

FEDERICA CASAROSA - GIOVANNI COMANDÉ

ASPETTANDO LA NIS2: OVVERO IL DIRITTO PRIVATO DELLA *CYBERSECURITY*

SOMMARIO: 1. Introduzione. — 2. La *cybersecurity* nel quadro giuridico italiano. — 3. La direttiva sulla sicurezza delle reti e dei sistemi informativi. — 3.1. La strategia nazionale sulla sicurezza dei sistemi di rete e informativi. — 3.2. Gli operatori essenziali. — 4. L'implementazione italiana. — 5. L'evoluzione del quadro normativo. — 6. Le questioni aperte e l'esigenza di approfondimento.

1. INTRODUZIONE.

Assai di rado la cyber sicurezza è messa in relazione con gli istituti privatistici. Eppure, l'evoluzione normativa, il crescente intrecciarsi delle dipendenze economiche ed organizzative tra enti, strutture, operatori economici, e pubbliche amministrazioni rendono sempre più evidenti i reciproci influssi tra la disciplina generale e speciale della sicurezza informatica e fisica con sempre più numerosi plessi normativi tipici del diritto privato e dei suoi istituti.

Lo scopo di questo contributo è innanzitutto di utilizzare la ricostruzione storica della normativa europea nel suo svolgimento nazionale fino alla prospettiva di attuazione della cosiddetta direttiva NIS2 per iniziare ad evidenziare queste interferenze critiche assieme alle prospettive di implementazione di quest'ultima normativa.

In questa direzione si evidenzieranno sia momenti di sovrapposizione e/o di tensione tra plessi normativi ed istituti, sia esigenze di collegamento e traduzione di quelli che sono i requisiti giuridici in esigenze tecniche per concludere con suggerimenti di politica normativa e di prassi interpretativa. Sullo sfondo il contributo evidenzia l'emergere di una relazione sempre più intricata tra

* La ricerca è stata svolta nell'ambito del progetto PNRR "SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics" (CUP B53C220017600

06) ed anche nell'ambito del Progetto PNRR "Partenariato Esteso" SERICS (PE00000014) - Eraclito, Spoke 7, finanziato dall'Unione europea - Next Generation EU.

esigenze di sicurezza fisica ed informatica delle catene del valore e i diversi livelli di normazione che ad esse devono cercare di dare attuazione.

2. LA CYBERSECURITY NEL QUADRO GIURIDICO ITALIANO.

La *cybersecurity*, o sicurezza informatica¹, comprende le strategie e le normative che operano a livello nazionale e sovranazionale volte a mitigare e reagire agli eventuali attacchi che possano mettere in crisi la stabilità e lo sviluppo sia delle imprese sia delle amministrazioni pubbliche². Se da un punto di vista pratico possiamo parlare di *cybersecurity* sin dal momento in cui i computer sono entrati in connessione attraverso la rete Internet, è solo dalla fine degli anni 2000 che si è assistito ad un incremento di attenzione sia del legislatore che del pubblico a questa tematica. Il punto di svolta può essere facilmente attribuito all'attacco subito dall'infrastruttura informatica dell'Estonia nel 2007, quando una serie di attacchi di tipo DDoS (*Distributed Denial of Service*) sono riusciti a paralizzare tale infrastruttura a livello nazionale³. Da questo momento in poi, numerosi stati hanno iniziato a considerare l'opportunità, anzi la necessità, di adottare documenti strategici sulla *cybersecurity*⁴.

Se da un lato la sensibilità verso i rischi sulla sicurezza è aumentata, anche gli attacchi informatici si sono moltiplicati,

¹ Per un'analisi della definizione di *cybersecurity* si veda European Union Agency for Cybersecurity, Definition of Cybersecurity - Gaps and overlaps in standardization, 2015; Vagelis PAPA-KONSTANTINOU, *Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?* (2022) 44 *Computer Law & Security Review* 105653.

² Per quanto riguarda l'Italia, il riferimento fondamentale è costituito dal Programma Nazionale per la Ricerca PNR (<https://www.mur.gov.it/sites/default/files/2021-01/Pnr2021-27.pdf>) del MUR, in particolare l'allegato esteso sulla sicurezza dei sistemi sociali (https://www.mur.gov.it/sites/default/files/2021-08/3.AllegatoEsteso_Sicurezza.pdf). Le priorità ivi definite hanno indirizzato le scelte relative alla Legge di Bilancio 2023 che prevede due fondi legati ai temi della *cybersecurity*: il Fondo per l'attuazione della Strategia Nazionale di Cybersecurity, che finanzia gli investimenti volti al conseguimento dell'autonomia tecnologica in ambito digitale; e il Fondo dedicato ai progetti PNRR sulla *cybersecurity*, con risorse pari a 10 milioni di euro per il 2023, 50 per il 2024 e 70 milioni di euro annui a decorrere dall'anno 2025.

³ M. LESK, *The New Front Line: Estonia under Cyberassault*, in *IEEE Security & Privacy*, vol. 5, no. 4, pp. 76-79, July-Aug. 2007; SCOTT J. SHACKELFORD, *Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks*, *Journal of Internet Law*, 2010, disponibile all'indirizzo: <https://ssrn.com/abstract=1499849>.

⁴ Si vedano gli interventi adottati nel Regno Unito, *The UK Cyber security Strategy: Protecting and Promoting the UK in a Digitalised World* (2011), in Austria il *National ICT Security Strategy* (2012); in Estonia la *Cybersecurity strategy* (2008), in Francia, il *Défense et sécurité des systèmes d'information: Stratégie de la France* (2011), nel Paesi bassi la *Defence Cyber Strategy* (2012). Per una comparazione dei temi nelle rispettive legislazioni e politiche nazionali si veda Stefano MELE, *I principi strategici delle politiche di cybersecurity*, 5 Dicembre 2013, disponibile all'indirizzo: <https://www.sicurezza nazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html>. Per l'Italia si veda R. BALDONI e L. MONTANARI (a cura di), *Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security*, Research

inclusi gli attacchi alla *supply chain* che mirano al cyberspionaggio, al *ransomware* o all'interruzione completa dei servizi⁵. L'esposizione ad incidenti di sicurezza informatica e al loro potenziale impatto è legata ovviamente alla pervasività dell'uso delle tecnologie dell'informazione e della comunicazione rispetto a tutti i settori dell'attività economica, dal momento che le amministrazioni pubbliche, le aziende e i cittadini sono più interconnessi e interdipendenti. Peraltro, la recente aggressione militare della Russia contro l'Ucraina ha mostrato come le operazioni informatiche siano sempre più integrate nelle strategie ibride e di guerra⁶, con effetti significativi sull'obiettivo. La minaccia di un possibile incidente su larga scala che provochi interruzioni e danni significativi alle infrastrutture critiche richiede dunque una maggiore preparazione a tutti i livelli dell'ecosistema della sicurezza informatica.

L'Italia ha riconosciuto i rischi per la sicurezza informatica già da metà degli anni 2000 e si sono succeduti numerosi interventi legislativi che hanno introdotto norme che ambivano a prevenire e mitigare tali rischi. È interessante osservare l'evoluzione che ha caratterizzato gli interventi legislativi nel corso degli ultimi vent'anni.

Il decreto legislativo n. 82 del 2005⁷, il codice dell'amministrazione digitale, segna il momento in cui il processo di informatizzazione delle Pubbliche Amministrazioni ha subito una accelerazione. In particolare, il testo include all'art. 51 un primo intervento sulla sicurezza dei dati, affermando che "Le norme di sicurezza definite nelle regole tecniche ... garantiscono l'esattezza, l'accessibilità, l'integrità e la riservatezza dei dati" e che "I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità di raccolta". Dello stesso anno è poi la legge n. 155/2005⁸ recante misure urgenti per il contrasto del terrorismo internazionale, in cui viene incluso l'articolo 7-bis relativo alla sicurezza telematica. Tale norma prevede che "*l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche*

center of cyber intelligence and information security - Università di Roma Sapienza, 2015, disponibile all'indirizzo <http://www.cybersecurityframework.it>.

⁵ CLUSIT, Rapporto 2023 sulla sicurezza ICT in Italia, disponibile all'indirizzo <https://clusit.it/rapporto-clusit/>.

⁶ Luca ZORLONI, *L'invisibile Cyber guerra della Russia per piegare l'Ucraina*,

21 febbraio 2023, disponibile all'indirizzo: <https://www.wired.it/article/ucraina-russia-guerra-attacchi-informatici-malware-ddos-energi/>.

⁷ Decreto legislativo 7 marzo 2005, n. 82. Codice dell'amministrazione digitale.

⁸ Legge 31 luglio 2005, n. 155 recante misure urgenti per il contrasto del terrorismo internazionale.

informatizzate di interesse nazionale individuate con decreto del ministero dell'Interno". La responsabilità della protezione delle infrastrutture critiche è quindi in capo al Ministero dell'Interno, con il ruolo di *enforcement* allocato alla Polizia postale in caso di attacco cibernetico. Le infrastrutture critiche informatiche di interesse nazionale sono peraltro definite grazie ai criteri e alle procedure individuate nel decreto 9 gennaio 2008⁹, che include fra le infrastrutture critiche tutti i sistemi e servizi informatici di supporto ai ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute¹⁰. Ad esse si aggiungono la banca d'Italia e le autorità indipendenti, così come le società partecipate dallo stato, dalle regioni e dai comuni nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque.

Dagli anni 2010 gli interventi relativi alla *cybersecurity* si sono intensificati, ponendo una maggiore attenzione alle specificità che possono emergere sia sotto il profilo della tutela delle pubbliche amministrazioni sia sotto il profilo della difesa nazionale. Nel 2012 viene definita l'Agenda digitale italiana. Stabilita con il decreto del Ministero dello sviluppo economico, essa prevede la creazione di una agenzia per l'Italia Digitale (AgID). L'agenzia, istituita con decreto-legge 83/2012 (convertito in Legge n. 134/2012)¹¹, ha il compito di coordinare *“le azioni in materia di innovazione per promuovere le tecnologie ICT a supporto delle pubbliche amministrazioni, garantendo la realizzazione degli obiettivi dell'Agenda digitale italiana, in coerenza con l'Agenda digitale europea”*. L'importanza dei temi della sicurezza informatica si posiziona fra le prime azioni strategiche dell'AgID, con la strategia per la realizzazione dell'agenda digitale del 2013¹².

Il decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013, recante *“indirizzi per la protezione cibernetica e la sicurezza informatica nazionale”*¹³ è quindi il primo atto legislativo che mira a coordinare le attività legate alla *cybersecurity*, coinvolgendo sia le pubbliche amministrazioni che le comunità di

⁹ Decreto 9 gennaio 2008, Individuazione delle infrastrutture critiche informatiche di interesse nazionale.

¹⁰ È importante notare che tale decreto anticipa di quasi un anno la direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione. I settori coperti da tale direttiva sono soltanto energia e trasporti in assenza di un accordo a livello europeo.

¹¹ Decreto-legge del 22 giugno 2012 n. 83, recante misure urgenti per la crescita del Paese.

¹² Per un'analisi delle attività svolte dall'AgID, si veda Marta ZILIANI, *Verso un'architettura digitale unica e sicura per la P.A.: il ruolo di AgID e Consip*, in *LLR*, n. 2, 2017, 81.

¹³ D.P.C.M., 24 gennaio 2013 n. 67251, *“Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale”*.

intelligence¹⁴. I successivi documenti strategici nazionali, il “Quadro strategico nazionale per la sicurezza dello spazio cibernetico”¹⁵ e il “Piano nazionale per la protezione cibernetica e la sicurezza informatica”¹⁶, definiscono l’organizzazione interna che permetta di rispondere tempestivamente e in maniera coordinata alle minacce cibernetiche laddove queste ultime abbiano come obiettivi gli *asset* nazionali. Ciò che emerge è la necessità di mantenere continuo l’aggiornamento delle strategie di difesa a fronte di tecnologie in costante evoluzione, e dall’altro lato la necessità di un coinvolgimento ad ampio raggio degli attori coinvolti in questo processo, non soltanto soggetti pubblici e privati, ma anche i cittadini che facendo uso delle tecnologie informatiche possono cogliere le future minacce cibernetiche¹⁷.

Il 2016 segna il momento di cambiamento derivante dalla necessità di ridefinire il quadro organizzativo e di controllo alla luce delle indicazioni provenienti dall’Unione Europea con la Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (Direttiva NIS)¹⁸, che rappresenta il primo intervento legislativo orizzontale intrapreso a livello europeo per la protezione delle reti e dei sistemi informativi in tutta l’Unione.

Come evidente dalla precedente analisi il legislatore è dovuto intervenire per adattare il sistema preesistente alle norme europee. Tuttavia, a differenza di altri paesi europei, l’incidenza delle modifiche è stata limitata giacché sia le competenze sia le strutture organizzative erano già state individuate nel corso del decennio precedente. Un importante stimolo al miglioramento del quadro normativo esistente è stata la necessità di definire in modo dettagliato i requisiti previsti per la prevenzione e resilienza dei c.d. operatori dei servizi essenziali. Per comprendere tale quadro è necessario analizzare la direttiva NIS e comprendere come il legislatore italiano ha implementato la strategia nazionale per la sicurezza informatica.

¹⁴ La nuova organizzazione prevede un ruolo apicale al Presidente del Consiglio dei ministri e i Ministri che compongono il Comitato per la sicurezza della Repubblica (CISR) con compiti di tipo politico-strategico. Il supporto operativo è poi offerto dal Comitato interministeriale, presieduto dal Direttore generale del Dipartimento delle Informazioni per la Sicurezza (DIS), che svolge sia l’attività istruttoria dei lavori del Comitato interministeriale, sia il coordinamento tra amministrazioni e uffici competenti, nonché tra questi e i soggetti pubblici e privati chiamati ad attuarlo.

¹⁵ Disponibile all’indirizzo: <https://www.agid.gov.it/sites/default/files/repository>

[_files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf](https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf).

¹⁶ Disponibile all’indirizzo: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf>.

¹⁷ Per un’analisi più dettagliata si veda, C. CENCETTI, *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Roma, 2014.

¹⁸ 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, GU L 194, 19.7.2016, p. 1.

3. LA DIRETTIVA SULLA SICUREZZA DELLE RETI E DEI SISTEMI INFORMATIVI.

La Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (Direttiva NIS) è la prima normativa orizzontale intrapresa a livello UE per la protezione delle reti e dei sistemi informativi in tutta l'Unione. La base giuridica di questo intervento è da ricondursi all'art. 114 TFUE a tutela del mercato interno: l'approccio adottato dal legislatore è quello di valutare l'eventuale interruzione o incidente che colpisca i servizi e i prodotti basati sulle tecnologie dell'informazione e della comunicazione come una minaccia per il funzionamento del mercato interno. L'obiettivo previsto è dunque quello di raggiungere un *“elevato livello comune di sicurezza dei sistemi di rete e di informazione all'interno dell'Unione, al fine di migliorare il funzionamento del mercato interno”* (Art. 1 NIS).

La direttiva NIS ha tre pilastri principali:

1. rafforzare la cooperazione strategica e lo scambio di informazioni a livello europeo, attraverso la creazione di un gruppo di cooperazione e di una rete di squadre di risposta agli incidenti di sicurezza informatica (rete *Computer Incident Response Team* - CSIRT);

2. richiedere l'adozione di piani strategici nazionali di *cyber-security* a livello nazionale, compresa la creazione di autorità nazionali competenti e di CSIRT per i servizi essenziali; e

3. identificare i meccanismi di prevenzione e resilienza per i c.d. operatori dei servizi essenziali (OSE) e per i c.d. fornitori di servizi digitali.

I pilastri (2) e (3) sono i più interessanti e innovativi e saranno analizzati in dettaglio.

3.1. *La strategia nazionale sulla sicurezza dei sistemi di rete e informativi.*

Secondo l'art. 7 NIS, ogni Stato membro deve adottare un quadro nazionale che includa la strategia nazionale sulla sicurezza dei sistemi di rete e informativi e la designazione delle autorità responsabili del monitoraggio dell'attuazione della direttiva NIS. La strategia deve prevedere una serie di aspetti predefiniti:

- a) gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi;

- b) un quadro di governance per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti;

- c) l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;

d) un'indicazione di programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

e) un'indicazione di piani di ricerca e sviluppo relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

f) un piano di valutazione dei rischi per individuare i rischi;

g) un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi.

A parte gli aspetti sopra elencati, tuttavia, la direttiva lascia agli Stati membri la libertà di progettare la propria strategia nazionale.

Questo approccio può essere in contrasto con l'obiettivo di armonizzazione fissato dalla direttiva, ma si è dimostrato inizialmente efficace, in quanto gli Stati membri sono stati in grado di adattare le disposizioni della direttiva alle esigenze e alle caratteristiche specifiche delle imprese che operano sul loro territorio. Inoltre, la direttiva definisce una serie di salvaguardie per promuovere la convergenza fra le strategie nazionali: da un lato, la possibilità di richiedere l'assistenza e il supporto da parte dell'Agenzia ENISA (art. 7(2) NIS)¹⁹; dall'altro, la possibilità di utilizzare standard definiti a livello europeo o internazionale (art. 19 NIS).

Gli articoli 8, 9, 11 e 12 della direttiva NIS individuano poi le autorità e gli altri organismi incaricati di monitorarne l'applicazione a livello nazionale e dell'UE²⁰. Ogni Stato membro deve designare un punto di contatto unico nazionale per mantenere i contatti e garantire la cooperazione transfrontaliera con gli altri Stati membri. Sebbene la direttiva non richieda una struttura o una gerarchia specifica per l'autorità nazionale, quest'ultima dovrebbe ricevere adeguate risorse tecniche, finanziarie e umane per svolgere, in modo efficace ed efficiente, i compiti ad essa assegnati.

Un'innovazione rilevante è la creazione di squadre di risposta

¹⁹ Si vedano gli strumenti resi disponibili dall'ENISA per poter offrire supporto agli Stati membri nella definizione delle rispettive strategie di cybersecurity nazionali. ENISA, *National Cyber Security Strategies: An Implementation Guide*, 2012, disponibile all'indirizzo: <https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide>; ID, NCSS Good Practice Guide, 2016, disponibile all'indirizzo: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>; *Ib.*, *Building Effective Governance Fra-*

meworks for the Implementation of National Cybersecurity Strategies, 2023, disponibile all'indirizzo: <https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies>.

²⁰ Per una comparazione delle scelte operate nei diversi Stati Membri si veda Alessandro LAURO, *Sicurezza Cibernetica e Organizzazione Dei Poteri: Spunti Di Comparazione* [2021] *Rivista Gruppo di Pisa*, 529.

agli incidenti di sicurezza informatica (CSIRT) a livello nazionale che ha il compito di monitorare gli incidenti a livello nazionale, fornire un allarme tempestivo, avvisi e informazioni alle parti interessate sui rischi e sugli incidenti, rispondere agli incidenti, fornire un'analisi dinamica dei rischi e degli incidenti e aumentare la consapevolezza della situazione, nonché partecipare a una rete di CSIRT in tutta Europa ²¹.

3.2. *Gli operatori essenziali.*

La direttiva NIS interessa due categorie di imprese, con un approccio certamente differenziato in termini di obblighi imposti a ciascuna di esse: gli operatori di servizi essenziali e i fornitori di servizi digitali.

Gli operatori di servizi essenziali (OSE) sono definiti come soggetti pubblici o privati che operano in settori rilevanti per il sistema economico nazionale (art. 4 NIS). All'interno dell'allegato II della Direttiva NIS sono elencati in dettaglio i settori individuati come essenziali: energia, trasporti, banche, infrastrutture del mercato finanziario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali. L'articolo 5 NIS specifica, inoltre, altri criteri per determinare gli operatori essenziali, in particolare:

(a) un'entità fornisce un servizio essenziale per il mantenimento di attività sociali e/o economiche critiche;

(b) la fornitura di tale servizio dipende da sistemi di rete e di informazione; e

(c) un incidente avrebbe effetti dirompenti significativi sulla fornitura di tale servizio (per la definizione di effetto dirompente significativo, l'art. 6 NIS prevede criteri specifici).

Di conseguenza, non tutti gli operatori di servizi essenziali che operano nei settori individuati dalla direttiva rientrano nell'ambito di applicazione della stessa. Spetta agli Stati membri verificare i criteri previsti all'art. 5 e individuare l'elenco degli OSE a livello nazionale. Tale determinazione non viene resa pubblica e rimane segreto di stato, per proteggere gli stessi operatori da eventuali attacchi informatici. Ciascuno degli stati membri è tenuto ad informare la Commissione della selezione, tenendo aggiornato l'elenco almeno ogni due anni per tenere conto dei potenziali cambiamenti nel mercato.

L'applicazione di criteri uniformi nel processo di identificazione degli OSE è fondamentale al fine di tener conto non soltanto dell'eventuale presenza di dipendenze transfrontaliere, ma anche per garantire condizioni di parità per gli operatori che operano

²¹ Articolo 12 NIS.

all'interno del mercato interno e ridurre il rischio di interpretazioni divergenti²². Tuttavia, è necessario notare che eventuali divergenze fra le legislazioni di implementazione nazionali non sono escluse, poiché la direttiva si basa su un'armonizzazione minima, pertanto gli Stati membri possono adottare una legislazione che garantisca un livello di sicurezza più elevato oppure estendendo gli obblighi di sicurezza e di notifica anche agli operatori di settori economici che al momento non sono inclusi nello raggio di applicazione²³.

A fronte della qualificazione come OSE, la direttiva NIS prevede una serie di obblighi di comunicazione e requisiti di sicurezza previsti ai sensi dell'art. 14 NIS. Gli OSE devono adottare misure tecniche e organizzative adeguate e proporzionate per gestire i rischi e prevenire e ridurre al minimo l'impatto degli incidenti alla sicurezza delle reti e dei sistemi informativi, al fine di garantire la continuità del servizio.

I requisiti di sicurezza sono definiti dagli Stati membri, e basati su di un approccio *risk based*: i controlli tecnici e organizzativi devono essere adeguati e proporzionati sulla base dei rischi legati alla tipologia di servizio svolto. Tuttavia, la Direttiva non indica il tipo di metodologia per effettuare le pertinenti valutazioni di rischio né la forma di tecnologia da utilizzare. Ciò è giustificabile non soltanto per il fatto che l'identificazione di un approccio specifico rischierebbe di essere rapidamente obsoleto, visti i rapidi sviluppi del settore, ma anche perché la valutazione del rischio dovrebbe essere adattata ai diversi settori.

Tuttavia, dato l'intreccio tra i requisiti di sicurezza e la notifica degli incidenti, la direttiva sembra implicare che l'approccio alla gestione del rischio debba includere una duplice fase²⁴.

Dato l'ampio margine di manovra concesso agli Stati membri e, di conseguenza, all'OSE per quanto riguarda i requisiti di sicurezza, si è reso necessario un intervento da parte degli organi di coordinamento istituiti dalla direttiva stessa al fine di evitare la frammentazione e i rischi di incoerenze. In questo senso, l'intervento del gruppo di cooperazione NIS²⁵ è stato fondamentale, in quanto ha fornito diversi documenti di orientamento. Ad esempio,

²² Si vedano i risultati della Relazione della Commissione al Parlamento Europeo e al Consiglio, di valutazione della coerenza degli approcci adottati dagli Stati membri per l'identificazione degli operatori di servizi essenziali conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi, Bruxelles, 28.10.2019, COM(2019) 546 final.

²³ Per esempio, le amministrazioni pubbliche, il settore postale, il settore ali-

mentare, l'industria chimica e nucleare, il settore ambientale e la protezione civile.

²⁴ L'approccio alla gestione del rischio dovrebbe includere un "processo di monitoraggio" in due fasi: una finalizzata alla selezione di specifici meccanismi di controllo valutati come appropriati per la gestione del rischio, e una finalizzata all'attuazione dei meccanismi di controllo selezionati in caso di incidenti.

²⁵ Si veda in particolare, Reference document on security measures for Opera-

il documento di riferimento sulle misure di sicurezza per gli operatori dei servizi essenziali stabilisce alcuni principi generali che dovrebbero essere presi in considerazione da tutti gli Stati membri nell'adozione di misure di sicurezza ²⁶. Tali misure devono essere efficaci, personalizzate, compatibili, proporzionate, concrete, verificabili e inclusive.

In caso di incidenti significativi, l'OSE è obbligato a notificare tali incidenti: l'art. 14 stabilisce che gli OSE sono tenuti a notificare, senza indebito ritardo, gli incidenti che hanno un impatto significativo, rispettivamente sulla continuità del servizio e sulla fornitura del servizio, allo CSIRT nazionale. Gli OSE sono tenuti a segnalare gli incidenti significativi, ovvero gli incidenti che hanno un grave impatto sul servizio fornito. Per identificare gli incidenti significativi, la direttiva prevede una serie di criteri:

- il numero di utenti interessati dall'interruzione di un servizio essenziale;
- l'intervallo di tempo durante il quale il servizio essenziale non è stato operativo;
- l'estensione geografica dell'area interessata dall'incidente.

Va notato che la disposizione, per quanto riguarda i tempi di notifica, fa riferimento alla terminologia indefinita, poiché richiede la notifica “senza indebito ritardo”. Questa ambiguità è risolta solo a livello nazionale, tuttavia esistono differenze tra gli Stati membri ²⁷. Queste discrepanze possono diventare un problema in quanto gli OSE che offrono i propri servizi in più Stati membri possono essere soggetti a requisiti e tempi di notifica diversi ²⁸.

Una volta effettuata la notifica dell'incidente significativo, l'autorità nazionale competente o il CSIRT supporteranno l'ente notificante nella gestione dell'incidente. A volte è necessario notificare l'incidente al pubblico; in questo caso l'autorità nazionale competente o il CSIRT, dopo aver consultato l'operatore dei servizi essenziali che ha effettuato la notifica, può comunicare il singolo incidente al pubblico per sensibilizzarlo alla prevenzione o alla gestione di un incidente in corso ²⁹.

Va sottolineato che gli incidenti non qualificati come significativi non sono soggetti all'obbligo di notifica. Lo stesso vale per le persone giuridiche non identificate come OSE. Tuttavia, in en-

tors of Essential Services, CG Publication 01/2018, disponibile all'indirizzo https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643.

²⁶ <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>.

²⁷ Per esempio, in Gran Bretagna la tempistica per la notifica degli incidenti è di 72 ore, mentre per l'Estonia non deve superare le 24 ore. In altri casi, tale quantifi-

cazione non è neppure individuata in modo preciso, come nel caso della Germania.

²⁸ Si veda Sandra SCHMITZ-BERNDT and Stefan SCHIFFNER, *Don't Tell Them Now (or at All) - Responsible Disclosure of Security Incidents under NIS Directive and GDPR* (2021) 35 *International Review of Law, Computers & Technology* 101.

²⁹ Articolo 14 (4) NIS.

trambi i casi, le aziende possono presentare notifiche volontarie al CSIRT di incidenti che hanno un impatto materiale sulla continuità dei servizi che forniscono³⁰. L'intento della Direttiva NIS è infatti quello di favorire la più ampia diffusione di una cultura consapevole in materia di *cybersecurity* e un conseguente aumento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni.

Va notato anche che tali obblighi di notifica hanno portata più limitata rispetto a quelli relativi a violazioni dei dati personali che vanno sempre notificati a mente dell'art. 33 GDPR "a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche". Il differente regime e la differenza di criteri di valutazione nel caso, per esempio, di un *data breach* rilevante anche come incidente ai sensi NIS che coinvolga dati personali comportano complessità organizzative e di compliance non solo non indifferenti ma pure contraddittori in termini di esigenze di tutela e loro rilevanza anche economica.

Ciò pone in evidenza il problema del coordinamento fra l'obbligo di notifica per gli incidenti legati alla sicurezza informatica e l'obbligo di notifica previsto dal Regolamento generale per la protezione dei dati personali in caso *data breach*. Considerando che in molti casi un *data breach* può essere allo stesso tempo un incidente di sicurezza, lo stesso operatore essenziale che opera come titolare del trattamento dei dati, è tenuto ad inviare due diverse notifiche, l'uno allo CSIRT nazionale in merito all'incidente di sicurezza e l'altro all'Autorità garante per la protezione dei dati per il *data breach*. Se nel primo caso l'obbligo deve avvenire "senza indebito ritardo", nel secondo caso il GDPR impone un vincolo temporale specifico di 72 ore dall'avvenuta conoscenza dell'evento con conseguenti regole di aggiornamento delle informazioni e necessità di giustificazioni dell'eventuale ritardo.

4. L'IMPLEMENTAZIONE ITALIANA.

La Direttiva NIS è stata recepita nell'ordinamento italiano con il Decreto Legislativo n. 65 del 18 maggio 2018, che definisce il quadro normativo per le misure di sicurezza della sicurezza delle reti e dell'informazione da adottare e individua i soggetti competenti per l'attuazione degli obblighi previsti dal quadro giuridico europeo³¹. Tuttavia, lo stato italiano ha deciso di rafforzare le

³⁰ Articolo 20 NIS.

³¹ Decreto legislativo 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consi-

glio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

norme e le procedure al fine di garantire un più elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle pubbliche amministrazioni, nonché degli enti e degli operatori pubblici e privati nazionali, attraverso l'istituzione del cosiddetto "Perimetro di Sicurezza Nazionale Cibernetica" con il Decreto-Legge del 21 settembre 2019 (decreto Perimetro)³². La motivazione alla base dell'adozione del Decreto Perimetro è l'istituzione di un quadro giuridico coerente e completo che rafforzi la portata della direttiva NIS per sostenere la sicurezza nazionale. Infatti, l'ambito di applicazione della direttiva non copre pienamente la totalità degli operatori pubblici e privati da cui dipende un funzionamento dello Stato o la fornitura di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali nell'interesse dello Stato; il malfunzionamento, l'interruzione o l'uso improprio di questi servizi possono tuttavia essere dannosi per la sicurezza nazionale.

In questo contesto, l'articolo 1 (8) Decreto Perimetro prevede che gli OSE e i fornitori di servizi digitali osservino i requisiti di *cybersecurity* delineati nel decr. leg. n. 65/2018, se sono almeno equivalenti a quelli stabiliti dal decreto di attuazione del Perimetro. Lo stesso articolo conferisce all'Agenzia nazionale per la sicurezza informatica il potere di definire misure aggiuntive per soddisfare gli standard di sicurezza stabiliti dal Perimetro. Il Decreto prevede inoltre che le norme attuative per specificare ulteriormente gli obblighi dei soggetti coinvolti siano definite attraverso successivi interventi legislativi che si sono concretizzati in quattro Decreti del Presidente del Consiglio dei ministri, un Decreto del Presidente della Repubblica, nonché una serie di atti e comunicazioni di vari comitati.

Il Governo italiano ha adottato il primo D.P.C.M. n. 131 del 30 luglio 2020, in cui si individuano i soggetti pubblici e privati che rientrano nel Perimetro, nonché i criteri per la creazione di elenchi di reti, sistemi informativi e servizi informatici rilevanti dei soggetti stessi. Il secondo D.P.C.M., n. 81 del 14 aprile 2021, definisce la procedura per la segnalazione degli incidenti, nonché le misure tecniche di sicurezza obbligatorie. Il terzo intervento, il D.P.R. 5 febbraio 2021, n. 54, stabilisce un quadro procedurale per l'approvvigionamento di beni ICT da utilizzare su reti, sistemi informativi e servizi IT da parte degli enti ricadenti nel Perimetro; le categorie di tali beni sono ulteriormente individuate dal D.P.C.M. 15 giugno 2021.

Ebbene proprio questa disciplina di controllo pubblico su procedure di acquisto pubbliche e private rappresenta un altro nodo

³² Decreto-legge 21 settembre 2019, n. 105. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

di interferenza/interazione tra disciplina pubblicistica della cybersicurezza e disciplina dei rapporti tra privati. Infatti, “prima dell’avvio delle procedure di affidamento ovvero, ove non siano previste, prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT di cui all’articolo 1, comma 6, lettera a)” del D.P.C.M. 54/2021 deve essere fatta notifica al CVCN o ai CV chiamati a eseguire i *test*, di cui all’articolo 6 e all’articolo 7 ma, soprattutto, a dettare “eventuali condizioni e test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, di cui all’articolo 5, nonché eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro,” (Art. 4 comma 3). Emergono, infatti, alcuni profili interessanti. Innanzitutto, si demanda ad una autorità amministrativa (tecnicamente la CVCN è una articolazione interna di una Agenzia e non di una Autorità indipendente) la possibilità di dettare limiti, tanto stringenti quanto non definiti a livello generale ed astratto, alla autonomia negoziale di soggetti privati, peraltro esposti come si vedrà a sanzioni non indifferenti ove non seguano le indicazioni o non segnalino le procedure o i contratti. Infatti, l’operazione commerciale, anche eventualmente interamente privata, può essere del tutto vietata se la procedura dà esito negativo, o sottoposta a condizioni più o meno invasive dell’autonomia contrattuale ed imprenditoriale (es. limitazioni di uso, di durata, inserimento di clausole contrattuali).

Orbene, considerato che la appartenenza al Perimetro di sicurezza cibernetica nazionale dovrebbe essere un segreto, ove l’interlocuzione con un particolare interlocutore economico/industriale abbia condotto ad una valutazione negativa o condizionante l’operazione contrattuale da parte del CVCN, è di immediato rilievo che l’operatore economico coinvolto si trova a dovere negoziare (ed a farsi carico dei relativi costi) del contenuto delle clausole fino al punto di dovere rompere le trattative — con le conseguenti responsabilità giuridiche ed economiche — o meglio o, peggio, non concludere un contratto già in fase conclusiva senza potere neppure spiegarne le ragioni. Del resto, ove le proposte clausole contrattuali da parte del CVCN fossero strutturate in modo tale da non dissimulare adeguatamente le loro ragioni fondanti si esporrebbero a “rivelare” direttamente o indirettamente il collocamento all’interno de Perimetro dell’entità coinvolta con ancor più grave danno sia alla sicurezza generale che allo stesso soggetto coinvolto. È quindi di tutta evidenza che sia le procedure che le soluzioni adottate richiedono per il loro esercizio lo sviluppo di competenze e pratiche ad oggi non rilevate e che portano, per un verso, ad un coinvolgimento dei soggetti privati nella creazione del quadro generale della sicurezza cyberfisica nazionale e, per altro vero, a rendere necessario un aggiornamento (forse non solo) interpretativo di numerose discipline di diritto privato. Come vedremo più avanti il riferimento alla

sicurezza cyber-fisica non è casuale stante la interrelazione dei due tipi di sicurezza così come non lo sono le ripercussioni di quanto appena sottolineato nelle dinamiche contrattuali.

Sebbene non previsto originariamente dalla legge sul Perimetro, la Legge 4 agosto 2029, n. 102, (che converte il precedente Decreto-Legge 14 giugno 2021 n. 82) ridisegna significativamente l'architettura normativa del Perimetro in quanto istituisce l'Agenzia Nazionale per la *Cybersecurity*, che ospita anche il CSIRT nazionale e il Centro Nazionale di Certificazione e Valutazione (CVCN), che agisce come autorità nazionale di certificazione della *cybersecurity* ai fini dell'applicazione delle norme previste dal *Cybersecurity Act* (CSA)³³. Per completare il quadro normativo previsto dal Perimetro, il quarto D.P.C.M. 18 maggio 2022, n. 92, istituisce una rete di laboratori pubblico-privati a supporto del CVCN per la valutazione tecnologica.

Il D.P.C.M. n. 131/2020, come detto, stabilisce i criteri procedurali in base ai quali la pubblica amministrazione competente dovrà identificare i soggetti compresi nel Perimetro. L'identificazione delle entità incluse nel Perimetro, effettuata dalle pubbliche amministrazioni per ogni settore di competenza, segue un approccio risk based. Sulla base di un "meccanismo graduale" e di una valutazione del rischio, è stata data priorità all'identificazione dei soggetti che operano nel settore governativo, con l'autorità competente che è il "Comitato interministeriale per la *cybersecurity*" istituito presso la Presidenza del Consiglio dei ministri. Altri settori includono: interni; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche; enti di previdenza sociale e lavoro.

È interessante notare che l'elenco delle entità del Perimetro sarà inserito in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, non soggetto a pubblicazione. La *ratio* della non divulgazione risiede nella finalità sottesa alla tutela della sicurezza nazionale; tuttavia, la segretezza è più formale che reale, in quanto la maggior parte delle entità che rientrano nell'ambito del Perimetro è facilmente individuabile, poiché tali entità rappresentano gli attori più importanti nei settori individuati dalla normativa. È interessante notare che l'art. 1(5) Legge sul Perimetro e l'art. 3(1) D.P.C.M. n. 131/2020 prevedono un elemento di "flessibilità" in termini di adeguamenti del quadro giuridico nazionale in materia di sicurezza informatica: il primo stabilisce una base giuridica per l'aggiornamento dei decreti

³³ Regolamento (UE) 2019/831 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per

le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (« regolamento sulla cibersicurezza »), GU L 151, 7.6.2019, p. 15.

attuativi, mentre il secondo prevede esplicitamente la possibilità di estendere il campo di applicazione ad altri settori al momento dell'aggiornamento del decreto.

Gli enti che rientrano nel Perimetro sono obbligati a predisporre un elenco, aggiornato annualmente, delle reti, dei sistemi informativi e dei servizi IT che costituiscono gli *asset* ICT sotto il loro controllo. L'elenco deve essere redatto secondo un approccio scalabile e basato sul rischio, in modo tale da rendere evidente gli *asset* ICT che, in caso di incidente, causerebbero la completa interruzione della funzione o del servizio essenziale³⁴. Gli operatori inclusi nel perimetro sono poi tenuti a descrivere l'architettura e le parti componenti degli *asset* ICT precedentemente identificati, sulla base di un modello fornito dall'Agenzia nazionale per la sicurezza informatica³⁵. Questo obbligo potrebbe rivelarsi particolarmente impegnativo, soprattutto se si considera l'elevato tasso di digitalizzazione di molti operatori. Questi elenchi devono essere trasmessi all'Agenzia entro sei mesi dal ricevimento della notifica di registrazione nel Perimetro.

La procedura di segnalazione e le misure di gestione del rischio sono definite dal D.P.C.M. n. 81/2021. Gli incidenti relativi alla sicurezza informatica sono classificati in base al loro impatto sugli *asset* ICT. La tassonomia prevista distingue due tipologie di incidenti sulla base della gravità dello stesso: la Tabella 1 dell'Allegato A contiene gli incidenti meno gravi (e.g. infezione, guasto, installazione, movimenti laterali, azioni sugli obiettivi)³⁶ e la Tabella 2 quelli più gravi (e.g. azioni sugli obiettivi e disservizio)³⁷. Questa classificazione è funzionale alle diverse tempistiche necessarie per una risposta efficace. Pertanto, le entità del Perimetro dovranno riferire al CSIRT italiano entro un'ora nel caso di un incidente identificato nella Tabella 2, Allegato A, e sei ore nel caso di un incidente rientrante nella Tabella 1. Tali termini decorrono dal momento in cui l'ente viene a conoscenza dell'incidente, ad esempio attraverso le attività di monitoraggio, test e

³⁴ Articolo 1(2) D.L. 105/2019.

³⁵ Articolo 1(8) D.L. 105/2019.

³⁶ Ciascuna macrocategoria contiene numerosi casi specifici, per esempio nel caso del guasto sono inclusi: violazione del servizio atteso in termini di calcolo, memoria e/o banda passante, oppure di hot-replica e/o cold-replica e/o sito(i) di disaster recovery, se previsti, oppure ancora di perdita irreversibile o di corruzione irreversibile dei dati provenienti dalle componenti di campo (attuatori e sensori); dati hot-replica e/o cold-replica e/o sito(i) di disaster recovery e/o backup, se previsti, persi o corrotti in modo irreversibile; perdita di confidenzialità o integrità; perdita e/o corruzione dati

irreversibile; perdita e/o compromissione di chiavi di cifratura e/o certificati; perdita e/o compromissione di credenziali utenti; violazione del livello di servizio in termini di impossibilità di accesso fisico alle componenti.

³⁷ Anche in questo caso ciascuna delle due ipotesi include casi specifici, per esempio nel caso di disservizio sono inclusi i casi di violazione del livello di servizio atteso specie in termini di disponibilità, del bene ICT; divulgazione di dati corrotti o esecuzione operazioni corrotte tramite il bene ICT; divulgazione non autorizzata di dati digitali relativi ai beni ICT.

controllo svolte sulla base delle misure di *cybersecurity* previste dallo stesso decreto. Ai sensi dell'art. 3 D.P.C.M. n. 81/2021, la notifica degli incidenti di sicurezza informatica effettuata dagli enti NIS è conforme agli obblighi di notifica di cui agli articoli 14 e 16 NIS, che prevedono la notifica senza indebito ritardo.

Se l'ente viene a conoscenza di nuovi elementi significativi, tra cui specifiche vulnerabilità sfruttate o, più in generale, la rilevazione di eventi in qualche modo correlati all'incidente, la notifica deve essere modificata senza indebito ritardo dal momento in cui se ne viene a conoscenza, a meno che l'autorità giudiziaria procedente non abbia precedentemente richiesto specifiche esigenze di segretezza delle indagini³⁸. Inoltre, su richiesta del CSIRT, l'ente che ha notificato un incidente è tenuto, entro sei ore dalla richiesta, ad aggiornare la notifica, ad eccezione dei casi in cui sussistano specifiche esigenze di segreto investigativo. L'art. 4 D.P.C.M. n. 81/2021 prevede un'ulteriore segnalazione volontaria di incidenti per gli enti che rientrano nel Perimetro ma non qualificati come OSE. Il CSIRT deve dare priorità alle notifiche obbligatorie, prima di occuparsi di quelle volontarie. Queste notifiche riguardano (a) gli incidenti relativi alle risorse ICT che non sono coperte dall'Allegato A; e (b) gli incidenti, coperti dall'Allegato A, relativi alle reti, ai sistemi informativi e ai servizi informatici delle entità non incluse nell'elenco delle risorse ICT identificate.

Per quanto riguarda le misure di sicurezza informatica, l'Allegato B D.P.C.M. n. 81/2021 contiene una tassonomia complessa e molto dettagliata di misure di sicurezza informatica. Queste misure, che rientrano nella categoria dei controlli tecnici e sono raggruppate in base alle loro funzioni, ossia identificare, proteggere, rilevare, rispondere e recuperare, sono suddivise in due categorie. Le misure di cui alla categoria "A" dell'appendice n. 1 dell'Allegato B devono essere applicate ai beni ICT entro sei mesi dalla data di trasmissione degli elenchi di beni ICT o, se la trasmissione è avvenuta prima della data di entrata in vigore del D.P.C.M. n. 81/2021, entro sei mesi da quest'ultima data; i termini sono estesi fino a trenta mesi per le misure che rientrano nella categoria "B". Le entità devono notificare all'Agenzia per la sicurezza informatica senza indebito ritardo l'adozione di tali misure; la notifica è richiesta anche per i relativi aggiornamenti. È interessante notare che il D.P.C.M. n. 81/2021 prevede specificamente aspetti legati alla sicurezza dei dati, integrando anche i requisiti previsti dal Regolamento generale per la protezione dei dati, n. 679/2016. La struttura adottata dal legislatore per individuare le misure sulla sicurezza informatica riprende il modello

³⁸ Articolo 3 (5) D.P.C.M. 81/2021.

del Cybersecurity Framework elaborato dal National Institute of Standards and Technology (NIST) nel 2014³⁹ e adottato a livello statunitense per ridurre i rischi per la sicurezza informatica. Infatti, il modello italiano è suddiviso, così come lo standard NIST, in cinque classi o funzioni: *Identify* (identificare), *Protect* (proteggere), *Detect* (indagare), *Respond* (reagire), *Recover* (riparare). Ciascuna funzione è poi suddivisa in categorie, e in sottocategorie che rappresentano i singoli controlli da trattare nell'analisi e valutazione del rischio. Ovviamente, rispetto al modello statunitense, il quadro dei requisiti previsti a livello italiano è più ampio in quanto include, come detto, le sottocategorie legate all'implementazione delle norme legate alla protezione dei dati personali. Come evidenziato nella ricerca svolta nel quadro del progetto ERACLITO, i requisiti legali e tecnici che sono previsti dalla normativa sono molteplici e dettagliati che richiedono numerosi interventi e investimenti sia di tipo tecnico che organizzativo alle imprese che ricadono nella perimetro al fine di dimostrare la compliance⁴⁰.

L'Allegato C, infine, identifica diversi controlli di base sulla *cybersecurity* che si applicano all'elenco dei soggetti del Perimetro, agli elenchi della descrizione dell'architettura e dei componenti, nonché all'analisi dei rischi, agli elementi dei rapporti di notifica degli incidenti e alla documentazione relativa alle misure di *cybersecurity* di cui all'Allegato B.

Il D.L. n. 82/2021 ha istituito l'Agenzia nazionale per la sicurezza informatica al fine di assumere il ruolo di autorità nazionale per la sicurezza informatica come punto di contatto unico ai fini della direttiva NIS e di autorità nazionale di certificazione della sicurezza informatica ai fini della CSA. Pertanto, le attività di ispezione e audit, un tempo affidate al Ministero dello Sviluppo Economico e alla Presidenza del Consiglio dei ministri, rientrano ora nelle competenze dell'Agenzia. A questo proposito, il capo IV del D.P.R. n. 54/2021 stabilisce i poteri e le procedure di vigilanza in materia di ispezioni e audit in relazione all'adempimento dei vari obblighi imposti dai D.P.C.M. Oltre al monitoraggio periodico, il capo IV prevede anche ispezioni *ad hoc* se ritenute necessarie in casi eccezionali (ad esempio a seguito di notifiche di incidenti, mancato rispetto di uno qualsiasi degli obblighi derivanti dall'applicazione della normativa in materia e notifiche da parte di altre autorità pubbliche). Le attività di audit vengono

³⁹ Cybersecurity Framework V1.1 (Aprile 2018), disponibile all'indirizzo <https://www.nist.gov/cyberframework/framework>.

⁴⁰ Si veda l'analisi svolta nel Delivera-

ble 1.1 Project Requirements, in cui sono presentati i requisiti tecnici e giuridici, disponibile all'indirizzo <https://www.lider-lab.it/en/eraclito-2/>.

svolte attraverso analisi e verifiche documentali ⁴¹. L'articolo 16(5) e (6) D.P.R. n. 54/2021 stabilisce le scadenze per la conclusione dei diversi tipi di ispezioni, garantendo il completamento tempestivo delle procedure.

Il Decreto Perimetro peraltro introduce una serie di diverse sanzioni amministrative per il mancato rispetto degli obblighi imposti dal Decreto Perimetro e dai suoi decreti attuativi. Ad esempio, l'inosservanza dell'obbligo di redigere, aggiornare e presentare gli elenchi delle reti, dei sistemi informativi e dei servizi ICT è soggetta a una sanzione amministrativa che va da 200.000 a 1,2 milioni di euro, mentre la mancata notifica di incidenti di *cybersecurity* o l'implementazione di misure di *cybersecurity* sono soggette a multe comprese tra 250.000 e 1.5 milioni di euro. È interessante notare che sanzioni più severe vengono comminate in caso di mancato rispetto dei requisiti per gli appalti: un'entità che non notifica il contratto di fornitura di beni ICT al CVCN e non rispetta le condizioni stabilite dal CVCN può essere multata fino a 1,8 milioni di euro. Inoltre, l'art. 1(11) Decreto Perimetro prevede anche la sanzione penale della reclusione da uno a tre anni per la fornitura di informazioni, dati o elementi di fatto falsi, o l'omissione di comunicare i suddetti dati, al fine di ostacolare o influenzare il completamento delle procedure relative alla notifica di incidenti, alle misure di gestione della *cybersecurity*, agli appalti o alle ispezioni, nonché alle attività di vigilanza.

5. L'EVOLUZIONE DEL QUADRO NORMATIVO.

Mentre gli Stati membri si adoperavano per implementare la direttiva NIS, la Commissione — nel dicembre 2020 — ha presentato il nuovo strumento legislativo finalizzato a sostituire la direttiva NIS, superando alcuni dei difetti di quest'ultima, la direttiva 2555/2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (Direttiva NIS 2) ⁴². L'approccio non è cambiato e sia la NIS che la NIS 2 condividono la stessa base giuridica, ovvero l'art. 114 TFUE. Di conseguenza, la NIS 2 mira ancora a migliorare il livello di sicurezza per salvaguardare il mercato interno digitale, stabilendo norme armonizzate nel settore della gestione del rischio di cybersicurezza e della segnalazione degli incidenti. Questo approccio è confermato anche dall'estensione del numero di aree che rientrano nell'ambito di applicazione della NIS 2, che di conseguenza aumenterà il numero

⁴¹ Articolo 14 D.P.R. n. 54/2021.

⁴² Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nel-

l'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), GU L 333, 27.12.2022, p. 80

di entità che saranno vincolate dagli obblighi e dai requisiti della NIS 2. Va da sé che l'incremento del numero delle entità coinvolte avrà di per sé un effetto amplificativo dei fenomeni di interferenza con la autonomia contrattuale prima evidenziato.

Ma ciò non basta. Infatti, è importante sottolineare che l'attuale struttura della NIS 2 si basa sulla valutazione e sulla stesura di relazioni sull'impatto della direttiva NIS ⁴³. Infatti, una delle prime sfide emerse dalla struttura della NIS 1 è stata l'identificazione degli attori inclusi nel campo di applicazione. La NIS 2 modifica tale modalità di identificazione e individua come primo criterio la dimensione dell'impresa, escludendo dal suo campo di applicazione le piccole e microimprese (art. 2(1) NIS 2). Sebbene la Commissione ammetta che questo criterio *“non è necessariamente un criterio ideale a sé stante per determinare l'importanza e/o la criticità”* di un'entità, si tratta di una *“proxy significativa”* per determinare se certe entità hanno ruoli chiave per la società e l'economia. Se, da un lato, è comprensibile l'esigenza di limitare l'impatto di una normativa chiaramente impegnativa per i soggetti privati coinvolti, dall'altro rimane problematica la selezione prioritaria di un criterio quantitativo che, a dispetto delle eccezioni, non presenta sufficienti, oggettivi e flessibili criteri oggettivi capaci di *“pesare”* la qualità del soggetto da coinvolgere.

Invero, il testo prevede un ampio elenco di eccezioni, che si applicano indipendentemente dalle dimensioni dell'azienda. Ad esempio, le dimensioni sono irrilevanti nel caso di servizi forniti da fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, o da fornitori di servizi fiduciari, o anche da registri di nomi di dominio di primo livello e da fornitori di servizi di sistemi di nomi di dominio; nel caso di entità che siano l'unico fornitore in uno Stato membro di un servizio essenziale per il mantenimento di attività sociali o economiche critiche; nel caso in cui l'interruzione del servizio fornito dall'entità possa avere un impatto significativo sulla sicurezza pubblica, sulla pubblica sicurezza o sulla salute pubblica; o per entità della pubblica amministrazione ⁴⁴.

Il secondo criterio è l'attività svolta in uno dei settori individuati negli allegati I e II della direttiva NIS 2. È interessante notare che la NIS 2 estende in modo significativo l'ambito di applicazione della NIS 1, aggiungendo nuovi settori come le telecomunicazioni, le piattaforme di social media e la pubblica amministrazione.

Gli allegati I e II prevedono un'altra delle innovazioni della NIS 2: il passaggio dalla distinzione tra operatori di servizi essenziali

⁴³ Si veda Relazione della Commissione di valutazione della coerenza degli approcci adottati dagli Stati membri per

l'identificazione degli operatori di servizi essenziali, cit.

⁴⁴ Articolo 2 (2) NIS 2.

e fornitori di servizi digitali alla distinzione tra i cosiddetti soggetti essenziali (essential entities - EE) e i soggetti importanti (important entities - IE). La distinzione non è giustificata da un diverso insieme di requisiti e obblighi di notifica, come accadeva nella direttiva NIS, ma riguarda solo il tipo di meccanismi di sorveglianza del mercato applicabili.

Tuttavia, anche le eccezioni individuate non sono in grado di intercettare agevolmente situazioni sempre più attuali quali quelle di anelli delle catene produttive relative il cui ruolo non rientra direttamente nelle eccezioni; per esempio, nel caso in cui le imprese non rappresentino in uno Stato membro un servizio essenziale per il mantenimento di attività sociali o economiche critiche ma nel contempo rappresentino un collo di bottiglia per la catena produttiva che abilita il soggetto ricondotto all'interno del perimetro o che più in generale sia identificabile come soggetto essenziale o importante. Questa constatazione ci porta ad anticipare un ulteriore corto circuito normativo ed operativo che si può generare. Infatti, in assenza di idonei strumenti e criteri di verifica qualitativi per individuare i colli di bottiglia nelle catene produttive nonché, forse, di idonea capacità tecnica ed economica da parte delle EE/IE queste hanno responsabilità nette nel propagare le esigenze e gli obblighi di sicurezza lungo la loro catena produttiva e di approvvigionamento.

Ancora una volta non ci risulta che a fronte di questi costi effettivi di *compliance* ad alto impatto sull'autonomia contrattuale ed imprenditoriale esistano modalità di assistenza finanziaria o di altro genere. Il risultato concreto, dunque, potrebbe portare sia ad alti costi di *compliance* sia a livelli insoddisfacenti di efficacia degli stessi.

Gli articoli 21 e 23 NIS 2 chiariscono che sia gli EE che gli IE sono soggetti agli stessi requisiti di sicurezza informatica e agli stessi obblighi di notifica. La NIS 2 è anche più dettagliata in termini di linee guida relative ai requisiti di sicurezza, sebbene ripeta la formulazione già utilizzata nell'articolo 14 NIS 1 sulle misure "appropriate e proporzionate" e sullo standard dello "stato dell'arte", aggiunge un elenco di sette elementi chiave che tutte le aziende devono affrontare o implementare, tra cui la risposta agli incidenti, la sicurezza della catena di approvvigionamento, la crittografia e la divulgazione delle vulnerabilità.

L'articolo 21 (2) prevede che le misure di sicurezza includano almeno quanto segue:

- a) politiche sull'analisi dei rischi e sulla sicurezza dei sistemi informativi;
- b) gestione degli incidenti;
- c) la continuità operativa, come la gestione dei backup e il ripristino in caso di disastro, e la gestione delle crisi;
- d) la sicurezza della catena di approvvigionamento, compresi

gli aspetti relativi alla sicurezza delle relazioni tra ciascun ente e i suoi fornitori diretti o prestatori di servizi;

e) la sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di reti e sistemi informativi, compresa la gestione e la divulgazione delle vulnerabilità;

f) politiche e procedure per valutare l'efficacia delle misure di gestione del rischio di sicurezza informatica;

g) pratiche di igiene informatica di base e formazione in materia di sicurezza informatica;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) la sicurezza delle risorse umane, le politiche di controllo degli accessi e la gestione degli *asset*;

j) l'uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e di testo protette e di sistemi di comunicazione di emergenza protetti all'interno dell'entità, ove opportuno.

Per paradosso, i soggetti EE ed IE, oltre a dovere essere in grado di identificare ed implementare le misure “appropriate e proporzionate”, sono comunque chiamati a occuparsi della “sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza delle relazioni tra ciascun ente e i suoi fornitori diretti o prestatori di servizi”. Il risultato ancora una volta è l'imposizione di obblighi e di capacità di analisi dei rischi, nonché di disegno di modelli sia economici che giuridici per governarli sulle realtà private che a dispetto della imposizione normativa potrebbero prima di averne le capacità non averne neppure consapevolezza.

Per quanto riguarda gli obblighi di notifica, la NIS 2 prevede un approccio in due fasi alla segnalazione degli incidenti che supera i problemi emersi nell'attuazione della NIS. Durante la prima fase, l'entità interessata deve informare, con un rapporto iniziale, l'autorità nazionale o il CSIRT entro 24 ore da quando viene a conoscenza di un incidente. Successivamente, lo stesso soggetto fornirà un rapporto completo entro 72 ore da quando è venuto a conoscenza dell'incidente. La seconda fase riguarda il ripristino completo del problema, con la presentazione di un rapporto finale ad un mese dopo il rapporto iniziale.

Si noti che la segnalazione di incidenti significativi è obbligatoria, mentre per qualsiasi altro incidente di livello inferiore non è necessaria la notifica. Tuttavia, al fine di acquisire un quadro completo del panorama delle minacce, l'articolo 29 NIS 2 fornisce una base giuridica per le notifiche volontarie di incidenti significativi, minacce informatiche e quasi incidenti da parte di entità che non rientrano nell'ambito di applicazione della direttiva NIS2, lasciando agli Stati membri la scelta di dare priorità al trattamento delle notifiche obbligatorie rispetto a quelle volontarie.

La differenziazione tra EE e IE prevista dalla NIS 2 riguarda il tipo di vigilanza applicata a ciascuno di essi. L'art. 32 NIS 2 stabilisce i poteri di vigilanza e monitoraggio applicabili alle EE e distingue tra vigilanza *ex ante*, ossia l'adozione di misure di vigilanza in anticipo, e vigilanza *ex post*, ossia l'adozione di misure di vigilanza quando vengono fornite prove o indicazioni che un'entità non soddisfa i requisiti di sicurezza informatica e di notifica degli incidenti. Gli EE sono soggetti a un regime di vigilanza "a tutti gli effetti" che comprende sia la vigilanza *ex ante* che quella *ex post*. Mentre l'art. 33 NIS 2 prevede che gli IE siano soggetti a un regime di vigilanza "leggero", che comprende solo la vigilanza *ex post*.

Per quanto riguarda l'enforcement, la direttiva stabilisce un elenco minimo di sanzioni amministrative pecuniarie per i casi in cui i soggetti violino le norme sulla gestione del rischio di cyber-sicurezza o gli obblighi di notifica previsti dalla direttiva NIS 2. Ad esse si aggiungono poi i poteri previsti per le autorità nazionali, che includono avvertimenti, l'adozione di istruzioni vincolanti e l'attuazione delle raccomandazioni (art. 32(4) NIS 2).

6. LE QUESTIONI APERTE E L'ESIGENZA DI APPROFONDIMENTO.

La rapida evoluzione del quadro normativo a livello europeo in merito alla sicurezza informatica con l'adozione della direttiva NIS 2 porta ad una serie di considerazioni relative alle modalità di implementazione a livello nazionale.

In primo luogo, alla luce del diverso livello di dettaglio previsto dall'art. 21 NIS 2 in merito alle misure che le EE e IE devono adottare sulla sicurezza informatica rispetto alle laconiche indicazioni previste dall'art. 14 NIS, sarà necessario per il legislatore italiano valutare se gli attuali requisiti previsti dalla Tabella B del D.P.C.M. n. 81/2021 siano sufficienti e conformi alle previsioni del nuovo quadro legislativo. Peraltro, è da segnalare anche il processo di aggiornamento dello stesso standard NIST: nell'agosto del 2023 è stata infatti presentata la bozza del c.d. NIST 2.0⁴⁵. Anche in questo caso, numerosi sono i cambiamenti che potrebbero essere rilevanti, laddove il legislatore italiano voglia mantenere una affinità (*rectius* conformità) rispetto allo standard statunitense⁴⁶.

Un aspetto legato al precedente è poi la necessità di armonizzare a livello europeo i requisiti previsti dagli stati membri per la sicurezza informatica. Se è vero che il ruolo di supporto e

⁴⁵ <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-2.0/ipd>.

⁴⁶ È interessante notare che il NIST dichiarava di essere finalizzato alla sicu-

rezza delle infrastrutture critiche statunitensi, la versione 2.0 è stata modificata per concentrarsi sulle organizzazioni di tutto il mondo.

consulenza dell'ENISA ha consentito di indirizzare le scelte dei governi nazionali nella stessa direzione, tuttavia la presenza di requisiti anche solo parzialmente diversi potrebbe comportare per le imprese che offrono servizi essenziali in più di uno Stato membro. In questo senso, il ruolo del Gruppo di cooperazione, previsto dall'art. 14 NIS 2, può rappresentare un importante contesto nel quale non soltanto scambiare migliori prassi e informazioni relative all'attuazione della direttiva (art. 14(3)(c) NIS 2) ma anche individuare scelte e approcci comuni per quanto riguarda gli standard di sicurezza da adottare.

Uno degli aspetti problematici della NIS 2 è peraltro la scelta di escludere dallo scopo di applicazione le piccole e microimprese. Tali soggetti, alla luce del criterio dimensionale previsto dalla direttiva, non sono sottoposti ad alcun obbligo per l'adozione di misure di tutela per la sicurezza informatica. Per quanto siano previste numerose eccezioni legate all'importanza e alla criticità dei servizi svolti dalle imprese presenti nel territorio europeo, rimangono comunque scoperte un ampio numero di imprese⁴⁷. Ciò comporta un incremento del rischio, poiché non soltanto le gran parte delle micro e piccole imprese hanno minori risorse economiche e organizzative investite nella sicurezza informatica e diventano dunque un bersaglio privilegiato degli attacchi informatici⁴⁸.

In questo caso, appare dunque fondamentale utilizzare una forma indiretta di implementazione delle misure di sicurezza informatica attraverso controllo della catena di approvvigionamento. Come previsto dall'art. 21(2) lett. d) NIS 2, le misure di sicurezza che devono essere adottate dagli EE e IE includono anche la verifica del livello di sicurezza adottato dai fornitori diretti o prestatori di servizi. La definizione della direttiva in questo caso non pone vincoli: ogni tipologia di fornitori e prestatori, indipendentemente dalle dimensioni, dal settore di riferimento, e dalla tipologia di prodotti e servizi offerta viene inclusa. Questo aspetto è cruciale per poter garantire che le minacce e gli attacchi informatici non possano essere perpetrati attraverso falle o vulnerabilità riconducibili a componenti utilizzate dall'EE o IE nella loro attività. Dal punto di vista pratico, quindi l'EE o IE dovrà prevedere una mappatura dei propri fornitori e prestatori

⁴⁷ Dai dati del 2021, il 98% delle imprese presenti nel territorio europeo possono essere qualificate come micro e piccole imprese, si vedano i dati Eurostat disponibili all'indirizzo: <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ledn-20220627-1>.

⁴⁸ La direttiva NIS 2 richiede un impegno a livello statale di intervento nel qua-

dro della strategia nazionale per la cybersecurity; tuttavia, l'articolo 7 (2)(i) impone soltanto un 'rafforzamento dei valori di riferimento relativi alla ciberresilienza e all'igiene informatica delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, fornendo orientamenti e sostegno facilmente accessibili per le loro esigenze specifiche'.

di servizi e applicare ad essi le misure di sicurezza equivalenti a quelle già adottate a livello di impresa ⁴⁹. Tale mappatura è peraltro un'informazione critica anche per l'autorità di controllo a livello nazionale: prevedere una condivisione con l'Agenzia nazionale per la *Cybersecurity* della catena di approvvigionamento permetterebbe alla stessa agenzia di verificare eventuali sovrapposizioni, ad esempio nel caso di fornitori e prestatori che operano con più EE o IE. Laddove si presenti una minaccia informatica focalizzata su uno specifico componente sviluppato da un fornitore, sarebbe possibile anticipare eventuali controlli anche sugli altri EE e IE che utilizzino lo stesso fornitore. Inoltre, nel caso di fornitori o prestatori non stabiliti nello stesso paese europeo, o ancora al di fuori del territorio europeo, sarebbe possibile anticipare forme di controllo coordinato a livello europeo attraverso il già citato Gruppo di cooperazione previsto ex art. 14 NIS 2.

Se queste conclusioni sono valide in termini di politica del diritto e di implementazione della NIS2, rimane a nostro avviso fondamentale la conclusione che l'analisi ci ha permesso di raggiungere in punto di criticità normative. Questo primo esercizio ci conduce a sottolineare l'importanza della mappatura combinata degli obblighi previsti dalle normative di cybersecurity e del quadro della digitalizzazione. Si tratta di un contributo essenziale non solo per abilitare la *compliance* ma, soprattutto, per abilitarla in modo da sfruttare le sinergie tra obblighi che possono essere soddisfatti con le stesse risorse, evitando duplicazioni che, oltre a rappresentare un costo, presentano anche un sicuro rischio di confusione nei soggetti chiamati ad attuarli.

Tuttavia, la mappatura ragionata degli obblighi e dei loro destinatari, così come la identificazione dei corrispondenti controlli, costituisce solo un primo passo per evidenziare le nuove linee di convergenza e tensione tra plessi normativi diversi e sempre più in reciproca relazione.

Quello che ci pare inizi ad emergere è un quadro normativo generale della *cybersecurity* che non necessita più solo di rapportarsi con le discipline alleate legate alla digitalizzazione e alla società dei dati (ad esempio la disciplina della protezione dei dati personali o del loro governo) ma anche con istituti generali del diritto privato, come la disciplina generale dei contratti. Ulteriori approfondimenti saranno necessari per esplorare significati, limiti ed effetti di queste relazioni per identificare sia le interdi-

⁴⁹ Sotto questo profilo, resta aperta la questione circa le modalità attraverso le quali le EE e IE potranno imporre requisiti e misure di sicurezza alle imprese nella rispettiva catena del valore. Una ipotesi po-

trebbe essere rappresentata dai contratti di rete. Si veda Gian Domenico Mosco, *La collaborazione tra imprese per la sicurezza informatica*, LLR, n. 2, 2017, 157.

pendenze con discipline ed istituti generali (per esempio la responsabilità precontrattuale del privato contraente che a causa di clausole “imposte” dalla CVCN non sottoscriva il definitivo) sia le interrelazioni nuove che si aprono tra settori specifici a valle degli ampliamenti che sta apportando la NIS 2 nel panorama normativo e nel sistema delle relazioni tra imprese e tra imprese e sicurezza nazionale.

Abstract

The article analyses the EU cybersecurity regulations, both present and forthcoming, from a private law perspective pointing out what may be the consequences of non-compliance by business in contractual relationships and in the event of claims for damages.