Memoria su Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (c.d. NIS 2) richiesta dalle Commissioni I Commissione Affari Costituzionali e della IX Commissione Trasporti

di ERIK LONGO (*Università degli Studi di Firenze*)

1. Introduzione al quadro europeo di riferimento

Lo schema di decreto legislativo sottoposto alla nostra attenzione è volto a recepire la direttiva (UE) 2022/2555, cosiddetta "Direttiva NIS 2" (*Network and Information Systems*), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione europea, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS), e, conseguentemente, ad abrogare e sostituire il decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva NIS del 2016.

La Direttiva NIS 2 è stata pubblicata il 14 dicembre 2022 e richiede che gli Stati membri la recepiscano entro il 17 ottobre 2024. La prima direttiva NIS, adottata nel 2016, mirava a fornire un elevato livello comune di sicurezza informatica in tutti gli Stati membri, ma si è rivelata di difficile attuazione, come dimostrato anche dal lento recepimento italiano (Longo 2024).

Per rispondere alle nuove minacce poste dalla digitalizzazione e all'aumento generale degli attacchi informatici, l'UE ha deciso di rivedere questo quadro per rafforzare i requisiti di sicurezza, garantire la continuità della catena di approvvigionamento, semplificare la rendicontazione degli incidenti e introdurre misure di vigilanza e applicazione più rigorose (Vandezande 2024). A tali elementi si deve anche aggiungere che il quadro della legislazione europea in materia di cybersicurezza è notevolmente cambiato negli ultimi cinque anni. L'Ue ha adottato infatti il Regolamento n. 2019/881 del 17 aprile 2019 sull'ENISA (European Union Agency for Cybersecurity) e sulla cybersicurezza delle comunicazioni informatiche e le certificazioni (c.d. Cybersecurity Act) e poi una nuova Strategia sulla cybersicurezza nel 2020 (Commissione 2020).

La Strategia dell'UE per la cibersicurezza del 2020 definiva lo scenario per una serie di futuri strumenti, tra i quali vi è proprio la direttiva NIS 2. Un altro importante atto è la Direttiva n. 2022/2557 sulla resilienza delle entità critiche (c.d. direttiva CER). La nuova direttiva CER, che sostituisce la direttiva sulle infrastrutture critiche del 2008, designa le entità critiche distinguendole in undici settori. Questi si sovrappongono in larga misura alla designazione di entità essenziali da parte della NIS 2. Tale scelta è frutto di un preciso obiettivo. Mentre, infatti, la direttiva CER riguarda principalmente la sicurezza fisica di tali entità, la NIS 2 riguarda la loro sicurezza informatica. Data la forte interconnessione tra i due aspetti, la NIS 2 stabilisce un approccio coerente con la direttiva CER. Pertanto, i soggetti destinatari di queste regole potrebbero dover rispettare

entrambe le discipline, così come le autorità competenti per entrambe dovrebbero collaborare strettamente su alcune questioni adiacenti.

Un'altra disciplina adottata nel medesimo pacchetto è contenuta nel Regolamento n. 2022/2554 sulla resilienza delle operazioni digitali per il settore finanziario (c.d. regolamento DORA). Il regolamento DORA si concentra specificamente sulle realtà finanziarie, con un elenco di ventuno tipi di soggetti regolamentati, tra cui gli istituti di credito, gli istituti di pagamento e di moneta elettronica, le imprese di investimento, le imprese di assicurazione e riassicurazione, i fornitori di servizi di crowdfunding, ecc. Oltre ai soggetti finanziari in sé, DORA si applica anche, in una certa misura, a terzi che forniscono loro servizi legati alle ICT.

Questo quadro si completerà a breve con un'altra disciplina, sempre di natura regolamentare, il "Cyber Resilience Act", relativo ai prodotti digitali (soprattutto i prodotti IoT) (Chiara 2023). L'obiettivo è quello di risolvere il problema dei dispositivi, come computer e smartphone, che spesso vengono immessi sul mercato con vulnerabilità di sicurezza o con la mancanza di aggiornamenti di sicurezza per tutta la durata della loro vita. Tale disciplina completa il quadro della NIS 2, la quale non affronta tutti i problemi che possono derivare dall'immissione nel mercato di hardware e software vulnerabili alla sicurezza.

In sintesi, in un contesto esterno ed interno notevolmente cambiato la Commissione ha inteso rinnovare la disciplina generale sulla cybersicurezza cercando di risolvere alcuni dei problemi principali della direttiva NIS, la quale, come già ricordato, ha lasciato un notevole grado di discrezionalità agli Stati membri nel recepire le norme sovranazionali. Questo ha determinato divergenze e disparità significative tra gli Stati membri, non sostenibili nell'ottica di una società sempre più dipendente dai prodotti e servizi digitali. Ad esempio, si rileva che in alcuni Stati membri gli ospedali sono considerati "soggetti essenziali" ai sensi della direttiva NIS, mentre in altri Stati membri non lo sono. Allo stesso modo, in alcuni Stati membri i grandi operatori ferroviari rientrano negli obblighi NIS, ma in altri un operatore di dimensioni simili non vi rientrano. Queste differenze hanno un effetto negativo sia sulla concorrenza, in quanto gli enti di uno Stato membro possono dover sostenere i costi operativi per conformarsi a questo quadro normativo, sia sulla resilienza agli attacchi informatici che può determinare, come purtroppo è accaduto, una forte compressione di diritti fondamentali.

In termini tecnici, la proposta di direttiva NIS 2 è stata pubblicata alla fine del 2020. Al Parlamento europeo la proposta è stata discussa soprattutto nella commissione Industria, Ricerca ed Energia (ITRE). Nella sua relazione, la commissione sottolinea la forte crescita di reati informatici commessi all'interno dell'UE, ed il sottofinanziamento delle imprese europee quanto a sicurezza informatica.

2. Il contesto della cybersicurezza (sintesi)

Prima di entrare nel merito dell'esame, giova premettere una brevissima indicazione circa il contesto della cybersicurezza nell'Unione europea. I numeri e

le tendenze sono un'ottima ed efficace via per capire l'importanza di una legislazione come quella in esame.

Una indagine di Eurostat riporta che nel 2021 il 22% delle imprese localizzate nel territorio dell'Unione europea ha subito varie conseguenze a causa di incidenti di sicurezza legati alle tecnologie dell'informazione e della comunicazione (Eurostat 2023). Nel 2018 la percentuale era solo del 12% (Eurostat 2020). Tali conseguenze comprendono la mancata disponibilità di servizi, la distruzione o la corruzione di dati o addirittura la divulgazione di dati riservati.

Malgrado un numero significativo di incidenti sia riconducibile a guasti hardware o software, moltissimi sono il frutto di eventi dolosi. Gli attacchi ransomware sono cresciuti del 41% nel 2022 (ENISA 2022). Anche gli attacchi via e-mail, compreso il phishing, sono aumentati del 48% nel 2022 (ENISA 2023). Gli attacchi hanno iniziato a concentrarsi sull'interruzione delle catene di approvvigionamento, già perturbate dopo la pandemia e ancora di più dall'inizio della guerra in Ucraina.

Le conseguenze economiche di questi incidenti sta salendo alle stelle. Uno studio del 2020 del Joint Research Centre (JRC) dell'Ue ha stimato che il costo globale della criminalità informatica avrebbe raggiunto i 5,5 trilioni di euro entro la fine del 2020, rispetto ai 2,7 trilioni di euro del 2015 (Baldini et al. 2020). Le stime per il 2025 arrivano a 10,5 trilioni di dollari USA. Il costo medio globale di una violazione dei dati nel 2022 è stato stimato a 4,35 milioni di dollari USA (Morgan 2020). Naturalmente, ciò dipende dal settore (le violazioni dei dati sanitari ammontano in media a 10,10 milioni di dollari) dal tipo di attacco (gli attacchi distruttivi ammontano in media a 5,12 milioni di dollari) dal tipo di azienda (le violazioni dei dati delle grandi aziende negli Stati Uniti producono in media danni per 9,44 milioni di dollari).

I danni della criminalità informatica non si limitano solo alle reti e strutture informatiche colpite. Oltre il 45% delle violazioni riguarda i dati personali, ciò espone i cittadini di tutto il mondo a vari rischi, come il furto di identità e le frodi finanziarie. Una situazione che peggiorerà ancora di più con l'uso dell'IA generativa (Meda 2024). I danni non sono solo economici. Con gli ospedali e le infrastrutture critiche, come le centrali nucleari, sempre più spesso presi di mira, c'è anche un chiaro rischio di limitazione della stessa vita umana.

Nonostante le politiche adottate negli USA (Biden 2021), prima, e in Europa (Eckhardt and Kotovskaia 2023), poi, per rendere resilienti aziende ed enti pubblici contro le minacce informatiche, il 54% dei soggetti privati e pubblici riferisce di non essere adeguatamente attrezzato per gestire i cyberattacchi più avanzati. Si stima, inoltre, che il 95% dei problemi di cybersecurity possa essere ricondotto a un errore umano, evidenziando la necessità di una maggiore alfabetizzazione sulla cybersecurity nella popolazione generale (Vandezande 2024).

3. Un breve riepilogo delle novità della direttiva NIS 2

In questa fase analizzeremo alcuni aspetti innovativi della direttiva NIS 2 rispetto alla direttiva NIS. Il quadro complessivo rimane lo stesso di prima:

stabilire misure “per raggiungere un elevato livello comune di cibersicurezza in tutta l’Unione, al fine di migliorare il funzionamento del mercato interno” (art. 1 direttiva NIS e NIS 2). Tuttavia, muta lo spettro di applicazione dello stesso obiettivo. Mentre la prima direttiva NIS si concentrava sulla “sicurezza delle reti e dei sistemi informativi”, la direttiva NIS 2 si concentra sulla più ampia nozione di “cybersecurity” definita nel *Cybersecurity Act* (art. 2). La nuova direttiva non protegge solo le reti e i sistemi informativi, ma anche “gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche” (Chiara 2022). Visti i rischi che i cyberattacchi comportano per gli utenti dei sistemi digitali, si tratta di un ampliamento di non poco momento, il quale rappresenta un segno che della cybersicurezza non possiamo fare più a meno (Longo 2024).

Il cambiamento si riflette già nel titolo della nuova direttiva. La NIS 2 concerne “misure per un elevato livello comune di cibersicurezza in tutta l’Unione”. Sebbene in senso stretto lo stesso acronimo NIS non rappresenti più il contenuto reale della direttiva, ora che il titolo va oltre i meri sistemi di rete e di informazione, si può ritenere essere stato opportuno averlo mantenuto per garantire continuità e riconoscibilità della strategia europea in materia di sicurezza informatica (Vandezande 2024).

A parte questi aspetti centrali dell’intervento normativo, le principali novità introdotte sono: l’ampliamento dell’ambito soggettivo di applicazione della disciplina anche alla pubblica amministrazione centrale, le piccole e microimprese, e i fornitori di servizi di comunicazione elettroniche pubbliche e di reti di comunicazione elettronica accessibili al pubblico; la distinzione tra “soggetti essenziali” e “soggetti importanti” in base ai requisiti dimensionali e alla tipologia di prodotti o servizi forniti, al fine di superare l’attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri; la razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria; l’adozione di un approccio “multirischio”; la regolamentazione della divulgazione coordinata delle vulnerabilità (CVD) e l’ampliamento delle funzioni di coordinamento dei *Team* di risposta agli incidenti di sicurezza informatica CSIRT (*Computer Security Incident Response Team*) nazionali; l’istituzionalizzazione della cooperazione tra Stati membri nella nuova rete CyCLONe (*Cyber Crises Liaison Organisation Network*), per la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala.

Queste aggiunte esemplificano l’attenzione del NIS 2 verso l’effettiva applicazione delle sue misure che, secondo la valutazione d’impatto compiuta dalla Commissione europea, non era stata pienamente realizzata con la direttiva NIS.

In termini di campo di applicazione (art. 2, comma 2 della direttiva NIS 2), la NIS 2 si applica a soggetti pubblici o privati di medie o grandi dimensioni nei settori ad alta criticità (elencati nell’allegato I della direttiva) e in altri settori critici (elencati nell’allegato II della direttiva). Con questa formulazione, la direttiva mira a escludere dal suo campo di applicazione le piccolissime e le microimprese. Tuttavia, la direttiva può essere applicata a entità di qualsiasi dimensione nei settori elencati negli allegati I e II (si pensi ai soggetti che forniscono servizi di registrazione di nomi di dominio). Sono inclusi anche i fornitori di servizi fiduciari, che erano parzialmente esenti ai sensi della direttiva NIS e gli operatori del più

ampio settore delle telecomunicazioni. Ciò dimostra il fatto che la NIS 2 riconosce le comunicazioni elettroniche come essenziali per la nostra economia e società. Degna di particolare nota è pure l'inclusione delle amministrazioni pubbliche, soprattutto per via dell'importanza di tutti i tipi di servizi della p.a. e delle notevoli quantità di dati che tali soggetti generano, controllano e trattano.

La nuova direttiva esclude dall'ambito di applicazione gli enti pubblici operanti nei settori della sicurezza nazionale, della pubblica sicurezza e difesa, e del contrasto ai reati.

Sul piano dell'ambito di applicazione, la NIS 2 stabilisce obiettivi di armonizzazione minima. In un certo senso si tratta di una stretta necessità, data l'ampia portata del sistema e la grande diversità di organizzazione di questi enti e autorità negli Stati membri. L'armonizzazione minima non deve necessariamente comportare un ritardo di alcuni Stati membri rispetto ad altri, purché le norme minime siano di qualità sufficiente.

Per quanto riguarda gli altri atti legislativi dell'UE che impongono requisiti di cibersicurezza settoriali almeno equivalenti, la direttiva NIS 2 non si applicherà ai soggetti effettivamente coperti da tali atti. La NIS 2 deve quindi essere considerata come la *lex generalis* in termini di cybersicurezza, che non pregiudica le *lex specialis* settoriali. Ciò dimostra chiaramente la posizione della NIS 2 come nuovo testo legislativo di base nel campo della cybersicurezza nell'Ue, pur lasciando spazio ad altri testi adattati più specificamente a un particolare argomento (come il *Cyber Resilience Act*) o a un settore (come il regolamento DORA).

Il profilo forse più interessante della direttiva NIS 2 riguarda i destinatari. Per la NIS gli Stati membri godevano di una discrezionalità quasi assoluta nell'individuare gli operatori di servizi essenziali e forniva solo alcuni criteri generali per guidare gli Stati membri in questo esercizio, il quale spesso si basava su nozioni aperte all'interpretazione, come l'"effetto di disturbo significativo" (artt. 5 e 6 NIS). La NIS 2 ha un ampliamento sostanziale del campo di applicazione. La NIS 2 non distingue più tra operatori essenziali e fornitori di servizi digitali. La distinzione è invece tra settori altamente critici (essenziali), elencati sopra, e altri settori critici (importanti). Poiché questo elenco non è paragonabile alla direttiva NIS, tutte le voci sono considerate nuove.

Il risultato di questa espansione a quasi il doppio dei settori significa anche che un numero molto maggiore di soggetti pubblici e privati sarà coperto da questo quadro normativo. Secondo una stima, oltre 160.000 entità in tutta l'Ue saranno interessate dal nuovo quadro normativo. Sebbene possa sembrare un aumento sostanziale del campo di applicazione, la realtà della criminalità informatica e delle minacce informatiche non giustifica più il fatto che un quadro così rilevante sia limitato a pochi settori. L'espansione del NIS 2 è quindi solo un passo logico successivo e potrebbe addirittura rivelarsi un altro passo verso la trasformazione della disciplina in un quadro generale applicabile a tutte le entità.

Il NIS 2 attribuisce maggiori responsabilità agli organi di gestione dei soggetti privati e pubblici. Essi devono approvare le misure di gestione del rischio delle loro entità e controllarne l'attuazione. È anche esplicitamente dichiarato che possono essere ritenuti responsabili per le violazioni delle norme sulla cybersicurezza. Inoltre, sono tenuti a seguire una formazione in questo campo,

al fine di acquisire conoscenze e competenze sufficienti. Questa attribuzione diretta di responsabilità agli organi di gestione mira a garantire la loro partecipazione e il loro coinvolgimento nella sicurezza informatica della loro entità. Un punto spesso critico di insuccesso in questo campo è che i dipartimenti IT degli enti non ricevono un sostegno e un finanziamento adeguati dai vertici aziendali. Coinvolgendo i vertici aziendali in questo quadro, essi diventano diretti protagonisti del processo. Allo stesso tempo, ci si può chiedere quale sia il valore aggiunto della formazione dei dirigenti, dal momento che gli enti destinatari della NIS 2 avranno probabilmente membri del personale o addirittura interi dipartimenti dedicati all'informatica e alla sicurezza. Sebbene la consapevolezza della cybersecurity sia una competenza importante per tutti i soggetti, non tutti possono o devono essere esperti in materia. Inoltre, la NIS 2 richiede specificamente una formazione sulla valutazione e sulla gestione del rischio di cybersecurity; un argomento piuttosto avanzato e tecnico che per molti soggetti sarà sicuramente difficile da implementare.

La NIS2 elabora più chiaramente un approccio basato sul rischio, il quale deve essere seguito per gestire problemi di cybersecurity e impone persino una serie di elementi che devono essere comunque presenti. Questi includono elementi quali l'analisi del rischio, la gestione degli incidenti, la continuità operativa, la gestione delle crisi e il *disaster recovery*, ecc. In termini di valutazione dell'impatto, la NIS 2 dimostra l'ampliamento del campo di applicazione agli utenti dei servizi che subiscono l'impatto degli incidenti di cybersecurity, concentrandosi maggiormente sulla limitazione dell'impatto degli incidenti sugli utenti, piuttosto che sul fornitore di servizi stesso.

La NIS2 amplia l'ambito delle strategie nazionali che gli Stati membri devono adottare, passando dalla sicurezza delle reti e dei sistemi informativi alle strategie nazionali di sicurezza informatica. Come già osservato in precedenza, si tratta di un'estensione apprezzabile, in quanto richiede anche di prendere in considerazione la posizione dell'utente.

La direttiva NIS 2 prevede inoltre uno specifico apparato sanzionatorio, più severo e armonizzato a livello europeo, allo scopo di garantire una maggiore uniformità e deterrenza in tutta l'Ue, con sanzioni che arrivano fino a un massimo di almeno 10.000.000 di euro o di almeno il 2 per cento del fatturato totale annuo del soggetto.

Le differenze sono molte più, ma ci limitiamo a questi aspetti.

4. Il contesto nazionale ed il recepimento della NIS 2

Lo schema di decreto legislativo all'esame delle Camere è stato predisposto in forza della delega di cui all'articolo 1 della legge 21 febbraio 2024, n. 15 (Legge di delegazione europea 2022-2023) e nel rispetto dell'articolo 3 della stessa legge, che detta i principi e criteri specifici di delega, di cui si legge nell'Analisi di impatto della regolamentazione (AIR) allegata allo schema di decreto.

Successivamente a questa disciplina, il Governo italiano ha presentato un disegno di legge contenente "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", successivamente approvato e oggi divenuto la legge 28 giugno 2024, n. 90. Tale disciplina ha numerosi punti

di contatto con lo schema di decreto legislativo oggi all'esame delle commissioni riunite. Si tratta certamente di un importante passaggio, che rappresenta non l'anticipo ma il fattore abilitante, soprattutto per le pubbliche amministrazioni italiane, ai fini del pronto recepimento della disciplina NIS 2.

Lo schema di decreto legislativo, come si legge nella relazione illustrativa, è pienamente coerente anche con quanto previsto dalla legge n. 90/2024.

Lo schema odierno di decreto legislativo, di recepimento della direttiva NIS 2, si compone di 44 articoli, suddivisi in 6 capi. Il capo I (articoli da 1 a 8) è dedicato alle disposizioni generali e, al suo articolo 5, recepisce anche il capo V (Giurisdizione e registrazione) della direttiva NIS 2; il capo II (articoli da 9 a 17) è dedicato al quadro nazionale di sicurezza informatica e, al suo articolo 17, recepisce anche il capo VI (Condivisione delle informazioni) della direttiva NIS 2; il capo III (articoli da 18 a 22) riguarda la cooperazione a livello dell'Unione europea e internazionale e, al suo articolo 18 (Gruppo di cooperazione NIS), recepisce anche parte dei due articoli che compongono il capo VIII (Atti delegati e atti di esecuzione) della direttiva NIS 2; il capo IV (articoli da 23 a 33) è dedicato agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente e, al suo articolo 27 (Uso di schemi di certificazione della cibersicurezza), recepisce parte dei due articoli che compongono il capo VIII (Atti delegati e atti di esecuzione) della direttiva NIS 2; il capo V (articoli da 34 a 39) è invece dedicato alla supervisione e recepisce e razionalizza le disposizioni contenute al capo VII (Vigilanza ed esecuzione) della direttiva NIS 2; infine il capo VI (articoli da 40 a 44) riguarda le disposizioni finali e transitorie, recependo il capo IX (disposizioni finali) della direttiva NIS 2.

5. Spunti conclusivi e rilievi critici

Nell'esame dello schema si ravvisano sinteticamente e conclusivamente alcuni i **punti di forza** e di debolezza.

Il *primo* ed essenziale punto di forza è legato alla scelta italiana di recepire prontamente la direttiva NIS 2 senza indugio. Ciò testimonia certamente l'importanza che la tutela della sicurezza cibernetica ha acquisito negli ultimi anni.

Il *secondo* elemento di forza è legato alla consapevolezza che la resilienza cibernetica ha acquisito un valore che colloca tale disciplina al servizio e al centro dell'obiettivo di protezione dei diritti. La distinzione tra soggetti essenziali ed importanti è certamente più efficace e veritiera della precedente distinzione contenuta nella direttiva NIS e restituisce la necessità di una protezione integrata delle libertà incise dai servizi e dalle comunicazioni digitali.

Il *terzo* elemento di forza è connesso a una struttura di governance che adesso è molto più chiara e organizzata per garantire la tutela delle infrastrutture cibernetiche, le imprese, le pubbliche amministrazioni e gli utenti stessi.

Sui **punti di debolezza** il discorso odierno si fa più complicato. Proviamo a descrivere alcuni problemi di fondo o anche rilievi al testo.

Il *primo* problema generale che si ravvisa riguarda l'eccessiva aderenza del testo dello schema di decreto legislativo, soprattutto relativo al "Capo IV", contenente gli "Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente", agli articoli della direttiva. Il tema non è

certamente nuovo. Il problema del "recepimento fotocopia" deriva dallo stesso meccanismo di attuazione del diritto derivato in Italia, il quale spesso avviene con la mera riproposizione delle norme della direttiva, senza aprire agli spiragli che la disciplina europea di solito apre verso gli Stati membri.

Il *secondo* problema riguarda il fatto che il decreto legislativo, nell'essere troppo aderente al testo della direttiva e nel non aver implementato abbastanza alcuni aspetti amministrativi lasciati agli Stati membri, sembra viziato da qualche timidezza di fondo. La NIS 2 continua a non essere troppo incisiva in alcune questioni legate agli incidenti, per esempio. Bisognerà vedere se il suo approccio rinnovato porterà a risultati migliori rispetto al suo predecessore. Tanto il legislatore europeo quanto il legislatore italiano in fase di recepimento non vuole imporre obblighi più severi in materia di reporting e condivisione delle informazioni. Ci sarebbe stato bisogno di previsioni che stabilissero incentivi per garantirne l'effettiva adozione di tali pratiche.

Il *terzo* problema che viene in evidenza concerne il rapporto di queste norme con le altre in fase di recepimento o approvazione a livello europeo. Se, da un lato, è certamente positivo che la NIS 2 lasci spazio a una legislazione settoriale più mirata alle problematiche specifiche riscontrate in quel settore, dall'altro, è necessario assicurarsi che ciò non porti a una frammentazione in cui questioni simili riscontrate in diversi settori vengano trattate in modo diverso. La sfida è molto ingaggiante sul punto. In questo senso, risulterebbe necessario provare a cercare una via di coordinamento, semplificazione e collazione della normativa nazionale in vigore magari attraverso un impianto normativo che possa mettere insieme una disciplina che oramai è diventata molto fitta. In questo senso è palese già un problema di coordinamento con la legge n. 90/2024 che andrebbe coordinata con le nuove norme.

Il *quarto* problema che vorremmo portare alla vostra attenzione, riguarda la "Divulgazione coordinata delle vulnerabilità" (DCV) contenuta nell'art. 16 dello schema. Così previsto, questo articolo non coglie la grande possibilità che è fornita dalla NIS 2 di innovare sul punto, introducendo forme di prevenzione che potrebbero innalzare il livello di protezione verso le minacce cibernetiche. Tra queste vi è certamente l'hacking etico. Nei considerando nn. 58 e 60 della direttiva viene evidenziata l'importanza del contributo dell'hacking etico alla sicurezza cibernetica e, per questo motivo, viene incentivata la regolamentazione e la partecipazione di soggetti interessati, quali sviluppatori, aziende, ricercatori e attività. Tutto ciò non è previsto nel decreto legislativo di recepimento. In questo senso il legislatore italiano sembra aver rimandato ancora una volta la possibilità di creare una normativa *ad hoc* nella materia di DCV, distanziandosi da Paesi come il Belgio o la Francia che ormai da tempo hanno provveduto a stilare linee guida specifiche per le pratiche di ethical hacking, delineando anche un'apposita regolamentazione circa la responsabilità penale degli operatori. Il Belgio, ad esempio, con la legge denominata "Whistleblower Act" del 15 febbraio 2023 ha legalizzato l'hacking etico a prescindere dal consenso del proprietario del sistema informatico, a patto che i ricercatori etici di vulnerabilità rispettino determinate condizioni specificate dalla norma stessa, così da escludere qualsiasi tipo di responsabilità penale in capo all'operatore.

In tale senso, anche lo schema, come prima la legge n. 90/2024 avvalora implicitamente l'impostazione tipica del legislatore penale circa l'inasprimento sanzionatorio. Un approccio che mal si lega alla necessità di prevenire, piuttosto che reprimere, i fenomeni di *cybercrimes*. I motivi della preferenza per tale impostazione sono ravvisabili in diversi fattori: in primo luogo è necessario ricordare la natura transnazionale della cybersicurezza e, in secondo luogo, le difficoltà dettate dalle caratteristiche intrinseche dell'agire dei cyber-criminali che rendono la loro identificazione e persecuzione ardua

L'ultimo rilievo attiene alla costruzione dello CSIRT Italia contenuta nell'art. 15. Sul punto occorre avere chiaro che l'esistenza di uno CSIRT a livello nazionale è una esigenza incomprimibile. Tuttavia, è necessario creare una federazione di organismi che svolgono un ruolo simile allo CSIRT Italia, a livello regionale o macro-regionale, per garantire una maggiore resilienza contro minacce e attacchi cibernetici. Le due previsioni contenute nei commi 5 e 6 dell'art. 15, le quali rispettivamente prevedono che in caso di "eventi malevoli per la sicurezza informatica, le strutture pubbliche con funzione di computer emergency response team (CERT) collaborano con il CSIRT Italia, anche ai fini di un più efficace coordinamento della risposta agli incidenti" e che "(l)l CSIRT Italia instaura rapporti di cooperazione con i pertinenti portatori di interesse nazionali del settore privato al fine di perseguire gli obiettivi del presente decreto in relazione alle proprie competenze" dovrebbero essere cesellate meglio per garantire una filiera di comunicazione e di notifica più efficace. Questa ultima dovrebbe prevedere articolazioni locali dello CSIRT Italia, direttamente da esso controllate, che possano funzionare in maniera coordinata tra di esse.

Riferimenti a dottrina e documenti istituzionali

Baldini, Gianmarco, Josefa Barrero, Stephane Chaudron, Iwen Coisel, Gerard Draper Gil, Duch Brown Nestor, Olivier Eulaerts, Dimitrios Geneiatakis, Luis Hernandez Ramos, and Geraldine Joanny. 2020. Cybersecurity, our digital anchor. Luxembourg.

Biden, Joe. 2021. Executive Order on Improving the Nation's Cybersecurity. Washington.

Chiara, Pier Giorgio. 2022. "The IoT and the new EU cybersecurity regulatory landscape." *International Review of Law, Computers & Technology* 36 (2):118-137. doi: 10.1080/13600869.2022.2060468.

Chiara, Pier Giorgio. 2023. "Il "Cyber Resilience Act": la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali." *Riv. it. inf. dir.* (1):143-153.

Commissione. 2020. La strategia dell'UE in materia di cibersicurezza per il decennio digitale. Brussels.

Eckhardt, Philipp, and Anastasia Kotovskaia. 2023. "The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive." *International Cybersecurity Law Review* 4 (2):147-164. doi: 10.1365/s43439-023-00084-z.

ENISA. 2022. Threat Landscape for Ransomware Attacks.

ENISA. 2023. Threat Landscape 2023. Brussels.

Eurostat. 2020. ICT security measures taken by vast majority of enterprises in the EU.

Eurostat. 2023. 22% of EU enterprises had ICT security incidents.

Longo, Erik. 2024. La disciplina della cybersicurezza nell'Unione europea e in Italia. In *La regolazione europea della società digitale*. Torino: Giappichelli.

Meda, Kennedy. 2024. Identity theft is being fueled by AI & cyber-attacks. Accessed 3 May 2024.

Morgan, Steve. 2020. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Accessed 13 November 2020.

Vandezande, Niels. 2024. "Cybersecurity in the EU: How the NIS 2-directive stacks up against its predecessor." *Computer Law & Security Review* 52:105890.