Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo

Flavia Bavetta

Abstract

Grazie ad una rapida trasformazione del digitale e all'interconnessione della società, i sistemi e servizi informatici, così come le infrastrutture di rete, occupano una posizione centrale nello svolgimento di tutte le attività che compiamo ogni giorno. Da tale considerazione ne discende inevitabilmente un'espansione del panorama delle minacce informatiche, le quali, ponendo nuove sfide al legislatore sia europeo che nazionale, richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. A tal riguardo, il legislatore europeo aveva emanato già nel 2016 la direttiva (UE) 2016/1148 (c.d. Direttiva NIS 1) con l'intento di innalzare i livelli di cybersecurity di un ristretto alveo di operatori ritenuti essenziali per la continuità operativa delle funzioni e dei servizi più importanti degli Stati membri. Tuttavia, tale obiettivo è stato solo parzialmente raggiunto, rendendosi così necessario un intervento in materia a distanza di pochissimi anni. Infatti, il 27 dicembre 2022 è stata emanata la direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, (cd. Direttiva NIS 2), con il preciso obiettivo di rendere il livello di *cybersecurity* di operatori considerati "essenziali" e "importanti" uniforme su tutto il territorio europeo.
Alla luce di ciò, il presente contributo analizza i principali adempimenti previsti dalla Direttiva NIS 2.

Thanks to a rapid digital transformation, ICT systems and services, as well as network infrastructures, occupy a central position in the maintenance of all the activities we carry out every day. Therefore, inevitably an expansion of the cyber threat landscape can be observed, posing new challenges to both European and national legislators, requiring appropriate, coordinated and innovative responses across all member states. In this regard, the European legislature had already enacted Directive (EU) 2016/1148 (NIS 1 Directive) in 2016 with the intention of raising the cybersecurity levels of a narrow range of operators deemed essential for the continuity of the most important functions and services of the member states. However, this goal has only been partially achieved, thus requiring more actions on the matter. Indeed, on December 27, 2022, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the

Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) was enacted, with the specific aim of making the level of cybersecurity of operators considered "essential" and "important" uniform throughout Europe.
In light of this, this paper analyzes the main obligations and novelties under the NIS 2 Directive.

Sommario

Keywords

cybersecurity - DirettivaNIS2 - misuredisicurezza - resilienza - UnioneEuropea.

1. L'aumento delle minacce cibernetiche e la risposta del legislatore

Grazie ad una rapida trasformazione del digitale e all'interconnessione della società, i sistemi e servizi informatici, così come le infrastrutture di rete, occupano una posizione centrale nello svolgimento di tutte le attività che compiamo ogni giorno.
Da tale considerazione ne discende inevitabilmente un'espansione del panorama delle minacce informatiche, le quali, ponendo nuove sfide al legislatore sia europeo che nazionale, richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Infatti, i dati degli ultimi anni dimostrano come il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti sia sempre più in aumento, rappresentando una grave minaccia per il funzionamento dei sistemi informatici e di rete che, nella maggior parte dei casi, hanno un impatto sulle infrastrutture necessarie per l'erogazione delle funzioni e dei servizi essenziali dello Stato. Tali incidenti hanno il potenziale di impedire l'esercizio delle attività economiche nel mercato interno, provocare perdite finanziarie, minare la fiducia dei cittadini e causare gravi danni all'economia e alla società dell'Unione[1]. Pertanto, l'efficacia delle misure di cybersicurezza sono oggi

[1] A tal proposito, si veda l'ENISA Threat Landscape 2022. Tale documento riporta indicazioni sullo stato delle minacce di *cybersecurity* a livello globale. In particolare, il *report* ha l'obiettivo di identificare le principali minacce, le tendenze osservate rispetto a queste ultime, l'evoluzione di *threat actors* e di tecniche di attacco, nonché l'analisi del loro impatto. Nel merito, da quanto osservato dall'Autorità, con oltre 10 *terabyte* di dati rubati mensilmente, il *ransomware* è ancora una delle principali minacce, mentre

più che mai essenziali per il corretto funzionamento del mercato interno, soprattutto considerato che esse sono un fattore abilitante fondamentale per molti settori critici. A tal riguardo, il legislatore europeo aveva emanato già nel 2016 la direttiva (UE) 2016/1148 (c.d. Direttiva NIS 1) con l'intento di innalzare i livelli di *cybersecurity* di un ristretto alveo di operatori ritenuti essenziali per la continuità operativa delle funzioni e dei servizi più importanti degli Stati membri. Tuttavia, tale obiettivo è stato solo parzialmente raggiunto, rendendosi così necessario un intervento in materia a distanza di pochissimi anni. Infatti, il 27 dicembre 2022 è stata emanata la direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, (cd. Direttiva NIS 2), con il preciso obiettivo di rendere il livello di *cybersecurity* di operatori considerati "essenziali" e "importanti" uniforme su tutto il territorio europeo. Come espressamente sancito nelle disposizioni finali, gli Stati membri dovranno emanare le normative di recepimento a livello nazionale entro e non oltre il 17 ottobre 2024 al fine di permettere agli operatori ricompresi di raggiungere i precisi obiettivi previsti dalla Direttiva NIS 2.

2. Ambito di applicazione della Direttiva NIS 2

Con riguardo all'ambito applicativo della direttiva, a differenza della precedente Direttiva NIS 1, il legislatore ha ampliato il novero di soggetti ivi compresi. A tal proposito, l'art. 2 della direttiva chiarisce innanzitutto che essa si applica a soggetti pubblici o privati che, congiuntamente:

- operino in settori strategici, quali quelli dell'energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari, dell'acqua potabile, della sanità e delle infrastrutture digitali, dell'*e-commerce*, dei motori di ricerca e del *cloud computing*;
- siano considerati medie imprese ai sensi all'art. 2, par. 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al par. 1 di tale articolo. A tal proposito, si precisa che la raccomandazione 2003/361 individua come soglie per la definizione di media impresa l'occupazione di più di 250 persone, un fatturato annuo superiore agli euro 50 milioni o un totale di bilancio annuo superiore agli euro 43 milioni; e
- prestino i loro servizi o svolgono le loro attività all'interno dell'Unione.

Inoltre, la Direttiva NIS 2 si applica, indipendentemente dalle dimensioni degli operatori, qualora:

il *phishing* è identificato come il vettore iniziale più comune per tali attacchi. In aggiunta, l'importanza del tema è ancor più chiara a seguito della situazione geopolitica e, in particolare, dell'invasione russa dell'Ucraina, che può essere considerata come punto di svolta per l'identificazione della rilevanza del dominio dello spazio cibernetico. A tal proposito, l'ENISA osserva un continuo aumento del numero di minacce, l'emergere di una gamma più ampia di vettori come *exploit zero-day*, disinformazione e *deepfake*. Tra l'altro, secondo quanto indicato nel rapporto, gli attacchi cibernetici sono aumenti nella seconda metà del 2021 e durante il 2022, non solo in termini di vettori e numeri, ma anche in termini di impatto. Tutti i settori sono coinvolti. Gli attacchi sono diretti sia verso i settori della pubblica amministrazione (24%), che nei confronti dei *digital service providers* (13%) e del pubblico in generale (12%), nonché, più diffusamente, verso i soggetti operanti in ogni settore dell'economia.

- i servizi siano forniti da:
  - fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;
  - prestatori di servizi di fiducia;
  - registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
- il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
- il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;
- il soggetto sia un ente della pubblica amministrazione;
- il soggetto sia identificato come critico ai sensi della direttiva (UE) 2022/2557.

3. Soggetti essenziali e importanti

Un'ulteriore novità della Direttiva NIS 2 è la distinzione dei soggetti ivi ricompresi tra "soggetti essenziali" e "soggetti importanti". Nella prima categoria vi rientrano, a differenza della precedente normativa, anche le pubbliche amministrazioni, che si affiancano ad operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali, delle acque. Tra i "soggetti importanti", invece, si annoverano, *inter alia*, operatori di servizi postali e di corriere, di gestione dei rifiuti, del settore chimico, del settore agroalimentare.

4. Gli adempimenti della Direttiva NIS 2

Nonostante le normative di recepimento nazionale dettaglieranno la portata di molti degli adempimenti previsti dalla Direttiva NIS 2, è possibile già in questa fase analizzarne alcuni e, in particolare:

a) l'adozione di misure in materia di gestione dei rischi di cybersicurezza (artt. 20 – 21 – 24);
b) l'adempimento di obblighi di segnalazione (art. 23);
c) l'adozione di canali per la condivisione delle informazioni sulla cybersicurezza (artt. 29 – 30);
d) la sottoposizione a misure di vigilanza e di esecuzione (artt. 32 – 33).

4.1. Misure in materia di gestione dei rischi di cybersicurezza

Tra gli obblighi previsti dalla normativa che avranno un impatto diretto sui soggetti "essenziali" e "importanti" rientrano (i) quelli relativi alle misure in materia di gestione dei rischi di cybersicurezza; (ii) l'individuazione del ruolo dei membri degli organi gestori; e (iii) gli obblighi di formazione.

4.1.1. Misure in materia di gestione dei rischi

In particolare, ai sensi dell'art. 21 della direttiva, al fine di assicurare un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti, «gli Stati membri provvedono affinché i soggetti essenziali e i soggetti importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.
Le [predette] misure […] sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
b) gestione degli incidenti;
c) continuità operativa, come la gestione del *backup* e il ripristino in caso di disastro, e gestione delle crisi;
d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;
g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso».

Pertanto, la lista ivi descritta risulta di particolare importanza in quanto permette di comprendere, almeno in linea generale, quali siano le misure di sicurezza che gli operatori soggetti alla Direttiva NIS 2 saranno tenuti ad implementare.
In aggiunta a quanto sopra e per mera completezza, si segnala che, ai sensi dell'art. 24 della direttiva, «al fine di dimostrare il rispetto di determinate prescrizioni di cui

all'art. 21, i soggetti essenziali potranno utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza adottati a norma dell'art. 49 del regolamento (UE) 2019/881». Dunque, nell'implementazione delle misure di sicurezza precedentemente illustrate, anche al fine di facilitarne l'attuazione, gli operatori potranno servirsi di prodotti sviluppati da soggetti che abbiamo acquisito la certificazione di cybersicurezza ai sensi del Regolamento sulla cybersicurezza.

4.1.2. Ruolo dei membri degli organi gestori

Inoltre, l'art. 20 prevede che i membri degli organi di gestione approvino le misure di gestione dei rischi di cybersicurezza, adottate ai sensi dell'art. 21. A tal proposito, si precisa che essi dovranno sovraintendere alla loro attuazione e potranno essere ritenuti responsabili di ogni violazione della Direttiva NIS 2. Dunque, la direttiva identifica il ruolo centrale degli organi di gestione degli operatori che, per legge, dovranno essere coinvolti nell'attuazione degli obblighi da questa derivanti. Ciò anche considerato che, come verrà meglio chiarito dalle legislazioni nazionali, essi potranno essere ritenuti responsabili della mancata adozione delle misure atte a rendere gli operatori conformi alle prescrizioni della normativa.

4.1.3. Obblighi di formazione

In ultimo, si segnala che ai sensi dell'art. 20, c. 3, della direttiva i membri dell'organo di gestione saranno tenuti a seguire una specifica formazione, al fine di acquisire conoscenze e competenze sufficienti per individuare i rischi e valutare le modalità di gestione dei rischi di cybersicurezza, nonché il loro impatto sui servizi offerti. Tra l'altro, il medesimo articolo consiglia di estendere la stessa iniziativa anche nei confronti dei dipendenti. Dunque, al fine di adempiere ai suddetti obblighi, gli operatoti dovranno tenere sessioni di formazione per i membri dell'organo di gestione volte all'acquisizione delle conoscenze e competenze in materia di cybersicurezza.

4.2 Obblighi di segnalazione

Secondo quanto stabilito dall'art. 23 della Direttiva NIS 2 «i soggetti essenziali e i soggetti importanti notificano senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al par. 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi quali indicati al par. 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi».

A tal proposito, l'art. 23, c. 3, della direttiva precisa che per incidenti significativi devono intendersi quegli eventi in grado di causare (i) una grave perturbazione dei servizi o perdite finanziarie o (ii) di avere ripercussioni su altre persone fisiche o giuridiche.
Inoltre, viene indicato che i soggetti importanti ed essenziali dovranno comunicare qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente.
Pertanto, qualora gli operatori subiscano un incidente qualificabile come "significativo" dovranno comunicarlo all'autorità competente e ai destinatari dei loro servizi, fornendo:

a) senza indebito ritardo, e comunque entro 24 ore da quando sarà venuta a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo sia sospettato di essere il risultato di atti illegittimi o malevoli o possa avere un impatto transfrontaliero;
b) senza indebito ritardo, e comunque entro 72 ore da quando sarà venuta a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera *a)* e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
c) su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione;
d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera *b)*, che comprenda:
    - una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;
    - il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;
    - le misure di attenuazione adottate e in corso;
    - se opportuno, l'impatto transfrontaliero dell'incidente;
e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera *d)*, una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

Dunque, alla luce dell'*iter* descritto, gli operatori dovranno adeguare i propri processi interni alle richieste del legislatore, nonché prevedere un'apposita procedura che individui gli obblighi da adempiere in caso di incidente.

4.3 Condivisione delle informazioni sulla cybersicurezza

4.3.1 Accordi di condivisione delle informazioni sulla cybersicurezza

Secondo quanto previsto dall'art. 29 della direttiva gli Stati membri dovranno prevedere dei canali che diano la possibilità ai soggetti essenziali e importanti di scambiare, su base volontaria, pertinenti informazioni sulla cybersicurezza, comprese informazioni

relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cybersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cybersicurezza per individuare le minacce informatiche. Inoltre, ai sensi del comma 2, tale scambio potrà avvenire anche nei confronti dei fornitori. Pertanto, al netto delle specifiche indicazioni che verranno fornite dagli Stati membri, è necessario segnalare che gli operatori, su base volontaria, potranno valutare se condividere le informazioni sopra indicate. Chiaramente, una simile scelta implica anche la valutazione di diversi aspetti legali – come quelli contrattuali nei confronti dei fornitori – a cui i soggetti "essenziali" e "importanti" dovranno necessariamente porre attenzione.

4.3.2. Notifica volontaria di informazioni pertinenti

In aggiunta a quanto sopra, ai sensi dell'art. 30 della direttiva, si precisa che, unitamente alle notifiche trasmesse in ossequio all'art. 23, potranno essere notificati al CSIRT su base volontaria:

- gli incidenti, ovvero un evento che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;
- le minacce informatiche, ovvero qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone;
- i quasi incidenti, ovvero qualsiasi evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.

Dunque, anche in questo caso, gli operatori dovranno valutare diversi aspetti legali al fine di decidere se procedere con la notifica di incidenti su base volontaria.

4.4. Misure di vigilanza e di esecuzione

In ultimo, si segnala che alla luce dell'art. 32 della Direttiva NIS 2, dedicato agli aspetti generali delle misure di vigilanza e di esecuzione, gli operatori potranno essere soggetti alle seguenti attività di vigilanza:

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
b) *audit* sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;
c) *audit ad hoc*, ivi incluso in casi giustificati da un incidente significativo o da una violazione della direttiva da parte del soggetto essenziale;
d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non di-

scriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cybersicurezza adottate dal soggetto interessato, comprese le politiche di cybersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti;
f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;
g) richieste di dati che dimostrino l'attuazione di politiche di cybersicurezza, quali i risultati di *audit* sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Qualora, nell'ambito dello svolgimento delle attività sopra descritte, le autorità competenti accertino delle violazioni, si precisa che esse avranno il potere di emanare avvertimenti, adottare istruzioni vincolanti o ingiunzioni che impongano agli operatori di adottare le misure necessarie per porre fine alle violazioni riscontrate e, più in generale, di irrogare sanzioni.

5. Misure sanzionatorie

In relazione al quadro sanzionatorio, l'art. 34 prevede che ove i soggetti importanti violino l'art. 21 (Misure in materia di gestione dei rischi di cybersicurezza) o l'art. 23 (obblighi di segnalazione), essi saranno soggetti a sanzioni pecuniarie amministrative pari a un massimo di almeno 10.000.000 EUR o a un massimo di almeno il 2% del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

Laddove, invece, sia un soggetto importate a violare le suddette disposizioni, esso potrà essere sottoposto a sanzioni pecuniarie amministrative pari a un massimo di euro 7.000.000 o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

In aggiunta a quanto sopra, ai sensi dell'art. 35 della direttiva, qualora le autorità competenti, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto che la violazione degli obblighi di cui agli artt. 21 e 23 può comportare una violazione dei dati personali, ne informano senza indebito ritardo l'Autorità garante per la protezione dei dati personali. Laddove tale autorità di controllo irroghi una sanzione amministrativa ai sensi del GDPR, le autorità competenti non imporranno una sanzione amministrativa pecuniaria a norma dell'art. 34 della direttiva per una violazione imputabile al medesimo comportamento, già punito con l'ammenda amministrativa pecuniaria.

6. Conclusione

In conclusione, dall'analisi della direttiva risulta chiaro come un *corpus* normativo dalla

portata applicativa tanto ampia abbia certamente l'intento di migliorare le capacità di resilienza e di risposta agli incidenti da parte dei soggetti pubblici e privati, cercando di risolvere le criticità di forte frammentazione che la Direttiva NIS 1 aveva creato. Tuttavia, è necessario notare come la Direttiva NIS 2 complichi notevolmente il quadro normativo sulla sicurezza delle infrastrutture critiche in termini di coordinamento, rendendo lo svolgimento dei suoi adempimenti molto gravoso per gli operatori. Infatti, è necessario ricordare come nell'attesa che il legislatore europeo definisse il nuovo testo normativo, diversi parlamenti nazionali – come quello italiano con il d.l. 105/2019 che istituisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) – hanno provveduto a colmare l'allora sussistente lacuna normativa in ambito di *cybersecurity*. Ciò, se da un lato alimenta un virtuoso meccanismo che innalza l'attenzione sui temi della cybersicurezza, dall'altro può sovraccaricare gli attori privati e pubblici di costosi adempimenti normativi. Infatti, laddove non sussista un chiaro allineamento tra le previsioni del PSNC e le disposizioni nazionali di attuazione della direttiva, moltissimi grandi *player* europei e nazionali dovranno affrontare ingenti costi di *compliance*, conseguendo, tuttavia, obiettivi nella pratica già raggiunti – nel caso italiano – grazie al PSNC.

Pertanto, il recepimento della Direttiva NIS 2 negli ordinamenti nazionali rappresenta un'opportunità per ricomporre in modo coerente il mosaico delle normative in materia di *cybersecurity*. In tale contesto, è, dunque, auspicabile che questa opera di sistematizzazione venga compiuta di concerto con gli Stati membri dell'Unione europea, al fine di evitare che i margini di discrezionalità lasciati a ciascuno rischino di creare differenze normative e tecniche tali da ridurre o addirittura vanificare gli obiettivi fissati dalla normativa europea.