decreto legislativo n. 138/2024, entrato in vigore il 18 ottobre 2024.

[3] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA e alla certificazione della cybersicurezza.

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).

L'introduzione della Direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici (CER), che integra la NIS2 affrontando non solo i rischi digitali ma anche quelli fisici, con l'obiettivo di tutelare il funzionamento continuativo di settori strategici per la società e l'economia europea, ha completato il quadro normativo in parola[5].

Le principali normative cui si è fatto cenno rappresentano la più ampia cornice delineata dalla Strategia dell'UE per la cybersicurezza del 2020, che individua come priorità la promozione di un cyberspazio aperto, sicuro e stabile, sostenuto da un'effettiva cooperazione tra Stati membri, istituzioni europee ed il mondo privato[6].

Il contesto normativo globale in materia di sicurezza informatica è intuibile sia configurato come un sistema complesso e articolato, in costante evoluzione, orientato a contrastare e a rispondere in maniera coordinata e integrata alle sfide in continua evoluzione che la trasformazione digitale e le minacce cibernetiche globali presentano. La coerenza tra le diverse fonti normative, il loro recepimento a livello nazionale e la successiva attuazione, costituiscono elementi cruciali per la costruzione di una vera sovranità digitale europea.

## 1.2 Obiettivi delle direttive NIS e NIS2

Il processo di digitalizzazione globale cui si faceva riferimento in precedenza ha reso necessario la nascita di un quadro normativo solido e armonizzato in ambito europeo per fronteggiare l'esponenziale crescita delle minacce informatiche. In questo contesto si inseriscono le due direttive NIS (Network and Information

[5] Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sulla resilienza dei soggetti critici, recepita in Italia con Decreto Legislativo n. 134 del 4 settembre 2024.

[6] Commissione Europea, EU Cybersecurity Strategy for the Digital Decade, COM (2020) 605 final. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Security), che rappresentano i due cardini dello sviluppo della strategia dell'Unione Europea in materia di cybersicurezza.

La Direttiva NIS (Direttiva (UE) 2016/1148), entrata in vigore nel luglio 2016, è stata la prima normativa europea particolareggiata in ambito sicurezza delle reti e dei sistemi informativi. Il suo obiettivo primario era quello di innalzare il livello complessivo di sicurezza informatica negli stati membri, cercando di uniformare l'approccio nella gestione dei rischi digitali e la notifica degli incidenti di sicurezza[7].

Tra gli obiettivi generali della NIS si possono individuare:

a) il miglioramento delle capacità nazionali in materia di cybersicurezza attraverso l'istituzione di Autorità dedicate e competenti in materia, come il CSIRT (Computer Security Incident Response Teams) e di strategie nazionali;

b) la promozione di una maggiore cooperazione tra gli Stati membri, operativa attraverso la costituzione del Gruppo di Cooperazione NIS;

c) l'introduzione di obblighi di sicurezza e di notifica per gli operatori di servizi essenziali (OSE) e per alcuni fornitori di servizi digitali (FSD), finalizzati ad aumentare la resilienza dei settori strategici[8].

Tuttavia, la rapida evoluzione del panorama delle minacce cyber e le disomogeneità riscontrate nell'implementazione della NIS nei diversi Stati membri, ma come vedremo non solo per questi motivi, hanno reso necessaria una rivisitazione della direttiva e da qui la nascita della Direttiva NIS2 (Direttiva

[7] ENISA – European Union Agency for Cybersecurity (2017). *"Overview report on the implementation of the NIS Directive"*.

[8] Commissione Europea (2016) *"Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 relativa a misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"*.

(UE) 2022/2555), adottata nel dicembre 2022 ed entrata in vigore nel gennaio 2023.

La NIS2, come accennato recepita in Italia ed entrata in vigore nell'ottobre del 2024, amplia significativamente il campo di applicazione della precedente direttiva, includendo nuovi settori e categorie di soggetti, tra cui spiccano sanità, pubblica amministrazione, fornitori di servizi cloud e infrastrutture digitali allo scopo di garantire a livello UE un più elevato livello comune di cybersicurezza, superando le lacune normative della NIS[9].

Tra gli elementi innovativi introdotti dalla NIS2 si segnalano in particolar modo:

a) l'estensione degli obblighi di sicurezza e notifica a un numero più ampio di entità pubbliche e private, classificate come "*essenziali*" o "*importanti*"[10];

b) il rafforzamento della responsabilità a livello di *governance*, imponendo agli organi direttivi delle organizzazioni obblighi specifici in termini di gestione del rischio;

c) la promozione di una cooperazione rafforzata tra Autorità nazionali ed europee, anche tramite la creazione dell'EU-CyCLONe (European Cyber Crises Liaison Organisation Network)[11], incaricato di coordinare la gestione delle crisi informatiche transfrontaliere.

---

[9] Parlamento Europeo e Consiglio dell'Unione Europea (2022) *"Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione"*.

[10] Commissione Europea (2020). *"Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione"*. COM (2020) 823 final.

[11] Questa rete, creata nel 2020 su impulso italo-francese e formalmente istituita con l'entrata in vigore della Direttiva NIS2, è finalizzata a sostenere la gestione coordinata di incidenti e crisi cyber su vasta scala e a garantire lo scambio regolare di informazioni tra gli Stati membri e le istituzioni dell'Unione, enti ed agenzie. In tale contesto assicura il livello operativo, che nell'architettura europea di gestione delle crisi cyber si pone come strato intermedio tra il livello tecnico e quello

In conclusione, le direttive NIS e NIS2 sono tappe fondamentali nel percorso dell'Unione Europea verso un sistema di digitalizzazione più sicuro e resiliente. La NIS ha rappresentato le basi per una cooperazione strutturata e per un primo livello minimo di protezione, la recentissima entrata in vigore della NIS2 mira a consolidare tali risultati e ad adattarli al mutato scenario ed alle nuove sfide della trasformazione digitale, rafforzando il sistema europeo di cybersicurezza.

## 2. LA DIRETTIVA NIS

### 2.1 Obiettivi principali, ambito di applicazione, criticità e ruolo degli *operatori di servizi essenziali* e dei *fornitori di servizi digitali*

L'introduzione della direttiva NIS rappresenta un momento di svolta nelle politiche europee in materia di sicurezza informatica. La crescente digitalizzazione dei servizi pubblici e privati ha determinato l'azione urgente dell'Unione Europea nel predisporre un quadro normativo comune in grado di rafforzare la resilienza delle infrastrutture digitali. La direttiva, per la prima volta, obbliga giuridicamente in modo vincolante i Paesi membri e determinati operatori economici considerati strategici[12]. In tal senso, essa impone la designazione di Autorità nazionali competenti, la creazione di CSIRT (Computer Security Incident Response Teams), nonché l'elaborazione di strategie nazionali di cybersicurezza in linea con gli obiettivi europei[13].

Gli obiettivi principali della direttiva comprendono: il rafforzamento delle capacità nazionali di gestione della sicurezza informatica, la promozione della cooperazione tra Stati membri, l'innalzamento del livello di sicurezza degli

strategico/politico. ENISA (2023) *"NIS2 Directive: A high common level of cybersecurity in the EU"*.

[12] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, (1) e (3).

[13] ibidem, artt. 7, 8 e 9.

operatori di servizi essenziali[14] e dei fornitori di servizi digitali, e l'obbligo per questi ultimi di notificare eventuali incidenti rilevanti alle Autorità competenti[15]. L'ambito di applicazione della Direttiva è piuttosto ampio e include settori strategici quali energia, trasporti, banca, infrastrutture dei mercati finanziari, sanità, approvvigionamento e distribuzione di acqua potabile e infrastrutture digitali[16]. Anche alcuni fornitori di servizi digitali, come motori di ricerca, servizi *cloud* e piattaforme di *e-commerce*, rientrano tra i soggetti destinatari della norma[17].

Tuttavia, nonostante le sue ambizioni iniziali, la direttiva NIS ha evidenziato diverse criticità nella fase applicativa. Una delle problematiche principali riguarda l'eterogeneità con cui gli Stati membri hanno recepito e attuato le disposizioni, con approcci divergenti nella definizione dei soggetti coinvolti, nella capacità operativa dei CSIRT e nei meccanismi di vigilanza[18].

La nascita della Direttiva NIS ha consentito un passo fondamentale nella costruzione di un quadro normativo comune europeo per la sicurezza delle reti e dei sistemi informativi, frutto della crescente consapevolezza del ruolo strategico ricoperto dall'infrastruttura digitale nell'ambito economico, geopolitico, ma anche nella sicurezza e nel funzionamento delle società europee.

Tra le principali novità introdotte dalla Direttiva, occupa un ruolo rilevante la classificazione di due categorie di attori responsabili della sicurezza informatica

---

[14] La definizione di *"servizi essenziali"*, sebbene delineata all'articolo 5 e nell'Allegato II della Direttiva 2016/1148, ha lasciato ampi margini interpretativi. Gli Stati membri hanno avuto difficoltà nell'applicare criteri uniformi per l'identificazione degli operatori di servizi essenziali, causando differenze significative nell'attuazione della direttiva tra i vari Paesi.

[15] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, artt. 14 e 16.

[16] ibidem art. 4 e Allegato II.

[17] ibidem, art. 16.

[18] ENISA, European Union Agency for Cybersecurity, *"NIS Directive: Lessons Learned"*, 2020.

in generale: da una parte gli *operatori di servizi essenziali* (OSE), dall'altra i *fornitori di servizi digitali* (FSD). Entrambi questi attori contribuiscono alla protezione delle infrastrutture digitali europee con obblighi e responsabilità differenti.

Gli *operatori di servizi essenziali* sono entità – pubbliche o private – che operano in settori considerati critici per il funzionamento della società e dell'economia come, ad esempio, il settore energetico, i trasporti, la sanità, la fornitura di acqua potabile e le infrastrutture digitali. L'interruzione o la compromissione di questi servizi potrebbe avere effetti gravi sulla collettività, per questo la Direttiva richiede agli operatori di servizi essenziali di adottare misure tecniche e organizzative appropriate per prevenire e gestire i rischi legati alla sicurezza dei sistemi informatici da cui dipendono[19].

A tali soggetti viene richiesto anche di notificare, *senza ingiustificato ritardo*, qualsiasi incidente che abbia un impatto rilevante sulla continuità e sulla qualità del servizio offerto. Queste segnalazioni vanno indirizzate alle Autorità nazionali competenti o ai CSIRT, che hanno il compito di coordinare la risposta a livello nazionale e, se necessario, a livello europeo[20].

Come accennato, accanto agli operatori di servizi essenziali, la norma individua i *fornitori di servizi digitali*, categoria che include le piattaforme di e-*commerce*, i motori di ricerca *online* e i fornitori di servizi di *cloud computing*, i quali, sebbene non rientrino nella classificazione come *"essenziali"* nel senso più stretto, rivestono un ruolo sempre più centrale nella quotidianità del mondo sociale e nelle dinamiche economiche. La Direttiva riconosce che anche questi attori

[19] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, art. 4, par. 4.

[20] ibidem, art. 14.

possono essere esposti a rischi informatici che, se non gestiti adeguatamente, possono avere impatti significativi[21].

In tal senso, la Direttiva adotta un approccio più flessibile ed elastico per i fornitori di servizi digitali, attraverso obblighi di sicurezza presenti ma meno rigidi ed invasivi, anche a livello di controllo, da parte delle autorità. La minor rigidità verso questi attori è dettata dai servizi offerti che spesso hanno natura diversa e dalla loro dimensione che è spesso transnazionale, rendendo chiaramente più complessa l'applicazione di norme di dettaglio emanate a livello nazionale fuori dai confini.

La Direttiva NIS introduce, dunque, un primo modello di governance della cybersicurezza fondato sulla collaborazione tra attori pubblici e privati, in cui ciascun soggetto è chiamato a giocare un ruolo importante. Gli operatori di servizi essenziali e i fornitori di servizi digitali sono così coinvolti in un articolato sistema di prevenzione e risposta agli incidenti informatici che mira a garantire la stabilità, l'affidabilità e la resilienza di tutto il *mondo* cyber europeo.

La direttiva ha rappresentato un primo, importante passo verso l'armonizzazione delle norme europee nell'ambito della sicurezza informatica che rappresenta uno snodo cruciale per la tutela degli interessi economici, sociali, geopolitici ed istituzionali degli Stati membri. Il suo impianto ha posto le basi per un approccio condiviso, in cui la protezione delle infrastrutture digitali non è solo una questione tecnica, ma una responsabilità collettiva che, come vedremo nel seguito di questo elaborato, rappresenterà in maniera sempre più determinante il cardine delle politiche europee del settore.

[21] ibidem, art. 16.

## 2.2 Problematiche riscontrate nell'implementazione della Direttiva NIS e necessità di una revisione normativa.

Senza alcun dubbio la Direttiva NIS (2016/1148) ha rappresentato un significativo e importantissimo passo in ambito UE finalizzato a rafforzare il panorama della cybersicurezza a livello comunitario, introducendo, come detto, obblighi per gli Stati membri relativi all'identificazione di operatori di servizi essenziali (OSE), alla designazione dei Computer Security Incident Response Teams (CSIRT) e alla predisposizione di strategie nazionali di cybersicurezza.

Tuttavia, la sua implementazione ha evidenziato già nell'immediato diverse criticità che hanno ostacolato l'efficacia del progetto normativo e reso necessaria una successiva revisione.

In primo luogo, tra le principali problematiche riscontrate si evidenzia l'eterogeneità nell'attuazione da parte degli Stati membri in quanto, atto legislativo di armonizzazione minima, la Direttiva ha lasciato ampi margini di discrezionalità e di manovra alle autorità nazionali, con il risultato di approcci diversi e talvolta divergenti sia nella designazione degli operatori di servizi essenziali (OSE) che nella definizione degli obblighi di sicurezza e notifica degli incidenti[22].

Tale criticità ha provocato la compromissione dell'approccio europeo alla cybersicurezza, che si era prefissato il legislatore europeo limitando di fatto la capacità dell'Unione di rispondere in modo coordinato, coerente ed efficace alle minacce cyber. Ulteriore criticità è stata evidenziata dalla diversità nei requisiti tecnici e procedurali che hanno creato un carico amministrativo sproporzionato per le imprese che operavano in più Paesi dell'Unione.

[22] European Commission, *"Cybersecurity: Implementation of the NIS Directive"*, COM(2020) 605, Brussels, 2020.

Nello specifico, è utile ricordare l'emersione di una mancanza di chiarezza nella classificazione dei soggetti obbligati, con particolare riferimento alle soglie per l'identificazione degli OSE e dei FSD, dove, in assenza di criteri uniformi prestabiliti, ciascuno Stato membro ha adottato metodologie differenti, generando ulteriore incertezza per gli operatori economici attivi su scala transfrontaliera. Il quadro delineato evidenzia un'applicazione quantomeno disomogenea degli obblighi di cybersicurezza, con effetti distorsivi che si riflettono nel medio-lungo periodo sul mercato interno e sulla concorrenza[23].

In secondo luogo, ulteriore elemento critico è stato rappresentato dalla debolezza del meccanismo di cooperazione tra gli Stati membri, ovvero il Network dei CSIRT e il Gruppo di cooperazione istituiti dalla Direttiva. La collaborazione tra i CSIRT nazionali è risultata spesso minata dalla mancanza di fiducia reciproca, da barriere linguistiche e da differenti livelli di maturità tecnologica derivante dalle diverse evoluzioni normative adottate da ogni Stato[24]. Inoltre, il sistema di scambio di informazioni e la gestione degli incidenti non sempre hanno garantito tempestività ed efficacia.

Alla luce non solo delle principali criticità citate ma anche a causa del contesto geopolitico globale in continua evoluzione nonché del profondo processo di digitalizzazione, il legislatore europeo ha ritenuto necessario procedere con la revisione normativa che porterà all'attuale adozione della Direttiva (UE) 2022/2555, nota come Direttiva NIS 2, entrata in vigore il 16 gennaio 2023 e recepita in Italia nell'ottobre del 2024. In breve, la nuova direttiva mira a superare i limiti della NIS attraverso un approccio più omogeneo e più vincolante, ampliando l'elenco dei settori critici ed introducendo criteri oggettivi per

---

[23] DE CAPITANI di VIMERCATI S. (2021) *"La Direttiva NIS e il futuro della sicurezza informatica in Europa"*, Rivista di diritto dell'informazione e dell'informatica, n. 1, pp. 35–58.

[24] ENISA, "State of Cybersecurity in the EU under the NIS Directive", 2021, https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu

l'identificazione dei soggetti obbligati. Tutto ciò sotto meccanismi di controllo rafforzati in ambito di governance e a livello europeo[25] che vedremo più nello specifico esaminando le principali novità introdotte dalla NIS2.

Qui è importante ricordare l'introduzione della responsabilità diretta degli organi di gestione delle imprese soggette, che devono garantire l'attuazione delle misure di cybersicurezza previste e l'introduzione di regimi sanzionatori più severi in caso di inadempienza, al fine di garantire un'effettiva dissuasione e un convincente invito ad adeguarsi rapidamente ed efficacemente alle norme.

Questo approccio rappresenta un cambiamento di paradigma, che considera la cybersicurezza non più come una mera questione tecnica, gestita da soli tecnici, ma come una componente strategica della governance aziendale che diviene assolutamente centrale per il rispetto e l'applicazione della norma.

In conclusione, l'esperienza dell'attuazione della Direttiva NIS evidenzia l'importanza di un quadro normativo coerente e condiviso, accentrato e adattabile alla rapida evoluzione delle minacce cibernetiche. Il passaggio alla NIS 2 rappresenta un tentativo concreto di rispondere alle esigenze descritte, ma la sua efficacia dipenderà, come d'altronde la gran parte delle normative emanate dall'UE non di diretta applicazione, ineluttabilmente dall'impegno profuso dagli Stati membri nella sua implementazione e dal rafforzamento della cooperazione con gli altri Stati membri.

In Italia, l'attuazione della Direttiva NIS ha visto una prima formalizzazione con il D.lgs. 65/2018, che ha individuato i soggetti pubblici e privati rientranti tra gli OSE ed i FSD[26].

---

[25] European Parliament and Council, *"Directive (EU) 2022/2555 (NIS 2 Directive)"*, Official Journal of the European Union, L 333/80, 27.12.2022.

[26] Il D.lgs. 65/2018 rappresenta il recepimento della Direttiva NIS e introduce, per la prima volta nell'ordinamento italiano, obblighi specifici in materia di sicurezza informatica per gli OSE ed i FSD. Il decreto stabilisce criteri per l'identificazione di tali soggetti, impone l'adozione di misure tecniche e organizzative adeguate al fine di prevenire e gestire gli incidenti informatici e introduce l'obbligo di notifica degli stessi

Successivamente con l'introduzione della NIS 2, il governo italiano ha avviato un processo di aggiornamento normativo, culminato con l'adozione del D.lgs. 82/2023, volto a recepire integralmente la nuova direttiva, rafforzando i poteri dell'Agenzia per la Cybersicurezza Nazionale (ACN) e ampliando significativamente il perimetro dei soggetti obbligati[27].

## 3. LA DIRETTIVA NIS2

### 3.1 Evoluzione normativa e principali novità rispetto alla NIS

L'introduzione della Direttiva (UE) 2022/2555 (NIS2) rappresenta indubbiamente una delle più originali ed ambiziose riforme normative in materia di cybersicurezza in ambito europeo negli ultimi anni. La normativa rappresenta un cambio di passo rispetto al precedente quadro delineato dalla direttiva (UE) 2016/1148 (NIS), introducendo elementi profondamente innovativi sia sul piano concettuale, sia su quello operativo e sanzionatorio. Il contesto sociale, geopolitico ed economico che ha condotto all'adozione della NIS2 è stato caratterizzato da una crescente complessità delle minacce informatiche, come evidenziato e confermato dalle più recenti anali che mostrano un incremento esponenziale di attacchi cyber a infrastrutture critiche, aziende private e

agli organismi competenti. Inoltre, definisce la governance nazionale in ambito di cybersicurezza, individuando il Ministero dello Sviluppo Economico (oggi MIMIT), l'Agenzia per l'Italia Digitale (AgID) e il Ministero dell'Interno tra le autorità responsabili per l'attuazione della norma e la vigilanza del perimetro delineato.

[27] Il D.lgs. 82/2023 ha ampliato il perimetro nazionale di sicurezza, includendo nuovi settori e rafforzando i meccanismi di vigilanza, coordinamento e ispezione. L'ACN è stata incaricata di svolgere un ruolo centrale non solo nella gestione degli incidenti e nella prevenzione, ma anche nella promozione di una cultura diffusa della sicurezza cibernetica presso le pubbliche amministrazioni, le imprese e i cittadini, iniziando un processo di adeguamento agli standard europei e tentando di rafforzare la resilienza del proprio sistema economico e istituzionale - Presidenza del Consiglio dei Ministri – Agenzia per la Cybersicurezza Nazionale, *"Linee guida per il recepimento della Direttiva NIS 2"*, Roma, 2023.

pubbliche amministrazioni in tutto il territorio europeo e non solo. Ad esempio, un report del 2022 pubblicato da ENISA, ha evidenziato che, nel solo 2021, circa il 66% degli incidenti gravi è dipeso da vulnerabilità nella supply chain, ossia da debolezze nei sistemi dei fornitori terzi[28].

Una delle innovazioni più rilevanti è senza dubbio l'ampliamento dell'ambito soggettivo e oggettivo della normativa, in quanto la Direttiva NIS si applicava soltanto agli operatori di servizi essenziali e ai fornitori di servizi digitali, identificati preventivamente dagli Stati membri, la NIS2, invece, introduce criteri molto più armonizzati e oggettivi per la classificazione automatica degli enti obbligati, distinti in enti essenziali ed enti importanti, includendo nuovi ed importanti settori strategici come i servizi postali, la gestione dei rifiuti, le telecomunicazioni, la pubblica amministrazione centrale e, in alcuni casi, anche le PMI se operanti in ambiti ad alta rilevanza sistemica[29].

L'articolo 5 della direttiva stabilisce in modo puntuale i criteri dimensionali, indicando che un'entità è soggetta alla stessa se supera la soglia di 50 dipendenti o 10 milioni di euro di fatturato annuo[30].

Tale estensione risponde all'esigenza, emersa nella prassi applicativa della NIS, di superare i disallineamenti nazionali e di garantire una protezione più omogenea del tessuto economico europeo. Come ha osservato il *white paper* del Competence Center Cyber 4.0 in collaborazione con TIM, *"la NIS2 si propone di superare la frammentazione e di consolidare un quadro europeo realmente integrato per la sicurezza cibernetica"*[31].

---

[28] ENISA, *"Threat Landscape 2022"*, European Union Agency for Cybersecurity, 2022.

[29] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, Allegati I e II.

[30] ibidem, art. 5, par. 2.

[31] Cyber 4.0 – TIM Enterprise, *White Paper NIS2*, Roma, 2023.

Anche in Italia, il recepimento di tale direttiva è avvenuto con il D.lgs. 15 novembre 2023, n. 82, che attribuisce un ruolo centrale all'Agenzia per la Cybersicurezza Nazionale (ACN), alla quale è demandata la vigilanza sull'adempimento degli obblighi di sicurezza da parte degli operatori, come stabilito dall'art. 8, comma 1, lett. b)[32] e sui quali torneremo più avanti.

Sul piano degli obblighi, l'approccio della NIS2 è orientato alla gestione integrata e preventiva del rischio cibernetico, piuttosto che alla mera risposta agli incidenti che si verificano. Gli articoli 20 e 21 della direttiva impongono alle entità obbligate di adottare misure tecnico-organizzative adeguate e documentate, quali ad esempio: l'analisi del rischio, la gestione degli incidenti, la continuità operativa, il controllo degli accessi, la cifratura dei dati, la sicurezza dei sistemi durante l'intero ciclo di vita e, soprattutto, la valutazione della sicurezza dei fornitori e subappaltatori ICT, elemento che segna il vero cambio di paradigma nella norma e che sana una lacuna della precedente NIS1[33].

ENISA ha dedicato un intero manuale alle buone pratiche nella gestione della sicurezza della *supply chain*, sottolineando che "l'approccio sistemico ai fornitori deve diventare un pilastro delle strategie di resilienza digitale"[34].

Questa esigenza è stata colta anche dalla stampa economica, come evidenziato da *Il Sole 24 Ore*, "con la NIS2, la sicurezza dei fornitori entra definitivamente nel perimetro di responsabilità delle aziende, con implicazioni contrattuali e reputazionali"[35].

---

[32] D.lgs. 15 novembre 2023, n. 82, art. 8, co. 1, lett. b), G.U. n. 273 del 22.11.2023.

[33] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 21.

[34] ENISA, *Good Practices for Supply Chain Cybersecurity*, 2021, https://www.enisa.europa.eu

[35] M. Ruggiero, *"NIS2, svolta digitale per la sicurezza delle imprese italiane"*, in *Il Sole 24 Ore*, 2023.

Non meno importante è la responsabilizzazione degli organi direttivi delle entità soggette alla norma, tanto da introdurre il principio di *accountability verticale* con attribuzione ai vertici aziendali, non solo della supervisione, ma anche della responsabilità effettiva della compliance normativa in materia di cybersicurezza[36].

Come osserva Pizzetti, "la cybersicurezza diventa parte della cultura di impresa e della legalità organizzativa"[37]. Questa impostazione si inserisce in un più ampio processo di convergenza e armonizzazione tra le normative europee di settore ed in particolare tra NIS2 e GDPR, che condividono la logica della responsabilizzazione e della *"privacy by design/security by design".*

Il sistema di notifica degli incidenti è stato anch'esso rafforzato e strutturato secondo una procedura che prevede diverse fasi e che analizzeremo più avanti; esso va dalla notifica iniziale (entro 24 ore), ad un aggiornamento (entro 72 ore) per finire con una relazione dettagliata (entro un mese)[38].

La complessità crescente degli attacchi — si pensi ai casi di *ransomware* del 2023 contro strutture ospedaliere e logistiche in Francia e Germania[39] — ha spinto il legislatore a definire tempistiche più precise ed una sequenza comunicativa maggiormente standardizzata e scadenze predeterminate.

A livello istituzionale, l'introduzione del concetto di *governance multilivello* prevista dalla direttiva coinvolge il Gruppo di cooperazione, i CSIRT nazionali e la nuova rete EU-CyCLONe, che opera nei casi di crisi cibernetiche su larga

---

[36] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 20.

[37] Pizzetti D., *La cybersicurezza come diritto fondamentale*, Giappichelli, 2022, p. 89.

[38] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 23.

[39] *"Cybersicurezza, UE in allerta dopo i cyberattacchi a settori sanitari e logistici"*, in *la Repubblica*, 2 giugno 2023.

scala[40]. Questa scelta è stata ribadita dalla Commissione Europea come l'architettura più efficace essendo multilivello e destinata a integrarsi con altri importanti strumenti normativi settoriali come il regolamento DORA (settore finanziario) e la direttiva CER (resilienza fisica delle infrastrutture critiche)[41].

A ciò si aggiunge l'importanza crescente del concetto di *cyber resilience*, intesa come la capacità non solo di prevenire e rispondere agli attacchi, ma anche di adattarsi e continuare a operare in condizioni di crisi digitale. Tale approccio è stato al centro anche del Cyber Resilience Act proposto dalla Commissione Europea nel 2022, orientato a sanare le mancanze dei requisiti di sicurezza dei prodotti con elementi digitali fin dalla progettazione (security by design) e lungo l'intero ciclo di vita del prodotto stesso[42].

Dal punto di vista dottrinale, diversi autori hanno sottolineato la necessità di un approccio integrato tra NIS2 e altre normative in materia di gestione dei rischi ICT. Ad esempio, Ferretti evidenzia come la NIS2, il GDPR e il regolamento DORA rappresentino un set di norme finalizzato a regolare la sicurezza, la continuità e la responsabilità nel trattamento dei dati e nell'uso delle tecnologie digitali in ambito economico e pubblico[43]. Inoltre, l'integrazione tra NIS2 e altri strumenti normativi dell'Unione, come il Cybersecurity Act (Regolamento UE 2019/881), contribuisce a delineare un ecosistema regolatorio sempre più coerente e multilivello, in cui certificazione, vigilanza e risposta agli incidenti costituiscono tasselli interconnessi di una strategia unitaria[44].

---

[40] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, artt. 14–16 e 28.

[41] Commissione Europea, Cybersecurity Strategy for the Digital Decade, COM(2020) 605 final.

[42] Commissione Europea, Proposal for a Regulation on Cyber Resilience Act, COM(2022) 454 final.

[43] Ferretti G., Regolazione multilivello e cybersicurezza, in *"Rivista italiana di informatica e diritto"*, n. 2/2023.

[44] Regolamento (UE) 2019/881, Cybersecurity Act.

In questo contesto, il ruolo svolto da ENISA è fondamentale, non solo come organo tecnico giuridicamente riconosciuto ma anche come promotore di cultura e standard comuni: le sue pubblicazioni, tra cui i rapporti annuali e i *framework* di valutazione del rischio, costituiscono riferimenti imprescindibili e affidabili per tutti gli operatori del settore pubblico e privato[45].

È interessante osservare come anche la stampa specialistica abbia seguito da vicino l'evoluzione normativa: la rivista *Cybersecurity Trends* ha dedicato uno speciale al confronto tra la NIS e la NIS2, evidenziando l'ampliamento del perimetro, la maggiore incisività sanzionatoria e il rafforzamento degli obblighi organizzativi come segni di una vera e propria maturazione dell'approccio europeo alla cyber policy[46].

### 3.2 Ampliamento dell'ambito di applicazione, rafforzamento dei requisiti di sicurezza, introduzione di sanzioni più severe e meccanismi di *enforcement*.

L'adozione della Direttiva NIS2, come detto, segna una svolta decisiva nel sistema integrato di norme europeo in materia di cybersicurezza e nell'ambito della resilienza digitale a tutela dei servizi essenziali e finalizzata al contrasto delle minacce informatiche in forte ascesa negli ultimi anni, si sono moltiplicate in termini di frequenza, sofisticazione e impatto[47].

Il perimetro soggettivo e settoriale di applicazione della NIS2 rappresenta senza dubbio uno degli elementi più rilevanti dell'evoluzione normativa della norma,

---

[45] ENISA, Annual Report 2021, www.enisa.europa.eu/publications.

[46] Cybersecurity Trends, "Speciale NIS2", n. 4/2023.

[47] Commissione Europea, *EU Cybersecurity Strategy for the Digital Decade*, Bruxelles, 2020.

introducendo criteri oggettivi e armonizzati a livello europeo per l'identificazione delle entità soggette, classificate come "essenziali" o "importanti"[48].

Le aziende non vengono più incluse nell'ambito di applicazione della norma in virtù di una decisione statale, ma è data dalla combinazione tra appartenenza a uno dei settori elencati negli Allegati I e II e dal superamento di soglie dimensionali, escludendo generalmente le microimprese, salvo eccezioni motivate[49]. Ora l'elenco dei settori inclusi dalla norma risulta significativamente esteso: oltre a quelli già tradizionalmente considerati critici (energia, trasporti, sanità, finanza, infrastrutture digitali, approvvigionamento idrico), vengono introdotti i servizi postali e di corriere, la gestione dei rifiuti, la produzione e distribuzione alimentare, l'industria chimica, le pubbliche amministrazioni centrali e regionali, nonché una vasta gamma di fornitori di servizi digitali, tra cui DNS, *cloud*, piattaforme *social*, motori di ricerca, *marketplace online*, fornitori di servizi ICT gestiti (MSP/MSSP), data center e infrastrutture *edge*[50].

L'ampliamento dei soggetti interessati non è di natura puramente quantitativa, ma risponde a un cambio di schema: l'ambiente digitale oggi rappresenta un ecosistema interconnesso nel quale ogni attore può rappresentare un punto critico per l'intera rete. Gli attacchi alla *supply chain* – esempi noti ne sono SolarWinds (2020) o Kaseya (2021) – hanno dimostrato che un attacco informatico a un soggetto "periferico" può produrre conseguenze devastanti a livello sistemico[51].

---

[48] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, artt. 2 e 3.

[49] Commissione Europea, *Raccomandazione 2003/361/CE* relativa alla definizione di micro, piccole e medie imprese.

[50] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, Allegati I e II.

[51] Dragoni M., *"Supply chain e cybersicurezza: dalla NIS2 alla compliance preventiva"*, in *Cybersecurity360*, 2023.

In tale ottica la nuova norma obbliga i soggetti coinvolti a valutare e mitigare i rischi derivanti da terze parti, promuovendo un approccio sistemico alla cybersicurezza che comprende l'intera catena di fornitura e che obbliga tutti gli operatori a estendere le proprie misure di controllo, gestione e monitoraggio anche ai propri fornitori di servizi ICT, software e infrastrutture digitali[52].

Oltre al perimetro soggettivo e di settore, la normativa innalza notevolmente il livello minimo dei requisiti di sicurezza, infatti l'articolo 21 elenca in modo dettagliato le misure tecniche, operative e organizzative che le entità devono adottare, sulla base di un approccio *"risk-based"*. Tra queste si evidenziano: la predisposizione di politiche di gestione del rischio informatico, piani di risposta agli incidenti e di continuità operativa, come la gestione del *backup* e il ripristino in caso di disastro *(disaster recovery)*, misure per la sicurezza delle reti e dei sistemi, gestione delle vulnerabilità, protezione fisica e logica delle infrastrutture, utilizzo di autenticazione a più fattori, sicurezza delle comunicazioni e aggiornamenti tempestivi dei *software*. Un'attenzione particolare è riservata alla cybersicurezza nella *supply chain*, che rappresenta una delle innovazioni più significative del nuovo impianto regolatorio[53].

Gli obblighi di governance diventano un nodo cruciale per l'applicazione del nuovo sistema di norme, rivelandosi una novità nel campo dell'IT, nel quale i soggetti coinvolti non sono più autorizzati a considerare la sicurezza cyber quale ambito tecnico di esclusiva competenza dei responsabili *"tecnici"* dell'azienda, ma, al contrario, essa viene inquadrata come una responsabilità gestionale e strategica formalmente individuata, che coinvolge direttamente i vertici aziendali. L'articolo 20 impone agli organi di amministrazione o direzione il compito di supervisionare l'implementazione delle misure di sicurezza, promuovere la formazione continua del personale e garantire una cultura aziendale improntata

---

[52] ENISA, *Cybersecurity for Supply Chains – Good Practices*, 2022.

[53] ENISA, *Technical Guidelines for Minimum Security Measures under NIS2*, 2023.

alla resilienza digitale. In particolare, il paragrafo 2 del citato articolo, prevede che i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e che i soggetti essenziali e importanti debbano offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto coinvolto dalla norma. Questo orientamento è coerente con il principio della *"security by governance"* e apre la strada a responsabilità anche di tipo personale per i dirigenti che trascurano tali obblighi[54].

Anche il meccanismo di notifica degli incidenti ha subito un significativo potenziamento come già accennato in precedenza. Le entità devono notificare un incidente significativo all'autorità competente (CSIRT o altra autorità designata) entro 24 ore dalla sua rilevazione, con un rapporto iniziale, cui seguono un aggiornamento entro 72 ore e una relazione finale entro un mese[55]. Questo schema si ispira, nella struttura, al modello già adottato dal GDPR per le violazioni dei dati personali, ma lo estende anche a tutte le minacce rilevanti per l'integrità, la disponibilità e la riservatezza dei sistemi e dei servizi digitali.

Il significativo salto di qualità della norma rispetto alla precedente è senz'altro rappresentato dall'introduzione di un sistema sanzionatorio rigido e strutturato, finalizzato a colmare le incompletezze del precedente impianto, in cui le sanzioni erano affidate alla discrezionalità nazionale e per questo non particolarmente efficaci.

Con l'articolo 34, la NIS2 stabilisce un modello armonizzato di enforcement che attribuisce alle autorità nazionali competenti il potere di infliggere sanzioni pecuniarie fino a 10 milioni di euro o al 2% del fatturato mondiale annuo

---

[54] Floridi L., *"Governance della cybersicurezza: responsabilità e compliance dopo la NIS2"*, in *European Journal of Digital Law*, 2024.

[55] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 23.

dell'impresa, ma soprattutto, la possibilità di scelta dell'importo maggiore[56]. Il quadro sanzionatorio, così impostato, ricalca quello introdotto dalla norma GDPR e rafforza la deterrenza nei confronti delle grandi imprese e dei fornitori digitali globali. Per le pubbliche amministrazioni, pur non essendo prevista la pena dell'irrogazione di sanzioni pecuniarie vere e proprie, gli Stati membri hanno comunque l'obbligo di garantire la possibilità di imporre misure correttive, disciplinari o sostitutive, al fine di assicurare un'effettiva responsabilità funzionale[57].

In tal senso i meccanismi di *enforcement* sono multilivello. Difatti, le autorità nazionali – in Italia l'Agenzia per la Cybersicurezza Nazionale (ACN), in coordinamento con il CSIRT e il CERT-AgID – sono dotate di ampi poteri ispettivi, tra cui l'accesso ai sistemi, la possibilità di condurre audit, richiedere documentazione, ordinare l'adozione di misure tecniche correttive e, nei casi più gravi, sospendere l'attività o revocare l'autorizzazione all'erogazione dei servizi[58]. In tale contesto, la mancata cooperazione con l'autorità costituisce da sola una violazione sanzionabile, indipendentemente dal verificarsi o meno di un incidente.

Ulteriore e decisivo rafforzamento normativo che ritroviamo nella NIS2 è rappresentato dai meccanismi di cooperazione europea. Infatti, attraverso il Gruppo di Cooperazione, composto dai rappresentanti degli Stati membri e coordinato dalla Commissione europea, e mediante l'azione dell'ENISA, viene

---

[56] ibidem, art. 34.

[57] ibidem, cfr. (87).

[58] Decreto-legge 82/2021, convertito in Legge 4 agosto 2021, nr. 109, recante: "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".

promossa una condivisione sistematica delle pratiche ispettive, dei dati relativi agli incidenti, dei piani di risposta e dei criteri di valutazione del rischio[59].

La ricerca dell'omogeneizzazione tra le autorità nazionali diviene, con l'evoluzione delle minacce che assumono sempre più carattere transfrontaliero, una necessità non più differibile. L'interconnessione degli ecosistemi digitali impone una resilienza che lega a doppio filo i vari attori tanto da farla considerare come unica e soggetta al comportamento di ognuno; essenziale, dunque, è la costruzione di una cybersicurezza realmente europea, fondata su standard condivisi, *enforcement* coerente e responsabilità multilivello.

### 3.3 Sfide per l'adeguamento alla direttiva NIS2 e buone pratiche di conformità

La direttiva NIS2 pone alle organizzazioni coinvolte un insieme di sfide pratiche, tecniche e di governance. L'adeguamento ai nuovi requisiti richiede di gestire ambienti ICT sempre più eterogenei e distribuiti. Attualmente molte aziende operano su architetture multi-cloud, con numerose applicazioni e infrastrutture ibride, spesso integrate da fornitori esterni di servizi. Questo scenario accresce i rischi cyber e rende più onerosa la governance della sicurezza essendo composta da fattori ed attori diversificati[60]. Ad esempio, la NIS2 impone tempistiche molto serrate per la segnalazione iniziale degli incidenti gravi, ovvero entro 24 ore, obiettivo difficile da rispettare senza una visibilità completa ed istantanea sui sistemi. La nuova direttiva inoltre impone alle entità di designare un punto di contatto unico NIS come detto e di registrarsi presso la piattaforma digitale nazionale gestita dall'ACN, un adempimento organizzativo ulteriore che

[59] ENISA, *Cooperation Group Mechanisms – Best Practices for Enforcement*, 2023.

[60] ENISA, *"Cybersecurity Threat Landscape 2023"*, ottobre 2023.

richiede preparazione anticipata[61]. Senza un inventario centralizzato degli asset e una gestione unificata dei log, il rispetto dei tempi di notifica e la rilevazione tempestiva degli incidenti in ambienti così frammentati risultano particolarmente complessi.

Allo stesso modo, la gestione delle vulnerabilità e la garanzia di continuità operativa rappresentano sfide complesse: secondo un rapporto di ENISA, quasi la metà degli operatori (49%) identifica *continuity management* e *vulnerability management* come gli obblighi NIS2 più difficili da attuare[62]. Questi dati evidenziano come molte organizzazioni – in particolare le medie imprese ora incluse nel perimetro NIS2 – debbano colmare significativi gap tecnici e di competenze per soddisfare gli standard richiesti. La NIS2 richiede l'implementazione di processi strutturati per la gestione e la divulgazione delle vulnerabilità, allineando le imprese alle best practice internazionali in materia[63]. Ciò detto, l'assenza di competenze specializzate e/o di un monitoraggio continuo delle minacce può rallentare l'identificazione e la risoluzione tempestiva delle criticità, esponendo gli operatori al rischio di non risultare conformi alla norma. Anche le pubbliche amministrazioni, spesso incluse tra le entità essenziali NIS2, dovranno aggiornare le proprie misure di sicurezza di base – ad esempio quelle previste dalle circolari AgID – allineandole ai requisiti più stringenti introdotti dalla direttiva e alle indicazioni fornite dall'ACN[64].

Una delle criticità maggiori è relativa alla gestione dei fornitori ICT e della *supply chain*, che ora rientra nel perimetro di responsabilità delle entità soggette. Eventi

---

[61] D.lgs. 138/2024, art. 20; Determinazione ACN n. 38565/2024 (registrazione delle entità NIS2 sulla piattaforma ACN).

[62] ENISA, *"NIS Investments 2024 – Trends and Priorities in Cybersecurity Spending"*, marzo 2024, p. 16.

[63] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 21, par. 2, lett. e).

[64] Circolare AgID 18 aprile 2017, n. 2/2017 recante *"Misure minime di sicurezza ICT per le Pubbliche Amministrazioni".*

come, ad esempio, l'attacco subito dalla Regione Lazio nel 2021, originato da una compromissione delle credenziali di un fornitore esterno, dimostrano quanto sia importante valutare i rischi derivanti da terze parti[65]. Tuttavia, molti operatori non dispongono ancora di strumenti contrattuali, processi di *due diligence* o criteri di valutazione della postura cyber dei *vendor*, rendendo quindi complicato assicurare la conformità lungo tutta la filiera.

La NIS2 norma l'obbligo di adottare misure per mitigare i rischi cyber lungo la *supply chain*: le entità devono considerare le vulnerabilità specifiche di ciascun fornitore critico e la qualità delle pratiche di sicurezza dei *partner* esterni[66]. L'integrazione dei requisiti e le clausole di sicurezza nei contratti, nonché la conduzione di verifiche periodiche sui *vendor* e, ove possibile, la richiesta di certificazioni o di attestazioni di conformità, rappresentano cruciali aspetti che molte aziende ancora non posseggono in modo sistemico.

Dal punto di vista giuridico, l'applicazione della direttiva pone sfide di interpretazione e coordinamento con altre normative europee, in particolare con il GDPR, il regolamento DORA e il Cyber Resilience Act. La coesistenza di più obblighi – con soglie, terminologie e modalità di segnalazione diverse – richiede un approccio integrato alla compliance, pena il rischio di sovrapposizioni, duplicazioni o, peggio, omissioni rilevanti[67]. Considerando un incidente, ad esempio, lo stesso potrebbe innescare obblighi di notifica diversi, sia ai sensi della NIS2 sia del GDPR (in caso di violazione di dati personali), comportando comunicazioni verso autorità diverse ma con tempistiche che potrebbero rivelarsi

---

[65] *Il Sole 24 Ore*, *"Attacco hacker alla Regione Lazio, compromesse credenziali di un fornitore"*, 2 agosto 2021.

[66] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 21, par. 2, lett. d) e par. 3.

[67] Ferretti G., *"NIS2, DORA, GDPR: verso un modello integrato di compliance digitale"*, in *Riv. Dir. e Tecnologie*, 2023.

non allineate[68]. Allo stesso modo, gli operatori finanziari soggetti anche al nuovo regolamento DORA dovranno coordinare i requisiti di resilienza digitale di quest'ultimo con gli obblighi previsti dalla NIS2, evitando conflitti e ridondanze[69]. Il Cyber Resilience Act, imporrà, in tal senso, ai fornitori di prodotti digitali requisiti di cybersicurezza fin dalla fase di progettazione, l'introduzione di un ulteriore livello regolamentare da considerare nei programmi di gestione del rischio ICT delle entità in scope[70].

Anche gli obblighi di governance costituiscono una novità significativa. La responsabilità degli organi di amministrazione o direzione implica un cambio di passo, in cui la cybersicurezza diventa una questione di gestione e non solo tecnica demandata ai manager "tecnici" dell'azienda. La NIS2 stabilisce infatti che i membri dei vertici aziendali (management body) approvino le misure di sicurezza e siano tenuti a seguire percorsi di formazione periodica sulla cybersecurity, formalizzando così una responsabilità diretta in materia[71].

Il recepimento italiano della direttiva, con il D.lgs. 138/2024, prevede sanzioni specifiche sostanziali per l'omissione dolosa o colposa di tali responsabilità, incluso il possibile allontanamento temporaneo dai ruoli dirigenziali[72]. Questo determina la necessità di una maggiore sensibilizzazione e formazione anche a livello apicale, tali da non poter delegare a cascata le citate responsabilità.

Per affrontare queste sfide, si stanno affermando alcune buone pratiche. Tra queste: l'adozione di sistemi di gestione della sicurezza basati su standard internazionali come ISO/IEC 27001, l'esecuzione di audit interni e *penetration*

---

[68] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 23; Regolamento (UE) 2016/679 (GDPR), art. 33.

[69] Regolamento (UE) 2022/2554 (Digital Operational Resilience Act – DORA).

[70] Regolamento (UE) 2024/2847 (Cyber Resilience Act).

[71] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 20, par. 1-2.

[72] D.lgs. 138/2024, art. 34, comma 6.

*test* periodici, l'adozione dell'autenticazione multifattoriale, l'uso di strumenti SIEM per il monitoraggio continuo e la formazione continua del personale[73]. È inoltre fondamentale costruire un sistema di governance cyber in cui siano chiari i ruoli (es. CISO, Data Protection Officer, responsabile NIS2), le responsabilità e le linee di escalation interna in caso di incidenti, sempre che, a parere dello scrivente, non si cerchi di ridurre i costi del personale facendo convergere su figure uniche i diversi ruoli, di certo una pessima pratica. In quest'ottica è utile adottare *framework* di riferimento: ad esempio il Framework Nazionale per la Cybersecurity e la Data Protection – sviluppato dal Laboratorio Nazionale di Cybersecurity (CINI) e promosso da ACN – offre alle organizzazioni uno strumento per valutare la propria postura di sicurezza e individuare le priorità di adeguamento, in coerenza con gli standard internazionali e con i requisiti NIS2[74].

Inoltre, le linee guida e i *tool* di *self-assessment* forniti da ENISA rappresentano risorse preziose per misurare il livello di maturità aziendale in ambito cyber e orientare di conseguenza i piani di adeguamento da adottare.

Infine, molte organizzazioni si stanno dotando di "*playbook*" o manuali operativi per la gestione degli incidenti informatici, che includono procedure standardizzate per la classificazione degli eventi, la notifica alle autorità (ACN, CSIRT), la comunicazione interna ed esterna, e la continuità operativa. L'adozione di questi strumenti facilita non solo la conformità, ma anche l'efficacia della risposta agli incidenti, migliorando la resilienza complessiva. Di certo un insieme di pratiche e di sistemi da considerare in fortissima evoluzione e che dovranno adeguarsi repentinamente ai cambiamenti di scenario anche giuridici in pochissimo tempo.

---

[73] ISO/IEC 27001:2022 – *Information security, cybersecurity and privacy protection*.

[74] ACN, *Framework Nazionale per la Cybersecurity e la Data Protection*, v. 2.0, 2022.

# 4. ANALISI COMPARATIVA TRA NIS E NIS2

## 4.1 Struttura normativa e ridefinizione delle responsabilità

La Direttiva NIS (Direttiva (UE) 2016/1148) rappresenta il primo quadro organico a livello UE in materia di sicurezza delle reti e dei sistemi informativi, recepita in Italia con il d.lgs. 65/2018. A distanza di pochi anni, l'Unione europea ha adottato la Direttiva NIS2 (Direttiva (UE) 2022/2555) – pubblicata a dicembre 2022 – per superare i limiti emersi nell'attuazione della prima NIS e adeguare la normativa al crescente rischio cyber. La NIS2, in vigore dal 18 ottobre 2024 e recepita in Italia con d.lgs. 138/2024, abroga e sostituisce la precedente direttiva NIS, ampliandone significativamente l'ambito e inasprendo gli obblighi per i soggetti coinvolti.

In termini di *struttura*, la Direttiva NIS originaria contava meno di 30 articoli suddivisi in capitoli dedicati a strategie nazionali, requisiti per Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD), cooperazione e attuazione. La NIS2 presenta invece una struttura più estesa e articolata (oltre 60 articoli, inclusi allegati con settori e tipologie di soggetti), segno di un approccio più *sistematico e dettagliato*[75].

In particolare, la NIS2 aggiorna l'elenco dei settori critici soggetti alla disciplina, includendo nuovi ambiti ritenuti vitali per economia e società. Ai tradizionali settori già coperti da NIS (energia, trasporti, bancario, infrastrutture finanziarie, sanità, fornitura e distribuzione idrica, infrastrutture digitali, ecc.), la NIS2 aggiunge – tra gli altri – servizi postali e spedizioni, gestione dei rifiuti, industria manifatturiera critica, produzione alimentare, spazio, pubblica amministrazione e fornitori di servizi ICT. Si supera così la visione ristretta del 2016, adeguandola al contesto socio-economico odierno fortemente digitalizzato e interconnesso. Dal punto di

[75] Maugeri L. e Riccardi A., *"La Direttiva NIS2: il quadro giuridico italiano"*, in ictsecuritymagazine.com, 2024.

vista terminologico e di campo di applicazione, scompare la distinzione formale introdotta dalla NIS tra “operatori di servizi essenziali” e “fornitori di servizi digitali” – ritenuta ormai obsoleta e non più aderente all’importanza reale dei servizi per la collettività – in favore di una classificazione più ampia in *“soggetti essenziali”* e *“soggetti importanti”*. Tale nuova categorizzazione tiene conto sia del settore in cui l’entità opera sia soprattutto della sua dimensione aziendale. Diversamente dalla NIS1, che lasciava agli Stati membri il compito di identificare gli OSE secondo criteri discrezionali, la NIS2 introduce infatti un criterio uniforme di inclusione basato sul principio del *“size-cap rule”*: rientrano automaticamente nel campo di applicazione tutte le imprese medio-grandi[76] operanti nei settori critici elencati. Ne risultano coperte molte più organizzazioni a livello UE – non solo grandi operatori storicamente considerati “critici”, ma anche aziende di medie dimensioni sinora escluse – garantendo così una copertura più omogenea e capillare delle attività essenziali. Sono previste comunque eccezioni mirate: in generale micro e piccole imprese restano esentate, salvo che operino in ambiti di particolare rilievo per la sicurezza (ad es. registri di nomi a dominio, trust service providers, o specifici fornitori ICT indicati espressamente). Inoltre, la NIS2 include esplicitamente le *pubbliche amministrazioni* di rilievo nazionale e gli enti della PA locale di maggior dimensione tra i soggetti tenuti agli obblighi di cybersicurezza – mentre la NIS1 demandava agli Stati se ricomprenderle o meno. Questo ampliamento strutturale e soggettivo risponde all’esigenza di colmare le lacune e disomogeneità applicative riscontrate con la prima direttiva: la Commissione aveva infatti rilevato una frammentazione nel recepimento NIS tra Paesi, con differenze di perimetro, requisiti e livelli di *enforcement* che rischiavano di pregiudicare il mercato unico digitale e la resilienza collettiva. La NIS2 punta, dunque, a creare un quadro maggiormente armonizzato, imponendo

[76] Aziende con almeno 50 dipendenti o fatturato annuo >10 milioni €, secondo la definizione UE di PMI.

regole minime comuni più stringenti e meccanismi di coordinamento efficaci, a beneficio della sicurezza collettiva in UE.

Contestualmente, si assiste a una significativa evoluzione delle responsabilità sia in capo agli Stati membri sia agli operatori. Sul piano statale, la NIS del 2016 richiedeva a ciascun Paese di adottare una strategia nazionale di sicurezza cibernetica, designare uno o più organismi competenti NIS (autorità nazionali o settoriali) e un punto di contatto unico, nonché di istituire un CSIRT nazionale (Computer Security Incident Response Team). L'implementazione pratica era però rimessa in larga parte alle decisioni nazionali, con risultati eterogenei. In Italia, ad esempio, il d.lgs. 65/2018 individuò diverse Autorità competenti per ciascun settore essenziale (ministeri o autorità indipendenti di settore) coordinate da un Punto di contatto unico presso la Presidenza del Consiglio, mentre il CERT-PA fungeva da CSIRT nazionale. La Direttiva NIS2 consolida e rafforza questo impianto: gli Stati devono comunque dotarsi di strategie e strutture nazionali di cybersecurity, ma con obblighi più incisivi di *coordinamento e collaborazione* reciproca[77]. In particolare, ciascuno Stato deve designare una o più autorità competenti NIS2 e il relativo punto di contatto unico, garantendo opportune risorse e poteri a tali organismi (es. poteri ispettivi e sanzionatori). Si incoraggia la centralizzazione delle funzioni in un'agenzia nazionale specializzata (modello seguito dall'Italia con l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), oggi autorità unica NIS2 e punto di contatto nazionale[78], ferma restando la possibilità di coinvolgere autorità settoriali di supporto. Agli Stati viene richiesto di aggiornare periodicamente la propria strategia cyber tenendo conto del quadro UE e di partecipare attivamente ai nuovi meccanismi europei di cooperazione[79]. Inoltre, la NIS2 impone agli Stati membri di introdurre un regime sanzionatorio efficace per le violazioni degli obblighi da parte dei soggetti regolati, con sanzioni

[77] D.lgs. 138/2024, art. 14.

[78] ibidem, art. 1, comma 2, lett. c 2) e lett. e, art. 9, comma 2, lett. c. e art. 10.

[79] www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

amministrative che raggiungano soglie minime comuni elevate (fino a 10 milioni di euro o 2% del fatturato) – un netto inasprimento rispetto alle esigue multe previste da molti ordinamenti col recepimento NIS (in Italia, max 150.000 € per le violazioni più gravi. Ciò uniforma il potere deterrente a livello UE, avvicinandolo a quello di altre normative come il GDPR. Dal lato degli operatori, la Direttiva NIS1 obbligava gli OSE e FSD identificati ad adottare misure tecniche e organizzative adeguate alla gestione dei rischi informatici e a notificare gli incidenti significativi alle autorità nazionali competenti.

Tali obblighi generali sono stati profondamente rafforzati e dettagliati nella NIS2. Anzitutto, come visto, si estende la platea dei destinatari includendo automaticamente tutte le medie e grandi imprese in settori critici, il che comporta per molte aziende *nuove responsabilità di compliance* in ambito cyber. Inoltre, la NIS2 esplicita che la responsabilità ultima della cybersecurity aziendale ricade anche sugli organi direttivi: i vertici societari (amministratori delegati, consigli di amministrazione) devono impegnarsi attivamente nella supervisione delle misure di sicurezza e possono essere ritenuti personalmente responsabili in caso di inadempienze. Questa è una novità sostanziale rispetto alla NIS1, che non menzionava direttamente i doveri del top management. La NIS2 invece prevede obblighi di formazione specifica per i dirigenti e consente, in caso di gravi violazioni, sanzioni quali l'interdizione temporanea da ruoli manageriali[80]. Si tratta di un cambio di approccio che punta a coinvolgere il *governo aziendale* nella creazione di una cultura di sicurezza, superando la prassi di delegare tutto all'IT. Complessivamente, dunque, la NIS2 ridefinisce le responsabilità su più livelli: maggiore accountability per gli Stati (chiamati a un recepimento uniforme, con autorità competenti dotate di reali poteri e coordinamento sovranazionale) e per gli operatori essenziali/importanti (chiamati non solo a rispettare obblighi tecnici, ma anche a integrare la gestione del rischio cyber nella governance aziendale,

[80] Di Giacomo L., *"In GU il decreto NIS 2: ecco chi si deve adeguare e come"*, in diritto.it, 2024.

sotto pena di sanzioni significative). Questo aggiornamento normativo riflette la maturazione del quadro giuridico della cybersecurity, divenuto in pochi anni più prescrittivo e rigoroso per far fronte a minacce in costante evoluzione.

## 4.2 Gestione del rischio, notifica degli incidenti, impatti su PMI e operatori essenziali

L'evoluzione dell'approccio alla gestione del rischio e della segnalazione degli incidenti di sicurezza, rappresentano i punti fondamentali del passaggio normativo tra le 2 direttive che hanno provocato importanti sviluppi pratici sia per le imprese di grandi dimensioni, sia per le piccole e medie imprese (PMI) coinvolte. La Direttiva NIS1 stabiliva un obbligo generale per gli OSE (operatori essenziali) di adottare *"misure tecniche e organizzative adeguate e proporzionate"* per gestire i rischi per la sicurezza delle reti e dei sistemi informativi utilizzati nelle proprie operazioni e per prevenire incidenti. Tali prescrizioni però sono rimaste ampie e di principio, lasciando agli Stati e agli stessi operatori un ampio margine di discrezionalità nell'interpretazione dei requisiti di sicurezza da adottare. Allo stesso modo, in caso di incidenti aventi un impatto significativo sulla continuità dei servizi essenziali, la NIS1 imponeva di darne notifica *"senza indebito ritardo"* all'autorità o CSIRT competente, ma senza fissare tempistiche uniformi perentorie e senza fissare, soprattutto, i dettagli relativi al contenuto della segnalazione; solo per i FSD (fornitori digitali) la Commissione ha successivamente definito alcuni parametri di impatto attraverso l'adozione di un regolamento attuativo.

Da tale contesto si è delineata un'implementazione non sempre omogenea: ad esempio, in Italia il D.lgs. 65/2018 prevedeva tempi brevi per la notifica, ma soglie

di impatto qualitativo da valutare caso per caso, mentre altri Paesi adottarono metriche diverse[81].

Il legislatore, consapevole di queste difformità, introduce con la NIS2 un approccio molto più strutturato, rigido e vincolante sia sul fronte del *risk management,* sia su quello del *reporting* degli incidenti. Infatti, vengono elencate un set minimo di misure di sicurezza[82] che *tutti* i soggetti essenziali e importanti devono implementare, adottando il principio dell'*"all-hazards approach"*[83].

Tali misure comprendono, tra le altre: politiche di analisi e valutazione del rischio e di sicurezza dei sistemi informativi; procedure per la gestione degli incidenti (*Incident Response*) e la continuità operativa (piani di *disaster recovery* e *crisis management*); misure di sicurezza nella catena di fornitura e nei rapporti con fornitori/partner (*supply chain security*); criteri di sicurezza per l'acquisizione, sviluppo e manutenzione di sistemi e software, inclusa la gestione delle vulnerabilità (*vulnerability handling* e *disclosure*); politiche per testare l'efficacia delle misure (audit, monitoraggio); pratiche di igiene informatica di base e formazione continua del personale; misure specifiche su controllo degli accessi, sicurezza delle identità digitali, utilizzo della crittografia e dell'autenticazione a più fattori. Si tratta di una codificazione puntuale delle *best practice* di cybersecurity, che la NIS1 non dettaglia ma che ora diventano obblighi giuridici espliciti ai quali sottostare. Ad esempio, la formazione del personale in materia di sicurezza, prima elemento meramente auspicabile, con NIS2 diventa requisito esplicitamente menzionato; allo stesso modo la gestione dei rischi di fornitori terzi

---

[81] D. lgs. n. 65 del 18 maggio 2018, art. 12.

[82] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 21.

[83] L'approccio *"all-hazards"* nella sicurezza informatica, come nella gestione più ampia delle emergenze, è una strategia completa focalizzata sulla preparazione alla reazione di un'ampia gamma di potenziali minacce, compresi incidenti sia informatici che non informatici. Invece di creare piani separati per ogni specifica minaccia, pone l'accento sullo sviluppo di capacità di base e protocolli flessibili che possono essere applicati in diverse situazioni.

e la sicurezza delle *supply chain* (tematica che racchiude attualmente elementi fortissima criticità) viene inserita tra gli obblighi primari. Ogni entità dovrà quindi adottare un approccio proattivo e sistematico alla sicurezza informatica, documentando l'analisi dei rischi e le contromisure su base continuativa. Ciò comporta per gli operatori un impegno organizzativo e finanziario maggiore – specialmente per quelli di dimensioni medio-grandi che finora non erano soggetti NIS – ma mira a innalzare il livello complessivo di resilienza cibernetica nei settori decisivi.

In caso di incidenti di sicurezza (cyber attacchi, guasti o altre compromissioni che incidano sui servizi), la NIS2 uniforma, aggiungerei opportunamente, in tutta l'Unione Europea, le regole di notifica, introducendo scadenze tassative e una procedura graduale di *reporting*. In base all'art. 23 NIS2, ogni "incidente significativo" – definito come un evento che causa gravi perturbazioni operative o perdite economiche all'entità interessata, o che provoca impatti rilevanti su persone fisiche/giuridiche – deve essere segnalato secondo *quattro step* principali[84].

Avremo infatti:

1) allerta preliminare entro 24 ore dal momento in cui l'entità ha rilevato l'incidente *(early warning report),* contenente le prime informazioni disponibili e un'indicazione se si sospetta un atto doloso o con impatto transfrontaliero;

2) notifica incidentale dettagliata entro 72 ore dall'identificazione *(incident notification)*, fornendo un quadro iniziale degli indicatori di compromissione, severità e impatto dell'incidente;

3) su richiesta, report intermedi sullo stato della gestione incidentale;

[84] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 23, comma 4.

4) relazione finale entro un mese dalla notifica, con analisi completa della causa, misure di rimedio adottate e impatti riscontrati.

In caso di incidenti prolungati ancora in corso allo scadere del mese, è previsto un *progress report* e poi un report finale entro un mese dalla risoluzione. Queste tempistiche – in particolare la prima notifica entro 24 ore – sono più stringenti persino rispetto al GDPR (72 ore per i *data breach*)[85] e riflettono la necessità di *reazione tempestiva*: l'obiettivo è consentire alle autorità e ai CSIRT di attivarsi subito in attività di supporto, mitigazione e coordinamento, generando una risposta coordinata e collettiva. Le autorità destinatarie (CSIRT e/o Autorità competente) devono infatti confermare ricevuta e fornire un riscontro iniziale all'ente segnalante entro 24 ore, fornendo eventuali istruzioni sulle azioni di mitigazione da intraprendere. Inoltre, se l'incidente ha natura transfrontaliera o potrebbe propagarsi ad altri Stati, scatta un meccanismo di condivisione immediata di informazioni tra punti di contatto nazionali ed ENISA, così da allertare gli altri Paesi potenzialmente coinvolti.

Si introduce persino la raccolta di dati sui *"near misses"* (mancati incidenti gravi)[86]: i singoli punti di contatto nazionali invieranno a ENISA, con cadenza trimestrale, un report aggregato anonimo su incidenti significativi, minacce e quasi-incidenti notificati sul territorio. ENISA a sua volta informerà periodicamente il gruppo di cooperazione e la rete CSIRT sulle tendenze emerse.

La NIS2 delinea, dunque, un importante sistema di notifica armonizzato a livello europeo, che sostituisce le previgenti normative nazionali, eterogenee e non coordinate tra loro, garantendo sia alle autorità un flusso informativo costante, sia agli operatori regole chiare sulla tempistica e sulle modalità di segnalazione

---

[85] Regolamento (UE) 2016/679 ("GDPR").

[86] Un cosiddetto "incidente mancato" è un accadimento che porta informazioni di grande interesse per stabilire le debolezze all'interno delle nostre difese e consentire il miglioramento dell'efficacia del sistema di protezione dei dati. Si tratta, dunque, di un ottimo indicatore di rischio preventivo.

di un incidente. Il nuovo approccio al rischio e agli incidenti appena descritto, da un lato aumenta gli oneri di *compliance* per le aziende quanto ad investimenti in sistemi di monitoraggio, procedure di *incident response* strutturate e capacità di *reporting* veloce, dall'altro, però, mira a migliorare in modo decisivo la resilienza e la capacità di reazione coordinata a livello europeo, riducendo i tempi di risposta e favorendo l'interscambio di informazioni critiche in caso di attacchi transfrontalieri su larga scala.

Le nuove disposizioni in tema di misure di sicurezza e notifiche di incidente hanno implicazioni rilevanti per le PMI e per gli operatori critici.

Per quanto riguarda le PMI, occorre notare che la NIS2 – come detto – esenta in linea generale le micro e piccole imprese (meno di 50 dipendenti) dal proprio campo di applicazione, salvo specifiche eccezioni. Difatti la maggior parte delle *microimprese* e molte *piccole imprese* non saranno direttamente coinvolte negli obblighi della nuova normativa, evidentemente in ragione della loro limitata capacità organizzativa. Tuttavia, una consistente parte delle aziende classificabili come "medie imprese" (50-249 addetti e fatturato fino a €50 milioni) in settori ritenuti rilevanti entreranno per la prima volta nel perimetro di azione della norma. In tal senso, medie realtà aziendali del settore sanitario, energetico, dei trasporti locali o numerosi fornitori ICT di medie dimensioni, ad esempio, essendo essenziali o importanti per funzione, dovranno dotarsi di strutture di cybersecurity paragonabili a quelle di grandi operatori. Ciò rappresenterà senza dubbio la vera sfida dal momento che molte PMI in Europa faticano ad implementare misure avanzate di sicurezza – studi indicano che solo una minoranza delle piccole aziende ha policy ICT robuste, a fronte di costi elevati e scarsa consapevolezza del rischio[87].

[87] Kaiser E., *"The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations"* in MediaLaws www.astrid-online.it, 2023.

La direttiva NIS2, consapevole di queste difficoltà di adeguamento, sollecita gli Stati membri a sostenere le PMI nel loro percorso di sviluppo, evidenziando che le PMI costituiscono l'ossatura del tessuto economico europeo ma spesso mostrano *bassa maturità cyber* e sono bersagli crescenti di attacchi (come il *ransomware* e gli attacchi *supply chain*). Pertanto, gli Stati dovrebbero prevedere misure di supporto dedicate, ad esempio punti di contatto nazionale o regionale per fornire guida e assistenza alle PMI in materia di cybersecurity, nonché promuovere servizi condivisi (es. piattaforme per scansione vulnerabilità, configurazione sicura dei siti web, strumenti di *logging*) accessibili anche a microimprese prive di competenze interne. L'obiettivo è evitare che l'applicazione della NIS2 si traduca in un onere insostenibile per le PMI, favorendone invece la graduale rispondenza alla norma e innalzando il livello di sicurezza anche nella filiera. Difatti un *anello debole* nella sicurezza di una piccola impresa può riverberarsi in modo estremamente negativo su operatori maggiori collegati (fornitori strategici, subappaltatori, etc.).

In sintesi, le PMI pur non essendo l'obiettivo principale della nuova regolamentazione – orientata a rendere sempre più *compliant* le entità medio-grandi di rilievo per servizi essenziali – sono indirettamente ed inevitabilmente coinvolte:

- le medie imprese perché incluse e quindi obbligate a investire in misure cyber più solide ed in sistemi interni di resilienza;
- le micro-piccole perché comunque destinatarie di azioni di sensibilizzazione e supporto da parte degli Stati, e perché inserite in catene di fornitura dove i partner più grandi esigeranno standard di sicurezza più elevati rispetto al passato.

Per quanto concerne gli operatori "critici" in senso stretto – ossia quelli che la NIS2 qualifica come *soggetti essenziali* nei settori vitali (energia, trasporti, finanza, sanità, acqua, infrastrutture digitali, ecc.) – l'impatto principale è un

ulteriore irrigidimento degli obblighi e dei controlli rispetto al regime NIS precedente.

Questi operatori già soggetti agli obblighi contemplati dalla NIS1, ora vedono:

(a) ampliate le misure di sicurezza da adottare, spesso richiedendo l'aggiornamento dei propri piani di gestione del rischio e investimenti in nuove tecnologie (es. strumenti avanzati di *detection*, autenticazione multifattoriale diffusa, cifratura potenziata dei dati);
(b) maggiore pressione sulla governance interna, dovendo coinvolgere attivamente i vertici societari e rendicontare periodicamente lo stato della sicurezza;
(c) un regime di vigilanza più stringente da parte delle Autorità. La NIS2, infatti, distingue tra *sorveglianza ex ante* sugli enti essenziali ed *ex post* sugli enti importanti: per i soggetti essenziali le autorità possono condurre audit, ispezioni e verifiche periodiche di conformità anche in assenza di violazioni (data la criticità dei servizi forniti), mentre per gli enti importanti l'intervento avviene principalmente a seguito di incidenti o evidenze di mancato adeguamento. Ciò significa che gli operatori essenziali saranno sottoposti a uno scrutinio continuo e dovranno essere preparati a dimostrare la propria conformità in ogni momento (ad es. esibendo valutazioni di rischio, policy, evidenze di misure adottate), mentre gli importanti potrebbero avere controlli meno frequenti.

In Italia, il d.lgs. 138/2024 prevede un meccanismo di autoregistrazione: tutte le entità che rientrano nei criteri dimensionali e settoriali della NIS2 dovevano registrarsi sul portale dell'ACN entro scadenze prefissate (entro gennaio 2025 per talune categorie ICT e entro febbraio 2025 per tutte le altre), fornendo informazioni sulla propria attività – un obbligo pensato per censire gli operatori *in-scope* e facilitare l'attività di supervisione[88].

[88] Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 26.11.2024 di cui all'articolo 7, comma 6, e all'articolo 40, comma 5, lettera b), del

Tale contesto evidenzia come l'impatto della NIS2 per gli operatori essenziali, i quali posso incorrere in sanzioni anche solo per la mancanza di iscrizione sul portale ACN, sia duplice: da un lato li obbliga a rafforzare le proprie difese cyber, dall'altro li inserisce in un sistema di controllo pubblico più penetrante, con potenziali sanzioni molto elevate in caso di inadempienza (fino al 2% del fatturato mondiale, come visto).

In definitiva, la NIS2 alza l'asticella per tutti gli attori coinvolti:

- per i grandi operatori critici significa consolidare un approccio alla sicurezza a livello *enterprise* e accettare una vigilanza costante;
- per le medie imprese comporta l'ingresso in un regime regolatorio nuovo, con costi di adeguamento ma anche opportunità di migliorare la propria resilienza;
- per le piccole imprese comporta benefici indiretti in termini di maggiore assistenza e protezione nell'ecosistema digitale.

Tali misure, per quanto onerose nel breve termine, puntano a mitigare il rischio sistemico di cyberattacchi devastanti, la cui incidenza è in rapida crescita come evidenziato sin dal 2020 dal rapporto ENISA[89].

Mettendo in sicurezza anche gli anelli meno forti della catena (PMI) e standardizzando le difese dei soggetti chiave, la NIS2 mira a un innalzamento generalizzato del livello di cibersicurezza in tutta l'Unione.

---

D. lgs. 4 settembre 2024, n. 138, recante *"Termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimenti di designazione dei rappresentanti NIS nell'Unione"*.

[89] ENISA, *"Threat Landscape 2021"*, European Union Agency for Cybersecurity, april 2020 – july 2021.

## 4.3 Aspetti di governance istituzionale e cooperazione europea

La transizione normativa da NIS a NIS2 si accompagna a un potenziamento degli aspetti di governance del sistema di sicurezza cibernetica e a nuovi strumenti di cooperazione in ambito europeo, al fine di rendere più efficace l'azione coordinata contro le minacce informatiche transfrontaliere. Lato Italia, la NIS1 aveva già richiesto l'istituzione di strutture di coordinamento (strategie, autorità competenti, CSIRT), mentre la NIS2 ne rafforza l'impianto e affina la governance interna. In Italia, ad esempio,

Il recepimento della NIS2 con D.lgs. 138/2024 ha comportato la riorganizzazione delle competenze: l'ACN – Agenzia per la Cybersicurezza Nazionale è ora formalmente designata quale Autorità nazionale NIS2, con compiti centralizzati di indirizzo, controllo e sanzione sul rispetto della nuova direttiva, in precedenza frammentati tra vari ministeri e agenzie. Ora l'ACN funge anche da punto di contatto unico verso l'Unione europea, garantendo interlocuzione unitaria con gli organismi europei ed allo stesso tempo, il nuovo decreto prevede forme di coordinamento con le altre autorità settoriali nazionali (es. Banca d'Italia per servizi finanziari, Ministero della Salute per sanità, etc.), che restano coinvolte in sede di settore ma sempre sotto la regia dell'ACN[90].

Si delinea quindi un modello di governance nazionale accentrato, in cui un'agenzia specializzata, con piena legittimazione normativa, ha il compito di implementare la normativa (anche attraverso atti attuativi come decreti e linee

[90] Per l'adempimento degli obblighi di cui agli articoli 23, 24, e 25 del decreto NIS2, i soggetti coinvolti sono tenuti ad adottare le misure di sicurezza di base e a notificare al CSIRT Italia gli incidenti significativi di base stabiliti dalla determinazione ACN 164179 del 14 aprile 2025. Gli allegati tecnici alla determinazione sono stati elaborati sulla base dei riscontri pervenuti nel corso delle consultazioni con le Autorità di settore e con le associazioni di categoria. anche per mezzo dei tavoli settoriali di cui all'articolo 11, comma 4, lettera f), del decreto NIS. www.acn.gov.it

guida tecniche), vigilare sul rispetto degli obblighi e gestire eventuali crisi cibernetiche coordinando gli altri attori istituzionali.

Anche in altri Paesi UE si assiste a simili adeguamenti organizzativi, con ruoli rafforzati per le agenzie di cybersecurity nazionali (ad esempio ANSSI in Francia, BSI in Germania, CCN in Spagna) e revisione delle normative interne per evitare sovrapposizioni.

Il D.lgs. 138/2024, ad esempio, abroga espressamente il precedente D.lgs. 65/2018 e coordina la NIS2 con il preesistente "Perimetro di sicurezza nazionale cibernetica" introdotto nel 2019[91], al fine di assicurare coerenza tra i due regimi). Sul fronte europeo, la Direttiva NIS2 interviene a consolidare e ampliare i meccanismi di cooperazione istituiti dalla NIS1.

Quest'ultima aveva creato due organismi principali:

a) il Gruppo di Cooperazione (Cooperation Group) composto da rappresentanti degli Stati membri, Commissione ed ENISA, con funzioni di coordinamento strategico e scambio di *best practices*;
b) la rete dei CSIRT (CSIRTs Network), forum operativo tra i team di risposta nazionali per condividere informazioni tecniche su incidenti e minacce.

La NIS2 conserva tali organismi ma ne potenzia il ruolo.
In particolare, il Gruppo di Cooperazione viene confermato come sede di elaborazione strategica, con nuovi compiti quali:

a) sviluppare linee guida tecniche comuni per l'implementazione delle misure di sicurezza (promuovendo un'attuazione convergente della direttiva nei vari Stati);
b) formulare raccomandazioni e orientamenti in materia di politiche cybersecurity;

[91] DPCM 30 luglio 2020, n. 131 - Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

c) valutare periodicamente le tendenze di minaccia e le lezioni apprese dagli incidenti (anche grazie ai dati aggregati forniti da ENISA);
d) fornire *guidance* strategica alle altre reti (CSIRT network e EU-CyCLONe) su questioni emergenti.

La rete dei CSIRT continua a essere il pilastro del coordinamento operativo: i CERT/CSIRT nazionali (in Italia il CSIRT Italia, incardinato nell'ACN) vi condividono informazioni tecniche, allarmi rapidi, dettagli su vulnerabilità e attacchi in corso, migliorando la capacità collettiva di risposta. La novità maggiore introdotta da NIS2 in ambito cooperativo è la creazione, come già accennato, dell'EU–CyCLONe (European Cyber Crisis Liaison Organisation Network). Si tratta di un meccanismo inedito di gestione coordinata delle crisi cyber su larga scala: l'EU-CyCLONe connette i responsabili nazionali della gestione delle crisi cyber (cyber crisis management authorities) per assicurare il raccordo tra livello tecnico-operativo e livello politico durante gravi incidenti transnazionali. In pratica, in caso di un cyberattacco di ampia portata che colpisca contemporaneamente infrastrutture in più Stati dell'Unione, l'EU-CyCLONe funge da raccordo, per il lato tecnico, tra la rete CSIRT (impegnata nella risoluzione tecnica) e, per il lato politico, tra le autorità nazionali/europee che devono prendere decisioni di gestione della crisi[92].

ENISA fornisce il supporto di segreteria e piattaforme sicure per lo scambio informativo. Questo organismo permette di *coordinare le azioni di risposta a livello strategico*: ad esempio, condividere valutazioni di impatto, concordare messaggi comuni, allineare misure di contenimento o decisioni (come eventualmente lo spegnimento controllato di servizi, o richieste di assistenza reciproca).

L'istituzione di EU-CyCLONe colma una lacuna del precedente regime NIS, emersa di fronte a incidenti paneuropei, come i casi *WannaCry* o *NotPetya* del

[92] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, (68-71), artt. 16 e 17.

2017[93]: pur avendo i CSIRT condiviso informazioni tecniche, mancava un coordinamento ad alto livello tra i governi per le scelte operative. Ora, con EU-CyCLONe, l'UE dispone di un *meccanismo permanente di crisi* in ambito cyber, analogo a quelli esistenti per protezione civile o sanità, che può essere attivato rapidamente per fronteggiare gravi attacchi transnazionali. Accanto a ciò, la NIS2 consolida il ruolo di ENISA (Agenzia UE per la cybersicurezza) quale facilitatore della cooperazione: ENISA oltre a partecipare e supportare il Cooperation Group e fungere da segretariato di EU-CyCLONe e della rete CSIRT, riceve ora formalmente i report periodici sugli incidenti dai singoli Stati e può così svolgere un'azione di *hub* informativo e di analisi a livello UE.

ENISA è chiamata anche a sviluppare, in collaborazione con la Commissione europea, linee guida tecniche e strumenti comuni per la valutazione coordinata, ad esempio, dei rischi di supply chain o per la condivisione di informazioni sulle minacce, al fine di sostenere l'attuazione omogenea della direttiva[94].

Un altro elemento di governance europea è il raccordo della NIS2 con altri atti normativi: la direttiva, infatti, armonizza il proprio settore di intervento con le normative settoriali esistenti, evitando inefficaci duplicazioni. Ad esempio, per il settore finanziario la NIS2 rinvia al nuovo Regolamento DORA (Reg. (UE)

---

[93] Nel 2017, prima con il *ransomware-worm WannaCry*, poi con il *worm-wiper NotPetya*, si è avuta una evoluzione importante sia nella sofisticazione del *malware*, sia nella velocità di diffusione dello stesso e negli impatti procurati alle aziende di tutte le dimensioni rappresentando un problema grave da almeno 20 anni. Lo scenario che si dipinse all'epoca, con il diffondersi dei nuovi attacchi lanciati presumibilmente da Stati nemici, fece ipotizzare una forma di *"cyber-war economica"*, lanciata contro un occidente economicamente avanzato ma poco preparato sul fronte delle difese digitali, messo quindi in ginocchio e costretto a correre ai ripari stanziando investimenti rilevanti sul fronte della cybersecurity per preservare la propria dipendenza dai sistemi digitali. In definitiva, potenzialmente meno competitivo rispetto ad economie emergenti in cui il *security-by-design* stava diventando elemento competitivo sostanziale della nuova economia digitale. E. Vaciago, *"Le ultime evoluzioni del ransomware: cosa insegnano i casi WannaCry e NotPetya"* in The Innovation Group, 2017, www.theinnovationgroup.it.

[94] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, art. 22.

2022/2554) che disciplina specificamente la resilienza digitale degli operatori bancari e finanziari, esentando tali soggetti dagli obblighi previsti dalla NIS2 in modo da non sovrapporre regimi normativi diversi.
Analogamente, la NIS2 si coordina con il CER Directive (Direttiva (UE) 2022/2557) sulla resilienza delle entità fisiche critiche, stabilendo che per gli aspetti cyber si applica la stessa NIS2, mentre per la resilienza fisica delle infrastrutture vale la CER, contemplando la cooperazione tra le autorità competenti nei due diversi settori di intervento. Questo approccio integrato di governance assicura coerenza nell'ecosistema normativo della sicurezza: la cybersecurity è affrontata in modo specifico e completo dalla NIS2, che interagisce con le altre norme (GDPR, DORA, CER, ecc.) senza conflitti. Gli Stati membri sono chiamati a recepire tali raccordi nelle legislazioni nazionali: nel caso italiano, il D.lgs. 138/2024 prevede ad esempio tavoli di coordinamento settoriali come quello presso il Ministero della Salute per sanità digitale e misure per evitare sovrapposizioni con normative di settore già vigenti[95].

In definitiva, gli aspetti di governance e cooperazione nella NIS2 segnano un passo avanti verso un'Unione più coesa e preparata sul fronte cibernetico. A livello interno, le strutture nazionali vengono rafforzate e meglio coordinate, garantendo maggiore chiarezza di ruoli e rapidità decisionale. A livello sovranazionale, la rete di cooperazione europea diviene più densa: non solo si mantengono i forum di scambio informazioni, ma si istituzionalizzano *processi decisionali condivisi* per gestire le crisi (EU-CyCLONe) e si assicura un flusso costante di dati e feedback (tramite ENISA e i reporting trimestrali). Queste innovazioni riflettono la consapevolezza che le minacce informatiche attuali non conoscono confini e che possono essere contrastati efficacemente e risolti rapidamente solo con l'adozione di meccanismi di governance integrati. La Direttiva NIS2, con i suoi cinque capitoli tematici e gli allegati settoriali, offre

[95] Ministero della Salute, Decreto 14 gennaio 2025, recante *"Istituzione presso il Ministero della salute del tavolo settoriale per l'attuazione della direttiva NIS 2"*.

dunque un quadro più robusto: richiede agli Stati di agire all'unisono, pena anche procedure d'infrazione per mancato recepimento entro i termini, e agli operatori di elevare gli standard di sicurezza, sotto la guida attenta delle istituzioni.

Nel contesto giuridico italiano ed europeo, la Direttiva rappresenta un importante punto di svolta normativo, consolidando un modello di sicurezza collettiva basato sui pilastri della prevenzione, della collaborazione e della responsabilità condivisa.

In prospettiva, l'effettiva efficacia di questo modello dipenderà dall'impegno con cui Stati e aziende daranno attuazione ai nuovi obblighi e dalla continua evoluzione della minaccia: la sfida sarà mantenere il quadro normativo agile e aggiornato di fronte all'evoluzione tecnologica ed ai rischi emergenti. Tuttavia, il nuovo impianto normativo risulta fondamentale e decisivo per la costruzione di un cyberspazio europeo più resiliente, in cui governi, autorità e operatori uniscono le forze per tutelare i servizi essenziali e la fiducia dei cittadini nell'economia digitale.

# CONCLUSIONI

L'analisi comparativa tra la Direttiva NIS1 e la Direttiva NIS2 ha consentito di mettere in luce un processo di profonda maturazione normativa e strategica dell'Unione Europea in materia di cybersicurezza, tanto più se si pensa che ci troviamo a meno di 10 anni dal recepimento della prima norma europea di settore.

La transizione dalla NIS1 alla NIS2 non rappresenta una semplice revisione tecnica, ma una riforma strutturale che investe tanto la dimensione giuridica quanto quella politico-istituzionale, operativa e culturale, tutti aspetti con pesi specifici decisivi nel contesto considerato.

La NIS1 ha avuto il merito storico di porre per la prima volta la sicurezza delle reti e dei sistemi informativi al centro dell'azione normativa europea, introducendo obblighi minimi comuni per gli Stati membri e selezionando i soggetti strategici coinvolti. Tuttavia, il carattere di armonizzazione minima, la discrezionalità nella definizione degli OSE e dei FSD, l'assenza di criteri uniformi per la gestione degli incidenti e la debolezza del sistema di *enforcement* hanno reso nel tempo evidente l'insufficienza del suo impianto, minato dalla successiva applicazione spesso disomogenea a livello nazionale che ha generato una frammentazione normativa incapace di rispondere in modo coerente alle sfide sempre più complesse e interconnesse del cyberspazio europeo.

La Direttiva NIS2, in questo contesto, si configura come un deciso cambio di paradigma. Essa amplia in modo significativo il perimetro soggettivo e settoriale, abbracciando una più ampia gamma di entità pubbliche e private e introducendo un sistema classificatorio oggettivo e armonizzato basato su criteri dimensionali e settoriali definiti. Questo approccio garantisce maggiore chiarezza, equità e coerenza tra gli Stati membri, contribuendo alla creazione di un effettivo mercato unico digitale sicuro.

L’introduzione di requisiti di sicurezza dettagliati, la strutturazione delle notifiche di incidente in tempistiche ben definite e il rafforzamento dei poteri ispettivi e sanzionatori delle autorità nazionali segnano un’evoluzione verso una regolamentazione più incisiva e integrata. Particolarmente significativa è la responsabilizzazione dei vertici aziendali, chiamati a farsi garanti della conformità alle disposizioni NIS2, in un’ottica di *accountability* e *governance* proattiva della cybersicurezza, non più delegabile a cascata alle sole figure “tecniche” aziendali.

Sul piano istituzionale, l’evoluzione dalla NIS1 alla NIS2 evidenzia la volontà dell’Unione Europea di passare da una cooperazione ancora debole e frammentata a una *governance* multilivello strutturata e resiliente. La centralizzazione delle competenze in autorità nazionali specializzate, come l’Agenzia per la Cybersicurezza Nazionale (ACN) in Italia, l’istituzione del network EU-CyCLONe per la gestione delle crisi su larga scala e il rafforzamento dei meccanismi di cooperazione (CSIRT Network e Gruppo di Cooperazione) rappresentano passi fondamentali verso una cybersicurezza realmente europea.

La tesi ha anche evidenziato come la NIS2 si collochi all’interno di un ecosistema più ampio, che include ed interagisce normativamente con il GDPR, il Cybersecurity Act, il DORA, il Cyber Resilience Act e la Direttiva CER. In questo senso, si può parlare di una vera e propria infrastruttura giuridica multilivello, in cui la cybersicurezza è integrata in tutte le dimensioni della trasformazione digitale europea. È evidente la convergenza verso un modello normativo orientato ai concetti di *“security by design”* e *“resilience by governance”.*

Nonostante i significativi progressi introdotti dalla Direttiva NIS2 in termini di sviluppo normativo e strategico, il sistema europeo della cybersicurezza si trova ora di fronte a diverse nuove sfide. L’attuazione pratica della direttiva richiederà uno sforzo considerevole da parte delle imprese, in particolare delle PMI, chiamate a colmare lacune organizzative, tecnologiche e culturali. Questo processo di adeguamento dovrà essere sostenuto, anche finanziariamente, dalle autorità competenti per garantire una transizione efficace. Tuttavia, l’efficacia

della NIS2 non dipenderà solo dalla volontà delle imprese, ma anche dalla qualità dell'applicazione nazionale delle norme, dalla capacità delle autorità di vigilanza di esercitare un controllo efficace e dal supporto operativo fornito a tutti gli attori coinvolti. A tutto quanto sopra esposto, si aggiunga la crescente complessità del panorama regolatorio, che impone un approccio integrato alla compliance: le organizzazioni dovranno imparare a gestire obblighi normativi sovrapposti e responsabilità condivise in modo coordinato e non frammentato.

In questo contesto, la NIS2 rappresenta molto più di un inasprimento normativo: essa è la visione evoluta della cybersicurezza come bene comune europeo, essenziale per la sovranità digitale, la tutela democratica e la competitività dell'Unione nel contesto globale.

Rafforzando la resilienza collettiva, promuovendo l'armonizzazione normativa e responsabilizzando attori pubblici e privati, la direttiva crea le condizioni per una risposta più tempestiva e coordinata alle minacce digitali. Ma affinché questo potenziale trasformativo si realizzi appieno, sarà necessario un impegno continuo e condiviso da parte di istituzioni, imprese, società civile e mondo accademico.

Le sfide future non potranno limitarsi all'attuazione tecnica delle misure previste: l'Unione Europea dovrà anche affrontare tensioni strategiche sempre più complesse, come il bilanciamento tra apertura dei mercati e protezione delle infrastrutture critiche, tra cooperazione internazionale e difesa degli interessi strategici europei, tra innovazione tecnologica e garanzie di sicurezza, tra la spinta alla standardizzazione globale e la tutela delle specificità regionali. In questo scenario, la NIS2 si configura anche come uno strumento di politica estera, attraverso il quale l'UE ambisce a giocare un ruolo da protagonista nel nuovo ordine digitale mondiale.

Il successo di questa strategia dipenderà dalla capacità dell'Unione di conciliare esigenze di sicurezza con obiettivi di innovazione e competitività, preservando al contempo la propria autonomia strategica in un contesto internazionale sempre più polarizzato.

## BIBLIOGRAFIA


1. DIRETTIVA (UE) 2016/1148 (NIS1) del Parlamento europeo e del Consiglio, del 6 luglio 2016, relativa a misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione recepita in Italia con il Decreto legislativo n. 65 del 18 maggio 2018, entrato in vigore il 26 giugno 2018;
2. DIRETTIVA (UE) 2022/2555 (NIS2) del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recepita in Italia con il Decreto legislativo n. 138/2024, entrato in vigore il 18 ottobre 2024;
3. REGOLAMENTO (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA e alla certificazione della cybersicurezza;
4. REGOLAMENTO (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
5. DIRETTIVA (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sulla resilienza dei soggetti critici, recepita in Italia con Decreto Legislativo n. 134 del 4 settembre 2024;
6. COMMISSIONE EUROPEA, EU Cybersecurity Strategy for the Digital Decade, COM (2020) 605 final;
7. ENISA – European Union Agency for Cybersecurity (2017). "Overview report on the implementation of the NIS Directive";
8. COMMISSIONE EUROPEA (2020) "Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione". COM (2020) 823 final;
9. ENISA (2023) "NIS2 Directive: A high common level of cybersecurity in the EU";

10. ENISA, European Union Agency for Cybersecurity, “NIS Directive: Lessons Learned”, 2020;
11. EUROPEAN COMMISSION, “Cybersecurity: Implementation of the NIS Directive”, COM (2020) 605, Brussels, 2020;
12. DE CAPITANI DI VIMERCATI S. (2021) “La Direttiva NIS e il futuro della sicurezza informatica in Europa”, Rivista di diritto dell’informazione e dell’informatica, n. 1, pp. 35–58;
13. ENISA, “State of Cybersecurity in the EU under the NIS Directive”, 2021;
14. DECRETO LEGISLATIVO 18 maggio 2018, n. 65 di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio;
15. DECRETO LEGISLATIVO 15 novembre 2023, n. 82, art. 8, co. 1, lett. b), G.U. n. 273 del 22.11.2023;
16. ENISA, “Threat Landscape 2022”, European Union Agency for Cybersecurity, 2022;
17. CYBER 4.0 – TIM Enterprise, White Paper NIS2, Roma, 2023;
18. ENISA, Good Practices for Supply Chain Cybersecurity, 2021;
19. RUGGIERO M., “NIS2, svolta digitale per la sicurezza delle imprese italiane”, in Il Sole 24 Ore, 2023;
20. PIZZETTI D., La cybersicurezza come diritto fondamentale, Giappichelli, 2022;
21. LA REPUBBLICA “Cybersicurezza, UE in allerta dopo i cyberattacchi a settori sanitari e logistici”, 2 giugno 2023;
22. COMMISSIONE EUROPEA, Cybersecurity Strategy for the Digital Decade, COM (2020) 605, final;
23. COMMISSIONE EUROPEA, Proposal for a Regulation on Cyber Resilience Act, COM (2022) 454 final;

24. FERRETTI G., Regolazione multilivello e cybersicurezza, in “Rivista italiana di informatica e diritto”, n. 2/2023;
25. ENISA, Annual Report 2021;
26. CYBERSECURITY TRENDS, “Speciale NIS2”, n. 4/2023;
27. COMMISSIONE EUROPEA, EU Cybersecurity Strategy for the Digital Decade, Bruxelles, 2020;
28. COMMISSIONE EUROPEA, Raccomandazione 2003/361/CE relativa alla definizione di micro, piccole e medie imprese;
29. DRAGONI M., “Supply chain e cybersicurezza: dalla NIS2 alla compliance preventiva”, in Cybersecurity360, 2023;
30. ENISA, Cybersecurity for Supply Chains – Good Practices, 2022;
31. ENISA, Technical Guidelines for Minimum Security Measures under NIS2, 2023;
32. FLORIDI L., “Governance della cybersicurezza: responsabilità e compliance dopo la NIS2”, in European Journal of Digital Law, 2024;
33. DECRETO LEGGE 82/2021, convertito in Legge 4 agosto 2021, nr. 109, recante: “Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale”;
34. ENISA, Cooperation Group Mechanisms – Best Practices for Enforcement, 2023;
35. ENISA, “Cybersecurity Threat Landscape 2023”, ottobre 2023;
36. DETERMINAZIONE ACN n. 38565/2024 (registrazione delle entità NIS2 sulla piattaforma ACN);
37. ENISA, “NIS Investments 2024 – Trends and Priorities in Cybersecurity Spending”, marzo 2024, p. 16;

38. CIRCOLARE AgID 18 aprile 2017, n. 2/2017 recante “Misure minime di sicurezza ICT per le Pubbliche Amministrazioni”;
39. IL SOLE 24 ORE, “Attacco hacker alla Regione Lazio, compromesse credenziali di un fornitore”, 2 agosto 2021;
40. FERRETTI G., “NIS2, DORA, GDPR: verso un modello integrato di compliance digitale”, in Riv. Dir. e Tecnologie, 2023;
41. REGOLAMENTO (UE) 2022/2554 (Digital Operational Resilience Act – DORA);
42. REGOLAMENTO (UE) 2024/2847 (Cyber Resilience Act);
43. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection;
44. ACN, Framework Nazionale per la Cybersecurity e la Data Protection, v. 2.0, 2022;
45. MAUGERI L. e RICCARDI A., “La Direttiva NIS2: il quadro giuridico italiano”, in ictsecuritymagazine.com, 2024;
46. DI GIACOMO L., “In GU il decreto NIS 2: ecco chi si deve adeguare e come”, in diritto.it, 2024;
47. KAISER E., “The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations” in MediaLaws, 2023;
48. DETERMINAZIONE DEL DIRETTORE GENERALE dell’Agenzia per la cybersicurezza nazionale del 26.11.2024 di cui all’articolo 7, comma 6, e all’articolo 40, comma 5, lettera b), del D. lgs. 4 settembre 2024, n. 138;
49. ENISA, “Threat Landscape 2021”, European Union Agency for Cybersecurity, april 2020 – july 2021;
50. DETERMINAZIONE ACN 164179 del 14 aprile 2025;

51. DPCM 30 luglio 2020, n. 131 - Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;
52. VACIAGO E., “Le ultime evoluzioni del ransomware: cosa insegnano i casi WannaCry e NotPetya” in The Innovation Group, 2017;
53. MINISTERO DELLA SALUTE, Decreto 14 gennaio 2025, recante “Istituzione presso il Ministero della salute del tavolo settoriale per l’attuazione della NIS2”.

## SITOGRAFIA


- www.enisa.europa.eu
- www.ilsole24ore.com
- www.repubblica.it
- www.cybersecurity360.it
- www.ictsecuritymagazine.com
- www.diritto.it
- www.medialaws.eu
- www.theinnovationgroup.it
- https://ec.europa.eu
- www.gazzettaufficiale.it
- www.acn.gov.it
- digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
- www.enisa.europa.eu
- www.astrid-online.it
- www.theinnovationgroup.it
- www.eur-lex.europa.eu

## ACRONIMI

- **ACN** – Agenzia per la Cybersicurezza Nazionale
- **CERT-AgID** – Computer Emergency Response Team dell'Agenzia per l'Italia Digitale
- **CINI** – Consorzio Interuniversitario Nazionale per l'Informatica
- **CISO** – Chief Information Security Officer
- **CSIRT** – Computer Security Incident Response Team
- **DORA** – Digital Operational Resilience Act
- **DPO** – Data Protection Officer
- **ENISA** – Agenzia dell'Unione europea per la cybersicurezza
- **EU-CyCLONe** – European Cyber Crises Liaison Organisation Network
- **FSD** – Fornitori di Servizi Digitali
- **GDPR** – General Data Protection Regulation
- **ICT** – Information and Communication Technology
- **MSSP** – Managed Security Service Provider
- **MSP** – Managed Service Provider
- **NIS** – Network and Information Security (NIS1)
- **NIS2** – Network and Information Security Directive 2
- **OSE** – Operatori di Servizi Essenziali
- **SIEM** – Security Information and Event Management
- **TSP** – Trust Service Provider
- **UE** – Unione Europea

**ALLEGATO**

- ✓ Prof. Razzante, qual è, a Suo avviso, la novità più importante introdotta dalla Direttiva NIS2 rispetto alla Direttiva NIS1?

***Indubbiamente la responsabilizzazione dei vertici delle aziende per la resilienza delle strutture di appartenenza. Sulla scia di altre direttive Ue che hanno contenuti strategici per il settore imprese (si pensi all'antiriciclaggio), opportunamente si prevede che il management delle imprese obbligate approvi e risponda dell'attuazione delle policy riguardanti l'assetto interno della cybersicurezza, dalla strategia fino all'applicazione specifica.***

- ✓ In che modo la NIS2 potrà contribuire, in termini concreti, a rafforzare la resilienza cibernetica delle infrastrutture critiche europee?

***Potrà contribuire solamente se farà da propulsore di una nova cultura della cybersicurezza degli Stati, in primis, e poi delle infrastrutture che essi devono governare.***

- ✓ Ritiene che il tessuto imprenditoriale italiano, con particolare riferimento alle piccole e medie imprese, sia adeguatamente preparato ad affrontare gli obblighi previsti dalla nuova direttiva?

***Vari studi recenti ci dicono che le PMI italiane sono pronte per un 60% circa, mentre fino a un anno fa parlavamo della metà. Mi pare un passo avanti importante, ma serve una politica comune, che trovi il sostegno del Governo e dialoghi con le Associazioni di categoria. Ci sono limiti culturali, di awareness, non tanto di tecnologie, perché ci siamo mossi, insieme a gran parte degli Stati europei, colpevolmente in ritardo. Inoltre, le spese per la ricerca e la formazione da noi vengono sempre considerate superflue…lo dico molto decisamente e senza parafrasi…è un grande limite, sa di provincialismo…al di là dei sostegni fiscali, che pure (limitati) ci sono, le***

***imprese non possono pretendere che siano sempre i Governi a garantire il finanziamento alla ricerca. Non ci sono soldi per quella pubblica, figuriamoci…! È un concetto che ho ribadito più volte in occasioni istituzionali e convegnistiche, e che ribadisco volentieri in questa sede.***

- ✓ Che ruolo dovrebbe avere la cooperazione tra pubblico e privato nell'attuazione efficace della NIS2 e, più in generale, nella costruzione di una strategia europea di cybersicurezza robusta e realmente sostenibile?

***Un ruolo essenziale, come dicevo. Non basterebbero i soli finanziamenti senza una partnership tecnologica tra aziende già pronte e uffici pubblici che presidiano i rischi. Inoltre, essendo le risorse economiche per definizione insufficienti di cui gli Stati dispongono, non si potrà che auspicare la demoltiplica di questi finanziamenti a favore delle entità più piccole.***

- ✓ La NIS2 si integra in maniera adeguata con gli altri strumenti normativi europei in materia di cybersicurezza, come il *Cyber Resilience Act*, il regolamento DORA e il GDPR?

***Direi di sì. Aiuterà soprattutto proprio la previsione, in NIS, di obblighi in qualche modo già contenuti negli altri provvedimenti, che quindi, senza creare sovrapposizioni (pericolo comunque esistente), potranno essere "scalati" a seconda delle esigenze e della configurazione dei soggetti obbligati.***

- ✓ In prospettiva futura, ritiene auspicabile il superamento dello strumento della direttiva a favore, ad esempio, di un regolamento europeo direttamente applicabile in materia di sicurezza informatica?

***Assolutamente sì, dato che saranno urgenti delle revisioni sia per obsolescenza rapida delle regole, a causa dell'incessante evoluzione delle tecnologie, sia perché (spero di essere smentito, ovviamente) bisognerà sollecitare i Paesi più recalcitranti.***

- ✓ Quali sono, a Suo avviso, le direttrici evolutive che il diritto europeo in materia di cybersicurezza potrebbe seguire nei prossimi cinque o dieci anni?

***Innanzitutto, urge un codice di sicurezza cibernetica armonizzato, che superi i gap tecnologici e legislativi dei singoli Stati. Bisognerà poi provvedere ad una legislazione sugli obblighi che tenga conto delle tecnologie come "asset" e non come servizi. Non ultime, delle norme sulle responsabilità di chi utilizza gli strumenti in questione, che facciano chiarezza sia in sede civile che penale. Non possiamo pensare che chi utilizza, non solo in senso malevole, le tecnologie e, soprattutto, l'intelligenza artificiale, si senta in una zona franca solo perché opera sul web e attraverso canali non fisicamente evidenti.***

***L'attribuzione (c.d. "attribution") degli attacchi cyber è questione annosa, cui non si riesce a dare soluzione a causa, soprattutto, dei limiti imposti dal trattato delle Nazioni Unite e dal concetto di guerra e legittima difesa. Non siamo più né alla guerra fredda né al terrorismo tradizionali.***

***Il semplice adeguamento dei codici di rito non basta. Vanno fatti accordi internazionali e programmi strategici nuovi, multilaterali, che superino le rigidità delle legislazioni prudenziali dei tempi di pace. Senza timore di essere guerrafondai, non possiamo tollerare che il web sia terra di nessuno. Non è vero, infatti, che da guerre asimmetriche non possano derivare danni alle popolazioni: anche questa è una idea antiquata che va sicuramente rimossa dal pensiero delle Autorità e degli stessi cittadini.***