La dimensione della "resilienza" nel diritto UE della cybersicurezza

La dimensione della 'resilienza' nel diritto UE della cybersicurezza

The dimension of 'resilience' in EU cybersecurity law

Pier Giorgio Chiara[*] e Raffaella Brighi[*†]

Abstract:

Il concetto di 'cybersicurezza', in costante evoluzione, non si presta ad interpretazioni univoche. Allo stesso tempo, non esiste una definizione chiara di 'cyber resilienza', nel contesto del diritto della cybersicurezza di matrice comunitaria, né si riscontra un'attenzione da parte della dottrina di riferimento su come questo concetto si estrinsechi nei quadri giuridici nella neonata area di policy. In tale contesto, questo contributo propone un'analisi filosofico e informatico-giuridica del concetto di '(cyber) resilienza' nel quadro giuridico comunitario in materia di cybersicurezza. A tal fine, l'indagine intende i) fornire una definizione preliminare e funzionale di 'resilienza', guardando all'esperienza di altri ambiti scientifici; ii) estrapolare i fattori tipizzanti della nozione di resilienza dalle definizioni analizzate al fine di identificare gli elementi costitutivi della relazione tra '(cyber)resilienza' e 'cybersicurezza'; e, iii) esaminare come i recenti atti legislativi adottati e proposti dal legislatore comunitario nella nascente area di policy della cybersicurezza coniughino la relazione tra (cyber) resilienza e cybersicurezza.

Abstract (ENG):

The concept of 'cybersecurity', which is constantly evolving, does not lend itself to unambiguous interpretations. At the same time, there is no clear definition of 'cyber resilience' and little attention is paid by the relevant literature on how this concept is operationalised in EU cybersecurity legal frameworks. Against this backdrop, this contribution proposes a legal-analytical analysis of the concept of '(cyber) resilience' in the EU cybersecurity legal framework. To this end, the investigation intends to (i) provide a preliminary and functional definition of '(cyber)resilience', looking at the experience of other scientific fields; (ii) extrapolate the typifying factors of the notion of resilience from the analysed definitions in order to identify the constitutive elements of the relationship between '(cyber)resilience' and '(cyber)security'; and, (iii) examine how recent legislative acts adopted and proposed by the EU legislature in the emerging cybersecurity policy area combine the relationship between (cyber)resilience and cybersecurity.

Keyword:

Resilience – Cybersecurity – EU law – Legal Theory

Outline:

[*] Pier Giorgio Chiara, Università di Bologna, Dipartimento di Scienze Giuridiche. E-mail: piergiorgio.chiara2@unibo.it.

[*] Raffaella Brighi, Università di Bologna, Dipartimento di Scienze Giuridiche. E-mail: raffaella.brighi@unibo.it.

† Il contributo è il risultato di un lavoro di ricerca congiunto che impegna entrambi gli autori. Nel dettaglio, ai fini di questo saggio, Pier Giorgio Chiara è autore delle sezioni 2, 3 e 4; mentre Raffaella Brighi è autrice delle sezioni 1 e 5. *This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.*

1. Introduzione

Il tema della cybersicurezza presenta una rilevanza sempre crescente. Da tempo l'Unione europea ha indicato la cybersecurity tra le priorità della propria agenda digitale e, a partire dal 2013, ha emanato tre diverse Strategie in materia[2]. L'Italia, in attuazione delle riforme previste dal Piano Nazionale di Ripresa e Resilienza (PNRR), ha istituito dal 2021 l'Agenzia per la Cybersicurezza Nazionale[3] con il compito, tra gli altri, di attuare la Strategia Nazionale di Cybersicurezza adottata dal Presidente del Consiglio per pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro e *resiliente*[4].

Se le minacce *cyber* colpiscono soggetti diversi (privati cittadini, imprese, enti pubblici, istituzioni, organizzazioni) sfruttandone le vulnerabilità, la tutela delle persone e dei loro diritti, la sicurezza pubblica e la difesa della Nazione non può non passare dall'adozione di processi, tecniche e programmi che proteggano i dispositivi, i dati e le reti informatiche. Poiché la sicurezza dell'intero sistema dipende dalla (in)sicurezza dell'elemento più debole e i danni su questo si ripercuotono a catena su tutti gli elementi connessi, per contrastare la pericolosa espansione del perimetro delle vulnerabilità è estremamente opportuno non solo avviare un processo di istituzionalizzazione della cybersicurezza, ma anche creare consapevolezza rispetto ai rischi collegati alla violazione dei requisiti che essa pone.

Ogni aspetto della realtà nella quale viviamo – servizi pubblici, istruzione, lavoro, economia e processi democratici – dipende da reti, sistemi informativi e tecnologie in continua evoluzione. Il diffondersi di sistemi cyber-fisici interconnessi e l'intelligenza artificiale pone nuove sfide di sicurezza. Tuttavia, siamo ancora lontani dal raggiungere un livello di protezione di base[5]. Se la pandemia da Covid 19, con il repentino e irreversibile spostamento verso una generale digitalizzazione delle attività e dei servizi, ha sviluppato la consapevolezza che la sicurezza informatica sia un elemento abilitante imprescindibile alla base della trasformazione dell'economia e della società[6], l'aggravarsi del panorama delle minacce informatiche volte a minare la stabilità politica degli Stati a seguito delle tensioni geopolitiche legate al recente conflitto russo-ucraino[7] ha reso evidente che il rischio *cyber* è globale e di primaria importanza[8].

---

[2] Commissione europea e alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza JOIN(2013) 1 final; JOIN(2017) 450 final; JOIN(2020) 18 final.

[3] L'Agenzia, che è il cardine della infrastruttura italiana di cybersecurity, è stata istituita con il d.l. 82/2021 e organizzata con il d.p.c.m. 223/2021. Una panoramica sulle attività, i dati e le progettualità della Agenzia è fornita nella Relazione annuale al Parlamento.

[4] La Strategia 2022-2026 e il Piano di implementazione prevedono il raggiungimento di 82 misure entro il 2026 con gli obiettivi di (i) assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo, (ii) anticipare l'evoluzione della minaccia cyber; (iii) contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida, (iv) raggiungere il coordinamento tra tutti i soggetti pubblici e privati interessati, per dare una risposta pronta in caso di eventi cyber sistemici; (v) raggiungere l'autonomia strategica nazionale ed europea nel settore del digitale.

[5] Il Rapporto Clusit 2023 sulla sicurezza ICT in Italia evidenzia che il 64% degli incidenti hanno come causa azioni "maldestre", degli utenti o del personale ICT. Malware, Vulnerabilità, Phishing e Account Cracking sono indice di carenze nella cyber igiene degli utenti che restano vulnerabili alle tecniche di più comuni di ingegneria sociale.

[6] ENISA, L'anno in rassegna (2020).

[7] Il Rapporto di Europol *Internet Organised Crime Assessment* (IOCTA) 2023 evidenzia che gli effetti di trascinamento della situazione geopolitica si sono manifestati con una raffica di attacchi informatici dirompenti non solo contro obiettivi ucraini e russi, ma anche a livello mondiale, soprattutto nell'UE. L'aumento di queste attività dannose contro gli Stati membri dell'UE è dovuto principalmente a un numero significativo di attacchi DDoS (Distributed Denial of Service) che hanno colpito istituzioni pubbliche nazionali e regionali. Questi attacchi sono stati spesso motivati politicamente e coordinati da gruppi di hacker filorussi in risposta a dichiarazioni o azioni a sostegno dell'Ucraina.

[8] Su veda sul punto anche la Relazione annuale (2022) al Parlamento della Agenzia per la Cybersicurezza nazionale.

Inoltre, attacchi più aggressivi e sofisticati, che sfruttano la maggior superficie di esposizione[9], saranno motori di altri rischi non strettamente tecnologici ma di grave impatto: attacchi terroristici e conflitti tra stati; proliferazione di attività economiche illecite, campagne di disinformazione, concentrazione del potere digitale, disuguaglianza, discriminazioni e controllo sociale, fino all'erosione lenta delle democrazie[10].

L'analisi previsionale presentata da ENISA (Agenzia dell'UE per la cybersicurezza) in prospettiva 2030[11] conferma la necessità di mettere in atto sin da subito politiche di mitigazione dei rischi in grado di aumentare la sicurezza e la resilienza dei sistemi per far fronte a scenari complessi e ancora di difficile comprensione. La manomissione dei dispositivi *smart* con il conseguente sfruttamento di dati comportamentali e sensibili degli individui, l'abuso di sistemi di IA con la manipolazione intenzionale degli algoritmi e dei dati di addestramento, la compromissione della supply chain a causa della vulnerabilità dei molteplici componenti e servizi integrati nei nuovi prodotti digitali sono alcune delle minacce che vanno prese in considerazione per rendere resilienti l'insieme delle infrastrutture su cui si fonderanno le città del futuro[12].

Chiaramente tra il lato della difesa e il lato dell'attacco c'è una grande asimmetria, il compito della difesa è enormemente più difficile e si estrinseca su più livelli di intervento. Ad un alto livello, la Commissione UE, attraverso le Strategie in materia di cybersicurezza – dal 2013 in avanti, identifica tre macroaree di intervento. Esse sono: i) resilienza; ii) contrasto al cybercrimine; iii) cyberdifesa e cyberdiplomazia.

In particolare, nel quadro della dimensione della *resilienza* sono stati adottati e proposti, dal 2013 al 2023, diversi atti giuridici ancorché con obiettivi e oggetti diversi tra loro[13]. Una prima direttrice, che ha il suo focus nella Direttiva NIS (*Network and Informatin Security* – Direttiva (UE) 2016/1148) e nella sua recente revisione, la c.d. Direttiva NIS2 (Direttiva (UE) 2022/2555), ha inteso rafforzare la sicurezza delle reti e dei sistemi informativi promuovendo la cooperazione tra gli Stati membri per aumentare il livello di 'cyber resilienza' di tutti i settori, pubblici e privati, che svolgono una funzione essenziale per l'economia e la società.

In questa linea si collocano anche la c.d. direttiva CER (*critical entities resilience directive,* Direttiva (UE) 2022/2557) e il c.d. regolamento DORA (*digital operational resilience act* - Regolamento (UE) 2022/2554), che stabilisce obblighi in relazione alla sicurezza delle reti e dei sistemi per le entità operanti nel settore bancario e finanziario.

Una seconda direttrice riguarda la creazione di un quadro europeo di certificazione della cybersicurezza, attraverso il c.d. *Cybersecurity Act* (Regolamento (UE) 2019/881), allo scopo di garantire elevati standard di sicurezza per prodotti, servizi e processi ICT secondo un approccio di *sicurezza by design*. La promozione dei requisiti di sicurezza sin dalla progettazione, per garantire prodotti hardware e software più sicuri, si concretizza anche nella proposta di nuove norme orizzontali per i prodotti con elementi digitali, attraverso il c.d. *Cyber Resilience Act*, presentato nel settembre 2022.

[9] Si pensi, ad esempio, ai c.d. attacchi 'zero-day', ossia quegli attacchi che sfruttano vulnerabilità di sistemi che non siano ancora note al produttore o sviluppatore.

[10] The Global Risks Report 2023, 18th Edition, World Economic Forum. Si veda Denardis 2021.

[11] ENISA 2023.

[12] Sul punto Montemagni 2022.

[13] Per una attenta disamina in argomento si veda tra gli altri Pietropaoli 2022:99-114.

Infine, una terza direttrice può essere individuata nella creazione di un 'ciberscudo europeo', disegnato inter alia dalla proposta del c.d. *Cyber Solidarity Act* che, attraverso quadri di cooperazione operativa, intende rafforzare la capacità della UE di prepararsi e gestire gli attacchi su larga scala.

Raggiungere un alto livello di sicurezza adottando solo misure tecnico-organizzative di protezione che mirano a ridurre l'incertezza e a portare il rischio a un livello accettabile, è impossibile stante la complessità dei sistemi attuali e futuri e l'imprevedibilità di pericoli intrinseci agli ambienti sociotecnici. Proprio per l'impossibilità di raggiungere l'assenza di esiti avversi (il c.d. 'rischio zero'), il quadro giuridico, le politiche e i piani di investimento sembrano promuovere, unitamente alla progettazione e allo sviluppo di sistemi *robusti*, la capacità degli stessi di essere *resilienti*.

Nel quadro comunitario brevemente tratteggiato, i concetti di cybersicurezza e di (cyber) resilienza si intrecciano, sembrano avere significati mutevoli, talvolta interscambiabili e comunque non esaustivamente definiti e dunque difficilmente mappabili nei rispettivi concetti in chiave tecnico-scientifica. Soprattutto in un contesto in cui il diritto viene ad intersecarsi con un sapere scientifico quale è l'informatica, è necessario giungere a un significato uniforme e coerente dei concetti, delle procedure, delle metodologie in uso. L'ambiguità concettuale sottesa al termine 'resilienza' – non chiarita dal legislatore nelle Strategie e nei testi legislativi – potrebbe portare con sé il rischio di minare la coerenza interna del quadro giuridico di riferimento, compromettendo altresì il principio di certezza del diritto.

In tale contesto, questo contributo propone un'indagine analitica in chiave filosofico e informatico-giuridica del concetto di '(cyber) resilienza' nel quadro giuridico comunitario in materia di cybersicurezza. A tal fine l'analisi nelle sezioni che seguono intende (i) fornire una definizione preliminare e funzionale di 'resilienza', guardando all'esperienza di altri ambiti scientifici; (ii) estrapolare i fattori tipizzanti della nozione di resilienza dalle definizioni analizzate al fine di identificare gli elementi costitutivi della relazione tra '(cyber)resilienza' e 'cybersicurezza'; e, infine, (iii) esaminare come i recenti atti legislativi adottati e proposti dal legislatore comunitario nella nascente area di policy della cybersicurezza coniughino la relazione tra (cyber) resilienza e cybersicurezza. La terza direzione di indagine (iii) avrà uno spazio prevalente, dal momento che è proprio nell'ambito dell'analisi del diritto comunitario in materia di cybersicurezza che si cercherà l'orizzonte di senso del termine 'resilienza'.

2. Il concetto polisemico di 'resilienza' nella regolamentazione della cybersicurezza

Questa sezione affronta la prima sfida giuridica enucleata nell'introduzione, cioè un'analisi sistematica del perimetro concettuale di 'resilienza' nel quadro giuridico comunitario in materia di cybersicurezza, in tre fasi. In primo luogo, si cercherà di fornire una definizione preliminare e funzionale di 'resilienza', anche guardando all'esperienza di altri ambiti più maturi, e sul perché sia importante questa riflessione; in secondo luogo, si estrapoleranno degli indicatori funzionali dalle definizioni di resilienza emerse al fine di identificare gli elementi costitutivi della relazione che intercorre tra '(cyber)resilienza' e 'cybersicurezza'; infine, l'analisi volgerà l'attenzione alla concettualizzazione di 'resilienza' nelle Strategie della Commissione europea in materia di cybersicurezza.

Resilienza è certamente un concetto complesso, scivoloso, che si presta a interpretazioni non univoche, anche a seconda del contesto in cui è utilizzato. Eppure, definire gli elementi fondamentali di un concetto è cruciale nel diritto[14], soprattutto negli ordinamenti moderni che, per governare la crescente complessità

[14] Si vedano *ex multis* Sartor 2009; Hage e Pfordten 2009; Hacker 1969; Macagno 2010.

del reale, si avvalgono sempre di più di ampie descrizioni ed astrazioni[15]. In tal senso, da una parte, la filosofia analitica del diritto fornisce un quadro di riferimento per esaminare il ruolo delle definizioni nel ragionamento giuridico, nell'interpretazione e nel funzionamento del sistema giuridico[16].

Dall'altra, sul versante filosofico-linguistico, è opportuno richiamare, anche brevemente, l'impianto teorico di Searle circa la classificazione tra regole 'regolative' (come obblighi, divieti e permessi) e 'costitutive' (regole che stabiliscono che qualcosa, all'interno di un determinato contesto, assuma un dato valore e quindi un determinato significato)[17] per meglio comprendere la natura della dimensione della 'resilienza' nell'ambito del diritto della cybersicurezza in UE. Pertanto, questa prima fase è dedicata ad un'analisi concettuale comparata del termine 'resilienza' in diversi ambiti per comprendere quali siano i fattori comuni del concetto.

Da un punto di vista tecnico-ingegneristico, un report ENISA risalente al 2011 – prima quindi che il mandato fosse reso permanente dal Cybersecurity Act, contestualmente ad un potenziamento dei compiti e delle funzioni – definisce 'resilienza' nei sistemi moderni come l'opposto di 'fragilità', riferendosi alla capacità di un sistema o di un'organizzazione di riprendersi da un grave malfunzionamento e, più in generale, alla sua capacità di sopravvivere di fronte alle minacce, tornando ad uno *status quo*[18].

Invece, la capacità di adattamento, e quindi di trasformazione sostenendo e accettando il cambiamento del sistema, in considerazione dei mutamenti dell'ambiente in cui il sistema è posto, è una caratteristica della resilienza nata dall'esperienza nella biologia dei sistemi[19]. Similmente, tale approccio socio-ecologico è stato adottato anche dalla c.d. 'resilienza urbana': la capacità dei centri urbani di *rispondere, adattarsi* e *trasformarsi* a diversi rischi e sollecitazioni, sia naturali che di origine antropica[20].

In ambito sociopolitico, inoltre, discussioni intorno alla resilienza sono da tempo una parte integrante delle riflessioni sulla securitizzazione delle democrazie moderne[21]. Per quanto attiene alla relazione tra il concetto di (cyber)resilienza e cybersicurezza, un certo filone dottrinale trova un consenso attorno alla scriminante che vedrebbe la resilienza trattare gli eventi cyber anche avversi all'organizzazione come aspetti *fisiologici* delle operazioni, mentre la (cyber)sicurezza sarebbe più concentrata su aspetti prodromici di prevenzione e robustezza – eludendo pertanto le domande scomode poste dalla *realtà* della minaccia cyber avente il potenziale di tramutarsi in incidente[22].

In altri termini, secondo questa ricostruzione, la (cyber)resilienza parte, a differenza della cybersicurezza, dal presupposto che, nonostante le robuste misure di sicurezza, gli incidenti possono comunque verificarsi: le organizzazioni e gli individui devono essere preparati per mitigarne l'impatto e ripristinare rapidamente le operazioni normali. Da una parte, la resilienza è vista come l'abilità di realizzare gli esiti attesi in modo continuativo nonostante gli eventi cibernetici avversi. Dall'altra, sul piano del rapporto con la cybersicurezza, la resilienza – secondo questa linea di pensiero – giocherebbe un ruolo cruciale

---

15 Biagioli 1998.

16 Hart 1961:13: *«we are looking not merely at words ... but also at the realities we use words to talk about. We are using a sharpened awareness of words to sharpen our perception of the phenomena»*. Cfr. con Guastini 2012:52-53.

17 Searle 1995. Sulla tensione tra regole constitutive e regolative, nonché circa l'importanza della strutturazione dell'ambiente alla base delle applicazioni di tecnologie digitali, in particolare dell'intelligenza artificiale (IA), si veda Floridi 2022.

18 ENISA 2011: 16. Si veda, inoltre, Woods, Leveson, Hollnagel 2006.

19 Walker, Cooper 2011; cfr. con Holling 1973 e Wagner 2008; si veda anche Song et al. 2019.

20 Datola, Bottero, De Angelis 2021.

21 Dunn Cavelty, Kaufmann, Søby Kristensen 2015; Christou 2016. Cfr. inoltre con Carayannis et al.

22 Rothrock 2017.

consentendo alle organizzazioni di incorporare contromisure e piani di emergenza come parte di quella che potrebbe essere considerata la nuova condizione di 'normalità'[23].

Alla luce delle diverse definizioni di 'resilienza' presentate in diversi ambiti scientifici, si possono già estrapolare degli indicatori comuni al fine di mettere a fuoco il concetto:

> dato uno stato X di un osservabile Y [organizzazione; sistema; ambiente urbano/naturale], l'osservabile Y sarà *resiliente* tanto più saprà i) adattarsi agli eventi avversi, pervenendo ad uno stato X migliorato però dall'esperienza (stato X+); e ii) realizzare i propri obiettivi durante e nonostante la perturbazione.

Sul piano del rapporto che intercorre tra (cyber)resilienza e cybersicurezza, è opportuno riprendere più attentamente il concetto di 'robustezza', per separare i due concetti e chiarire le interazioni con il termine 'resilienza'. Infatti, tradizionalmente – ad un alto livello di astrazione – la cybersicurezza si compone di tre dimensioni: robustezza, resilienza e risposta. Generalmente, nella progettazione dei sistemi, con robustezza ci si riferisce al grado di *resistenza* alle sollecitazioni, di varia natura, ad esempio prevedendo sistemi significativamente più robusti di quanto sia legittimo attendersi per un normale funzionamento[24].

Ne consegue, pertanto, che secondo una ricostruzione classica della sicurezza informatica la resilienza sia una 'categoria' o, meglio, una dimensione della cybersicurezza – al pari di robustezza e risposta – attraverso la quale quest'ultima può raggiungere i suoi obiettivi che non sarebbero difformi a quelli della resilienza, come visto sopra, ma che anzi si porrebbero in un'ottica di strumentalità. In altre parole, questa visione respingerebbe una concettualizzazione della cybersicurezza limitata alla prevenzione e alla protezione dalle minacce informatiche, con la cyber resilienza che includerebbe invece le capacità di risposta e ripristino.

Su questo sfondo, nelle tre diverse Strategie dell'Unione europea sulla cybersicurezza non viene data una definizione puntuale di 'resilienza' nel quadro normativo comunitario di riferimento[25]. La prima Strategia dell'UE in materia di cybersicurezza del 2013 introduce come necessità strategica per l'Unione la promozione e il rafforzamento della 'ciberresilienza'[26]; nel documento programmatico della Commissione, tale dimensione sembrerebbe sostanziarsi soprattutto nell'ambito della sicurezza delle reti e dell'informazione[27]. Ed è in questo contesto che si sviluppa la proposta per una direttiva recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, poi Direttiva (UE) 2016/1148, considerata quale il primo atto giuridico dell'Unione sulla cybersicurezza in senso stretto. Nemmeno nella direttiva NIS, tuttavia, si trova una definizione di resilienza.

---

[23] Björck, Henkel, Stirna, Zdravkovic, 2015. In Marshall 2022:154, si pone l'interrogativo di definire 'cybersicurezza' e 'cyberresilienza', in particolare, con riferimento al settore dell'aviazione. Tuttavia, il contributo non elabora un impianto teorico atto a separare i due aspetti.

[24] Si veda, *ex multis,* Taddeo 2019:350.

[25] Christou 2016:11: «*Many cybersecurity strategies within and beyond Europe refer to developing effective cyber resilience, but without adequately defining and deconstructing what resilience is, what it looks like at different stages, and the preconditions and governance forms required to achieve it*».

[26] Commissione europea e Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza 2013.

[27] Fino ad allora, il tema della sicurezza dell'informazione digitale era stato affrontato nell'ambito del quadro normativo sulle telecomunicazioni (Direttiva 90/387/CE; Direttiva 90/388/CE) e con riferimento alla protezione dei dati (Direttiva 95/46/EC; direttiva 97/66/EC): come peraltro evidenziato da una comunicazione della Commissione UE risalente al 2001, le necessarie misure strategiche in materia di sicurezza delle reti e dell'informazione sarebbero state complementari ai quadri normativi più maturi in materia di protezione dei dati, telecomunicazioni e di criminalità informatica. Cfr. con Commissione europea 2001: 3.

La Strategia del 2017, insistendo sull'approccio *multi-stakeholder* che vede la cybersicurezza quale una sfida sociale comune[28], nell'asse di intervento circa la 'ciberresilienza' dell'Unione ai cyberattacchi, sposta l'attenzione dalla sicurezza delle reti e dei sistemi informativi al rafforzamento dell'ENISA[29] e alla creazione di un quadro europeo di certificazione della cybersicurezza. Questi due obiettivi vengono realizzati con il Regolamento (UE) 2019/881: benché sia il primo atto giuridico dell'UE a prevedere una definizione di 'cybersicurezza'[30], non fornisce una definizione di (cyber)resilienza.

Infine, la Strategia del 2020 – ponendosi in una prospettiva di continuità con i precedenti documenti programmatici – contiene un quadro di proposte a livello normativo, di investimento e politico, per tre settori di intervento, tra cui figura, in particolare, 'resilienza, sovranità tecnologica e leadership'[31]. L'obiettivo strategico di migliorare la resilienza, che permea l'intera Strategia, ha un raggio d'azione notevolmente ampliato rispetto alle precedenti Strategie, dal momento che oggetto dell'attenzione della Commissione sono: i prodotti connessi[32]; le capacità industriali e tecnologiche nel campo della cybersicurezza[33]; la catena di approvvigionamento[34]; e, più generalmente, la società[35].

Premesso il fatto che, anche in questo caso, la Commissione ha deciso di non definire 'resilienza' o 'cyber resilienza', la domanda che è opportuno porre – alla luce di un progressivo aumento dell'utilizzo del termine come giustificazione di scelte politiche e normative – è quale visione della cyber resilienza emerga dal documento. Da una parte, l'iniziativa strategica circa una regolamentazione degli oggetti connessi (o IoT) è esplicitamente reputata cruciale «sia per garantire la resilienza complessiva che per aumentare la cibersicurezza»[36]. Questo dettato sembrerebbe riconoscere implicitamente la teoria che vorrebbe cyber resilienza e cybersicurezza aventi obiettivi distinti. Dall'altra, nel contesto del contrasto alla criminalità informatica, la Strategia considera che una dissuasione efficace non può essere ottenuta mediante la sola resilienza[37].

Eppure, se accettassimo la visione del rapporto cyber resilienza-cybersicurezza visto poc'anzi, una simile omissione di altre dimensioni tipiche della cybersicurezza, come la robustezza, o della cybersicurezza stessa, come nel caso di misure per una 'Internet delle cose sicura', risulterebbe fuori luogo. Per rendere le cose ancor più complesse, poi, con riferimento alla gestione dei database dei nomi di dominio e dei dati di registrazione (c.d. 'WHOIS data'), si fa – nuovamente – riferimento a «sicurezza, stabilità e resilienza»[38].

---

[28] Commissione europea e Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza 2017: 4.

[29] Nel documento programmatico dell'ENISA per il biennio 2023-2025, l'obiettivo principale riconosciuto dal c.d. *mission statement* dell'Agenzia è aumentare la 'resilienza' dell'infrastruttura e servizi dell'Unione e mantenere la società e i cittadini 'digitalmente' sicuri. Si veda: https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025.

[30] Art. 2, punto 1, regolamento (UE) 2019/881: «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]».

[31] Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza 2020. Gli altri due settori di intervento dell'UE sono: sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta e promozione di un ciberspazio globale e aperto.

[32] Id., p. 5.

[33] Id., p. 6.

[34] Id., p. 9.

[35] Id., p. 6.

[36] Id., p. 10.

[37] Id., p. 17.

[38] *Ibid.*

Per districare la relazione tra (cyber)resilienza e cybersicurezza nel contesto del diritto della cybersicurezza dell'UE, che appare di difficile risoluzione stando all'ultima Strategia della Commissione, l'analisi si concentrerà piuttosto sul come queste due nozioni operano nei quadri normativi rilevanti. In particolare, nella sezione che segue saranno presi in esame gli atti giuridici proposti nell'ambito della Strategia del 2020: la direttiva NIS2, la direttiva CER e il regolamento DORA.

3. Segue: resilienza nei quadri legislativi di cybersicurezza nel contesto della Strategia del 2020

Unitamente alla pubblicazione della Strategia, nel dicembre 2020, la Commissione ha proposto anche un pacchetto legislativo composto dal disegno di revisione della direttiva NIS e una proposta di direttiva sulla resilienza di entità critiche.

Per quanto concerne la revisione della direttiva NIS, che poi diventerà la direttiva (UE) 2022/2555[39], in vigore dal 16 gennaio 2023, l'articolo 1, paragrafo 1, stabilisce che l'oggetto e ambito di applicazione dello strumento consiste «in misure volte a garantire un livello comune elevato di *cibersicurezza* nell'Unione in modo da migliorare il funzionamento del mercato interno [enfasi aggiunta]». Tuttavia, nella Strategia, la Commissione propone di riformare le regole poste dalla direttiva NIS «per aumentare il livello di *ciberresilienza* di tutti i settori pertinenti, pubblici e privati, che svolgono una funzione importante per l'economia e la società [enfasi aggiunta]»[40].

La NIS2 non definisce resilienza o 'ciberresilienza', ma fornisce una definizione di 'sicurezza', quale «la capacità dei sistemi informatici e di rete di *resistere*, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi [enfasi aggiunta]»[41]. L'enfasi posta sul tratto della resistenza richiama alcuni connotati tipici della definizione data di resistenza nella sezione precedente, anche se altri aspetti fondanti, quali la capacità di mantenere o riprendere le operazioni durante o dopo un attacco o un'interruzione, rimangono fuori.

In questo quadro apparente privo di coerenza, una lettura combinata dei primi due considerando della direttiva può essere utile per formulare un'ipotesi: da una parte, viene detto che la direttiva NIS «mirava a sviluppare le capacità di *cibersicurezza* in tutta l'Unione [enfasi aggiunta]»[42]; dall'altra si riconosce che «dall'entrata in vigore della direttiva (UE) 2016/1148 sono stati compiuti progressi significativi nell'aumentare il livello dell'Unione in materia di *ciberresilienza* [enfasi aggiunta]»[43]. Alla luce di ciò, sembra lecito affermare che, quantomeno nell'ambito della sicurezza delle reti e dei sistemi informativi (oggetto delle direttive NIS e NIS2), il legislatore comunitario usi i termini *cibersicurezza* e *ciberresilienza* in modo interscambiabile, identificando pertanto gli stessi ambiti di protezione e gli stessi obiettivi.

---

[39] Ad un alto livello, la NIS2 stabilisce i) obblighi per gli Stati membri di adottare strategie nazionali in materia di cybersicurezza e designare autorità nazionali competenti e CSIRT; ii) misure in materia di gestione dei rischi di cybersicurezza e obblighi di segnalazione per i soggetti 'essenziali ed importanti' in ambito di applicazione dello strumento - notevolmente ampliato rispetto al precedente standard della NIS; iii) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza; iv) obblighi in materia di vigilanza ed esecuzione per gli Stati membri. Per una panoramica generale sulle novità introdotte dalla direttiva NIS2, si veda *ex multis*: Sievers 2021; Schmitz-Berndt, Chiara 2022.

[40] Id., p. 6.

[41] Direttiva (UE) 2022/2555, Art. 6, punto 2.

[42] Direttiva (UE) 2022/2555, considerando 1.

[43] Direttiva (UE) 2022/2555, considerando 2.

Come detto, la Commissione pubblica, congiuntamente alla proposta per una nuova direttiva NIS2, una proposta di 'direttiva sulla resilienza di entità critiche'. E come la NIS2, anche la c.d. direttiva CER (*critical entities resilience directive*)[44] sarà pubblicata nella Gazzetta Ufficiale dell'UE il 14 dicembre 2022. L'eponimia fin troppo evidente della direttiva CER costituisce un ottimo spunto per un'analisi comparata con la 'gemella' NIS2. La CER, infatti, definisce esplicitamente 'resilienza' come la «capacità di un soggetto critico di *prevenire*, *attenuare*, *assorbire* un incidente, di *proteggersi* da esso, di *rispondervi*, di *resistervi*, di *adattarvisi* e di *ripristinare* le proprie capacità operative [enfasi aggiunta]»[45].

Questa prima definizione di 'resilienza' in un testo giuridico dell'Unione nell'area – largamente intesa – della (cyber)sicurezza impone un triplice ordine di riflessioni. In primo luogo, andando a riprendere le definizioni funzionali di 'resilienza' proposte nella sezione precedente, appare evidente come l'ampio dettato normativo della direttiva CER integri non solo gli elementi costitutivi di una nozione tecnico-ingegneristica, bensì anche gli aspetti di *adattamento* e *trasformazione* più vicini all'approccio socio-ecologico.

Sul versante del rapporto con la cybersicurezza, invece, occorre sottolineare come la resilienza dell'infrastruttura critica oggetto della direttiva CER inerisca alla sicurezza *fisica* (seguendo, peraltro, un approccio c.d. '*all hazards*'[46]) e non anche a quella cyber o digitale, ancorché i due aspetti siano complementari. Pertanto, l'ambito di applicazione della direttiva CER non ricomprende anche le materie disciplinate dalla direttiva NIS2[47], dal momento che l'aspetto della cybersicurezza è trattato in modo sufficiente da quest'ultima direttiva (UE) 2022/2555[48], atteso che gli Stati membri sono chiamati ad attuare entrambe le direttive in modo coordinato[49].

Infine, il richiamo alle dimensioni della prevenzione e della risposta – fasi logicamente antecedenti l'evento dannoso[50] – implica un allargamento del perimetro operativo della resilienza in aree tradizionalmente connesse alla sicurezza (e anche cybersicurezza, come abbiamo visto nella precedente sezione).

Unitamente alla NIS2 e alla CER, il 14 dicembre viene pubblicato nella G.U. dell'Unione il regolamento (UE) 2022/2554, c.d. DORA (*digital operational resilience act*)[51]. Questo regolamento ha come obiettivo principale il conseguimento di un livello comune elevato di *resilienza* operativa digitale; a tal fine, stabilisce diversi obblighi alle sole entità operanti nel settore bancario e finanziario in relazione alla sicurezza dei sistemi informatici e di rete a sostegno dei processi commerciali[52].

In questo quadro normativo, 'resilienza operativa digitale' è definita quale «la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la *propria integrità e affidabilità operativa*, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per *garantire la sicurezza dei sistemi informatici e di rete*

[44] La direttiva CER, ad un alto livello, stabilisce obblighi in capo agli Stati membri (ad es., in merito all'identificazione dei soggetti critici, nonché al sostegno di questi ultimi nell'adempimento dei loro obblighi) e ai soggetti critici al fine di rafforzare la loro resilienza e la loro capacità di fornire servizi.

[45] Direttiva (UE) 2022/2557, Art. 2, para. 2; considerando 2.

[46] Nel condurre le valutazioni di impatto e le analisi del rischio, i soggetti critici dovranno tenere in conto tutti i rischi rilevanti, sia naturali che artificiali, accidentali o intenzionali. Cfr. direttiva (UE) 2022/2557, considerando 4; Art. 2, punto 7.

[47] Direttiva (UE) 2022/2557, Art. 1, para. 2.

[48] Direttiva (UE) 2022/2557, considerando 9.

[49] Direttiva (UE) 2022/2557, Art. 1, para. 2.

[50] Rød, Lange, Theocharidou, Pursiainen 2020:2; si veda inoltre Niemi, Sill Torres 2022.

[51] Per una panoramica di carattere generale sul regolamento DORA, si veda: Clausmeier 2023.

[52] Regolamento (UE) 2022/2554, Art. 1, para. 1.

utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, *anche in occasione di perturbazioni* [enfasi aggiunta]»[53].

Questa definizione, ad una prima lettura, appare lontana dalle concettualizzazioni viste finora. Tuttavia, una più attenta analisi mostra come gli indicatori comuni alle varie definizioni analizzate di 'resilienza' siano in realtà presenti anche nel regolamento DORA; inoltre, l'adattamento alla realtà specifica del settore finanziario comporta necessariamente l'inclusione di elementi che risulterebbero ultronei in altre definizioni più 'orizzontali'.

Tuttavia, nel medesimo settore, la Banca Centrale Europea, si riferisce a cyber resilienza come la capacità di proteggere i dati e i sistemi elettronici dagli attacchi informatici e di riprendere rapidamente le operazioni aziendali in caso di attacco riuscito[54]. Tale definizione riflette un approccio olistico: in primo luogo, i beni da proteggere dagli attacchi informatici (e non anche attività accidentali) sono sia i dati che i sistemi elettronici e di rete; in secondo luogo, affianco alle dimensioni tipiche della resilienza, quale il ripristino delle operazioni in caso di attacco compiuto, sono inclusi anche aspetti più inerenti alla sicurezza (es. protezione).

Alla luce di ciò, la chiave interpretativa della 'resilienza operativa digitale' (e quindi, cyber resilienza), ancorché limitatamente al settore finanziario come presentata in maniera piuttosto involuta nel regolamento DORA, è proprio la necessità di garantire, da una parte, un livello elevato di integrità e affidabilità delle capacità operative; dall'altra, la sicurezza dei sistemi informatici e di reti anche nell'eventualità di perturbazioni – accidentali o dolose.

Rispetto all'impianto della direttiva CER, dove – come detto – sembra essere implicito un allargamento del perimetro della resilienza a scapito di aree tradizionalmente appartenenti alla sicurezza, il regolamento DORA adotta una prospettiva diversa, per certi versi opposta, identificando la (cyber)sicurezza delle reti e dei sistemi informativi quale fine per la resilienza operativa digitale. In tal senso, si può tracciare un parallelismo con la direttiva NIS2: in entrambi gli atti giuridici, la cybersicurezza sembra essere la categoria maggiore all'interno della quale viene sussunta la cyber resilienza.

L'analisi di questi tre atti giuridici dell'Unione, pubblicati nella Gazzetta Ufficiale dell'UE lo stesso giorno, mostra come nel diritto UE della cybersicurezza, da una parte, i perimetri concettuali di (cyber)resilienza e (cyber)sicurezza contengano alcuni indicatori caratterizzanti (es., sicurezza è certamente maggiormente connessa ad una dimensione di protezione, mentre resilienza si identifica di più nella risposta alle sollecitazioni e all'adattamento); dall'altra, ad un alto livello d'astrazione[55], i quadri legislativi rilevanti non paiono in imbarazzo a fronte di un utilizzo unificato od interscambiabile dei due termini.

La cyber resilienza non è fondamentalmente diversa dalla cybersicurezza nella sua implementazione come norma giuridica[56]. Ulteriore argomentazione a conferma di questa tesi può essere rinvenuta nel documento riassuntivo dei 10 temi chiave nel dibattito pubblico e nell'agenda politica dell'Unione per il 2023 a cura del servizio di ricerca del Parlamento europeo: le sfide per i quadri normativi comunitari in materia di cybersicurezza vengono classificate sotto il titolo '*cyber-resilience in the EU*'[57].

[53] Regolamento (UE) 2022/2554, Art. 3, punto 1.
[54] Si veda https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html.
[55] Floridi 2008.
[56] Bygrave 2022:31.
[57] EPRS 2023: 14-15.

Alla luce di ciò, è opportuno ora volgere l'attenzione al *Cyber Resilience Act* (CRA) e al *Cyber Solidarity Act* (CSA) per analizzare come gli ultimi atti giuridici proposti dalla Commissione in materia di cybersicurezza declinino il concetto di 'resilienza'; in altre parole, quale sia la prospettiva adottata in questi due regolamenti alla luce degli indicatori estrapolati dall'impianto teorico di cui sopra.

4. Resilienza nel contesto delle nuove proposte legislative in materia di cybersicurezza: il caso del *Cyber Resilience Act* e del *Cyber Solidarity Act*

Il 15 settembre 2022, la Commissione ha pubblicato una proposta di regolamento "sulla ciberresilienza" (*Cyber Resilience Act*, CRA)[58], contenente nuove norme in materia di cybersicurezza per i prodotti con elementi digitali per garantire hardware e software più sicuri, i quali sono sempre più soggetti ad attacchi informatici, con pregiudizi per un'intera organizzazione o un'intera supply chain.

Infatti, tali prodotti – sempre più presenti nel mercato interno – presentano generalmente un basso livello di cybersicurezza, testimoniato da vulnerabilità diffuse e dalle forniture insufficiente di aggiornamenti di sicurezza[59]. Inoltre, il consumatore medio non è in grado di valutare il livello complessivo di sicurezza di un prodotto connesso, atteso che spesso l'accesso alle informazioni inerenti alle proprietà di cybersicurezza dei prodotti è limitato se non impossibile[60]. Infine, da un punto di vista giuridico, il quadro normativo comunitario appare frammentato in relazione ai requisiti di cybersicurezza per tali prodotti[61].

Come già la direttiva CER e il regolamento DORA, anche il CRA contiene nel nome[62] il termine resilienza. Eppure, da un punto di vista meramente quantitativo, 'resilienza' compare poche volte nel testo della proposta e con riferimento alla resilienza dei servizi forniti dai soggetti in ambito di applicazione della NIS2[63], alla resilienza della supply chain[64] e più generalmente alla cyber resilienza *tout court*[65].

Volendo indagare la valutazione d'impatto in accompagnamento alla proposta CRA pubblicata dalla Commissione, nella prima parte del report figura una sezione dal titolo suggestivo: *security and resilience*[66]. In tale sezione, il ragionamento di fondo – che informa peraltro la proposta intera – è che l'introduzione di requisiti obbligatori in tema di sicurezza dei prodotti porterebbe ad un innalzamento della sicurezza dei prodotti stessi e, di conseguenza, «della sicurezza e resilienza degli utilizzatori»[67]. Il rapporto tra sicurezza e resilienza nel contesto della proposta CRA, quindi, non è chiarito nemmeno dalla valutazione di impatto, che anzi presenta i due termini quasi in un'endiadi.

---

[58] 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). Per una panoramica generale sul CRA, si veda inoltre Chiara 2023.

[59] Proposta CRA, considerando 1.

[60] *Id.*

[61] Proposta CRA, considerando 4.

[62] Papakonstantinou, Hert 2022.

[63] Proposta CRA, considerando 9.

[64] Proposta CRA, Art. 6, para. 5.

[65] Proposta CRA, considerando 67; 33.

[66] Commissione europea, "Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", SWD(2022) 282 final, pp. 67-69.

[67] *Ibid.,* p. 68.

Non stupisce pertanto non trovare, all'articolo 3 della proposta CRA, contenente le definizioni, il termine resilienza (o cyber resilienza). Così come non viene fornita una definizione di 'sicurezza', come fatto per esempio nella NIS2. Il CRA rimanda invece alla NIS2 per quanto concerne la nozione di rischio[68], a cui si aggiunge il 'rischio di cibersicurezza significativo'[69].

Richiamando gli elementi della definizione di resilienza visti sopra, se il 'rischio di cybersicurezza' è anche la '*perturbazione* causata da un incidente' (lo stesso lemma viene usato nel regolamento DORA nella definizione di 'resilienza operativa digitale'), sembra plausibile poter affermare che nel regolamento CRA la cyber resilienza sia concepita quale dimensione della cybersicurezza, dal momento che la capacità di resistere alle perturbazioni è un elemento fondante del concetto di resilienza[70].

Inoltre, i requisiti essenziali (relativi alle proprietà dei prodotti e ai processi messi in atto dal fabbricante nella gestione delle vulnerabilità), a cui i fabbricanti dei prodotti con elementi digitali dovranno conformarsi per immettere i prodotti sul mercato[71], di cui all'allegato I della proposta CRA, sono esplicitamente di 'cibersicurezza' e non di cyber resilienza. Alla luce di quanto detto nelle sezioni precedenti, questa categorizzazione regge, dal momento che tali requisiti[72] si collocano logicamente in una fase antecedente rispetto alla potenziale perturbazione, e cioè a quella della progettazione e sviluppo, integrando aspetti chiave della dimensione della robustezza, anziché della resilienza.

Nell'aprile 2023, la Commissione propone un nuovo regolamento, sulla 'cyber solidarietà'[73]. Questo nuovo atto giuridico si basa sui già esistenti quadri di cooperazione operativa e di gestione delle crisi di

[68] Direttiva (UE) 2022/2555, Art. 6, punto 9: «potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi".

[69] Proposta CRA, Art.3, punto 36.

[70] Su come la resilienza dovrebbe essere resa operativa nel CRA, si veda Rosager Ludvigsen, Nagaraja 2022.

[71] La proposta CRA si basa sui principi e gli istituti del c.d. 'nuovo quadro normativo' in materia di legislazione della sicurezza dei prodotti. Questo impianto ruota attorno alla definizione di 'requisiti essenziali' di alto livello in termini di sicurezza che i prodotti devono soddisfare per essere immessi nel mercato interno; tali requisiti sono poi dettagliati da norme tecniche armonizzate (standards) elaborate dagli organismi europei di normazione sulla base di una richiesta di normazione da parte della Commissione. Si veda Commissione europea, "La guida blu all'attuazione della normativa UE sui prodotti 2022", C247, 2022.

[72] Tra i requisiti tecnici che i prodotti devono possedere, l'Allegato I, sezione I elenca: la configurazione sicura per impostazione predefinita; la protezione da accessi non autorizzati mediante meccanismi di controllo appropriati; la protezione della riservatezza dei dati personali o di altro tipo trattati mediante una crittografia all'avanguardia; etc.

[73] Contestualmente è stato anche proposto un regolamento che modifica il Cybersecurity Act per consentire la futura adozione dei sistemi di certificazione per i «servizi di sicurezza gestiti" (COM(2023) 208 final).

cybersicurezza (EU-CyCLONe[74] e la rete di CSIRTs[75]) al fine di rafforzare le capacità dell'UE di individuare, preparare e rispondere a minacce e attacchi significativi e su larga scala[76].

La capacità di rispondere a minacce e attacchi (quindi, perturbazioni), come abbiamo già visto, è un tratto fondamentale della resilienza. Non stupisce, pertanto, che nel testo della proposta si legga come sia necessario per l'Unione accrescere la *resilienza* di cittadini, imprese ed organismi operanti in settori critici ed altamente critici contro le crescenti minacce alla sicurezza informatica, che possono avere impatti devastanti sulla società e sull'economia[77].

Infatti, uno dei tre obiettivi postulati dall'articolo 1 della proposta è «migliorare la resilienza dell'Unione e contribuire a una risposta efficace, *esaminando e valutando* incidenti significativi o su larga scala*, traendone insegnamenti* e, se del caso, raccomandazioni [enfasi aggiunta]»[78]. L'elemento riflessivo che emerge dal testo, che è senza dubbio da accogliere positivamente, considerata l'estrema dinamicità del panorama delle minacce, allinea il concetto di resilienza espresso nel Cyber Solidarity Act alle definizioni date in ambito socio-ecologico (vedi sezione 2), dove risultavano cruciali i temi dell'adattamento e della trasformazione.

Il paradigma dell'adattamento e della trasformazione si evince soprattutto dal capo IV della proposta sulla cyber solidarietà, che introduce il meccanismo di revisione degli incidenti di cybersicurezza. L'ENISA, infatti, è incaricata di elaborare un report di revisione collaborando con tutti i portatori di interessi rilevanti – conformemente alla spinta verso un approccio *multi-stakeholder* e cooperativo dell'ultima Strategia[79] – di un determinato incidente di larga scala, su richiesta della Commissione, della rete di CSIRT o di EU-CyCLONE, che analizzi le minacce, le vulnerabilità, le azioni di mitigazione e, ovviamente, le c.d. *lessons learned*[80].

L'analisi degli ultimi due regolamenti proposti dalla Commissione europea in materia di cybersicurezza conferma l'ipotesi conclusiva avanzata nella sezione precedente. Da una parte, è possibile ravvisare nei quadri giuridici rilevanti fattori tipizzanti di un concetto di resilienza consolidato nella letteratura tecnico-

[74] EU-CyCLONe è istituita dall'art. 16 della NIS2 al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione, operando pertanto come intermediario tra il livello tecnico e politico. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e della Commissione; ENISA mantiene il segretariato e sostiene lo scambio sicuro di informazioni.

[75] Una rete di CSIRT (*computer security incident response team*) nazionali era già stata introdotta dalla NIS1. La NIS2 mantiene tale assetto (art. 15), al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri. È composta da rappresentanti dei CSIRT nazionali e della squadra di pronto intervento informatico dell'Unione (CERT-UE). La Commissione partecipa in qualità di osservatore, mentre ENISA ne assicura il segretariato e fornisce attivamente assistenza alla cooperazione fra i CSIRT.

[76] Commissione europea, "Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents" COM(2023) 209 final.

[77] Proposta Cyber Solidarity Act, considerando 3.

[78] Proposta Cyber Solidarity Act, Art. 1, para.2, lett. c. Gli altri due obiettivi sono: a) rafforzare l'individuazione comune dell'Unione e la consapevolezza situazionale delle minacce e degli incidenti informatici, consentendo così di rafforzare la posizione competitiva dei settori dell'industria e dei servizi dell'Unione nell'economia digitale e di contribuire alla sovranità tecnologica dell'Unione nel settore della cybersicurezza; b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e rafforzare la solidarietà sviluppando capacità di risposta comuni contro incidenti di cybersicurezza significativi o su larga scala, anche mettendo a disposizione dei Paesi terzi associati al Digital Europe Programme (c.d. 'DEP') il sostegno dell'Unione per la risposta agli incidenti di cybersicurezza.

[79] Si veda *ex multis* Barrinha, Christou 2022:372; Brandão, Camisão 2022; Backman 2023; cfr. con Dunn Cavelty, Smeets, 2023.

[80] Proposta Cyber Solidarity Act, Art. 18.

scientifica. Dall'altra, in termini di osservazione scientifica, scegliendo come livello d'astrazione il piano di applicazione normativa, emerge una sostanziale indifferenza nell'inquadrare il problema come un tema di (cyber)resilienza o di cybersicurezza, rilevando, piuttosto, il quadro sostanziale e procedurale sotteso alla direzione tracciata dai due termini citati – come avviene, similmente in forum internazionali come l'ONU dove 'resilienza' viene utilizzata come un concetto vago e flessibile per indicare un senso di direzione[81]. In termini 'tardo-Wittgensteiniani', il significato è dato dall'uso[82].

5. Conclusione

Secondo la norma ISO 10459[83] sicurezza è lo «studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa, che possono danneggiare le risorse materiali, immateriali ed umane di cui l'azienda dispone e necessita per garantirsi un'adeguata capacità concorrenziale». Tre, dunque, secondo lo standard internazionale, sono le fasi in cui la sicurezza si estrinseca, fasi che possono essere trasposte nelle dimensioni classiche della sicurezza informatica: (i) robustezza, (ii) resilienza e (iii) risposta.

La robustezza è un requisito primario e consolidato: tutte le parti del sistema devono essere configurate, gestite e mantenute secondo criteri di protezione, definiti da norme tecniche del settore, fin dalla progettazione. In ottica preventiva e di protezione essa si fonda sul trattamento del rischio con un 'approccio reattivo'[84] che identifica, valuta e gestisce rischi noti sulla base di esperienze pregresse.

Nei sistemi odierni, dove la natura dei problemi cambia e i rischi possono emergere in modo diverso, è quantomai necessario integrare la dimensione della prevenzione con metodologie e soluzioni flessibili che, in chiave proattiva, siano in grado di adattare e aggiustare il sistema a seguito dell'evento avverso, perché anche durante la perturbazione si possano realizzare gli obiettivi (continuità operativa) trovando una nuova condizione di normalità.

È questa la definizione di *resilienza* che emerge dalla analisi condotta nel contributo rispetto a diversi ambiti scientifici. È la fase in cui l'organizzazione, seguendo un piano prestabilito, adotta misure per mitigare i danni dell'incidente informatico e mantenere l'operatività, rileva danni e responsabilità, segnala alle autorità competenti eventuali violazioni e getta le basi della ripresa in cui saranno ripristinati i dati e la piena operatività.

La (cyber) resilienza, come si è detto, è un requisito emergente nel quadro giuridico comunitario, politico e nei piani di investimento; il concetto, definito solo in alcuni atti giuridici, viene spesso richiamato senza una esplicita contestualizzazione, prestandosi quindi ad ambiguità interpretativa e di scopi anche in riferimento al concetto (di uso meno recente) di cybersicurezza. Su tale ambiguità il contributo ha inteso

[81] Le Nazioni Unite definiscono la resilienza come "la capacità di un sistema, di una comunità o di una società esposta ai pericoli di resistere, assorbire, adattarsi e riprendersi dagli effetti di un pericolo in modo tempestivo ed efficiente, anche attraverso la conservazione e il ripristino delle sue strutture e funzioni di base essenziali". Si veda Kimber 2019.

[82] Wittgenstein 1953.

[83] International Organization for Standardization, ISO è una importante organizzazione a livello mondiale per la definizione di norme tecniche internazionali, fra cui la famiglia ISO 2700 "Information Security Management Systems Family of Standards" standard di riferimento per la sicurezza delle informazioni.

[84] Viene fatto qui riferimento alla c.d. 'retroazione', ossia al raffinamento delle misure e dei controlli tecnici di sicurezza informatica in una prospettiva circolare e non statica (ciclo di denim).

far luce, domandandosi quali siano i fattori tipizzanti del concetto di resilienza e in quale relazione esso sia con il concetto di cybersicurezza.

L'analisi della nuova area di policy del diritto comunitario ha mostrato che, mentre nel contesto della sicurezza delle reti e dei sistemi (Direttiva NIS e NIS2) il legislatore utilizza i due termini in modo sostanzialmente interscambiabile, identificando dunque gli stessi ambiti di protezione e gli stessi obiettivi, in altri contesti – tra cui le nuove proposte legislative del Cyber Resilience Act e Cyber Solidarity Act – resilienza e cybersicurezza hanno alcuni indicatori caratterizzanti.

Cybersicurezza è maggiormente intesa come la capacità di proteggere i sistemi attraverso controlli preventivi, mentre (cyber) resilienza identifica la capacità di risposta alle sollecitazioni e di adattamento post incidente, abbracciando la visione di resilienza che emerge dalla letteratura tecnico-scientifica. D'altra parte, la linea di demarcazione non pare così netta e l'analisi di come le due nozioni operano negli atti giuridici rilevanti evidenzia un utilizzo unificato e spesso interscambiabile dei due termini, rimandando piuttosto ai profili sostanziali e procedurali sottesi.

Per concludere, nel quadro del diritto della Cybersicurezza dell'UE, il concetto di resilienza è un concetto flessibile che talvolta ingloba il concetto di cybersicurezza mentre, altre volte, ne è una dimensione. È sempre chiara, tuttavia, la direzione che individua: progettare e sviluppare sistemi in grado di salvaguardare il proprio funzionamento, garantendo la fornitura delle funzioni essenziali in seguito a perturbazioni ed eventi avversi, promuovendo altresì capacità di adattamento al nuovo stato e il ripristino delle proprie capacità operative.

Bibliografia

Agenzia per la Cybersicurezza nazionale (2022). Relazione annuale al Parlamento.

Backman, S. (2023). *Risk vs. threat-based cybersecurity: the case of the EU*, «European Security», 32, 1, pp. 85-103.

Barrinha A., Christou, G. (2022). *Speaking sovereignty: the EU in the cyber domain*, «European Security», 31, 3, pp. 356-376.

Biagioli, C. (1998). *Strutturazione funzionale dei testi legislativi per la trasparenza degli ordinamenti*, in Pattaro E., Zannotti F. (eds), *Applicazione e tecnica legislativa,* Milano, Giuffré.

Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). *Cyber Resilience – Fundamentals for a Definition*, in Rocha, A., Correia, A. M., Costanzo, S., Reis, L. P. (eds), *New Contributions in Information Systems and Technologies*, eds., Springer, pp. 311-316.

Brandão, A. P., Camisão, I., (2022). *Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy*, «Journal of Common Market Studies», 60, 5, 1335-1355.

Bygrave, L. A., (2022). *Cyber Resilience versus Cybersecurity as Legal Aspiration*, in *14th International Conference on Cyber Conflict: Keep Moving!* (CYCON), Tallin, Estonia, pp. 27-43.

Carayannis, E. G. et al. (2021). *Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience*, «IEEE Transactions on Engineering Management», 68, 1, pp. 223-234.

Chiara, P.G. (2023). *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, «Rivista Italiana di Informatica e Diritto», fascicolo 1, pp. 143-153

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan.

Clausmeier, D. (2023). *Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)*, «International Cybersecurity Law Review», 4, 1, pp. 79-90.

Clusit (2023). Rapporto Clusit 2023.

Commissione europea (2001). *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo.*

Commissione europea e Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza (2013). *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro.*

Commissione europea e Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza (2017). *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE.*

Commissione europea e Alto Rappresentante dell'UE per gli Affari Esteri e la Politica di Sicurezza (2020). *La strategia dell'UE in materia di cibersicurezza per il decennio digitale.*

Datola, G., Bottero M., De Angelis, E. (2021). *Enhancing Urban Resilience Capacities: An Analytic Network Process-based Application*, «Environmental and Climate Technologies», 25, 1, pp. 1270-1283.

Denardis, Laura (2021). *Internet in ogni cosa - Libertà, sicurezza e privacy nell'era degli oggetti iperconnessi*, Luiss University Press, Roma.

Dunn Cavelty, M., Kaufmann, M., Søby Kristensen, K. (2015). *Resilience and (in)security: Practices, subjects, temporalities*, «Security Dialogue», 46, 1, pp. 3-14.

Dunn Cavelty, M., Smeets, M. (2023). *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority*, «Journal of European Public Policy», 30, 7, pp. 1330-1352.

ENISA (2011). *Inter-X: Resilience of the Internet Interconnection Ecosystem.*

ENISA (2022). L'anno in rassegna.

ENISA (2023). *Foresight Cybersecurity Threats for 2030*.

European Parliamentary Research Service (2023). '*Cyber-resilience in the EU'*, in *Ten Issues to Watch in 2023*.

Europol (2023). *Internet Organised Crime Assessment (IOCTA).*

Floridi, L. (2008). *The Method of Levels of Abstraction*, «Minds and Machines», 18, 3, pp. 303-329.

Floridi, L. (2022). *Etica dell'Intelligenza Artificiale*, Raffaello Cortina Editore.

Guastini, R. (2012). *Manifesto di una filosofia analitica del diritto*, «Rivista di filosofia del diritto», fascicolo 1, pp. 52-53.

Hacker, P. M. S. (1969). *Definition in Jurisprudence,* «The Philosophical Quarterly (1950-)», 19, 77, pp. 343-347.

Hage, J. C., Pfordten, D. (2009). *Concepts in Law,* Springer.

Hart, H. L. A. (1961). *The Concept of Law*, Oxford University Press.

Holling, C. S. (1973). *Resilience and Stability of Ecological Systems*, «Annual Review of Ecology and Systematics», 4, pp. 1-23.

Kimber, L. R. (2019). *Resilience from the United Nations Standpoint: The Challenges of Vagueness*, in Wiig S., Fahlbruch B. (eds.), *Exploring Resilience: A Scientific Journey from Practice to Theory*, Springer, pp. 89-96.

Macagno, F. (2010). *Definitions in Law,* «Bulletin suisse de linguistique appliquée», 2, pp. 199-217.

Marshall, D. M. (2022). *UAS Integration into Civil Airspace: Policy, Regulations and Strategy*, Wiley & Sons.

Montemagni, E. (2022). *Le pubbliche amministrazioni nell'era delle tecnlogie cloud ed edge computing tra opportunità e rischi: il piano nazionale di ripresa e resilienza e le comunità digitali* in Abba, L., Lazzaroni, A., Pietrangelo M. (eds), *La Internet govenance e le sfide dalla trasfomazione digitale*, Editoriale scientifica Napoli, pp. 251-266.

Niemi, A., Torres, F. S., (2022). *Evaluation of the proposed European Commission directive on critical entities resilience and its potential to consolidate the resilience terminology*, in Leva, M. C., Patelli, E., Podofillini, L., Wilson,

S. (eds.), *Proceedings of the 32nd European Safety and Reliability Conference* (ESREL 2022), Research Publishing, pp. 2773-2780.

Papakonstantinou, V., De Hert, P. (2022). *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, «Technology and Regulation Journal», pp. 48-60.

Pietropaoli, S. (2022). *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, Giappichelli.

Rød, B., Lange, D., Theocharidou, M., Pursiainen, C. (2020). *From Risk Management to Resilience Management in Critical Infrastructure*, «Journal of Management in Engineering», 36, 4.

Rosager Ludvigsen, K., Nagaraja, S. (2022). *The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act*, arXiv, https://arxiv.org/abs/2205.13196

Rothrock, R. A. (2017) *Digital Network Resilience: Surprising Lessons from the Maginot Line*, «The Cyber Defense Review», 2, 3, pp. 33-40.

Sartor, G. (2009). *Legal concepts as inferential nodes and ontological categories,* «Artificial Intelligence and Law», 17, pp. 217-251.

Schmitz-Berndt, S., Chiara, P.G. (2022). *One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive*, «International Cybersecurity Law Review», 3, 2, pp. 289-311.

Searle, J. R. (1995). *The Construction of Social Reality*, New York: The Free Press.

Sievers, T. (2021). *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations*, «International Cybersecurity Law Review», 2, 2, pp. 223-231.

Song J. et al. (2019). *Resilience-vulnerability balance to urban flooding: A case study in a densely populated coastal city in China*, «Cities», 95, 102381.

Taddeo, M. (2019). *Is Cybersecurity a Public Good?*, «Minds and Machines», 29, 3, pp. 349-354.

Wagner, A. (2008). *Robustness and Evolvability: A Paradox Resolved*, «ProcBiolSci», 275, pp. 91-100.

Walker J., Cooper, M. (2011). *Genealogies of resilience: From systems ecology to the political economy of crisis adaptation*, «Security Dialogue», 42, 2, pp. 143-160.

Wittgenstein, L. (1953). *Philsophical investigations,* Basil Blackwell.

Woods, D.D., Leveson, N., Hollnagel, E. (2006). *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing.

World Economic Forum (2023). *Global Risks Report, 18th Edition*.