Diritto e vulnerabilità - Studi e ricerche del CRID

Collana diretta da

Thomas Casadei e Gianfrancesco Zanetti

12

La collana "Diritto e vulnerabilità" è lo strumento del quale il Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità (CRID) dell'Università degli studi di Modena e Reggio Emilia, con sede presso il Dipartimento di Giurisprudenza, si è dotato per dare forma strutturata, in veste di pubblicazioni, ad alcuni studi e attività che costituiscono una parte integrante della sua *mission* – sono le promesse mantenute del Centro.

In essa trovano posto indagini teoriche e ricerche empiriche, ricostruzioni storiche e analisi istituzionali, nonché riflessioni e testimonianze della ricerca e del dibattito pubblico contemporanei, che hanno affrontato o affrontano vecchie e nuove configurazioni della discriminazione e della vulnerabilità.

È aperta a studiosi e studiose di ogni estrazione e di ogni orientamento dottrinale.

In copertina:
MARILENA TESEI, *Vele in libertà* (tecnica mista, 2023).

GIOVANI IN RETE

Guida per un uso consapevole delle tecnologie

a cura di
Thomas Casadei, Valeria Barone e Benedetta Rossi

G. Giappichelli Editore

ISBN/EAN 979-12-211-1551-2
ISBN/EAN 979-12-211-6419-0 (ebook)

I volumi pubblicati nella presente collana sono stati oggetto di procedura di doppio referaggio cieco (*double blind peer review*), secondo un procedimento concordato dai Direttori della collana con l'Editore, che ne conserva la relativa documentazione.

Volume finanziato nel quadro del progetto di ricerca "SAFELY - Social media Awareness For Education and Legal Youth" (PI. Prof. Thomas Casadei), realizzato mediante il Bando a Cascata emanato dall'ALMA MATER STUDIORUM – Università di Bologna in qualità di Spoke del Progetto SERICS – SEcurity and RIghts in the CyberSpace, Codice proposta: PE00000014, Finanziato dall'Unione Europea – NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano all'interno del PNRR – Missione 4 Componente 2, Investimento 1.3 "Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca" CUP: J33C22002810001.

Stampa: Rotolito S.p.A. - Pioltello (MI)

Indice

pag.

pag.

L'evoluzione del governo della cybersicurezza: un approccio olistico *

Pier Giorgio Chiara

Introduzione

Il progressivo processo di digitalizzazione ha ormai permeato le infrastrutture di ogni ambito della società: dalla sanità alla finanza, dalla gestione dei rifiuti alla formazione e alla ricerca. Tutti i settori del mercato, in aggiunta, fanno affidamento su reti, sistemi informativi e servizi informatici interconnessi ed interdipendenti [1]. Questo cambiamento paradigmatico ha portato con sé il mutamento del panorama delle minacce cibernetiche, sotto il profilo sia quantitativo sia qualitativo [2].

Gli impatti di attacchi informatici sempre più sofisticati, condotti da gruppi professionisti ed organizzati [3] – legati o meno a soggetti statuali – non sono *esclusivamente* riconducibili agli *asset* economici e finanziari delle imprese colpite, ma si estendono anche alla sfera dei diritti e delle libertà fondamentali degli individui (e.g., si pensi alla violazione dei dati personali), nonché dell'incolumità fisica [4],

* Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU.

[1] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013), pp. 2-3.

[2] L'Agenzia dell'Unione europea per la cybersicurezza (ENISA) pubblica ogni anno un report per approfondire lo stato dell'arte della minaccia informatica (*threat landscapes*): si veda ENISA, *ENISA Threat Landscape 2024*, 2024.

[3] M. SMEETS, *Ransom war: how cyber crime became a threat to national security*, Hurst & Co., London, 2025.

[4] C. MCGLAVE, H. NEPRASH, S. NIKPAY, *Hacked to pieces? The effects of ransomware attacks on hospitals and patients*, in "SSRN – Social Science Research Network", 2023.

fino alla paralisi – nei casi più estremi – dell'infrastruttura critica di un paese, intersecando quindi la sfera della sicurezza nazionale[5].

In questo contesto, il concetto di 'cybersicurezza', da questione prevalentemente tecnica, ha progressivamente acquisito rilievo sul piano strategico, sociale, politico e giuridico, a livello nazionale, sovranazionale (es, UE) e internazionale (es. ONU)[6].

Il presente contributo propone una ricognizione delle politiche e degli strumenti normativi adottati dall'Unione europea (§ 2) e dall'Italia (§ 3) in materia di cybersicurezza al fine di mostrare come tale ambito di *policy* sia evoluto nel corso degli ultimi tre decenni, progressivamente svincolandosi dai quadri normativi del diritto penale, della protezione dei dati personali e delle telecomunicazioni, cui è stato inizialmente ancorato[7]. La sezione conclusiva (§ 4) offre una chiave di lettura analitica per provare a comprendere il quadro di governo multi-livello (vale a dire sovranazionale e nazionale) della cybersicurezza in Europa che emerge dalle sezioni precedenti.

1. L'evoluzione del diritto della cybersicurezza nel diritto dell'Unione europea

Il tema della sicurezza informatica inizia ad avere rilevanza normativa nel corso degli anni '90 del Novecento. La gestione delle reti e dei sistemi informativi è interessata da tre grandi cambiamenti paradigmatici caratterizzanti l'inizio del terzo millennio, quali la globalizzazione, la liberalizzazione dei mercati e, più precipuamente per il contesto in esame, la convergenza: una larga parte delle reti di comunicazione è sempre più interconnessa (condivide, cioè, servizi e infrastrutture), transfrontaliera nonché gestita da soggetti privati multinazionali. La sicurezza pertanto diventa un aspetto dell'offerta del mercato.

Questi fenomeni, unitamente all'aumento della minaccia cibernetica – per sua natura transnazionale – hanno reso manifesta l'inefficacia di una risposta normativa sul piano nazionale, spingendo l'allora Comunità europea a pensare ad un quadro normativo unitario per la sicurezza delle reti e dell'informazione,

[5] Si pensi ai massicci attacchi coordinati subiti dall'Estonia nel 2007 o dalla Costa Rica nel 2022.

[6] Per un'accurata panoramica dei livelli e delle questioni in gioco si rinvia a R. BRIGHI, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in TH. CASADEI, S. PIETROPAOLI, *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 75-87. Si vedano anche R. BRIGHI, P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in "Federalismi.it", 21, 2021, pp. 18-42; R. BRIGHI, *Cybersicurezza e Intelligenza Artificiale. Un'analisi critica*, in "BioLaw Journal", 1, 2024, pp. 111-124, https://teseo.unitn.it/biolaw/article/view/3327.

[7] COMMISSIONE EUROPEA, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM(2001).

superando così la frammentazione delle misure di sicurezza tra diversi quadri normativi, in particolare in materia di telecomunicazioni, protezione dei dati personali e contrasto al crimine informatico [8].

Se nel 2004 viene creata l'Agenzia europea per la cybersicurezza (ENISA), è solo nel 2013 che l'Unione si dota di una Strategia per la cybersicurezza. Così, la 'cybersicurezza' diventa una politica dell'UE e il termine "cybersicurezza" diventa ufficialmente parte del linguaggio giuridico ed istituzionale del diritto dell'Unione.

La Strategia delinea un quadro articolato di strumenti giuridici e di investimenti adottando un approccio *multi-stakeholder*, che sappia, cioè, coordinare efficacemente le risposte di tutti gli attori coinvolti: istituzioni UE; Stati membri; operatori del settore privato. In particolare, vengono identificate cinque priorità strategiche: 1) raggiungere la cyber resilienza; 2) consolidare il contrasto al cybercrimine; 3) sviluppare una politica e delle capacità di cyberdifesa; 4) sviluppare risorse industriali e tecnologiche per la cybersicurezza; 5) creare una politica internazionale dell'UE sul cyberspazio.

La misura principale volta ad implementare la Strategia, nell'ambito della prima area d'azione, è la Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS – da *Network and Information Systems*), considerata il primo atto giuridico dell'Unione sulla cybersicurezza in senso stretto [9].

Al fine di rafforzare la cyber resilienza [10] delle reti e dei sistemi informativi nell'Unione, la Direttiva NIS ha imposto agli Stati di dotarsi di una strategia nazionale in materia NIS, nonché di designare autorità nazionali competenti, punti di contatto unici e gruppi di intervento per la sicurezza informatica in caso di incidente ('CSIRT'). Sul piano della governance unionale, al fine di promuovere la cooperazione strategica e lo scambio di informazioni tra Stati membri, la Direttiva ha istituito un gruppo di cooperazione composto da rappresentanti degli Stati, della Commissione e dell'ENISA, nonché una rete pan-europea dei CSIRT degli Stati membri, il segretariato della quale è stato affidato all'ENISA. In secondo luogo, la Direttiva ha individuato due categorie di soggetti, vale a dire, gli operatori di servizi essenziali [11] e i fornitori di servizi digitali [12], quali destinatari

[8] COMMISSIONE EUROPEA, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM(2001), pp. 20-21.

[9] Considerando 15, Regolamento (UE) 2019/881.

[10] Per quanto riguarda la non semplice demarcazione semantica, nonché giuridica, tra i concetti di 'cyber resilienza' e 'cybersicurezza', si permetta di rimandare a P.G. CHIARA, R. BRIGHI, *La dimensione della "resilienza" nel diritto UE della cybersicurezza*, in "Ragion Pratica", 2, 2024, pp. 405-426.

[11] Questi operatori sarebbero stati identificati dagli Stati membri tra i soggetti eroganti servizi essenziali per il mantenimento di attività sociali ed economiche fondamentali in sette settori, a condizione che rispettassero determinati requisiti.

[12] L'allegato III della Direttiva ha direttamente identificato i fornitori che sarebbero stati

di obblighi di adozione di misure di sicurezza [13] e di notifica degli incidenti [14].

Solamente un anno dopo l'adozione della Direttiva NIS, la Commissione e l'Alto Rappresentante dell'Unione hanno adottato una nuova Strategia per la cybersicurezza [15]. Sono stati principalmente due i fattori catalizzatori dell'aggiornamento della relativamente recente politica dell'Unione in materia: la rapida diffusione nel mercato interno delle tecnologie digitali e la conseguente amplificazione della minaccia, nonché dell'impatto degli incidenti, soprattutto alla luce di prodotti digitali insicuri. L'impianto della Strategia, comunque, non si discosta sostanzialmente da quello tracciato nel 2013. Da una parte, si richiama con forza la necessità di un approccio *multi-stakeholder*: la cybersicurezza viene rappresentata sempre di più come una sfida comune dal momento che ad essere minacciato non è solo il mercato unico digitale, ma anche "il funzionamento stesso delle nostre democrazie, le nostre libertà e i nostri valori" [16]. Dall'altra, le cinque aree strategiche della Strategia del 2013 vengono accorpate in tre macro-filoni di intervento: i) rafforzamento della cyber resilienza; ii) creazione di una cyber deterrenza a livello UE efficace; e iii) rafforzamento della cooperazione internazionale sulla cybersicurezza [17].

Gli sforzi legislativi sono volti soprattutto ad implementare le misure individuate nel primo filone. In particolare, il Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*) si propone di raggiungere due obiettivi strategici: 1) consolidare il ruolo dell'ENISA, attraverso un mandato permanente [18]; 2) creare un quadro di certificazione della cybersicurezza a livello UE per sostenere la crescita del mercato unico della cybersicurezza.

La prima parte del Regolamento riforma l'ENISA. Tra le nuove funzioni ed obiettivi dell'Agenzia rientrano: l'assistenza allo sviluppo e attuazione delle politiche dell'Unione in materia di cybersicurezza; il sostegno allo sviluppo delle capacità

ricompresi in questa categoria: fornitori di i) mercati online, ii) motori di ricerca online e iii) cloud computing.

[13] Operatori e fornitori adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni (art. 14, par. 1, Direttiva NIS1) e nel contesto dell'offerta di servizi (art. 16, par. 1, Direttiva NIS1).

[14] Operatori e fornitori notificano senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla continuità dei servizi essenziali prestati (art. 14, par. 3, Direttiva NIS1) e sulla fornitura di un servizio (art. 16, par. 3, Direttiva NIS1).

[15] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017), 450 final.

[16] *Ibidem*, p. 2.

[17] Su questi profili: R. BRIGHI, P.G. CHIARA, *La dimensione della "resilienza" nel diritto UE della cybersicurezza*, in "Ragion pratica", 2024, 2, pp. 405-426.

[18] Dal 2004, anno di istituzione, il mandato è stato prorogato con regolamenti per tre volte, nel 2008, nel 2011 e infine nel 2013.

cyber nell'Unione; la promozione della cooperazione a livello UE, compresa la condivisione delle informazioni; l'aumento delle capacità di cybersicurezza comune per prevenire e rispondere alle minacce; il contribuire alla creazione e al mantenimento della certificazione europea di cibersicurezza e la promozione di un elevato livello di consapevolezza in materia di cibersicurezza, aspetto quest'ultimo che chiama anche in causa anche la formazione delle nuove generazioni.

La seconda parte del Cybersecurity Act introduce il quadro europeo di certificazione della cybersicurezza, con l'obiettivo di garantire un livello adeguato di sicurezza dei prodotti, servizi e processi TIC nell'Unione, di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione in materia, nonché di rafforzare la fiducia dei consumatori.

Inoltre, il Cybersecurity Act è il primo atto giuridico dell'UE che definisce formalmente 'cybersicurezza', quale "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, *gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche* [enfasi aggiunta]" (art. 2, par. 1).

Nel dicembre 2020, Commissione e Alto Rappresentante pubblicano la terza, ed ultima (per ora), Strategia dell'Unione per la cybersicurezza[19]. Le tre aree di intervento in cui vengono proposte azioni e misure a livello normativo, di investimento e politico ricalcano ad un alto livello quelle già identificate nei documenti del 2013 e 2017: i) resilienza, sovranità tecnologica e leadership; ii) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta; e, iii) promozione di un ciberspazio globale e aperto.

In particolare, nell'ambito della prima area, vengono inquadrate diverse proposte sul piano legislativo, ad iniziare dal disegno di revisione della direttiva NIS, che porta alla Direttiva (UE) 2022/2555 (Direttiva NIS2).

La Direttiva NIS2 mira a risolvere diverse criticità emerse nella valutazione sul funzionamento della NIS1[20]. Innanzitutto, l'ambito di applicazione viene notevolmente ampliato. La distinzione tra operatori di servizi essenziali e fornitori di servizi digitali è sostituita dalla classificazione tra soggetti 'essenziali' ed 'importanti', che tiene conto del livello di criticità del settore o del tipo di servizio fornito, nonché del livello di dipendenza da altri settori o servizi. Inoltre, per superare le divergenze tra gli Stati circa l'identificazione degli operatori, la NIS2 introduce un criterio quantitativo: la direttiva si applica a tutte le medie e grandi imprese[21] che operano nei settori individuati dagli Allegati I (settori ad alta criticità) e II (altri settori critici).

[19] COMMISSIONE EUROPEA e ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020), 18 final.

[20] COMMISSIONE EUROPEA, *Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148*, COM(2020) 823 final, p. 4.

[21] Sono previste poi eccezioni per le quali a determinati soggetti, indipendentemente dalle loro dimensioni, si applicherà la direttiva.

Per quanto riguarda i quadri di misure di gestione del rischio di cybersicurezza, tutti i soggetti a cui si applica la NIS2 devono adottare delle misure tecniche, operative e organizzative adeguate e proporzionate ai rischi[22], contenute in un elenco minimo, non esaustivo, a differenza della precedente Direttiva che rimetteva l'intero processo di identificazione delle misure agli Stati membri e alla discrezione dei soggetti[23]. Anche i nuovi obblighi di notifica degli incidenti risultano più dettagliati. Da un punto di vista procedurale, il processo di notifica è suddiviso in fasi progressive con termini diversi: i soggetti comunicano all'autorità nazionale gli incidenti 'significativi' entro 24 ore dal momento in cui vengono a conoscenza dell'incidente (c.d. preallarme); quindi effettuano una notifica completa entro 72 ore, aggiornata con relazioni intermedie solo se richiesto dell'autorità; infine, producono una relazione finale entro un mese dalla notifica. Sotto altro profilo, un nuovo obbligo consiste nella comunicazione da parte dei soggetti NIS ai destinatari dei loro servizi potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o rimedio in risposta a tale minaccia[24], a testimonianza dell'approccio maggiormente proattivo della NIS2 al contrasto della minaccia informatica.

Sul piano della governance, la NIS2 rafforza le istituzioni e i meccanismi della precedente direttiva attraverso, ad esempio, l'indicazione di alcune misure strategiche che gli Stati devono includere nelle Strategie di cybersicurezza, oppure attraverso nuovi obblighi (es., dotarsi di quadri nazionali di gestione delle crisi cyber su vasta scala) o nuovi forum di cooperazione (la rete europea EU-CyCLONe per una gestione coordinata delle crisi di cybersicurezza su vasta scala). Inoltre, la NIS2 prevede la possibilità di attivare delle procedure di condivisione delle informazioni rilevanti (es., tecniche di attacco; misure di mitigazione; etc.) attraverso accordi di natura volontaria. Per rendere efficace l'esecuzione, la NIS2, a differenza della NIS1, stabilisce un elenco minimo di misure nonché sanzioni amministrative pecuniarie – stabilendo dei massimi seguendo l'approccio già delineato dal GDPR[25], tenendo conto di determinati fattori soggettivi e oggettivi.

Nel dicembre 2020, la Commissione presenta la proposta per la direttiva NIS2 insieme con la proposta per una direttiva sulla resilienza dei soggetti critici (*critical*

[22] Questo evidenzia come anche la Direttiva NIS2 si basi sul c.d. "approccio al rischio", coerentemente con la recente legislazione UE in materia digitale, si veda *ex multis* G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in "Common Market Law Review", 59, 2, 2022, pp. 473-500. Cfr., inoltre, nel dibattito giusfilosofico italiano: M. Buffa, *La Direttiva Nis II Cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in "Democrazia e diritti sociali", 1, 2023, pp. 47-64.

[23] Artt. 21 e 22, Direttiva NIS2. Queste includono, ad esempio, politiche di analisi dei rischi; gestione degli incidenti; continuità operativa (come la gestione del backup e il ripristino in caso di disastro) e gestione delle crisi; sicurezza della catena di approvvigionamento, ecc.

[24] Art. 23, par. 2, Direttiva NIS2.

[25] V. Papakonstantinou, P. De Hert, *The Regulation of Digital Technologies in the EU: Actification, GDPR Mimesis and EU Law Brutality at Play*, Routledge, London, 2024.

entities resilience, CER), poi pubblicata in G.U. dell'Unione come Direttiva (UE) 2022/2557. La direttiva CER stabilisce obblighi per gli Stati membri e i soggetti critici volti a rafforzare la loro resilienza e la loro capacità di fornire servizi essenziali per il mantenimento di funzioni vitali della società o di attività economiche. Tuttavia, occorre sottolineare come tale direttiva non si applichi alla materia disciplinata dalla NIS2, e cioè la cybersicurezza [26]; piuttosto, la CER insiste sulla resilienza *fisica* e non *digitale* dell'infrastruttura critica. In tal senso, il legislatore europeo prevede un'attuazione coordinata e complementare dei due strumenti.

Il Regolamento (UE) 2022/2554, c.d. Regolamento DORA (*digital operational resilience act*), completa il 'pacchetto' delle normative pubblicate in G.U. dell'UE nel dicembre 2022 (NIS2, CER e DORA). Rispetto alla NIS2, il regolamento DORA è un atto giuridico settoriale, dal momento che mira ad armonizzare gli obblighi in materia di 'resilienza operativa digitale' per i soggetti del settore finanziario [27]. In breve, gli obblighi e i requisiti posti dal regolamento DORA poggiano su cinque pilastri che, nel complesso, chiariscono la modalità di declinazione del c.d. 'approccio al rischio' da parte del Regolamento: i) gestione dei rischi informatici; ii) gestione, classificazione e segnalazione degli incidenti informatici; iii) test di resilienza operativa digitale; iv) gestione dei rischi informatici derivanti da terzi; v) meccanismi di condivisione delle informazioni.

Con il 'pacchetto' di normative di cybersicurezza del 2022, la Commissione ha provato ad aumentare la cybersicurezza del mercato dei servizi. Di converso, al fine di incentivare la sicurezza dei prodotti, la Commissione annunciava già nella Strategia del 2020 nuove possibili norme orizzontali in materia di cybersicurezza per i prodotti connessi [28], parallelamente ovviamente all'implementazione del quadro di certificazione della cybersicurezza. Proposto dalla Commissione il 15 settembre 2022, il 'regolamento sulla ciberresilienza' (*Cyber Resilience Act*, CRA) [29] entra in vigore nel dicembre 2024 come Regolamento (UE) 2024/2847.

L'ambito di applicazione del CRA è particolarmente esteso, dal momento che si applica ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete. In linea con i principi e gli istituti della legislazione armonizzata in materia di sicurezza dei prodotti [30], un prodotto che rientri nell'ambito di applicazione del CRA può essere

[26] Art. 1, par. 2, Direttiva CER.

[27] Considerando 28, Direttiva NIS2; Considerando 16, Regolamento DORA.

[28] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, n. 38, p. 10.

[29] COMMISSIONE EUROPEA, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il Regolamento (UE) 2019/1020*, 2022/0272(COD).

[30] COMMISSIONE EUROPEA, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 2022/C 247/01.

messo a disposizione sul mercato dal fabbricante, nel corso di un'attività commerciale, a condizione che soddisfi i requisiti essenziali di cui all'allegato I, parte I e II [31]. Il fabbricante dimostra che il prodotto rispetta i requisiti essenziali attraverso una procedura di valutazione della conformità, condotta dal fabbricante stesso o da terze parti a seconda del livello del rischio di cybersicurezza del prodotto.

L'ultimo regolamento adottato nel campo della cybersicurezza è il c.d. *Cyber Solidarity Act, CSoA* (Regolamento (UE) 2025/38), dopo essere stato annunciato nella comunicazione congiunta della Commissione e dell'Alto Rappresentante sulla politica di cyberdifesa nel novembre 2022. Il CSoA punta, da una parte, a migliorare il rilevamento e la conoscenza situazionale delle minacce e degli incidenti cyber nell'Unione e, dall'altra, ad intensificare la solidarietà tra gli Stati membri nella gestione degli incidenti di cybersicurezza significativi e su vasta scala. A tal fine, viene istituito il 'sistema europeo di allerta per la cybersicurezza' – costituito da una rete paneuropea di poli informatici per sviluppare le capacità degli Stati di rilevamento della minaccia in modo coordinato. Evidentemente, il sistema dovrà integrarsi senza sovrapposizioni alle azioni svolte dai gruppi introdotti dalla direttiva NIS2: la rete di CSIRTs; EU-CyCLONe; gruppo di cooperazione NIS. Il secondo pilastro del CSoA è costituito dal 'meccanismo per le emergenze della cybersicurezza' per sostenere gli Stati membri, dietro loro richiesta, nella gestione di incidenti significativi e su vasta scala attraverso una 'riserva per la cybersicurezza' a livello UE, costituita da prestatori di servizi cyber di fiducia. Infine, viene istituito un 'meccanismo europeo di riesame degli incidenti di cybersicurezza' per valutare specifici incidenti, attraverso il coinvolgimento dell'ENISA, traendo con ciò insegnamenti utili nell'ottica dell'accrescimento della cyber resilienza a livello unionale.

2. … e nel diritto interno

Come si è visto, la cybersicurezza "evoca un ambito di intervento piuttosto ampio, multilivello e trasversale" [32]: oggetto di protezione non sono solamente le reti e i sistemi informativi di soggetti privati, e quindi prodotti e servizi disponibili sul mercato unico – oggetto della legislazione armonizzata dell'Unione europea – ma anche le persone fisiche e i loro diritti fondamentali nonché le infrastrutture critiche del Paese [33]. Pertanto, una dimensione rilevante della cybersicurezza coincide con gli interessi statuali di tutela della sicurezza nazionale. Non a caso, la

[31] Art. 6, CRA.

[32] T. Giupponi, *Il governo nazionale della cybersicurezza*, in "Quaderni costituzionali", 2, 2024, 280, pp. 277-303.

[33] E. Longo, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna Parlamentare", 2, 2024, pp. 313-314.

normativa italiana in materia di cybersicurezza è inizialmente legata al Sistema di informazione per la sicurezza della Repubblica. Infatti, la legge 133/2012 attribuisce al Presidente del Consiglio dei Ministri il compito di impartire al Dipartimento delle informazioni per la sicurezza (DIS) e al comparto *intelligence* direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche, con particolare riguardo alla protezione cibernetica [34].

Tuttavia, è solo con il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) [35] del 2019 che l'Italia si dota di un impianto normativo autonomo e coordinato per "assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale" [36]. L'individuazione dei soggetti inclusi nel PSNC, ad opera delle amministrazioni dello Stato nell'ambito di rispettiva competenza [37], avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare da eventi avversi ai beni di rispettiva pertinenza oggetto di conferimento nel 'perimetro' (vale a dire, reti, sistemi informativi e servizi informatici) [38]. L'elenco dei soggetti 'perimetrati', contenuto in un atto amministrativo adottato dal Presidente del Consiglio dei Ministri, è segreto, non essendo soggetto a pubblicazione ed essendo escluso dall'ambito del diritto di accesso [39].

I soggetti inclusi nel PSNC hanno diversi obblighi, individuati dal d.l. 105/2019 e specificati, soprattutto sul piano procedurale, da successivi decreti attuativi. In primo luogo, sono tenuti a predisporre ed aggiornare annualmente l'elenco dei beni di rispettiva pertinenza ritenuti "strategici" per la fornitura dei servizi o delle funzioni essenziali [40]. Quindi, con riferimento a tali beni, i soggetti devono adottare misure tecniche e organizzative nell'ottica di assicurare elevati livelli di sicurezza [41]

[34] Art. 1, comma 3-*bis*, della legge 124/2007 introdotto dalla legge 133/2012.

[35] Istituito attraverso il d.l. 105/2019, convertito nella legge 133/2019.

[36] Art. 1, comma 1, d.l. 105/2019.

[37] Per il settore governativo provvedono le amministrazioni CISR; per il settore interno, il Ministero dell'interno; per il settore difesa, il Ministero della difesa; per il settore spazio e aerospazio, la Presidenza del Consiglio dei ministri; per i settori energia, telecomunicazioni e servizi digitali, il Ministero dello sviluppo economico; per il settore economia e finanza, il Ministero dell'economia e delle finanze; per il settore trasporti, il Ministero delle infrastrutture e dei trasporti; per il settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e per il settore enti previdenziali/lavoro, il Ministero del lavoro e delle politiche sociali.

[38] Art. 1, comma 2, lett. a, punto 2-*bis*, d.l. 105/2019; si veda anche l'art. 3, d.p.c.m. 131/2020.

[39] Art.1, comma 2-*bis*, d.l. 105/2019.

[40] Art. 1, comma 2, lett. b, d.l. 105/2019; art. 7 d.p.c.m. 131/2020.

[41] Art. 1, comma 3, lett. b, d.l. 105/2019. L'allegato B del d.p.c.m. 81/2021 individua una

e notificare eventuali incidenti al CSIRT Italia presso l'Agenzia per la Cybersicurezza Nazionale (ACN) [42]. I soggetti 'perimetrati' sono altresì tenuti a comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN), altra articolazione di ACN, l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sulle proprie reti, sistemi informativi e per l'espletamento dei servizi informatici [43].

Il legislatore è poi intervenuto nuovamente nel 2021 con un decreto-legge che ha riformato significativamente la governance nazionale della cybersicurezza. Il d.l. 82/2021, infatti, istituendo l'Agenzia per la Cybersicurezza Nazionale [44], ridisegna completamente l'assetto delle autorità aventi poteri e funzioni in materia. Aderente ad un modello di 'governance centralizzata', il d.l. 82/2021 attribuisce ad ACN le funzioni in materia di cybersicurezza che prima erano suddivise tra vari regolatori, quali Presidenza del Consiglio del Ministri [45], Dipartimento delle Informazioni per la Sicurezza (DIS), Ministero per lo Sviluppo Economico, Agenzia per l'Italia Digitale (AgID), soprattutto per quanto riguarda l'attuazione del PSNC.

ACN diventa autorità nazionale competente e punto di contatto unico ai fini della direttiva NIS, nonché autorità nazionale di certificazione della cybersicurezza ai sensi del Cybersecurity Act e centro nazionale di coordinamento ai sensi del Regolamento (UE) 2021/887 che istituisce lo *European Cybersecurity Competence Centre*. Presso l'Agenzia viene trasferito il 'CSIRT Italia' e vengono costituiti il Centro per la Valutazione e Certificazione Nazionale (CVCN) e il Nucleo per la cybersicurezza. Quest'ultimo, in particolare, è una struttura a supporto del Presidente del Consiglio dei Ministri per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi; è presieduto dal direttore generale di ACN e alle riunioni vi partecipano rappresentanti del DIS, delle agenzie di intelligence, dei Ministeri rappresentati nel Comitato Interministeriale per la Cybersicurezza (CIC) [46] e del dipartimento della protezione civile.

tassonomia di misure e controlli tecnici di sicurezza, suddivisi in funzioni, categorie e sotto-categorie. In linea con un approccio basato sul rischio, il d.p.c.m. distingue le misure in due classi (categoria A e B): i termini per l'adozione della misura da parte dei soggetti variano a seconda della classe di appartenenza della specifica misura (6 mesi dalla trasmissione degli elenchi degli asset per la categoria A e 30 mesi per la categoria B).

[42] Art. 1, comma 3, lett. a, d.l. 105/2019. L'allegato A del d.p.c.m. 81/2021 classifica gli incidenti in due categorie. Quelli di cui alla tabella 1, meno gravi, devono essere notificati al CSIRT Italia entro 6 ore dal momento in cui un soggetto viene a conoscenza dell'evento. Invece, gli incidenti di cui alla tabella 2, più gravi, devono essere comunicati entro 1 ora.

[43] Art. 1, comma 6, d.l. 105/2019. Si veda sul punto la disciplina dettata dal d.P.R. 54/2021 e dal d.p.c.m. 15 giugno 2021.

[44] ACN opera quale ente governativo di diritto pubblico con autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

[45] Fatto salvo il compito di individuare i soggetti inclusi nel PSNC.

[46] Incardinato presso la Presidenza del Consiglio dei Ministri, ha funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Il Comitato è presieduto dal Presidente del

Tra i compiti assegnati all'Agenzia, particolarmente importante è la predisposizione della Strategia nazionale di cybersicurezza, adottata dal Presidente del Consiglio e sull'attuazione della quale sorveglia il CIC. Inoltre, ACN sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta per la prevenzione e gestione degli incidenti; promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza (es., attraverso pareri non vincolanti su iniziative legislative o regolamentari); può costituire e partecipare a partenariati pubblico-privato (PPP); promuove lo sviluppo e la diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici.

Infine, con un nuovo intervento normativo (legge 28 giugno 2024, n. 90), il legislatore introduce, da una parte, disposizioni in materia di cyber resilienza per una serie di soggetti inizialmente esclusi dall'ambito di applicazione del PSNC[47] (e della direttiva NIS1 – non necessariamente dalla NIS2) e, dall'altra, apporta alcune modifiche alla disciplina del PSNC. Anche a tali nuovi soggetti viene esteso l'obbligo di notificare gli incidenti che impattano le reti, i sistemi informativi e i servizi informatici secondo i termini e le modalità già introdotti dalla Direttiva NIS2: l'incidente va segnalato all'autorità entro 24 ore dal momento in cui i soggetti ne vengono a conoscenza, mentre entro 72 ore deve essere prodotta una notifica completa. In aggiunta, questi soggetti devono individuare una struttura, anche esistente, che provveda allo sviluppo delle politiche ed espletamento delle funzioni in ambito cyber ed entro la quale è chiamata ad operare una nuova figura, il 'referente per la cybersicurezza', che *inter alia* svolge la funzione di punto di contatto unico con ACN.

Per altro verso, come detto, la legge 90/2024 modifica diversi atti giuridici esistenti in materia, segnatamente la disciplina PSNC. In particolare, introduce due obblighi '*erga omnes*' (vale a dire, per i soggetti PSNC, i soggetti identificati dalla legge 90/2024, i soggetti di cui ai decreti di recepimento della direttiva NIS1 e del codice delle comunicazioni elettroniche): i) provvedere entro 15 giorni dalla comunicazione dell'adozione degli interventi indicati da ACN circa specifiche vulnerabilità cui tali attori risultino potenzialmente esposti; ii) verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso non comportino vulnerabilità note e, nel caso in cui utilizzino soluzioni crittografiche,

Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili.

[47] Questi sono le pubbliche amministrazioni centrali; le regioni e le province autonome di Trento e Bolzano; le città metropolitane; comuni con popolazione superiore a 100.000 abitanti e capoluoghi di regione; società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti; società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali.

che rispettino le linee guida sulla crittografia e quelle sulla conservazione delle password adottate da ACN e dal Garante per la protezione dei dati personali. Viene poi introdotta una disciplina dei contratti pubblici di beni e servizi informatici in un contesto connesso a tutela interessi nazionali strategici. Infine, il Capo II della legge 90/2024 introduce modifiche al codice penale e di procedura penale per la prevenzione e il contrasto dei reati informatici [48].

Alcune riflessioni conclusive

Ancorché le prime riflessioni a livello sovranazionale sulla necessità di adottare un quadro giuridico che introducesse obblighi e misure per migliorare la sicurezza delle reti e dei sistemi informativi fossero risalenti al 2001 [49], è solo nel 2013, con la prima Strategia UE sulla cybersicurezza e la proposta per la direttiva NIS – come evidenziato, primo atto giuridico dell'Unione in materia di cybersicurezza – che la cybersicurezza acquista un rilievo politico, giuridico e sociale, cessando pertanto di essere una questione di natura esclusivamente tecnica.

Se da una parte il percorso di questa nuova politica dell'Unione ha visto un rapido sviluppo, grazie soprattutto alle tre Strategie UE, nel contesto delle quali sono state adottate diverse misure regolamentari volte ad implementare gli obiettivi strategici dell'Unione, dall'altra non è stato privo di ostacoli. Infatti, nel 2004 il Regno Unito faceva ricorso innanzi alla Corte di Giustizia dell'Unione europea chiedendo l'annullamento del regolamento (CE) del Parlamento europeo e del Consiglio 10 marzo 2004, n. 460, che istituiva l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) [50]. In particolare, il Regno Unito sosteneva che l'art. 95 CE non fornisse un fondamento normativo adeguato all'adozione di

[48] Tale inasprimento della risposta repressiva è stato criticato da più parti in dottrina in quanto poco efficace nello specifico contesto della cybersicurezza, caratterizzato da sfide peculiari rispetto a quelle che caratterizzano la dimensione analogica (es., la transnazionalità della minaccia; la difficoltà nell'individuazione dei responsabili di condotte criminose; il riconoscimento del potere esercitato da attori privati; ecc.). Si permetta di rimandare, *ex multis*, a P.G. CHIARA, *DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2*, in "Rivista Italiana di Informatica e Diritto", 1, 2024, pp. 31-34, p. 32. Cfr. S. PIETROPAOLI, *Un'occasione (forse) mancata. Considerazioni sulla revisione dei reati informatici proposta con il DDL Cybersicurezza*, in "Rivista Italiana di Informatica e Diritto", 1, 2024, pp. 47-53; E. LONGO, *Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717): Camera dei Deputati, Commissioni riunite I e II – Roma, 28 marzo 2024*, in "Rivista Italiana di Informatica e Diritto", 1, 2024, pp. 65-70, p. 67.

[49] COMMISSIONE EUROPEA, *op. cit.*

[50] Causa C-217/04, Regno Unito di Gran Bretagna e Irlanda del Nord vs. Parlamento europeo e Consiglio dell'Unione europea, Sentenza della Corte (Grande Sezione) del 2 maggio 2006, ECLI:EU:C:2006:279.

tale regolamento. La Corte di Giustizia respingeva però tale ricorso, constatando come l'istituzione dell'ENISA nonché gli obiettivi e compiti assegnatile dal regolamento potessero qualificarsi come «misure relative al ravvicinamento» ai sensi dell'art. 95 CE (§§ 60-64).

Più in generale, l'azione mossa dal Regno Unito è da inquadrarsi in un clima di diffusa avversione tra i regolatori nazionali nei confronti della percepita aspirazione dell'Unione europea di diventare un "super-regolatore" – per il tramite di un'Agenzia comunitaria – nel settore delle telecomunicazioni e, segnatamente con riferimento alle delicate questioni di sicurezza. Come brillantemente riassunto da Dunn Cavelty e Smeets, in questa fase non si trattava tanto del tipo di sicurezza che l'ENISA doveva fornire, né sul tipo di strumenti politici da adottare, quanto più sui timori che una siffatta agenzia potesse erodere i poteri nazionali a favore di competenze sovranazionali [51].

Gli Stati membri hanno inizialmente avvertito lo sviluppo delle norme armonizzate a livello UE come una potenziale minaccia alla propria sovranità nazionale [52], dal momento che le misure adottate a livello sovranazionale inevitabilmente intersecano con l'ambito della tutela degli interessi legati alla sicurezza nazionale (come peraltro dimostrato dalla normativa italiana che disciplina il PSNC), competenza esclusiva degli Stati membri ai sensi dell'art. 4(2) TUE [53]. La difficile ricomposizione delle 'tensioni' sulla competenza tra le istituzioni dell'UE e gli Stati membri sul governo della cybersicurezza, che ha segnato le origini delle politiche comunitarie in materia, è ancora presente, ancorché a diverso livello di intensità.

Così, i principali atti giuridici adottati a livello UE, richiamati nella sezione 2, adottano come fondamento normativo l'art. 114 TFUE relativo al ravvicinamento delle disposizioni legislative nazionali per il corretto funzionamento del mercato interno, in mancanza di una esplicita competenza dell'UE nei Trattati in osservanza del principio di attribuzione *ex* art. 5 TUE [54].

La prima evoluzione significativa del concetto normativo di cybersicurezza è da ricercarsi tra la Direttiva NIS del 2016 e il Cybersecurity Act del 2019. Se

[51] M. Dunn Cavelty, M. Smeets, *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority*, in "Journal of European Public Policy", 30, 7, 2023, pp. 1330-1352, p. 1338.

[52] Su questo aspetto si può vedere, per uno sguardo di taglio geo-politico, A. D'Attorre, *La sovranità digitale. Poteri privati, intervento pubblico e diritti individuali nel cyberspazio*, in Th. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, cit., pp. 313-324.

[53] L.A. Bygrave, *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes*, in "Computer Law & Security Review", 56, 2025, pp. 1-8, p. 4.

[54] Si vedano, *ex multis*, S. Schmitz-Berndt, M.D. Cole, *Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act*, in "Applied Cybersecurity & Internet Governance", 1, 1, 2022, pp. 1-17, p. 122; G. González Fuster, L. Jasmontaite, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. Christen, B. Gordijn, M. Loi (eds.) *The Ethics of Cybersecurity*, Springer, Cham, 2020, p. 98.

infatti la Strategia del 2013 e la Direttiva NIS erano ancora fermamente ancorate al concetto di 'sicurezza delle reti e dei sistemi informativi' [55] risalente all'inizio degli anni 2000, la Strategia del 2017, e segnatamente il Cybersecurity Act, ossia la misura regolamentare più significativa che implementa quest'ultima, segnano lo scarto con il passato introducendo nel diritto dell'Unione il concetto di 'cybersicurezza' allargandone contestualmente, in modo significativo, il suo perimetro operativo e concettuale. La concettualizzazione di cybersicurezza nel diritto dell'Unione ricomprende non solo l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, secondo il paradigma classico della prima governance UE della cybersicurezza, ma anche "gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche" [56].

In contesti socio-tecnici sempre più complessi di interazione tra persone, dispositivi con elementi digitali e servizi dell'informazione automatizzati, anche grazie all'integrazione di sistemi di intelligenza artificiale, un alto grado di cybersicurezza richiede un *approccio olistico* secondo nuove forme coordinate di gestione del rischio che contemplino la protezione dei diversi valori in gioco, nonché di tutti gli attori coinvolti [57].

Gli obiettivi di protezione pertanto non sono più confinati esclusivamente alle reti, ai sistemi informativi e ai servizi informatici, facenti o meno parte delle infrastrutture critiche degli Stati, ma si estendono agli individui (comprese le persone di minore età) che, nell'odierna società dell'informazione, fanno costantemente affidamento per le attività della quotidianità su prodotti, servizi e processi digitali [58].

In tal senso, la cybersicurezza ha progressivamente acquisito rilievo sul piano costituzionale dei diritti e delle libertà fondamentali, in particolare con riferimento alla tutela del diritto alla riservatezza e alla protezione dei dati personali, rispettivamente artt. 7 e 8 della Carta dei Diritti Fondamentali dell'UE [59], ed art. 8 della CEDU [60].

[55] L'art. 4, punto 2, della Direttiva NIS definiva la "sicurezza delle reti e dei sistemi informativi" come la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi.

[56] Art. 2, punto 1, Regolamento (UE) 2019/881.

[57] Per un approfondimento su questo aspetto si veda il contributo di R. BRIGHI a questo volume.

[58] P.G. CHIARA, *The Internet of Things and EU Law: Cybersecurity, Privacy and Data Protection Challenges*, Springer, Cham, 2024, p. 35.

[59] Nella giurisprudenza della Corte di Giustizia dell'UE, si vedano ad es., le cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e altri*, Sentenza della Corte (Grande Sezione) dell'8 aprile 2014, ECLI:EU:C:2014:238.

[60] Nella giurisprudenza della Corte EDU, invece, si veda soprattutto la *Causa Podchasov v. Russia*, Application no. 33696/19, decisa dalla terza sezione il 13 febbraio 2024.