G.E.O.



La normativa europea per la sicurezza cibernetica.

Direttiva NIS e sua evoluzione

Redatto da:

Alessandra Fiorani - Senior Reasercher Area Difesa & Sicurezza

Mondo Internazionale
Associazione culturale
Gallarate, Via Marco Polo 31
21013 - VA, Italia
C.F. 91071700123
P.IVA 03727710125

Mail: segreteria@mondointernazionale.com

INDICE

1. La strategia Europea per la sicurezza cibernetica

1.1 Trattazione della Direttiva NIS 2016/1148

1.2 L'implementazione italiana della NIS

2. Evoluzione degli scenari di sicurezza

2.1 La revisione della Direttiva NIS

2.2 Feedback emersi dalla consultazione pubblica

2.3 La proposta della Commissione Europea

2.4 Infrastruttura sottomarina



DIFESA E SICUREZZA – La normativa europea per la sicurezza cibernetica: Direttiva NIS e la sua evoluzione.

ABSTRACT

Al giorno d'oggi, la cybersecurity costituisce una sfaccettatura imprescindibile della sicurezza nazionale ed internazionale. La minaccia cibernetica è uno dei pericoli attuali con cui gli Stati e le istituzioni internazionali devono confrontarsi quotidianamente. Garantire la sicurezza dei sistemi e delle reti di telecomunicazione è uno degli obiettivi, per l'Unione Europea, affinché essa raggiunga- finalmente- una sovranità digitale ed un'autonomia strategica in campo tecnologico.

Il seguente report ha l'obiettivo di analizzare l'evoluzione della Direttiva NIS 2016/11548 in ambito Europeo, partendo dalle linee di guida che hanno reso possibile la sua creazione fino ad arrivare alle più recenti discussioni sulla materia. Nello specifico l'input della seguente elaborazione risulta essere la campagna di consultazione pubblica avviata dall'Unione Europea per procedere alla revisione della Direttiva NIS sulla base delle moderne esigenze del mondo cibernetico, o meglio all'elaborazione di quella che potremmo chiamare una *"Direttiva NIS 2"*. Nella seguente trattazione si è cercato di fornire una panoramica completa e approfondita, andando ad indagare l'evoluzione della normativa e le possibili prospettive future di attuazione.
Per la stesura del testo non stati consultati sia documenti ufficiali delle istituzioni europee sia dossier e report aziendali delle società che hanno preso parte alla consultazione pubblica.

Si è scelto, inoltre, di concentrare l'analisi sul contesto nazionale italiano allo scopo di indagare quali sono le recenti modalità di attuazione della Direttiva e i possibili elementi di contrasto o cambiamento rispetto alla normativa comunitaria.

Infine, dato che la rete dei cavi sottomarini può essere considerata la "nuova" frontiera della sicurezza globale, ci si è soffermati sull'esigenza di allargare la protezione delle reti anche a questa componente dell'infrastruttura cibernetica.

La normativa europea per la sicurezza cibernetica: Direttiva NIS e la sua evoluzione

1. La Strategia Europea per la sicurezza cibernetica.

Nel 2013 si consolida ufficialmente la strategia europea in materia di sicurezza cibernetica. Nello specifico viene emanata la C*omunicazione congiunta* al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni contenente le direttive della "*Strategia dell'Unione Europea per la cyber sicurezza".*[1] In questo documento lo spazio cibernetico viene descritto come uno spazio di libertà, in cui vengono abbattute le barriere tra gli Stati membri; considerandolo un contesto favorevole all'espansione dei diritti fondamentali dell'uomo. Da questa premessa, la Commissione Europea auspica la normalizzazione dello spazio cibernetico.

In questo scenario di regolamentazione, sorgono anche nuove esigenze di tutela. Prima fra tutte la necessità di salvaguardare le reti cibernetiche nazionali di gestione dei servizi essenziali.

Da questa consapevolezza nasce la Direttiva NIS (EU-2016/1148)[2] - *Network and Information Security.* La presente Direttiva interviene sul piano della sicurezza delle reti cibernetiche e, nello specifico, ha l'obiettivo di stabilire un elevato livello di sicurezza della rete e dei sistemi informativi.

Nel primo Considerando del testo, infatti, si afferma che: "*Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno".*

1.1 Trattazione della Direttiva NIS 2016/1148.

Per ragioni di economia di scrittura, la Direttiva verrà analizzata nei suoi tratti salienti. Per iniziare si riporta l'articolo 1 della Direttiva NIS 2016/1148, che descrive le principali misure da adottare per

[1] Commissione Europea, 07 febbraio 2013, Comunicazione Congiunta al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, *Strategia dell'Unione europea per la cibersicurezza*.

[2] Direttiva (Ue) 2016/1148 del Parlamento Europeo e Del Consiglio, del 06 Luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

raggiungere gli standard di sicurezza delle reti cibernetiche. Al comma 2, si dichiara che *"la presente direttiva*:

a) *fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi*[3]*;*
b) *istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi;*
c) *crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace;*
d) *stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;*
e) *fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi."*

L'obiettivo è quello di raggiungere un livello elevato di sicurezza delle reti, finalizzato a migliorare il funzionamento del mercato interno. Gli Stati membri sono gli artefici principali di tale obiettivo, che dovranno comunicare e coordinarsi con due categorie di attori individuate dalla normativa. Le figure a cui si fa riferimento sono:

- Operatori di servizi essenziali (OES);[4]
- Digital Service Provider (DSP), o meglio di fornitori dei servizi digitali.

I settori interessati dalla Direttiva NIS sono:

- Rete Idrica;
- Energia;
- Infrastrutture digitali;
- Infrastrutture del mercato bancario e finanziario;
- Salute;
- Trasporti.

Gli Stati hanno il compito di vigilare su tali soggetti, che hanno a loro volta l'obbligo di adottare delle misure efficaci di prevenzione dei rischi di incidenti e di comunicare e informare, in caso di incidenti, il CSIRT di competenza nazionale.

[3]Vedi paragrafo 2, articolo 1, della Direttiva NIS – Dir. EU 2016/1148, Oggetto e ambito di applicazione.
[4] Vedi articolo 5 della Direttiva NIS – Dir. EU 2016/1148, Identificazione degli operatori di servizi essenziali.

Gli obiettivi rientrano nello specchio della tutela delle reti dei servizi essenziali, e sono quelli di:

- gestione dei rischi di sicurezza;
- protezione contro i cyber attacchi;
- individuazione di incidenti di cyber sicurezza;
- riduzione dell'impatto degli incidenti di cyber sicurezza.

La Direttiva NIS è il prodotto del processo europeo di tutela dello spazio informatico, nello specifico ha lo scopo di rafforzare la sicurezza informatica in tutti i settori che si basano prevalentemente sulla tecnologia dell'informazione e della comunicazione (ITC). Ulteriore punto di novità e di rafforzamento è la disciplina degli incidenti informatici.

La Direttiva stabilisce i criteri per valutare la rilevanza di un incidente informatico con impatto significativo. Nello specifico, un incidente è rilevante se si verifica almeno una delle seguenti condizioni:

- *indisponibilità del servizio fornito per oltre 5.000.000 di ore utente;*
- *perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE;*
- *rischio per la sicurezza e/o l'incolumità pubblica oppure rischio in termini di perdite di vite umane;*
- *danni materiali superiori a 1.000.000 di Euro per almeno un utente nell'UE.*

La notifica degli incidenti di sicurezza va fatta al Computer Security Incident Response **Team (CSIRT)**, un'autorità delegata al repentino intervento in caso di attacco informatico ad uno dei servizi essenziali. Ogni Stato membro ha l'obbligo di costituire questo Gruppo di intervento rapido nel proprio territorio nazionale.

Per approfondire il tema è necessario illustrare il processo di adozione della Direttiva nel contesto italiano.

1.2 L'implementazione italiana della NIS

In Italia la Direttiva è stata recepita attraverso il **decreto legislativo n. 65 del maggio 2018** [5], che applica gli aspetti fondamentali della Direttiva NIS al contesto italiano e mira a creare un livello minimo di sicurezza delle reti e dei sistemi informatici.

Il testo nelle disposizioni generali e nei primi articoli prende le mosse del testo europeo, ha la stessa impostazione di fondo; tuttavia, ci sono elementi di novità che rappresentano delle specifiche italiane.

[5] DECRETO LEGISLATIVO 18 maggio 2018, n. 65**.** Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Gli articoli più importanti, in cui è possibile rintracciare gli adattamenti del legislatore italiano, sono l'articolo 6 e l'articolo 7.

All'articolo 6, denominato "*Strategia nazionale di sicurezza cibernetica",* da quanto riportato nel paragrafo 1:

"1. Il Presidente del Consiglio dei ministri adotta, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale "[6]

si può notare la perimetrazione dell'ambito d'intervento esclusivo dello Stato l'assenza del riferimento all'ENISA- Agenzia Europea per la cibersicurezza.

All'articolo 7 "*Autorità nazionali competenti e punto di contatto unico"*, vengono stabilite **le autorità competenti**. Non si sono create autorità indipendenti o aggiuntive rispetto alla struttura di governo. Ma, si sono definite le autorità competenti individuandole all'interno dei Ministeri; quest'ultimi si vanno così a configurare come punti di riferimento delle varie aree sensibili ed ottengono ulteriori funzioni.

Figura 1- Autorità competenti NIS nazionali[7]

Autorità competenti NIS nazionali	Ambito di competenza
Ministero dello Sviluppo Economico	Settore energia
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle Infrastrutture e dei Trasporti	Settore trasporti
Ministero dell'Economia e delle Finanze in collaborazione con Banca d'Italia e Consob	Settore bancario
	Settore infrastrutture dei mercati finanziari
Ministero della Salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'Ambiente e della Tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore fornitura e distribuzione di acqua potabile

Nell'impianto generale della NIS, l'Italia ha scelto di istituire più autorità competenti e all'interno dei ministeri, scelta precisa e chiara che racchiude anche un certo significato politico.

Al comma 3, il **punto di contatto unico** viene identificato nel vertice dei nostri servizi segreti: presso il DIS- Dipartimento per l'informazione e la sicurezza.

[6] *Ibidem.*

[7] Sistema di informazione per la sicurezza della Repubblica. *RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2020*. Relazione al Parlamento. Febbraio 2021

"3. Il Dipartimento delle informazioni per la sicurezza (DIS) è designato quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi."

Rispetto al ruolo del DIS nei confronti della revisione della Direttiva NIS, dal Rapporto del Dipartimento si evince la sua partecipazione, come autorità competente italiana, al **Gruppo di Cooperazione NIS** (NISCG)[8]. "*Il DIS partecipa in rappresentanza del nostro Paese alle attività del NISCG, nel cui ambito nel corso dell'anno è stato, tra l'altro, affrontato l'avvio del processo di revisione della Direttiva NIS (la cd. NIS 2), rispetto alla quale, operando in stretto coordinamento con le Autorità NIS italiane, sono state presentate delle proposte volte ad incrementarne l'efficacia*."

Il decreto del 2018 recepisce la direttiva NIS negli aspetti fondamentali e va a creare quel livello minimo di sicurezza delle reti e dei sistemi informatici. È un decreto importante che dà un orientamento, ma l'aspetto forse più importante ce lo rende il **Decreto-legge 21 settembre 2019 n.105.**

A complemento di questo recepimento, con il decreto-legge n. 105 del 2019[9] si è istituito il **"Perimetro Di Sicurezza Nazionale Cibernetica"**. All'articolo 1 del citato decreto-legge, viene sancita l'istituzione di suddetto perimetro, e vengono descritti i principali caratteri e finalità. I soggetti che vi rientrano sono essenzialmente: *"le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale."*

A più di anno circa dall'emanazione del decreto-legge n.105, il percorso per il completamento dell'istituzione di tale perimetro è stato rallentato dagli effetti della pandemia da Covid-19.

Tuttavia, è possibile illustrare le tappe fondamentali per la sua creazione, finora raggiunte. Prima fra tutte, è essenziale ricordare l'emanazione del **decreto n.131 del 30 luglio 2020,** che istituisce formalmente il perimetro di sicurezza. Tale normativa è entrata in vigore il 5 Novembre 202, ed è il primo dei 4 decreti che istituiscono tale misura di sicurezza cibernetica.

Ad ottobre 2020 è stato poi pubblicato in Gazzetta Ufficiale il primo DPCM che determinava quali erano i soggetti pubblici e privati idonei a poter essere inclusi nel Perimetro cibernetico. In sintesi,

[8] Per approfondimenti https://temi.camera.it/leg18/post/OCD15-13829/gruppo-cooperazione-nis-rapporto-sulla-valutazione-coordinata-livello-ue-rischi-cibersicurezza-reti-quinta-generazione-5g.html

[9] DECRETO-LEGGE 21 settembre 2019, n. 105. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

essenzialmente essi sono i soggetti e le categorie di chi presta un servizio essenziale per il funzionamento dello Stato. A fine gennaio 2021, è stata approvato con favore il testo del decreto attuativo.

A questi due testi, ne seguiranno altri due: uno relativo alle categorie che dovranno notificare al **CVCN- Centro di valutazione e certificazione nazionale**[10] e uno dedicato ai criteri di accreditamento dei laboratori competenti per le verifiche delle condizioni di sicurezza. Il governo italiano si è detto ottimista nel cercare di concludere il processo di creazione del perimetro nella primavera del 2021, tuttavia, ad oggi, il procedimento ha subito bruschi rallentamenti[11].

2. Evoluzione degli scenari e delle esigenze di sicurezza

Il 29 gennaio 2020 è stato pubblicato il nuovo programma di lavoro della Commissione europea. Nell'ambito della seconda priorità – *"A Europe fit for the digital age"*- la Commissione ha annunciato l'intenzione di avviare una revisione della direttiva sulla sicurezza delle reti- Direttiva NIS.

Con la Comunicazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Comitato economico e Sociale europeo e al Comitato delle Regioni viene presentata "*La strategia dell'UE per l'Unione della sicurezza"* per il periodo 2020-2025.[12] Strategia che si concentra su settori prioritari in cui l'Unione può apportare valore per sostenere gli Stati membri nel promuovere la sicurezza, in particolare la sicurezza informatica. Entro la fine del 2020, la Commissione prevede, tra l'altro, di completare la **revisione della Direttiva sui Sistemi di rete e di informazione- Direttiva NIS-**, di proporre la necessità di una Joint Cyber Unit e di adottare una nuova strategia per la sicurezza informatica.

Nella Comunicazione, la Commissione Europea ha fatto notare come la globalizzazione e l'evoluzione digitale in cui siamo costantemente immersi, siano sì delle opportunità di innovazione ma presentino anche dei rischi. Rischi che, provocano la nascita dell'esigenza di maggiore tutela alla sicurezza

[10] Per approfondimenti https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039261-istituito-il-centro-di-valutazione-e-certificazione-nazionale-cvcn

[11] Fonte, https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-di-sicurezza-nazionale-cibernetica-il-primo-decreto-attuativo-non-fa-primavera/

[12]Commissione Europea, 24 luglio 2020, Comunicazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Sulla strategia dell'UE per l'Unione della sicurezza*.

dell'Unione. *"Le minacce alla sicurezza diventano inoltre sempre più complesse"* o ancora "*gli attacchi possono verificarsi senza preavviso e lasciare dietro di sé poche o nessuna traccia; soggetti statali e non statali possono mettere in atto una serie di minacce ibride."*[13]

Con queste parole sono state introdotte le ragioni che rendono necessaria una definizione strategica degli interventi che l'UE deve attuare per creare *"un ambiente della sicurezza adeguato alle esigenze del futuro".*

È stato fatto richiamo anche alla principale minaccia di tutto il 2020: la pandemia da Covid-19. L'emergenza sanitaria prodotta dalla suddetta malattia ha evidenziato come in un mondo globalizzato le minacce alla sicurezza nazionale sono sempre più globali. Per affrontare tale pandemia l'Unione Europea ha dovuto adottare soluzioni comuni, in una maggiore ottica di integrazione comunitaria.

Si sostiene infatti, che gli Stati membri non siano in grado di affrontare singolarmente minacce di tale portata.

L'Unione si augura di *"rafforzare il suo sistema generale di gestione delle crisi"*. In questo scenario globale di gestione dei rischi non possiamo non far riferimento alla sicurezza cibernetica.

Per definizione[14] "[…] Il Cyberspace è un dominio globale e dinamico caratterizzato dall'uso combinato di uno spettro elettronico ed elettromagnetico, con lo scopo di creare, immagazzinare, modificare, scambiare, condividere ed estrarre, utilizzare, eliminare informazioni, gestire e compromettere beni fisici", essendo un dominio globale non può non interessare la strategia europea in materia di sicurezza.

Al capo IV della Comunicazione, la Commissione Europea individua **quattro priorità strategiche dell'Unione,** tra queste vi è: "*un ambiente di sicurezza adeguato alle esigenze del futuro"*, priorità che richiama l'esigenza di implementare la sicurezza nel dominio cibernetico. Nello specifico la necessità di proteggere le infrastrutture critiche e i servizi essenziali utilizzati dai cittadini nella vita di tutti i giorni. Viene affermato che: "*l'attuale quadro dell'UE in materia di protezione e resilienza delle infrastrutture critiche non è al passo con l'evoluzione dei rischi."* Questo appare come un esplicito richiamo alla Direttiva NIS, principale normativa in riferimento alla protezione dei servizi essenziali.

In questo scenario strategico si inserisce, dunque, la necessità della revisione della Direttiva NIS.

[13] Cit., vedi Comunicazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Sulla strategia dell'UE per l'Unione della sicurezza.*

[14] Viene riportata la definizione di D.T. Kuehl, *From Cyberspace to Cyber-power: Defining the Problem*, in *Cyberpower and National Security.*

2.1 La revisione della Direttiva NIS

La Commissione Europea dal mese di luglio 2020 ha avviato una consultazione pubblica sulla revisione della Direttiva NIS 2016/1148, finalizzata alla raccolta da parte degli stakeholders (riferiti ai settori dei servizi essenziali e delle infrastrutture critiche) di opinioni e potenziali modifiche alla normativa; opinioni che verranno poi confrontate con quelle degli Enti pubblici e statali, al fine di apportare le migliori ed efficienti modifiche.

La consultazione pubblica era già stata prevista nel teso del 2016 della Direttiva, precisamente all'articolo 23 individuando sotto la dicitura "*riesame*"[15] la possibilità di esaminare periodicamente il funzionamento della normativa.

Il processo di consultazione è avvenuto attraverso un portale web[16] istituito dall'Unione Europea sulla base del programma EU Survey, e si è concluso il 2 ottobre 2020.

Sul portale della Commissione Europea[17] vengono definiti come **soggetti target** a cui si rivolge la consultazione, i seguenti:

- Autorità competenti degli Stati membri;
- Organismi dell'Unione europea che si occupano di sicurezza informatica;
- Operatori di servizi essenziali;
- Fornitori di servizi digitali;
- Imprese di altri settori vulnerabili al di fuori del campo di applicazione della direttiva NSI attuale;
- Associazioni di categoria;
- Ricercatori e mondo accademico;
- Professionisti del settore della sicurezza informatica;
- Organizzazioni dei consumatori e cittadini.

Questi stakeholders sono chiamati a rispondere ad un questionario che si compone di tre parti, una prima di carattere generale, la seconda più tecnica e l'ultima che mira a raccogliere i suggerimenti da aggiungere alla normativa NIS.

[15] Vedi articolo 23 della Direttiva NIS EU-2016/1148, Riesame.

[16] https://ec.europa.eu/eusurvey/runner/NISreview?showecas=true

[17] Cybersecurity – review of EU rules on the security of network and information systems https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive/public-consultation

La consultazione ha due obiettivi:

n1. mira anzitutto a valutare il livello di funzionamento della Direttiva NIS all'interno di ciascun Paese dell'Unione;

n2. raccogliere opinioni sugli impatti di eventuali future modifiche dell'atto giuridico al fine di sostenere la valutazione previsionale.

2.2 Feedback emersi dalla consultazione pubblica.

L'elaborazione del seguente paragrafo si è basata sui commenti emersi[18] da parte di alcuni stakeholders che hanno preso parte alla consultazione.

Il GSMA- *Global System for Mobile Communications*- organismo commerciale per l'industria della telefonia mobile ha pubblicato il questionario con le proprie risposte e i propri suggerimenti per la revisione. GSMA consiglia alla commissione europea di implementare i soggetti che rientrano nelle due categorie di fornitori di servizi essenziali e di servizi digitali, suggerendo di comprendere anche i fornitori di software e hardware. Si rimprovera un approccio troppo burocratico e frammentato, e si suggerisce di snellire la procedura di notifica degli incidenti. Per ultimo si raccomanda alla Commissione di *"migliorare l'armonizzazione e la coerenza per i fornitori di servizi di comunicazione elettronica allineando strettamente la direttiva NIS con altri strumenti giuridici (legge sulla sicurezza informatica, codice europeo delle comunicazioni elettroniche (EECC)"*[19].

Altro commento analizzato è quello di ETNO- *European Telecommunications Network Operators' Association*- principale organismo per gli operatori europei di reti di telecomunicazione e comunicazione elettronica. Nel suo *Position Papers* si sono riscontrati molti punti in comune con il commento del GSMA.

L'Associazione dichiara che non può esistere una serie unica di misure di sicurezza informatica. Questo rimprovero si allinea alla proposta del GSMA di **migliorare l'armonizzazione** della NIS con ulteriori strumenti giuridici. Seguendo questa linea l'ETNO chiede di riformare il quadro legislativo per giungere ad un livello comune di sicurezza informatica e certezza giuridica.

Altro punto in comune tra i due commenti, si trova nella convinzione che i fornitori di hardware e software siano da includere nell'ambito di applicazione della legislazione.

[18] Sezione Europea dedicata ai feedback https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/feedback?p_id=8028476&page=3

[19] https://www.gsma.com/gsmaeurope/wp-content/uploads/2020/10/GSMA-Response-to-EC-public-consultation-on-NIS-Review.pdf

Infine il Paper riporta **ulteriori obiettivi** che la nuova Direttiva NIS dovrebbe perseguire, tra cui:

- Aumentare il livello di consapevolezza e collaborazione tra pubblico e privato, attraverso un'opera di sensibilizzazione;
- Armonizzare la nuova Direttiva con le legislazioni di tutti gli Stati membri, azzerare le discrepanze e raggiungere una coerente attuazione;
- Raggiungere un livello di coordinamento tra la NIS e le altre misure giuridiche, primo fra tutti il *Cybersecurity Act*[20] volto a colmare la lacuna che la Direttiva presenta in materia di 5G.

L'avvento de **5G** risulta essere uno dei principali temi su cui gli stakeholders hanno insistito maggiormente. Quello che si chiede alla Commissione EU è di prevedere nel nuovo testo delle misure per garantire tutela e sicurezza a tutti i dispositivi che supporteranno questa nuova connessione.

Anche la multinazionale italiana, Enel S.p.a.– azienda leader nel settore delle forniture energetiche- ha partecipato alla consultazione pubblica, e nel suo feedback[21] possiamo ritrovare la richiesta di implementare le misure per la protezione delle nuove tecnologie emergenti, come: il 5G, i droni e l'intelligenza artificiale.

Il gruppo Enel propone anche di migliorare l'identificazione degli Operatori di servizi essenziali (OES), in questo rimprovera al vecchio testo della Direttiva un notevole grado di frammentazione.

Possiamo affermare che questo suggerimento, di includere nuovi soggetti nella lista dei destinatari della NIS, è uno dei più gettonati. Dai gruppi di telefonia mobile chi chiedono di inserire anche i fornitori di hardware e software, passando per Enel che suggerisce di comprendere anche i fornitori di illuminazione pubblica, fino ad arrivare al gruppo belga Eurosmart[22] che chiede ci ampliare la lista anche ai servizi di telecomunicazioni, fornitori di e-Government e social network. Una delle tipologie mancanti tra i fornitori sono proprio quelli di servizi informatici che ogni giorno sono soggetti ad attacchi informatici.

[20] Regolamento Europeo 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sull'ENISA (Agenzia dell'Unione europea per la sicurezza informatica) e sulla certificazione in materia di sicurezza informatica delle tecnologie dell'informazione e della comunicazione.

[21] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F541131

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F543293

2.3 La proposta della Commissione Europea

A seguito del **processo di revisione**, il 16 dicembre 2020 è stata presentata dalla Commissione Europea la proposta legislativa[23]. La presente proposta fa parte di un pacchetto di misure volte a migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'Unione nel settore della sicurezza informatica e della protezione delle infrastrutture critiche. La proposta si basa sulla direttiva NIS in vigore e la abroga, allo scopo di modernizzare il quadro giuridico esistente tenendo conto dell'accresciuta digitalizzazione del mercato interno negli ultimi anni, dell'evoluzione del panorama delle minacce alla sicurezza informatica e, soprattutto, dell'esito della consultazione pubblica.

Il nuovo testo è diviso in sette capitoli e riporta in totale 43 articoli, di seguito enunceremo i fondamentali elementi di novità introdotti.

Viene soddisfatta l'esigenza, emersa dalla consultazione, di **ampliare la lista dei fornitori** a cui applicare la Direttiva, vi si aggiungono nuovi settori tra cui: servizi postali, gestione dei rifiuti, pubblica amministrazione in generale, settore aerospaziale, quello della produzione di dispositivi medici ed apparecchiature elettroniche, produzione e distribuzione di alimenti, e settore chimico. Vengono incluse tutte le medie e grandi imprese di questi settori, ritenuti essenziali per il funzionamento dell'economia e della società.

In riferimento ai **soggetti**, si elimina la distinzione tra Operatori di servizi essenziali e Fornitori di servizi informatici, e si abrogano i criteri per la loro identificazione che erano in capo al singolo Stato membro.

Per questi soggetti resta l'obbligo di impiegare misure di sicurezza adeguate alla prevenzione dei rischi informatici, e vengono aggiunte delle misure specifiche obbligatorie riportate all'articolo 18, tra cui: sistemi di gestione degli incidenti, utilizzo della crittografia, controllo della sicurezza informatica dei propri fornitori e sicurezza della catena logistica, procedure di testing e auditing per valutare l'efficacia delle misure di prevenzione.

Per quanto riguarda gli **incidenti** rimane l'obbligo di segnalazione e notifica, ma vengono precisati i tempi. Nel precedente testo infatti non veniva indicato l'arco temporale entro cui inviare la segnalazione, ma veniva suggerito di notificare "senza ingiustificato ritardo"; con la modifica viene

[23] Proposta di approvazione DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa a misure per un elevato livello comune di sicurezza informatica in tutta l'Unione, che abroga Direttiva (UE) 2016/1148. https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

stabilito che la segnalazione va inviata entro 24 ore dal momento in cui si viene a conoscenza dell'incidente.

Si riscontra anche un aumento dell'entità delle **sanzioni** previste in caso di violazione degli obblighi. Stabilire le sanzioni sarà compito dei singoli Stati membri, però la normativa enuncia le soglie entro le quali deve essere fissato il valore del provvedimento. Le multe andranno da un massimo di almeno 10 milioni di euro fino al 2% del fatturato totale annuo della relativa impresa.
Altro elemento di novità nella Direttiva NIS 2 è ***l'information sharing***. La raccomandazione che viene fatta a tutti gli Stati membri è di migliorare la cooperazione e la collaborazione, incrementando la condivisione di informazioni. Rispetto a questo avranno ruoli fondamentali sia l'ENISA che il *Cooperation Group*- gruppo di cooperazione per elaborare linee strategiche comuni a tutti gli Stati membri-.

Per **completare l'iter** di approvazione la proposta della Commissione EU sulla nuova Direttiva NIS dovrà superare il vaglio del Consiglio e del Parlamento Europeo. In queste fasi la suddetta proposta potrebbe subire modifiche. I tempi per l'entrata in vigore sono ancora lunghi: si parla di anni. Il testo, infatti dopo esser stato approvato dai legislatori europei dovrà anche essere attuato a livello nazionale.

2.4 Infrastruttura sottomarina

Se, come detto precedentemente, il campo principale di applicazione della NIS è la protezione tutela delle infrastrutture critiche, si può affermare che anche i cavi sottomarini rientrino nella sua giurisdizione.
Nella versione del 2016 però non sono riscontrabili riferimenti ai cavi sottomarini. Questi cavi, destinati *alle telecomunicazioni e al trasporto intercontinentale di informazioni tra gli Stati*[24] , rientrano nella più ampia definizione di reti e sistemi informativi; materia principe della Direttiva NIS.

È essenziale ricordare che il controllo di questa rete sottomarina ad oggi, rappresenta uno dei principali campi di competitività geopolitica tra gli Stati. I cavi sottomarini possono avere un ruolo strategico e uno dei principali obiettivi delle azioni di guerra cibernetica.

[24] *Alpha Institute*- ***Le sfide future per l'infrastruttura dei cavi sottomarini ed il ruolo dell'Italia per la NATO.*** Aprile 2021 https://www.alphainstitute.it/2021/04/12/le-sfide-future-per-linfrastruttura-dei-cavi-sottomarini-ed-il-ruolo-dellitalia-per-la-nato/

"La sicurezza del cablaggio sottomarino dev'essere una priorità di ogni Stato sovrano, per prevenire spiacevoli conseguenze di un qualsivoglia scenario bellico. L'Unione Europea sembra aver recepito finanche a livello legislativo l'importanza della tutela dei cavi, trattando del tema nel recovery fund e nella direttiva NIS, che si propone di realizzare un ravvicinamento di disciplina dei Paesi Ue, in punto di protezione delle reti e dei sistemi informativi all'interno dell'Unione."[25]

Nel 2020, durante il processo di consultazione pubblica per la revisione della NIS, la sicurezza dei cavi sottomarini si è inserita nel più ampio discorso della sicurezza e sovranità europea.

Ad oggi, è possibile basarsi su mere indiscrezioni che confermerebbero l'inserimento della tutela di questa infrastruttura sottomarina all'interno del testo della futura Direttiva NIS 2.0. [26] Secondo quanto riportato nell'articolo "*I cavi sottomarini entreranno nella nuova direttiva NIS"* della rivista online "*Formiche*"[27]; il delegato al digitale della rappresentanza permanente presso l'Unione europea del Portogallo, Felipe Batista, durante un dibattito dal titolo *China's Digital Silk Road and Undersea Cables: Prospects and Threats Posed to the EU* ha confermato che a seguito del processo revisionale della Direttiva europea, verranno inseriti prioritariamente dei riferimenti alla protezione dei cavi sottomarini.

Tale previsione futura si andrà ad inserire nella più ampia esigenza europea di garantire la propria sovranità digitale. Difatti, analizzando le recenti disposizioni europee in materia è possibile affermare che la sovranità digitale o tecnologica, sarà sempre maggiormente presente, come materia autonoma, nelle politiche dell'Unione. Il dibattito sul digitale non può non essere anche dibattito sulla sovranità ed autonomia strategica europea. Su tali concetti, maggiori sviluppi si sono avuti nel semestre tedesco di presidenza del Consiglio EU e a dettare la linea guida da seguire per il prossimo decennio è la comunicazione *"Decennio digitale europeo: obiettivi digitali per il 2030*[28]*"*, che si basa su quattro punti cardinali:

1. Sviluppo delle competenze digitali;
2. Infrastruttura sicura, efficiente e sostenibile;
3. Trasformazione digitale delle imprese,
4. Digitalizzazione dei servizi pubblici.

[25] Ibidem.
[26] https://formiche.net/2021/03/cavi-sottomarini-aggiornamento-nis/#:~:text=La%20Commissione%20europea%20aveva%20annunciato,all'aumento%20delle%20minacce%20cibernetiche
[27] https://rivista.formiche.net/?_ga=2.130590604.2065845337.1619465292-1143369768.1601019679
[28] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it

A nostro avviso nel punto n.3 è possibile riscontrare ed includere l'esigenza di tutelare l'infrastruttura dei cavi sottomarini da possibili attacchi *warfare*. Questo perché, la rete dei cavi sottomarini, costituisce un elemento costitutivo ed essenziale che contribuisce alla formazione del livello fisico sul quale poggia l'intero *cyberspace*. Per semplificare tale concetto basti pensare che: "*è la rete dei cavi sottomarini, diffusa in tutto il mondo, che consente a internet di funzionare*" o ancora che "*la rete dei cavi costituisce la "colonna vertebrale" dell'internet globale, essenziale per il commercio e le comunicazioni internazionali*".[29]

[29] Citazione del Professor Maurizio Mensi, membro dell'Organo di vigilanza sulla rete TIM, consigliere del Comitato economico e sociale europeo (CESE) e componente dell'Osservatorio CESE della transizione digitale.
https://www.bizdigital.it/2021/01/04/i-cavi-sottomarini-infrastruttura-chiave-per-internet-e-la-sicurezza-dei-dati/

BIBLIOGRAFIA

- Alpha Institute- *Le sfide future per l'infrastruttura dei cavi sottomarini ed il ruolo dell'Italia per la NATO.*

- Commissione Europea, 07 febbraio 2013, Comunicazione Congiunta al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, *Strategia dell'Unione europea per la cibersicurezza*.

- *Direttiva (Ue) 2016/1148 del Parlamento Europeo e Del Consiglio*, del 06 Luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

- *Regolamento Europeo 2019/881 del Parlamento europeo e del Consiglio*, del 17 aprile 2019, sull'ENISA (Agenzia dell'Unione europea per la sicurezza informatica) e sulla certificazione in materia di sicurezza informatica delle tecnologie dell'informazione e della comunicazione.

- *DECRETO LEGISLATIVO 18 maggio 2018,* n. 65**.** Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

- Sistema di informazione per la sicurezza della Repubblica. *RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2020*. Relazione al Parlamento.

SITOGRAFIA

- https://formiche.net/2021/03/cavi-sottomarini-aggiornamento-nis/#:~:text=La%20Commissione%20europea%20aveva%20annunciato,all'aumento%20delle%20minacce%20cibernetiche.
- https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/
- https://www.agendadigitale.eu/sicurezza/direttiva-nis-consultazione-e-processo-di-revisione-proposte-e-prossimi-step/
- https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-di-sicurezza-nazionale-cibernetica-il-primo-decreto-attuativo-non-fa-primavera/
- https://www.bizdigital.it/2021/01/04/i-cavi-sottomarini-infrastruttura-chiave-per-internet-e-la-sicurezza-dei-dati/
- https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it
- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F543293
- https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union