RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0123 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Federico Serini

La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana

Il trasferimento di questioni legate alla sovranità degli Stati all'interno di una dimensione sviluppata sugli ideali della a-gerarchia e del libero accesso, quale il cyberspazio, ne sta progressivamente cambiando le sue caratteristiche. Oltre ai tentativi di balcanizzare Internet o di modificarne la sua architettura, un altro tema di attuale interesse riguarda la sicurezza delle infrastrutture informatiche. Questa azione richiede il necessario bilanciamento da parte degli ordinamenti tra l'esigenza di libera circolazione dei beni ICT e la loro sicurezza dal rischio informatico. Il presente contributo intende concentrarsi su quest'ultimo aspetto, ponendo l'attenzione sui c.d. beni ICT posti al crocevia di tali valutazioni e interessi. Dopo aver delineato l'attuale quadro normativo sulla certificazione e standardizzazione di cybersicurezza a livello europeo e nazionale, saranno svolte alcune riflessioni conclusive sulle problematiche e sulle possibili prospettive relative alla sempre maggiore rilevanza della norma tecnica in questo settore.

Cybersecurity Act – Cyber Resilience Act – Procurement beni ICT – Standard e certificati di cybersicurezza

The fragmentation of the merceological cyberspace between certifications and cybersecurity standards. Some considerations in the light of the European and Italian disciplines

The transfer of issues related to the sovereignty of states within a dimension developed on the ideals of a-hierarchy and free access, such as cyberspace, is progressively changing its characteristics. In addition to the attempts to balkanise the Internet or modify its architecture, another issue of current interest concerns the security of information infrastructures This action requires the necessary balancing act on the part of legal systems between the need for free movement of ICT assets and their security from cyber risk. This contribution intends to focus on the latter aspect, focusing on the so-called ICT assets placed at the crossroads of these assessments and interests. After outlining the current legal framework on cybersecurity certification and standardisation on a European and national level, some concluding reflections will be made on the issues and possible perspectives on the increasing relevance of technical standards in this area.

Cybersecurity Act – Cyber Resilience Act – ICT assets procurement – Cybersecurity standards and certificates

L'Autore è dottorando di ricerca in Diritto pubblico, internazionale e comparato presso Sapienza – Università di Roma

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Il cyberspazio come dimensione merceologica: una prospettiva di studio

Spesso confuso o utilizzato come sinonimo di Internet, il cyberspazio rappresenta un concetto complesso e di difficile definizione univoca[1]. La letteratura sul punto, non solo giuridica, è tuttavia concorde nel precisare che le due nozioni non sono sinonimi.

Basti ricordare la definizione di Internet fornita da uno dei creatori della Rete, Vinton Cerf, come «il sistema di trasporto che sposta pacchetti di dati dal punto di origine alla destinazione [ove] diversi protocolli principali costituiscono l'Internet di base. Si tratta dell'*Internet Protocol* – IP, del *Transmission Control Protocol* – TCP e dell'*User Datagram Protocol* – UDP»[2].

Difatti, Internet è il servizio (costituito dalla summenzionata suite di protocolli) che ha permesso alle diverse reti continentali di connettersi tra di loro[3], costituendo lo spazio informazionale che occupa solo una regione del cyberspazio[4], in particolare quella responsabile della trasmissione dei dati e delle informazioni.

Ma ora cerchiamo di capire cosa si intende per cyberspazio. Precisiamo innanzitutto che non si tratta di un concetto giuridico, sebbene ormai diffusamente impiegato all'interno di leggi e regolamenti mediante l'uso del lemma "cyber"[5].

1. Secondo lo studioso F.D. Kramer esistono 28 differenti definizioni del termine *cyberspace*. Cfr. Kramer 2009.
2. Cerf 2022.
3. V. la definizione fornita dall'Enciclopedia Treccani ove l'Internet è definito come la «rete di elaboratori a estensione mondiale, mediante la quale le informazioni contenute in ciascun calcolatore possono essere messe a disposizione di altri utenti che possono accedere alla rete in qualsiasi località del mondo». Sul punto vedi anche Carotti 2016, p. XIII, ove l'A. definisce Internet come «una tecnica di trasmissione di dati».
4. Sul punto si faccia riferimento alla definizione elaborata nel 2022 dal Dipartimento della Difesa statunitense, secondo cui il cyberspazio è un dominio globale all'interno dell'ambiente informativo costituito dalla rete interdipendente di infrastrutture informatiche e di dati residenti «including the internet, telecommunications networks, computer systems, and embedded processors and controllers». Sul punto si rinvia al documento *Defense Primer: Cyberspace Operations* disponibile presso il sito del Congresso USA.
5. Sull'utilizzo del termine "cyberspazio" a livello giuridico si rinvia a Monti 2023a, p. 66, ove l'A. scrive che «invenzioni letterarie come il "ciberspazio" e il suo corollario "virtuale" hanno influenzato negativamente la riflessione giuridica […] essi non sono né fictio juris (come la persona giuridica) né metafore giuridiche (come la nozione di fonti del diritto), necessarie al funzionamento del Sistema. Di conseguenza, pur mantenendo

Come noto, la prima utilizzazione del termine la si trova in un romanzo di un genere letterario che stava prendendo piede negli anni Ottanta del secolo scorso, il *cyberpunk*. In *Neuromancer*, lo scrittore William Gibson ambienta il suo romanzo in una realtà futuristica e distopica ove i personaggi vivono esperienze alternative connettendosi – per l'appunto – al "cyberspace", spazio elettronico a cui è possibile accedere per archiviare, scambiare e trafugare dati e informazioni[6]. Alcuni autori hanno invece descritto il cyberspazio come una «realtà virtuale»[7], altri come una rete internazionale di computer costituente a tutti gli effetti una «electronic frontier»[8].

Con il tempo questa parola venne curiosamente utilizzata in ambiti poco attinenti con la letteratura, ossia a livello politico e militare. Tuttavia, se nel primo caso, come nelle diverse risoluzioni delle Nazioni Unite adottate a partire dal 1998, viene riconosciuta l'esistenza del cyberspazio senza dare definizione e limitandosi solo a definire i comportamenti degli Stati in questo "ambiente"[9]; nell'ambito militare il concetto assume una puntale rappresentazione nella sua struttura e nei suoi caratteri. In questo settore sono state infatti elaborate diverse formulazioni di cyberspazio che lo descrivono, nella gran parte dei casi, attraverso i concetti degli spazi fisici, definendolo quindi come un luogo, o come "dominio"[10].

Il tratto comune alle diverse formulazioni è nella individuazione dei livelli dello spazio cybernetico, anche noti come stratificazioni del cyberspazio. A partire dalla seconda metà degli anni 2000 alcuni studi hanno riorganizzato tali elementi secondo tre macro-livelli quali quello fisico, logico e sociale, di cui:

«a. the human layer: the users of computerization (communications and computers);
b. the logical layer: the software and bits. These move at the speed of light and represent information, instructions, cyberspace assets (such as valuable software, electronic funds), malware (such as Trojan horses), and more;
c. the physical layer: the network physical components, including hardware, mobile infrastructures, and stationary infrastructures, found on

un'indubbia utilità per spiegare fenomeni sociologici, psicologici e anche economici – come appunto, il metaverso – "ciberspazio" e i suoi derivati non dovrebbero avere alcun ruolo nell'individuazione di obiettivi normativi e nella loro trasposizione in leggi e regolamenti». Più diffusamente sul punto v. anche Monti 2023.

6. In particolare, Gibson descriveva il cyberspazio come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione […] Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità, linee di luce allineate nel non-spazio della mente, ammassi di costellazioni di dati» (Gibson 1984, p. 54).
7. L'informatico statunitense Jaron Lanier dà una definizione artistica del cyberspazio, sottolineando le potenzialità intrinseche del mezzo: «A twenty-first century art form that will weave together the three great twentieth-century arts: cinema, jazz and programming», v. Lanier 2017, p. 3.
8. V. Goldsmith-Wu 2006, p. 17 a proposito di John Perry Barlow.
9. Marrani 2020, p. 49 ss.
10. Nel *Warsaw Summit Communiqué* del 9 luglio 2016, l'Organizzazione del Trattato dell'Atlantico del Nord (NATO) ha riconosciuto il cyberspazio «as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea» (art. 70). Allo stesso modo, tempo addietro, nel 2003, la Casa Bianca con il *National Strategy to Secure Cyberspace* definiva lo "spazio cibernetico" come «un sistema nervoso – il sistema di controllo del Paese – composto da centinaia di migliaia di computer interconnessi, server, router, cavi in fibra ottica che permettono alle nostre infrastrutture critiche di lavorare. Così, il sano funzionamento dello spazio cibernetico è essenziale per la nostra economia e la nostra sicurezza nazionale». Nel 2009, Daniel Kuehl, ha definito il cyberspazio come: «un dominio globale nell'ambito dell'ambiente delle informazioni il cui carattere distintivo e unico è caratterizzato dall'uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare e sfruttare le informazioni tramite reti inter-indipendenti e interconnesse che utilizzano le tecnologie dell'informazione e della comunicazione» (Kuehl 2009, pp. 26-28). Lo stesso anno, Martin C. Libicki definisce il cyberspazio individuando tre livelli: fisico, sintattico e semantico: Libicki 2009.

land, at sea, in the air, and in space (henceforth, "the physical spheres")[11]».

Recenti studi, ritenendo ormai obsoleta tale impostazione statica[12], hanno formulato definizioni orientate ad esaltare il profilo dinamico del cyberspazio («la natura dromologica […] dell'ambiente cibernetico»), caratterizzato da due elementi: la velocità di propagazione e l'abbattimento dei confini[13]. Come scrive Luigi Martino, simili caratteristiche «insieme all'economicità dei mezzi, condiziona il rapporto di reciprocità tra territorio, interazioni sociali e dinamiche politiche»[14].

Aderendo a tale tesi, nel presente contributo si propone una scomposizione e reinterpretazione del cyberspazio come insieme di "merci"[15] – per l'appunto cyberspazio "merceologico" – quale realtà in continua espansione in funzione degli sviluppi delle tecnologie informatiche che fanno ingresso nei mercati e che seguono pertanto le relative logiche e regole, tra cui anche i relativi standard di produzione e di qualità.

A tal proposito, intendiamo innanzitutto tracciare una ricostruzione delle "merci" che costituiscono il cyberspazio alla luce della vigente disciplina europea. Partiamo dalla nozione di «rete e sistema informativo», di cui all'art. 6, par. 1, della Direttiva 2022/2555 (ossia la Direttiva NIS II) che la definisce come:

«a. una rete di comunicazione elettronica quale definita all'articolo 2, punto 1, della direttiva (UE) 2018/1972 [ossia come «i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata, e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le

11. Cfr. Even-Siman-tov 2012, p. 10. Analogamente vedi anche la definizione elaborata dal gruppo di esperti indipendenti riuniti nell'International Groups of Experts su invito della NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), in Schmitt 2017, Rule 1-Sovereignty (general principles par. 4, p. 12) «The physical layer comprises the physical network components (i.e. hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consist of the connection that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities». Altra definizione è data dalla norma tecnica ISO/IEC 27032:2012, *Information technology — Security techniques — Guidelines for cybersecurity, Introduction*, che definisce il cyberspazio come quel complesso ambiente risultante dall'interazione di persone, software e servizi su Internet per mezzo di dispositivi tecnologici e reti ad esso connessi, «which does not exist in any physical form».

12. Rattray 2009, pp. 253 ss., ove l'A. scrive che «the "geography" of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or "moved" by insertion of new coded instructions in a router or switch», salvo tuttavia riconoscere che «Cyberspace is not, however, infinitely malleable: limits on the pace and scope of change are governed by physical laws, logical properties of code, and the capacities of organizations and people».

13. Martino 2018, p. 66, ove l'A. scrive che la *National Military Strategy for Cyberspace Operations* (NMS-CO) del 2006 ha descritto il cyberspazio attraverso l'acronimo VUCA, ossia: *Volatility*, *Uncertainty*, *Complexity*, *Ambiguity*. Per un tentativo definitorio, secondo sia il profilo statico sia dinamico del cyberspazio, si veda la formulazione elaborata dal gruppo di ricerca istituito presso la Scuola Sant'Anna di Pisa in Mayer-Martino-Mazurier-Tzvetkova 2014.

14. Martino 2018, p. 66.

15. Cfr. Finocchiaro 2001, p. 571, ove l'A. scrive che Internet «non è un luogo ma è un mezzo di comunicazione» che non ha natura unitaria ma è composto da «un insieme di reti e di sottoreti, autonome e senza organizzazione gerarchica».

reti utilizzate per la diffusione radiotelevisiva, e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato»];
b. qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali; o
c. i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;»[16]

nonché anche i concetti introdotti all'art. 2, nn. 12, 13 e 14 del Regolamento (UE) 2019/881 (anche noto come *Cybersecurity Act*), sul quale si dirà più ampliamente dopo par. 4, relativi a:

«– "prodotto TIC": un elemento o un gruppo di elementi di una rete o di un sistema informativo;
– "servizio TIC": un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;
– "processo TIC": un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC».

La proposta di Regolamento relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, anche nota come proposta di *Cyber Resilience Act*, (d'ora in poi anche proposta CRA), definisce invece all'art. 3, n. 1, il "prodotto con elementi digitali" come «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente».

Formulazione che riteniamo essere sintesi di quella che era già stata introdotta con la Direttiva 2019/771, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il Regolamento (UE) 2017/2394 e la Direttiva 2009/22/CE, e che abroga la Direttiva 1999/44/CE. All'art. 2, n. 5, lett. b), la Direttiva descrive i "beni con elementi digitali" come «qualsiasi bene mobile materiale che incorpora o è interconnesso con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni del bene»; mentre ai n. 6 e 7 del medesimo disposto, sono fornite le definizioni di «"contenuto digitale": i dati prodotti e forniti in formato digitale»; «"servizio digitale": a) un servizio che consente al consumatore di creare, trasformare, memorizzare i dati o di accedervi in formato digitale; oppure b) un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore o da altri utenti di tale servizio o qualsiasi altra interazione con tali dati».

Inoltre, dato che i requisiti orizzontali dettati dalla la proposta CRA sono allineati[17] con gli obiettivi dei requisiti delle norme specifiche di cui all'art. 3, par. 3, lett. d), e) ed f) della Direttiva 2014/53/UE concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (c.d. RED), successivamente specificati dal Regolamento delegato (UE) 2022/30[18], riteniamo utile richiamare anche la definizione di "apparecchiature radio" che:

«i) sono di per sé in grado di comunicare tramite Internet, indipendentemente dal fatto che comunichino direttamente o tramite qualsiasi altra apparecchiatura («apparecchiature radio connesse a Internet»), vale a dire che tali apparecchiature connesse a Internet utilizzano protocolli necessari per lo scambio di dati con la rete Internet direttamente o tramite un'apparecchiatura intermedia;
ii) possono essere giocattoli con funzione radio che rientrano anche nell'ambito di applicazione della direttiva 2009/48/CE del Parlamento

16. Riproponiamo qui di seguito anche la definizione del concetto di «rete e sistema informativo» della Direttiva (UE) 2016/1148 (c.d. *Direttiva NIS I*), come «a) una rete di comunicazione elettronica ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE; b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; o c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione».

17 Cfr. considerando 15, della proposta CRA.

18. Chiara 2022.

europeo e del Consiglio oppure sono progettate o destinate esclusivamente alla cura dei bambini, come i monitor per bambini; o

iii) sono progettate o destinate, esclusivamente o non esclusivamente, ad essere indossate, oppure assicurate o appese a qualsiasi parte del corpo umano (compresa la testa, il collo, il tronco, le braccia, le mani, le gambe e i piedi) o a qualsiasi indumento (compresi copricapi, guanti e calzature) indossato da esseri umani, quali apparecchiature radio sotto forma di orologi da polso, anelli, braccialetti, cuffie, auricolari o occhiali («apparecchiature radio indossabili»)».

Alla luce di tali richiami, è possibile intuire, almeno per quanto riguarda l'ordinamento europeo e degli Stati membri, che l'infrastruttura logica e materiale del cyberspazio possa essere interpretata come un agglomerato di prodotti, processi e servizi che attengono alle tecnologie dell'informazione e della comunicazione (d'ora in poi "beni ICT") che circolano nel mercato globale.

In particolare, riteniamo che cyberspazio e mercato liberalizzato rispondano a regole simili[19]. Se per il primo è essenziale garantire il libero flusso delle informazioni per mezzo della tecnica informatica e il funzionamento delle tante infrastrutture che ne consentono la sua esistenza, per il secondo il fine è quello di garantire lo scambio di beni e di servizi che alimenta la circolazione dei beni ICT nei mercati.

L'Unione europea, come emerge dalla *Strategia per il mercato unico digitale*[20], intende coniugare queste due esigenze integrando le dinamiche della concorrenza con l'esigenza di sicurezza dei beni ICT (e dei contenuti digitali), promuovendo un circuito virtuoso che trova fondamento nella certezza giuridica e nella fiducia dei consumatori e dei venditori[21].

Nel presente lavoro si farà riferimento al concetto di cyberspazio "merceologico" al fine di tentare di analizzare gli effetti delle politiche pubbliche, europee e nazionali, su questa dimensione. Nello specifico, l'obiettivo sarà quello di studiare la gestione di tale complessità attraverso i recenti interventi in materia di certificazione e normazione tecnica a livello europeo e nazionale, quali strumenti che, a seconda del loro utilizzo, possono rappresentare o meno un "attrito" al dinamismo del cyberspazio[22].

2. La governance di cybersicurezza tra frammentazione tecnica e politica del cyberspazio

In *Connectography*, Paragh Khanna scrive che «Internet è stata pensata come una struttura a network, il cui obiettivo è quello di connettere tra loro i nodi di questo network, non certo di rappresentare le nazioni che ne fanno parte». Tuttavia preconizza lo studioso, questa rete oggi «sta evolvendosi dallo stato di collettività non statuale e non governata, dotata soltanto di una supervisione tecnica, a quello di arena geopolitica percorsa dai processi di intensa complessità»[23].

Tale situazione è frutto di un processo evolutivo della regolazione del cyberspazio che possiamo

19. Precisiamo tuttavia che non intendiamo assimilare la *lex informatica* alla *lex mercatoria*. Sul punto si rinvia a Finocchiaro 2001, p. 605 ss., ove l'A. svolge una fondamentale distinzione secondo cui «mentre la *lex informatica*, intesa come insieme di regole tecniche che veicolano scelte giuridiche, si applicherebbe ad ogni tipo di relazione, la *lex mercatoria* è, invece, diritto della classe dei mercanti, applicabile ai rapporti tra imprese». Tuttavia, l'espressione *lex mercatoria* non è sempre utilizzata in maniera univoca, questione che ha dato motivo di aprire un dibattito sul suo significato. A tal proposito v. Berger 1999; Galgano 2016; Goldman 1983; Teubner 1996, pp. 3-28; Mertens 1996, p. 31 ss..

20. COM(2015) 192, *Strategia per il mercato unico digitale in Europa*. In particolare, si faccia riferimento al punto 2.3 relativo a "Impedire i geoblocchi ingiustificati", e al punto 3.4 "Aumentare fiducia e sicurezza nei servizi digitali e nella gestione dei dati personali".

21. Cfr. considerando 5, Direttiva 2019/771 relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE.

22. Sul punto si faccia riferimento a Khanna 2016, p. 66 ss., ove l'A. prendendo in prestito dalla fisica i concetti di "flusso" e "attrito" propone uno studio sulla gestione della complessità delle connessioni, riferita non solo ad Internet ma ad ogni forma di interazione tra esseri umani e cose nel mondo.

23. *Ivi*, p. 451 ss.

distinguere in due macro-momenti. I primi decenni dalla creazione di Internet sono stati caratterizzati dall'assenza di vincoli da parte degli Stati. Durante questo periodo, i governi hanno infatti accettato la necessità di un modello di regolamentazione flessibile e favorevole all'innovazione, quale quello della *self-regulation*. Modello che tuttavia da una parte ha dato inizio all'uso commerciale di Internet[24], dall'altra ha segnato il fallimento del movimento libertario della Rete che auspicava la creazione di uno spazio fuori dalla giurisdizione dei poteri dei governi[25].

Nell'ultimo ventennio, la crescente consapevolezza sui rischi della Rete ha tuttavia portato i poteri pubblici a volgere l'attenzione verso il cyberspazio, dimostrando «non solo di [poterlo] regolamentare ma anche "iper-regolare"»[26].

La questione che ci si pone oggi quindi è in che maniera gli Stati, il cui intervento è successivo nel tempo, intendano regolare il cyberspazio, ora inteso come quel complesso di software e hardware che garantiscono la connettività universale grazie al servizio Internet in virtù dei principi di neutralità e libero accesso.

Il dato certo fornito dalla dottrina internazional-pubblicistica è che, mentre uno Stato può invocare la propria sovranità territoriale per regolamentare hardware e utenti che risiedono in esso, nessuno Stato – singolarmente considerato – può pretendere di regolare l'intero spazio informazionale cybernetico[27].

Non esiste neppure un'organizzazione internazionale competente a tal proposito. Anche a seguito delle modifiche alla struttura dell'ICANN volte a garantire l'indipendenza dal governo degli Stati Uniti del sistema di regolamentazione del *Domain Name Server* (DNS), non si è giunti alla conclusione di ritenere tale ente alla stregua di una organizzazione internazionale. Sia perché solo una parte del governo di Internet passa per i meccanismi giuridici che regolano il sistema DNS[28], sia perché, malgrado il tentativo di approdare verso un modello in cui tutte le parti interessate, compresi i governi, partecipino in condizioni di parità[29], gli USA continuano a gestire unilateralmente detto sistema[30].

Come ravvisato da Goldsmith e Wu in tempi recenti, vi sono aspetti delle reti che non possono essere regolati unilateralmente ma necessitano di uno sforzo di regolazione condivisa a livello globale[31]. Tuttavia, allo stato attuale, considerata l'incertezza dei rapporti tra i poteri sovrani e il cyberspazio[32], e nell'assenza di un «founding international constitutional moment»[33], gli Stati

24. Goldsmith-Wu 2006.
25. Barlow 1996.
26. Pollicino 2023, p. 415.
27. Hollis 2014, p. 11.
28. Ruotolo 2014, p. 249.
29. La gestione del sistema DNS è stata sin dalle origini affidata al Governo degli Stati Uniti, il quale tuttavia aveva concepito *ab origine* il proprio ruolo in maniera temporanea, come emerge dallo *Statement of Policy on the Management of Internet Names and Addresses* emanato il 10 giugno 1998 dal Dipartimento del commercio statunitense ove è espresso l'impegno ad una transizione che consenta al settore privato di avere un ruolo dominante nella gestione del DNS. Nel 2003, il *World Summit on Information Society* (WSIS) delle Nazioni Unite aveva studiato i possibili meccanismi idonei a garantire un più ampio coinvolgimento internazionale nella governance di Internet e in particolare nella gestione del sistema dei nomi di dominio, ove nessun governo avrebbe dovuto rivestire un ruolo preminente. Nonché si faccia riferimento anche al *Montevideo Statement on the Future of Internet Cooperation* del 2013 ove le principali organizzazioni responsabili della gestione tecnica di Internet (ICANN, IETF, ISoc) hanno auspicato un'accelerazione della globalizzazione delle funzioni di ICANN e IANA (*Internet Assigned Numbers Authority*, la sezione di ICANN, che concretamente gestisce il DNS). Sul punto più ampiamente si rinvia a Ruotolo 2016, p. 38.
30. *Ibidem*.
31. Goldsmith-Wu 2006, p. 164.
32. Lessig 2006, p. 302.
33. *Ibidem*.

stanno tentando di plasmare Internet e il cyberspazio secondo propri orientamenti ideologici e interpretativi[34].

A dire il vero il tema ha solitamente sollevato preoccupazioni circa la frammentazione di Internet, quale servizio concepito e sviluppato come universale e privo di barriere[35].

Data l'incertezza del termine, la letteratura sul punto ha enucleato tre tipologie di frammentazione: «*Technical Fragmentation*: conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points. *Governmental Fragmentation*: Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. *Commercial Fragmentation*: Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources»[36].

Tali definizioni ci sembrano utili in quanto riteniamo che così come si è soliti parlare della frammentazione di Internet, altra questione di non secondario rilievo è la frammentazione del cyberspazio. Gli standard e le certificazioni di cybersicurezza dei prodotti ICT sono un emblematico esempio in tal senso. Si tratta di strumenti frutto di un processo di normazione privata che, se uniformemente diffusi e utilizzati da tutti i soggetti interessati, possono costituire un utile incentivo alla circolazione dei beni ICT nel mercato ed allo stesso tempo essere portatori di indubbi benefici per la sicurezza delle reti e dei sistemi informatici a livello globale, concorrendo a colmare il vuoto dato dal fallimento del diritto internazionale nella stabilità del cyberspazio[37]. Diversamente, la moltiplicazione di norme tecniche e certificazioni diverse tra loro, se non addirittura incompatibili, ha l'effetto di creare barriere nel mercato[38], nonché di incidere negativamente sulla interoperabilità tecnica e sulla sicurezza dei sistemi[39] dal quale potrebbe derivare una inevitabile frammentazione del cyberspazio.

Anche in questo caso, l'elemento tecnico e quello economico appena evidenziati non prescindono da quello politico. Con il tempo gli standard – apparentemente tecnici e apolitici – hanno infatti mostrato di essere espressione di interessi ed esigenze che non sono più quelle del mondo privato e commerciale, ma degli Stati[40].

Un recente esempio sul punto può essere colto nella proposta avanzata nel settembre 2019 da Huawei, *China Mobile Communications Corporation*, China Unicom, e il Ministero cinese dell'industria e delle tecnologie dell'informazione in seno al *Telecommunication Standardization Advisory Group* (TSAG) dell'ITU circa la creazione di una nuova architettura di rete che possa far fronte ai futuri sviluppi delle tecnologie informatiche[41]. Ritenendo ormai obsoleto l'utilizzo del protocollo IPv6, soprattutto in previsione delle tecnologie quantistiche, Huawei ha infatti proposto lo sviluppo di un nuovo protocollo IP[42], facendone richiesta ai Gruppi di Studio del *Telecommunication Standardization Sector* (ITU-T) *Study Group*.

Le prime opposizioni sono state quelle dell'Olanda e della Gran Bretagna, le quali hanno ravvisato che i protocolli di rete sono stati sviluppati con un approccio *bottom-up* e pertanto tale proposta sarebbe dovuta essere presentata in altra sede

34. Eichensehr (2015), p. 329.

35. Bertola-Quintarelli 2023.

36. Drake-Cerf-Kleinwächter 2016, p. 4. Il contributo nasce dall'esigenza di chiarire l'argomento in questione al fine di facilitare il confronto in seno al *World Economic Forum's Multi-year Future of the Internet Initiative* (FII) dato che il concetto di "frammentazione" non ha univoco significato:«A human rights lawyer, a trade economist and a network engineer might each give the term a special shade of meaning based on their respective priorities and experiences» (p. 11).

37. Katagiri 2021.

38. World Trade Organization 2017.

39. Oddenino 2018, pp. 31-51.

40. Mattli-Büthe 2003, pp. 1-42. Sul punto vedi anche Wouters 2023, pp. 66-84.

41. Chen-Wang-Li-Lou-Jiang-Galis 2020.

42. Sulle caratteristiche del nuovo protocollo proposto si rinvia a Jiang 2019.

come l'*Internet Engineering Task Force* (IETF)[43]. Dello stesso avviso è stata anche l'Unione europea che, oltre a sottolineare l'inopportuna sede della proposta, ha anche evidenziato che non vi sono prove che l'attuale standard IP sia inadeguato rispetto allo sviluppo delle nuove funzionalità Internet[44].

Sebbene la proposta cinese sia stata poi respinta dall'ITU, il caso può essere preso in esame per l'analisi dei modelli e delle strategie di governo della Rete che si stanno delineando. Innanzitutto, diversamente dall'esperienza del WCIT-12[45], precisiamo che la proposta avanzata dalla Cina non ha avuto ad oggetto l'espressa revisione della governance di Internet, ma l'"aggiornamento" (*upgrade* nella documentazione ufficiale) del protocollo IP. Motivo che ha stimolato le censure degli oppositori sull'inadeguata sede della presentazione della proposta. Brevemente si precisa che mentre nell'IETF il processo decisionale è trasparente e aperto a tutte le parti interessate (inclusa l'industria, la società civile e il mondo accademico), l'ITU-T segue un modello multilaterale ove gli Stati membri sono gli unici partecipanti ad avere l'ultima parola sull'approvazione della proposta, o esprimere un voto, quando non c'è consenso[46].

Ma la questione che qui più interessa riguarda l'oggetto della proposta – per l'appunto il nuovo protocollo IP, una norma tecnica quindi – il cui utilizzo delineato nella proposta lascia intendere la natura politica delle norme tecniche e degli enti di normazione che le elaborano. Come è stato osservato da Emily Taylor, Kate Jones e Carolina Caeiro, nel caso di specie, «Standards-setting enables it [China] to build its own ideological tenets into the design and architecture of new technology in ways that until recently were largely beneath the radar of human rights bodies. By leading standardization processes, China is looking to reshape the architecture of the Internet and set the rules that will govern the technologies of the future»[47].

I processi di standardizzazione possono quindi consentire agli Stati di inserire i propri principi ideologici nella progettazione e nella architettura delle nuove tecnologie con modalità inedite[48].

Allo stesso modo, anche l'inserimento dell'obiettivo della «leadership on standards, norms and frameworks in cyberspace» che compone uno dei punti della *Strategia europea di cibersicurezza per il decennio digitale* presentata nel dicembre 2020 è un esempio di tale inedito uso delle norme tecniche[49]. Si apprende dal documento, che «[i]nternational standardisation is increasingly used by third countries to advance their political and ideological agenda, which often does not correspond with the values of the EU», motivo per cui l'Unione si impegna a: «Shaping international standards in

43. Sugli aspetti di dettaglio si rinvia a Wouters 2023, p. 71; nonché a Radu-DeGregorio 2023, p. 15 ss.

44. *Ibidem*.

45. Il riferimento è al *World Conference on International Telecommunications* (WCIT) tenutosi a Dubai nel Dicembre 2012. L'obiettivo dell'incontro era quella di applicare a Internet le condizioni dei servizi di telecomunicazione previsti nelle *International Telecommunication Regulations* (ITRs) elaborate dall'Unione Internazionale delle Telecomunicazioni (ITU), nel 1988 sul principio del «chi trasmette paga». Tuttavia altro argomento dell'incontro è stato il tentativo di revisionare la governance di Internet da parte di Cina, Russia e altri Stati del medio-oriente, il cui intento era quello di affidare la gestione della Rete ad un'organizzazione internazionale di stampo classico al fine di aumentare la rilevanza dei governi nella gestione della Rete. Sul punto si rinvia diffusamente a Ruotolo 2014, p. 545 ss.

46. Wouters 2023, pp. 71 e 72.

47. Caeiro-Jones-Taylor 2023, p. 186, ove gli AA. scrivono che «[s]tandards-setting enables it [China] to build its own ideological tenets into the design and architecture of new technology in ways that until recently were largely beneath the radar of human rights bodies. By leading standardization processes, China is looking to reshape the architecture of the Internet and set the rules that will govern the technologies of the future». Si rinvia al citato contributo soprattutto per riguarda l'analisi dell'impatto della proposta cinese sui diritti umani.

48. Mattli-Büthe 2003.

49. European Commission, *Joint communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18, 16 December 2020.

the areas of emerging technologies and the core internet architecture in line with EU values […] to ensure that the Internet remains global and open, that technologies are human-centric, privacy-focused, and that their use is lawful, safe and ethical. As part of its upcoming Standardisation Strategy, the EU should define its objectives for international standardisation, and conduct proactive and coordinated outreach to promote these at international level»[50].

Le due questioni attengono a particolari aspetti di governance del cyberspazio che si caratterizza per la contrapposizione di due approcci: quello multilaterale, quale metodo in uso nelle organizzazioni internazionali tradizionali, che prevede la sola partecipazione degli Stati (*state based model*, o *top-down*); e quello di governance *multistakeholder*, o *bottom-up*, che coinvolge anche altri soggetti di non secondaria rilevanza nel processo di regolazione, ossia le rappresentanze della società civile, e gli attori privati[51].

Contrapposizione di assetti che, rileva la dottrina di diritto internazionale dell'economia, si riflette anche nei modelli di formazione degli standard di cybersicurezza, di cui nello specifico: da una parte il modello *top-down*, *government-centred* e dall'altra quello *bottom-up*, *multistakeholder*[52].

Lo Standard *WLAN Authentication and Privacy Infrastructure* (WAPI) sviluppato dalla Cina è un tipico esempio riconducibile al primo modello. Tuttavia, il dato reale testimonia una netta maggioranza di standard di cybersicurezza frutto di processi *bottom-up* e quindi dell'affermazione nel mercato di norme tecniche di natura non cogente (volontaria per l'appunto), elaborate da organismi privati e da cui diversi governi, tra cui anche l'Italia, hanno tratto spunto per regolare con norme giuridiche la propria cybersicurezza interna (*rectius* incorporazione)[53].

È il caso del *Cybersecurity Framework* (CSF) sviluppato dal *National Institute of Standards and Technology* (NIST) degli Stati Uniti per la prima volta nel 2013[54], e il cui ultimo aggiornamento è atteso per il 2024[55]. Si tratta di una norma volontaria volta a migliorare la gestione della cybersecurity per le organizzazioni, sia nel settore pubblico che in quello privato. Come si apprende dal testo dell'*executive order* 13636, *Improving Critical Infrastructure Cybersecurity*, la formulazione del *framework* è avvenuta all'interno di una serie di consultazioni aperte alla partecipazione delle più ampie rappresentazioni del governo, ma anche del mondo imprenditoriale (tra cui anche gli stessi proprietari di infrastrutture critiche), mondo accademico, agenzie di normazione e società civile[56].

Sulla scorta di una breve panoramica sulla governance degli standard di cybersicurezza, il presente contributo si concentrerà sulla disciplina della standardizzazione e certificazione a livello europeo e nazionale. Pertanto nel prosieguo, dopo la presentazione di alcuni concetti introduttivi (par. 3), saranno analizzate la normazione tecnica europea (parr. 3.1, 3.2), avendo modo di soffermarci anche sugli standard e gli organismi di normazione di cybersicurezza a livello europeo (par. 3.3), e il quadro di certificazione europea introdotto con il *Cybersecurity Act* (par. 4), e le relative applicazioni a livello italiano (parr. 4.1 e 4.2). Sarà inoltre analizzata la proposta di regolamento *Cyber Resilience Act* (CRA), alla luce dei recenti dibattiti sorti durante il trilogo tra i co-legislatori europei (par. 5).

3. Brevi cenni su certificazione, normazione tecnica e ordinamento giuridico

Possiamo definire brevemente la normazione tecnica come quella «attività di produzione di norme atte ad individuare le caratteristiche tecniche, merceologiche e qualitative dei prodotti industriali da

50. *Ivi*, p. 20.

51. Raymond-DeNardis 2015, pp. 572–616.

52. Peng 2018, pp. 445-470.

53. Shackelford-Russell-Haut 2016.

54. NIST 2014.

55. Teplinsky 2023.

56. Si rinvia al sito della Casa bianca, alla sezione 6 del documento *Consultative Process*, del 12 febbraio 2013.

immettere sul mercato nonché, più recentemente, dei sistemi e processi industriali e dei servizi»[57].

Per certificazione si intende invece «l'attività di verifica e di accertamento del rispetto delle norme tecniche nei singoli prodotti, sistemi o servizi immessi sul mercato»[58].

La normazione tecnica nasce nel contesto industriale dapprima dall'esigenza delle singole aziende di definire le caratteristiche costruttive e dimensionali dei propri prodotti, generando di conseguenza effetti di c.d. *vendor lock-in* che obbligavano i clienti a rivolgersi sempre allo stesso fabbricante. Solo a seguito della rivoluzione industriale, e al progressivo sviluppo del tessuto produttivo, la normazione tecnica è passata da essere appannaggio di singole aziende agli enti di normazione privati, con il fine di uniformare la produzione industriale a standard comuni[59].

Passando ora al prodotto del processo di normazione, occorre distinguere i concetti di norma e specifica tecnica. Facendo riferimento al quadro definitorio vigente, dettato dal Regolamento 1025/2012 (vedi *infra* par. 3.2), per "norma tecnica" si intende «una specifica tecnica, adottata da un organismo di normazione riconosciuto, per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi»[60]. La "specifica tecnica" è invece «un documento che prescrive i requisiti tecnici che un determinato prodotto, processo, servizio o sistema deve soddisfare […]»[61].

Il medesimo Regolamento ha inoltre introdotto la "norma armonizzata", nozione rientrante nell'ampia categoria delle norme tecniche, intesa come «una norma europea adottata sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione»[62] (di cui si dirà dopo al par. 3.2).

Preme tuttavia precisare che l'ordinamento italiano, con legge 21 giugno 1986, n. 317, dando attuazione alla disciplina europea in materia di normazione e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, oltre alle definizioni di cui sopra, prevede anche il concetto di "regola tecnica" definita come «una specificazione tecnica o altro requisito o una regola relativa ai servizi, comprese le disposizioni amministrative che ad esse si applicano, la cui osservanza è obbligatoria, de iure o de facto, per la commercializzazione, la prestazione di servizi, lo stabilimento di un fornitore di servizi o l'utilizzo degli stessi in uno Stato membro dell'Unione europea o in una parte importante di esso, nonché, fatte salve quelle di cui all'articolo 9-*ter*, le disposizioni legislative, regolamentari o amministrative che vietano la fabbricazione, l'importazione, la commercializzazione o l'utilizzo di un prodotto oppure la prestazione o l'utilizzo di un servizio o lo stabilimento come fornitore di servizi […]»[63].

Dal punto di vista giuridico, sebbene prendano il nome di "norme", tali strumenti non hanno natura giuridica in quanto la loro formazione non avviene per mezzo di un processo giuridico-politico, ma attraverso alternative forme di aggregazione di interessi all'interno di soggetti non statuali[64], il cui fine è quello di definire univocamente caratteristiche di prodotti, metodi e processi di produzione, nonché caratteristiche o metodi e criteri di valutazione circa la prestazione di un servizio.

57. Caia-Roversi Monaco 1995, p. 13.

58. *Ibidem*.

59. Andreini 1995, p. 45 ss.

60. Art. 2, n. 1, Regolamento 1025/2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.

61. Art. 2, n. 4, Regolamento 1025/2012.

62. Art. 2, n. 1, lett. c), Regolamento 1025/2012.

63. Art. 1, lett. f, della legge 21 giugno 1986, n. 317, "Disposizioni di attuazione di disciplina europea in materia di normazione europea e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione".

64. Cesarini 1929.

Le norme tecniche costituiscono pertanto un complesso di regole, volontarie e consensuali, non impositive di un obbligo o un dovere, ma unicamente di un onere a carico di quei soggetti privati, solitamente attivi nel mondo dell'industria, o soggetti pubblici, come le amministrazioni, che intendono conformarvisi al fine di adeguare le loro attività, prodotti o servizi ad uno standard univoco riconosciuto a livello internazionale[65].

Gli enti di normazione sono soggetti, spesso di natura privata, responsabili della produzione delle norme tecniche. Operano nel multilivello e, «per motivi essenziali storici», non sono più di tre: uno per il settore elettronico, uno per il settore delle telecomunicazioni e l'altro per tutti gli altri settori[66].

A livello internazionale sono presenti l'*International Organization for Standardization* (ISO), l'*International Electrotechnical Commission* (IEC) e l'*International Telecommunication Union* (ITU). A livello europeo troviamo invece l'*European Committee for Standardization* (CEN), l'*European Committee for Electrotechnical Standardization* (CENELEC) e l'*European Telecommunications Standards Institute* (ETSI). In Italia gli Organismi riconosciuti sono l'Ente Nazionale Italiano di Unificazione (UNI) e il Comitato Elettrotecnico Italiano (CEI).

Tra le normative tecniche e l'ordinamento giuridico sussiste una relazione. La norma tecnica acquista rilevanza per l'ordinamento giuridico ogni qualvolta questa venga "assunta" al suo interno, e tipicamente ciò avviene attraverso gli istituti dell'incorporazione e del rinvio.

Vi è incorporazione quando il contenuto della norma tecnica viene trasposto *sic et sempliciter* all'interno di una fonte giuridica (generalmente primaria e/o secondaria), mentre il rinvio consiste nell'esplicito riferimento ad una norma tecnica puntualmente indicata (rinvio fisso o materiale), oppure nell'utilizzo di clausole generali all'interno di un disposto giuridico, come ad esempio il richiamo "alle migliori tecniche disponibili", "allo stato dell'arte" o piuttosto ai "migliori standard tecnici e di sicurezza", facenti riferimento al rispetto di normative tecniche quali presupposto di una buona pratica (rinvio mobile o formale)[67].

La norma tecnica viene così acquisita all'interno della norma giuridica, e quindi nell'ordinamento, suscitando non pochi interrogativi sulla natura di tale fonte una volta che sia stata incorporata o richiamata.

Relativamente al primo caso, nel dubbio se tale strumento potesse comportare una «tecnicizzazione della norma giuridica a contenuto tecnico o giuridicizzazione della norma tecnica incorporata nella norma giuridica»[68], la dottrina maggioritaria è pacificamente concorde nel ritenere che la norma tecnica venga "giuridicizzata", costituendo parte integrante del disposto giuridico. Diversamente, maggiori difficoltà interpretative sono state ravvisate in relazione alla qualificazione delle norme tecniche oggetto di rinvio, soprattutto se si considera che tali fonti, di natura privata, e protette da diritto d'autore, troverebbero una difficile cognizione e applicazione da parte di quei soggetti che non le abbiano acquistate.

Sul punto, alcuni hanno sostenuto che il «mero richiamo, in un documento ufficiale, del numero, titolo o data di applicazione della normativa» – ossia il rinvio materiale – porti alla «messa in corto circuito del diritto d'autore» poiché la norma tecnica così rinviata acquista rilevanza pubblicistica[69]. Tuttavia, il dubbio sembra persistere relativamente al rinvio mobile, solitamente utilizzato nei casi in cui la legge si limita a dettare la disciplina generale di una materia, per poi lasciare ampio margine ai destinatari circa l'utilizzo delle norme tecniche utili a raggiungere il risultato "al meglio delle buone pratiche".

In conclusione, escluso quest'ultimo caso, in cui la norma tecnica conserva il suo carattere di fonte volontaria non cogente, l'incorporazione e il rinvio fisso trasformano la norma tecnica in un atto giuridico, facendole così assumere la denominazione di "norma tecnica pubblica" o "regola tecnica".

65. Salmoni 2002, p. 150 ss.

66. Andreini-Caia-Elias-Roversi Monaco 1995, p. 32.

67. Greco 1999, p. 37 ss.

68. Salmoni 2002.

69. Gigante 1997, p 313 ss.

Tuttavia, come è stato precisato, il ricorso all'incorporazione e al rinvio non fanno dell'ordinamento tecnico un ordinamento giuridico, poiché i prodotti del primo acquistano forza normativa solo attraverso questo metodo di «selezione volontaria operata per il tramite della legge o di altro atto – fonte dell'ordinamento giuridico», conferendo quindi alla norma tecnica «non la qualificazione di fonte del diritto ma efficacia cogente»[70].

3.1. La normazione tecnica europea

L'esperienza dell'Unione europea nel settore nella normazione tecnica è di particolare interesse ai fini della presente trattazione. L'Unione ha fatto ricorso allo strumento della standardizzazione per facilitare il processo di integrazione del mercato unico, ed allo stesso tempo garantire fini sociali come la tutela dell'ambiente e la sicurezza individuale e collettiva[71].

Si distinguono due momenti che hanno caratterizzato la disciplina sulla standardizzazione europea. Fino alla metà degli anni Ottanta del secolo scorso, l'intervento della allora Comunità aveva come unico obiettivo quello di smantellare gli ostacoli tecnici che si frapponevano al libero scambio intracomunitario, tentando di addivenire ad un'armonizzazione degli standard tecnici nazionali per il tramite di direttive. Questo modello risultò tuttavia fallimentare stante la difficoltà di codificare le specifiche tecniche, nonché per le diverse opposizioni dei rappresentanti delle amministrazioni nazionali nelle votazioni all'unanimità in seno al Consiglio che ebbero l'effetto di allungare oltremodo i tempi di adozione delle norme tecniche rendendone ormai obsoleto il contenuto[72].

Successivamente, nel 1985 venne inaugurato il c.d. "Nuovo approccio" in materia di armonizzazione tecnica e normazione[73]. In questo sistema il legislatore comunitario si limitava a stabilire i requisiti minimi obbligatori di interesse collettivo, solitamente in ambiti come sicurezza, salute, ambiente e protezione dei consumatori, delegando agli enti di normazione l'elaborazione delle specifiche tecniche relative ai diversi settori che venivano poi pubblicate in Gazzetta ufficiale come norme armonizzate.

La Commissione affidava quindi, per mezzo di mandato[74], la produzione delle norme tecniche agli organismi di normazione riconosciuti a livello europeo (CEN, CENELEC ed ETSI) anche noti come *European Standardisation Organisations* (ESOs), i quali avevano il compito di elaborarle entro la cornice dettata dalle stesse istituzioni europee che vigilavano sulla loro conformità. La rinuncia della Commissione ad esercitare in via diretta le attribuzioni di rilevanza tecnica veniva così compensata con l'assolvimento di tre fondamentali compiti, ossia: la determinazione degli obiettivi; il controllo sulla "qualità" dell'attività degli enti di normazione e certificazione; e il controllo eventuale e successivo alla immissione nel mercato[75].

Questa strategia ebbe l'effetto di coniugare l'esigenza di tutelare le libertà economiche con la protezione dai rischi derivanti dallo svolgimento delle attività industriali, realizzando così «una integrazione stabile e permanente della regolazione sociale nella concorrenza, nella prospettiva di una ridefinizione di quest'ultima alla luce del principio dello sviluppo armonioso, equilibrato e sostenibile»[76].

70. Iannuzzi 2018, p. 78 ss.

71. Chiti 2003, p. 4027.

72. Andreini-Caia-Elias-Roversi Monaco 1995, p. 52.

73. Risoluzione 85/C 136/01, 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione.

74. Ancor prima dello "sconfinamento" verso ambiti non riservati alla normazione tecnica vi è la questione della "delega delle competenze normative" a soggetti diversi dai pubblici poteri. Sul punto v. Joerges-Schepel-Vos 1999. V. anche Bartoloni 2021.

75. Vesperini 1995, p. 146.

76. Chiti 2003, p. 4027. Sul passaggio dalla eliminazione delle barriere alla libera circolazione delle merci al perseguimento di interessi sociali, v. anche Joerges 1997, pp. 298-299.

Ad esempio, sono frutto di questo nuovo approccio sulla normazione armonizzata, le direttive sulla sicurezza dei giocattoli, la n. 378 del 1988[77], a cui ha fatto seguito la direttiva 2009/48/Ce, e la direttiva sulla sicurezza generale dei prodotti, la n. 59 del 1992, a cui ha fatto seguito la direttiva 2001/95/Ce. In tutti questi casi il legislatore comunitario è intervenuto con il fine di tutelare i consumatori attraverso un sistema di presunzione di sicurezza del prodotto conforme alle specifiche disposizioni comunitarie o, in mancanza, alla pertinente normativa nazionale.

3.2. Segue. Il Regolamento 1025/2012

Anche la nuova disciplina dettata dal Regolamento 1025/2012 sembra andare nella stessa direzione avviata con l'approccio del 1985[78].

Sebbene il fine della normazione resti quello di promuovere la competitività delle imprese – agevolando la libera circolazione dei beni e dei servizi, l'interoperabilità delle reti, i mezzi di comunicazione, lo sviluppo tecnologico e l'innovazione – dalla lettura dei considerando apprendiamo che tale vantaggio concorrenziale è parte del piano politico dell'Unione per fronteggiare le sfide sociali come «il cambiamento climatico, l'uso sostenibile delle risorse, l'innovazione, l'invecchiamento della popolazione, l'integrazione della persone con disabilità, la protezione dei consumatori, la sicurezza dei lavoratori e le condizioni di lavoro»[79].

In particolare, la realizzazione di detti fini, stabilmente integrati con le esigenze del libero mercato, sembra trovare concreta espressione nelle forme di cooperazione tra la Commissione europea e gli enti di normazione, e nell'enfasi posta sull'ampia partecipazione delle parti interessate[80], quali soggetti che rappresentano la dimensione dell'interesse pubblico nel processo di normazione e aiutano a rendere più accettabili le norme agli utilizzatori[81].

Il Regolamento del 2012 richiama in più occasioni tali forme di "pluralismo" nel processo di formazione degli standard quando prevede che le organizzazioni europee di normazione «incoraggiano e facilitano» la rappresentanza e la partecipazione di tutti i soggetti interessati alle proprie attività di normazione[82], e alle consultazioni per l'adozione del Programma annuale che identifica le priorità strategiche in materia di normazione europea[83].

Emerge pertanto il riconoscimento da parte dell'Unione del valore politico assunto dalla normazione tecnica e del suo impatto sulla società, che rende necessaria la più ampia partecipazione non solo dei soggetti destinatari delle norme tecniche, quali le industrie e i consumatori, ma anche le organizzazioni di rappresentanti di interessi pubblici diffusi[84].

77. Direttiva 88/378/CEE, relativa al ravvicinamento delle legislazioni degli Stati membri concernenti la sicurezza dei giocattoli.
78. Regolamento (UE) 1025/2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.
79. Considerando 19 Regolamento (UE) 1025/2012.
80. Zei 2008, p. 372 ss.
81. Comunicazione della commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo, *Integrazione degli aspetti ambientali nella normazione europea*, COM(2004) 130, del 25 febbraio 2004.
82. Cfr. artt. 5, 7, 10, 11, 13, 20 Regolamento (UE) 1025/2012.
83. Art. 8 Regolamento (UE) 1025/2012, si tratta del c.d. Programma di lavoro annuale dell'Unione per la normazione europea.
84. V. Zei 2008, p. 384 ss. In particolare sul valore politico degli standard, il riferimento è agli *Orientamenti generali per la cooperazione tra il CEN, il CENELEC e l'ETSI e la Commissione e l'Associazione europea di libero scambio*, del 28 marzo 2003, GUUE n. C 091 del 16 aprile 2003, in cui si riconosce che «le norme [tecniche] occupano uno spazio sempre maggiore in nuovi settori politici, quali la sicurezza sul luogo di lavoro, la protezione dei consumatori e dell'ambiente, il trasferimento al mercato dei risultati della ricerca o l'attuazione di reti transeuropee».

Tuttavia, dal quadro disciplinare appena descritto restano fuori le norme tecniche non armonizzate, ossia quelle norme prodotte da enti di normazione non europei e quindi elaborate fuori dai "principi fondatori" europei[85]. Questi standard, aventi natura volontaria e non cogente, costituiscono la maggior parte delle specifiche tecniche impiegate nel settore delle ICT. Già nel 2009, la Commissione europea, nel libro bianco sull'ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione, evidenziava come fossero divenuti sempre più attivi nell'elaborazione di tali norme forum e consorzi specializzati a livello globale, e come la politica comunitaria in tema di normalizzazione non rispecchiasse tale evoluzione[86].

Il tema interessa in particolare i requisiti tecnici nelle procedure di appalto pubblico per l'acquisto di hardware, software e servizi di tecnologia dell'informazione.

Il Regolamento 1025/2012 è intervenuto sul punto all'art. 13, ove è previsto che la Commissione, di propria iniziativa o su proposta di uno Stato membro, può decidere di identificare le specifiche tecniche delle ICT che non sono norme nazionali, europee o internazionali, purché non siano confliggenti con quest'ultime (nello specifico con l'Allegato II al Regolamento), «per consentire l'interoperabilità in materia di appalti pubblici».

La Commissione prende questa decisione previa consultazione della piattaforma multilaterale europea sulla normazione delle ICT, che comprende le organizzazioni europee di normazione, gli Stati membri e i soggetti interessati, e previa consultazione del comitato istituito dalla corrispondente legislazione dell'Unione, laddove esiste, o previe altre forme di consultazione di esperti del settore, qualora tale comitato non esista[87].

Al momento la Commissione ha emanato una serie di decisioni con le quali ha identificato come specificazioni ICT per gli appalti pubblici europei, quelli formati, tra gli altri, dall'IETF, l'*Organization for the Advancement of Structured Information Standards* (OASIS), l'*European Computer Manufacturers Association* (ECMA), e il *World Wide Web Consortium* (W3C)[88].

Per completezza aggiungiamo inoltre che, da ultimo, il Regolamento è stato oggetto di recenti interventi che non ne hanno comportato una totale abrogazione, quanto piuttosto un suo aggiornamento relativamente a particolari aspetti della disciplina generale. Nello specifico, con il Regolamento (UE) 2022/2480, si è provveduto a disciplinare le decisioni delle organizzazioni europee di normazione relative alle norme europee e ai prodotti della normazione europea, mentre con il Regolamento (UE) 2023/988, è stata aggiornata la disciplina della sicurezza generale dei prodotti (GDPSR).

3.3. Gli standard di riferimento di cyberiscurezza e gli Organismi di standardizzazione cyber a livello Ue

Gli standard di riferimento per la certificazione della cybersicurezza sono molteplici e si focalizzano sulla certificazione di prodotti (ad es. ISO/IEC 15408), di sistemi di gestione (ad es. ISO/IEC 27001), di servizi e di processi ICT.

Tuttavia, l'affermazione di tali categorie è stata graduale nel tempo[89]. Le prime norme tecniche sono state quelle volte a regolare i processi produttivi al fine di garantire determinate caratteristiche nei prodotti. Le norme di secondo tipo sono invece intervenute sulla progettazione e sulle caratteristiche prestazionali dei prodotti. Infine, con l'introduzione a livello internazionale della famiglia di norme ISO 9000, si sono aggiunte le norme tecniche di terzo tipo, volte a normare l'intero sistema di produzione attraverso la formulazione dei c.d. sistemi di gestione (nello specifico la ISO 9000 è la norma dei sistemi di gestione per la qualità).

Proprio all'interno di quest'ultima categoria, tra gli anni Ottanta e Novanta del secolo scorso, hanno iniziato a prendere forma le prime normative tecniche sulla sicurezza dei sistemi informativi e servizi informatici (*computer security*), nonché

85. Considerando 31, Regolamento (UE) 1025/2012.

86. Commissione delle comunità europee 2009.

87. Cfr. art. 13, par. 3, Regolamento 1025/2012.

88. Kanevskaia 2023, p. 83 ss.

89. Andreini-Caia-Elias-Roversi Monaco 1995, p. 45 ss.

sulla sicurezza delle informazioni (*information security*)[90]. A tal proposito si faccia riferimento ad alcune definizioni individuate nel bollettino dell'agenzia statunitense competente nella gestione delle tecnologie, il *National Institute of Standards and Technology* (NIST), ove per sicurezza informatica, o *computer security*, si intende «la protezione fornita ad un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (includendo hardware, software, firmware, dati e sistemi di telecomunicazione)» (NIST SP 800-14). Mentre la norma ISO/IEC 27000:2018, per sicurezza delle informazioni, o *information security*, fa riferimento alla «preservazione della riservatezza, integrità e disponibilità delle informazioni», in qualsiasi forma esse siano rappresentate (digitale o materiale), o qualunque sia la loro modalità di trasmissione (comunicazione elettronica, corriere ecc.).

Il fine principale di tali normative è quello di preservare le tre proprietà fondamentali delle risorse informatiche e delle informazioni affinché queste possano essere considerate sicure, ossia la riservatezza (*confidentiality*), l'integrità (*integrity*) e la disponibilità (*availability*), spesso indicate con l'acronimo R.I.D (o C.I.A. in lingua inglese).

Nello specifico, la riservatezza (o confidenzialità) è la proprietà per cui tali risorse possono essere accedute solo da chi è stato autorizzato o ne abbia il diritto; l'integrità concerne invece la preservazione della correttezza, coerenza e affidabilità e quindi anche la certezza che il sistema informativo e l'informazione non siano stati alterati o modificati da soggetti non autorizzati; infine, per disponibilità si intende la proprietà secondo cui le risorse informatiche e le informazioni dovranno essere utilizzabili ed accessibili ogni qualvolta il soggetto autorizzato lo richieda.

Sebbene esistano un gran numero di norme internazionali, europee e nazionali utili per la mitigazione dei rischi di cybersicurezza, per completezza aggiungiamo che, oltre alle norme tecniche per la sicurezza informatica e delle informazioni (IT) in particolare a livello europeo sono state recepite quelle della famiglia ISO 2700, vi sono anche le norme della serie EN IEC 62443 per le Tecnologie Operative (OT).

Date le brevi premesse sugli standard di cybersicurezza, possiamo passare agli organismi di normazione. A tal proposito, osserviamo che l'esigenza di cybersicurezza, particolarmente avvertita a livello europeo, ha avuto l'effetto di specializzare le tre ESOs. Innanzitutto nel 2011 è stato istituito il *CEN-CENELEC Focus Group on Cybersecurity* (CSCG), volto ad analizzare gli sviluppi tecnologici al fine di elaborare un insieme di raccomandazioni per la definizione di standard internazionali che assicurino un adeguato livello di equità per le imprese e le autorità pubbliche. Tra le diverse attività, nel 2016 il CSCG ha esaminato i diversi significati e utilizzi della parola "cybersecurity" da parte di vari portatori di interessi in diversi standard e ha finalizzato un documento sulla definizione di tale concetto[91].

Sempre nel 2017 è stato istituito il CEN-CLC/JTC 13 *Cybersecurity and Data protection*, il cui obiettivo principale è trasporre gli standard internazionali rilevanti come standard europei (EN) nel settore delle Tecnologie dell'Informazione (IT)[92]. Mentre il Comitato tecnico CLC/TC 65X *Industrial-process measurement, control and automation* è l'altro principale fornitore di standard correlati alla sicurezza informatica nel settore della Tecnologia Operativa (OT)[93].

L'organismo ETSI, nel 2014, ha istituito l'ETSI TC CYBER[94] che si occupa della sicurezza delle infrastrutture, dei dispositivi, dei servizi e dei protocolli, degli strumenti e delle tecniche di sicurezza, dei consigli sulla sicurezza, dell'orientamento e dei requisiti operativi di sicurezza per utenti, produttori e operatori di reti e infrastrutture

90. Russell-Gangemi 1991. In particolare sulla storia della norma tecnica ISO/IEC 27001, si rinvia a Gallotti 2019, p. 247 ss.

91. CSCG 2017.

92. Per ulteriori informazioni si rinvia al sito ufficiale CEN-CLC/JTC 13 Cybersecurity and Data protection.

93. Si rinvia al sito ufficiale del Comitato tecnico CLC/TC 65X Industrial-process measurement, control and automation.

94. Si rinvia al sito ufficiale dell'ETSI TC CYBER.

4. Il framework europeo di certificazione e valutazione: il *Cybersecurity Act*

Nel settembre del 2017, la Commissione ha introdotto un pacchetto di misure volte a potenziare la cybersicurezza europea con nuove iniziative operanti sotto il triplice profilo della resilienza, deterrenza e difesa (*Cybersecurity Package*)[95]. Dal documento si apprende che tra gli obiettivi diretti allo sviluppo della resilienza europea dai cyberattacchi vi è il rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

Come noto l'ENISA è stata istituita con il Regolamento della allora Comunità europea n. 460 del 2004[96] con l'obiettivo di creare «un clima di fiducia grazie alla sua indipendenza, alla qualità della consulenza fornita e delle informazioni diffuse, alla trasparenza delle sue procedure e metodi di funzionamento e alla diligenza nello svolgere i compiti ad essa assegnati», attraverso la stretta collaborazione con gli Stati e il settore privato[97]. L'Agenzia venne inizialmente dotata di un mandato temporaneo, via via esteso con i Regolamenti (UE) n. 1007/2008, n. 580/2011 e n. 526/2013. Tuttavia, con il pacchetto del 2017 è stata proposta una modifica legislativa volta a rafforzare il ruolo dell'ENISA a fronte delle nuove funzioni e responsabilità attribuitele dalla allora Direttiva (UE) 2016/1148 sulla Sicurezza delle Reti e delle Informazioni nel 2016 (Direttiva NIS I), nonché per il perseguimento di attività come la preparazione e organizzazione di esercitazioni annuali di cybersicurezza paneuropee che combinino la risposta a diversi livelli, e lo scambio di informazioni di cybersicurezza a livello tecnico, operativo e strategico in collaborazione con gli organismi competenti degli Stati membri, dell'Ue e di tutti gli attori interessati[98].

In sostanza il piano di riforma, poi concretamente formulato con la proposta del 2017[99], prevedeva che l'ENISA non si limitasse a fornire solo consulenze specialistiche, come prefissato nel 2004, ma che fosse fosse investita anche compiti operativi.

Per quel che qui interessa, l'attribuzione di rilievo è certamente quella relativa all'elaborazione della politica europea sulla certificazione di cybersicurezza dei beni ICT. Si tratta di un tema particolarmente sensibile in quanto avvicina la cybersicurezza alle dinamiche del mercato, nel caso di specie, del mercato unico europeo. Come anticipato, gli standard e le certificazioni sono strumenti che, se accettati e utilizzati da tutti gli operatori del settore, possono uniformare il mercato dettando parametri utili non solo sotto il profilo produttivo ma anche della qualità – e quindi della sicurezza – dei prodotti. Nel pacchetto del 2017 veniva denunciata l'esistenza di diversi schemi di certificazione di sicurezza per i prodotti ICT, di cui alcuni validi solo in determinati Stati membri e non in altri, creando così una frammentazione del mercato.

Precisiamo tuttavia che nel tempo sono stati compiuti sforzi per garantire il reciproco riconoscimento dei certificati all'interno dell'Unione, ma con risultati parziali. Esistono diverse iniziative internazionali, come i *Common Criteria for Information Technology Security Evaluation* (noti come *Common Criteria* o CC) per la valutazione della sicurezza delle tecnologie d'informazione e che costituiscono una norma tecnica internazionale per la valutazione della sicurezza informatica, ossia la ISO 15408[100]. I CC e l'associata Metodologia comune per la valutazione della sicurezza delle tecnologie d'informazione costituiscono la base tecnica per un accordo internazionale, il *Common*

95. Commissione Europea, Comunicazione congiunta al Parlamento europeo e al Consiglio, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 (anche nota come "Cybersecurity package").
96. Regolamento (EC) 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.
97. Cfr. considerando 11, Regolamento (EC) 460/2004.
98. Relativamente allo scambio di informazioni per il contrasto alle minacce informatiche a livello europeo sia concesso rinviare a Serini 2023.
99. Proposta di Regolamento 2017/0225 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, che abroga il Regolamento (UE) 526/2013, e sulla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione, COM/2017/0477 ("Cybersecurity Act").
100. Il riferimento è per l'appunto alla norma tecnica ISO/IEC 15408-1:2022, recentemente aggiornata, che stabilisce i concetti e i principi generali della valutazione della sicurezza IT.

Criteria Recognition Arrangement (CCRA), che garantisce che i certificati basati sui CC siano riconosciuti da tutti i firmatari del CCRA. Vi rientrano diversi Stati, sia membri dell'Unione europea, sia extra-Ue[101]. Tuttavia, nel 2017, solo 13 Stati membri risultavano essere firmatari dell'accordo.

Altre iniziative sono state coltivate dalle autorità di certificazione. È il caso dell'accordo di reciproco riconoscimento dei certificati rilasciati in conformità con l'accordo sulla base dei criteri comuni stipulato da parte del Gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (*Senior Officials Group – Information Systems Security*, SOG-IS)[102]. Si tratta tuttavia di un gruppo che comprende solo 12 Stati membri, più la Norvegia.

Data la fotografia del 2017, l'istituzione di un quadro comune sulla certificazione di tali prodotti è sembrata la risposta ad un'esigenza avvertita da tempo che avrebbe procurato evidenti vantaggi alle imprese, le quali non avrebbero più dovuto espletare processi di certificazione diversi per operare a livello transnazionale, rendendo gli elevati parametri di cybersicurezza una fonte di vantaggio competitivo[103].

La proposta, seppur volta ad innescare un circuito vantaggioso sia per l'economia sia per la sicurezza, non è stata scevra di critiche, soprattutto da parte degli Stati membri. Come si apprende dal documento finale del briefing legislativo del 2019 dal titolo *ENISA and the new Cybersecurity Act*[104], il 27 settembre 2017, il Senato francese ha adottato un parere motivato ove è stata contestata la conformità della proposta al principio di sussidiarietà. Nello specifico l'obiezione ha interessato due punti fondamentali. Il primo relativo alle basi di legittimità, le quali sarebbero dovute essere non solo l'articolo 114 TFUE, ma anche l'articolo 5 TUE concernente le questioni di sicurezza[105]; l'altro invece attinente al rapporto tra la sicurezza europea e le "sicurezze" degli Stati membri. Il Senato ha infatti osservato che «la cooperazione europea in materia di sicurezza informatica deve continuare sulla base della partecipazione degli Stati membri e della fornitura volontaria di informazioni sensibili, anche per quanto riguarda la sicurezza nazionale su cui l'ENISA non può quindi disporre di ulteriori poteri investigativi come previsto nell'articolo 7, punto 5 della proposta di regolamento»[106].

Altre osservazioni sono invece pervenute dal settore industriale, particolarmente interessato alla regolazione delle certificazioni di cybersicurezza. Tra i pareri avanzati dai diversi stakeholder, emergono due orientamenti di quelli a favore della certificazione volontaria, la maggior parte, e di quelli favorevoli alla certificazione obbligatoria per alcune categorie di prodotti.

La versione definitiva del *Cybersecurity Act* è stata adottata con il Regolamento 2019/881 con il quale è stato conferito mandato permanente all'Agenzia a fronte dell'ampliamento delle sue funzioni[107]. Tra queste, l'art. 8 del Regolamento,

101. Nazioni aderenti: Australia, Canada, Francia, Germania, India, Italia, Giappone, Malesia, Paesi Bassi, Nuova Zelanda, Norvegia, Repubblica di Corea del Sud, Singapore, Spagna, Svezia, Turchia, Stati Uniti, Austria, Repubblica Ceca, Danimarca, Etiopia, Finlandia, Grecia, Ungheria, Indonesia, Israele, Pakistan, Polonia, Qatar, Slovacchia, Regno Unito. Maggiori informazioni disponibili sul portale web del CCRA.

102. Per ulteriori informazioni si rinvia al sito ufficiale del Senior Officials Group – Information Systems Security, SOG-IS.

103. In realtà, secondo una fotografia dello stato dell'arte del quadro di certificazioni di cybersicurezza subito dopo l'adozione del *Cybersecurity Act*, i livelli di cybersicurezza dei prodotti ICT assicurati dalla normativa «are found to be largely inadequate in assisting organisations in the European Union internal market with resisting and recovering from cyber threats». Sul punto v. Stewart Ferguson 2022, pp. 51-114.

104. Il documento prodotto all'interno del Briefing EU Legislation in Progress del 2019 dal titolo *ENISA and the new Cybersecurity Act*.

105. Come si apprende dalla proposta di *Cybersecurity Act*, le basi di legittimità a cui si è fatto riferimento sono state, oltre all'art. 114 TFUE, l'art. 26 TFUE sull'instaurazione e funzionamento del mercato interno.

106. Si rinvia a par. 10 del documento *ENISA and the new Cybersecurity Act* di cui in nota 104.

107. Regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il

rubricato "Mercato, certificazione della cibersicurezza e normazione" prevede che l'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cybersicurezza dei beni ICT, attraverso le seguenti attività: a) monitorando continuamente gli sviluppi nei settori di normazione connessi e raccomandando adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cibersicurezza […], in assenza di norme; b) preparando proposte di sistemi europei di certificazione della cibersicurezza («proposte di sistemi») per prodotti TIC, servizi TIC e processi TIC […]; c) valutando i sistemi europei di certificazione della cibersicurezza adottati […]; d) partecipando a valutazioni inter pares […]; e) assistendo la Commissione nel provvedere alle funzioni di segretariato dell'ECCG […].

Si evince pertanto che l'Agenzia è stata posta al centro del processo di certificazione. Nel medesimo Regolamento sono istituiti anche altri due soggetti che supportano l'azione dell'Agenzia in questo settore. Si tratta del Gruppo dei portatori di interessi per la certificazione della cibersicurezza (art. 22 par. 2) e del Gruppo europeo per la certificazione della cibersicurezza – ECCG (art. 62).

Il Gruppo dei portatori di interessi per la certificazione della cibersicurezza, copresieduto dai rappresentanti della Commissione e dall'ENISA, è costituito da esperti riconosciuti che rappresentano diversi portatori di interessi, selezionati dalla Commissione, a seguito di un invito aperto e trasparente, su proposta dell'ENISA, e garantendo un equilibrio tra i diversi gruppi di portatori di interessi, nonché un opportuno equilibrio geografico e di genere.

L'attività del Gruppo consiste nel fornire consulenza alla Commissione sulle questioni strategiche riguardanti il quadro europeo di certificazione della cibersicurezza (lett. a), nonché, su richiesta, in materia di mercato, certificazione della cibersicurezza e normazione (lett. b); assistere la Commissione nell'elaborazione del programma di lavoro progressivo dell'Unione (lett. c) e formulare il relativo parere su detto programma (lett. d)[108]; in casi urgenti, fornisce consulenza alla Commissione e all'ECCG in merito alla necessità di sistemi di certificazione supplementari non inclusi nel programma di lavoro progressivo dell'Unione (lett. e)[109].

Il Gruppo europeo per la certificazione della cybersicurezza (ECCG), presieduto dalla

Regolamento (UE) n. 526/2013. Si precisa inoltre che con tale atto, il legislatore europeo ha introdotto per la prima volta, in un atto giuridico, all'art. 2, n. 1, il concetto di «cybersicurezza» inteso come «insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

108. Il programma di lavoro progressivo dell'Unione per la certificazione europea della cybersicurezza è disciplinato all'art. 47 del *Cybersecurity Act*. Si tratta dello strumento con il quale sono individuate le priorità strategiche per i futuri sistemi europei di certificazione della cibersicurezza. Ai sensi del disposto è previsto che «2. Il programma di lavoro progressivo dell'Unione include in particolare un elenco di prodotti TIC, servizi TIC e processi TIC o delle relative categorie che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza. 3. L'inclusione, nel programma di lavoro progressivo dell'Unione, di specifici prodotti TIC, servizi TIC e processi TIC o delle relative categorie è giustificata sulla base di una o più delle seguenti motivazioni: a) la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza relativi a specifiche categorie di prodotti TIC, servizi TIC o processi TIC e in particolare in relazione al rischio di frammentazione; b) la pertinente politica o il pertinente diritto dell'Unione o degli Stati membri; c) la domanda di mercato; d) gli sviluppi nel panorama delle minacce informatiche; e) la richiesta di preparazione di una specifica proposta di sistema da parte del'ECCG. 4. La Commissione tiene nella debita considerazione i pareri in merito al progetto di programma di lavoro progressivo dell'Unione espressi dall'ECCG e dal gruppo dei portatori di interessi per la certificazione della cibersicurezza. 5. Il primo programma di lavoro progressivo dell'Unione è pubblicato entro il 28 giugno 2020. Il programma di lavoro progressivo dell'Unione è aggiornato almeno ogni tre anni e più spesso se necessario».

109. Il disposto fa riferimento agli artt. 47 e 48 del *Cybersecurity Act*. L'art. 48, rubricato "Richiesta di un sistema europeo di certificazione della cibersicurezza" prevede che «1. La Commissione può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente sulla base del programma di lavoro progressivo dell'Unione. 2. In casi debitamente giustificati la

Commissione con l'assistenza dell'ENISA, è composto da rappresentanti delle autorità nazionali di certificazione della cybersicurezza o da rappresentanti di altre autorità nazionali competenti. Un membro dell'ECCG non può rappresentare più di due Stati membri. Tuttavia, i portatori di interessi e le parti terze interessate possono essere invitati a presenziare alle riunioni dell'ECCG e a partecipare ai suoi lavori.

Relativamente alle funzioni, l'ECCG svolge il ruolo di consigliere sia verso la Commissione nelle sue attività volte a garantire l'attuazione e l'applicazione del programma di lavoro progressivo dell'Unione, le questioni relative alla politica in materia di certificazione della cibersicurezza, il coordinamento degli approcci strategici e la preparazione dei sistemi europei di certificazione della cibersicurezza (lett. a), sia verso l'ENISA in relazione alla preparazione di una proposta di predisposizione, adozione e revisione di un sistema europeo di certificazione della cibersicurezza *ex* art. 49 (lett. b) su cui poi esprime un parere (lett. c); chiede all'ENISA di preparare le Richieste di sistemi europei di certificazione *ex* art. 48, par. 2 (lett. d); adotta pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cybersicurezza (lett. e); esamina gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di informazioni e buone pratiche sui sistemi europei di certificazione della cybersicurezza (lett. f); agevola la cooperazione tra le autorità nazionali di certificazione della cibersicurezza attraverso lo sviluppo della capacità e lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente scambio di informazioni in relazione a tutti gli aspetti della certificazione della cybersicurezza (lett. g); sostiene l'attuazione dei meccanismi di valutazione *inter pares* in conformità delle regole fissate da un sistema europeo di certificazione della cybersicurezza (lett. h); agevola l'allineamento dei sistemi europei di certificazione della cybersicurezza alle norme riconosciute a livello internazionale, rivedendo tra l'altro i sistemi europei di certificazione della cybersicurezza esistenti e, ove opportuno, rivolgendo raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale (lett. i).

L'ENISA, con il supporto di tali Gruppi, è quindi il soggetto responsabile del monitoraggio, nonché dell'aggiornamento del sistema europeo di certificazione, definito nel Regolamento come la «serie completa di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti ICT, servizi ICT e processi ICT»[110].

Tale sistema è tuttavia istituito all'interno del Quadro europeo di certificazione della cybersicurezza, il cui obiettivo è quello di «stabili[re] i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza da sviluppare e [in modo da consentire] di riconoscere e utilizzare i certificati europei di cibersicurezza e le dichiarazioni UE di conformità per i prodotti ICT, i servizi ICT o i processi ICT in tutti gli Stati membri»[111].

L'effetto di tale intervento normativo, da una parte è stato quello di sostituire i sistemi nazionali di certificazione per i beni ICT coperti da quello europeo (per quelli non coperti, il sistema nazionale resta in vigore)[112], dall'altra, ha inciso sull'organizzazione delle autorità nazionali di certificazione.

Innanzitutto, come si apprende dall'art. 58, gli Stati membri devono assicurare che le attività delle autorità nazionali di certificazione relative al

Commissione o l'ECCG può richiedere all'ENISA di preparare una proposta di sistema o di rivedere un sistema europeo di certificazione della cibersicurezza esistente non incluso nel programma di lavoro progressivo dell'Unione. Il programma di lavoro progressivo dell'Unione è aggiornato di conseguenza».

110. Cfr. art. 2, n. 9, Regolamento (UE) 2019/881. Si invita inoltre alla lettura combinata con l'art. 54, ove sono delineati gli "Elementi dei sistemi europei di certificazione della cybersicurezza".

111. Cfr. considerando 69, Regolamento (UE) 2019/881.

112. Cfr. art. 57, Regolamento (UE) 2019/881.

rilascio dei certificati siano «rigorosamente separate» dalle attività di vigilanza[113]. Altri profili riguardano invece la collaborazione e cooperazione tra le autorità a livello nazionale, nonché con la Commissione, attraverso lo scambio di informazioni e la redazione di relazioni annuali.

Tra questi adempimenti riteniamo opportuno evidenziare l'obbligo imposto agli Stati membri di informare preventivamente «la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersicurezza», al fine di evitare la frammentazione del mercato interno[114].

Preme evidenziare che le autorità nazionali di certificazione della cybersicurezza sono soggette a una procedura di valutazione *inter pares* di cui all'art. 59 del *Cybersecurity Act*, ossia una valutazione «effettuata sulla base di criteri e procedure di valutazione solidi e trasparenti, in particolare per quanto riguarda i requisiti strutturali, di risorse umane e procedurali, la riservatezza e i reclami» (par. 2). Tale valutazione deve essere svolta da almeno due autorità nazionali di altri Stati membri e dalla Commissione, nonché con l'eventuale partecipazione dell'ENISA, e ha luogo almeno una volta ogni cinque anni (par. 4).

Sono inoltre parte del sistema nazionale di certificazione l'organismo nazionale di accreditamento e gli organi di valutazione della conformità.

Il Regolamento 765/2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti, definisce l'organismo nazionale di accreditamento come l'unico soggetto che, su autorizzazione dello Stato, può certificare che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate (ISO/IEC 17011) e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità[115].

L'art. 2, n. 13 definisce invece gli organi di valutazione della conformità come organismi che svolgono attività di «valutazione della conformità, fra cui tarature, prove, certificazioni e ispezioni». Tuttavia, per poter erogare tale servizio, il *Cybersecurity Act* prevede che tali soggetti debbano essere accreditati dall'organismo nazionale di accreditamento, ossia «l'unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento»[116], qualora rispettino

113. Sulle attività delle Autorità nazionali di certificazione il comma 7 dell'art. 58 prevede che queste «a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersicurezza a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, servizi TIC e processi TIC con i requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti; b) controllano la conformità agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC o processi TIC che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi di tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza; c) fatto salvo l'articolo 60, paragrafo 3, assistono e sostengono attivamente gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del presente regolamento; d) monitorano e vigilano sulle attività degli organismi pubblici di cui all'articolo 56, paragrafo 5; e) ove applicabile, autorizzano gli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, e limitano, sospendono o revocano l'autorizzazione esistente qualora gli organismi di valutazione della conformità violino le prescrizioni del presente regolamento; f) trattano i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza rilasciati dagli organismi di valutazione della conformità in conformità dell'articolo 56, paragrafo 6, oppure in relazione alle dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 53, e svolgono le indagini opportune sull'oggetto di tali reclami e informa».

114. Cfr. art. 58, par. 4, Regolamento (UE) 2019/881.

115. Cfr. art. 2, nn. 10 e 11 Regolamento (UE) 765/2008.

116. Cfr. art. 2, n. 11, del Regolamento (UE) 765/2008.

determinati criteri, e per un periodo massimo di cinque anni rinnovabile.

Ai sensi dall'art. 58 del Regolamento 2019/881, gli organi sono soggetti ai poteri di vigilanza e controllo delle autorità di certificazione nazionale, le quali possono limitare, sospendere o revocare l'autorizzazione qualora tali soggetti si pongano in violazione delle prescrizioni del Regolamento.

Definiti brevemente i profili organizzativi del nuovo sistema di certificazione della cybersicurezza, riteniamo ora possibile concentrarci sulla disciplina del certificato di cybersicurezza europeo.

L'art. 2, n. 11 del *Cybersecurity Act* lo defnisce come «un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto ICT, servizio ICT o processo ICT è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza».

Considerate le istanze degli stakeholder sulla natura di tali strumenti, evidenziamo che il legislatore europeo all'art. 56, par. 2 del Regolamento ha stabilito che la certificazione di cybersicurezza è volontaria, salvo tuttavia quanto «diversamente specificato dal diritto dell'Unione o degli Stati membri». Sul punto prosegue, al par. 3, prevedendo che «La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della ciberiscurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di ciberiscurezza dei … [beni ICT] e migliorare il funzionamento del mercato interno».

Il tratto che riteniamo tuttavia di particolare rilievo ai fini della presente trattazione riguarda quanto articolato all'art. 52 del *Cybersecurity Act*, rubricato "Livelli di affidabilità dei sistemi europei di certificazione della cybersicurezza". Il disposto prevede infatti una gradazione dell'affidabilità dei beni ICT in tre livelli, "di base", "sostanziale" ed "elevato", commisurati al livello di rischio associato al previsto uso del prodotto in questione in termini di probabilità e impatto di un incidente.

Considerato che la sicurezza assoluta è una condizione mai reale, il legislatore europeo ha scelto di parametrare tali livelli di affidabilità in base alle abilità e risorse degli attori malevoli. Difatti, un certificato o una dichiarazione europei di conformità che si riferiscano al livello di affidabilità "di base" assicurano che il bene ICT sia stato valutato a un livello inteso a ridurre al minimo «i rischi di base noti di incidenti e attacchi informatici»[117].

Un certificato o una dichiarazione europei di conformità che si riferiscano al livello di affidabilità "sostanziale" assicurano invece che il bene ICT sia stato valutato a un livello inteso a ridurre al minimo «i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate»[118].

Infine, un certificato o una dichiarazione europei di conformità che si riferiscano al livello di affidabilità "elevato" assicurano che il bene ICT sia stato valutato a un livello inteso a ridurre al minimo «il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative»[119].

Ad ognuno di questi livelli il legislatore fa discendere una diversa disciplina delle attività di valutazione da intraprendere che vanno da «almeno un» riesame della documentazione tecnica, come nel caso dell'affidabilità "di base" al più complesso «riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC o i processi TIC attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione», relativo ai prodotti ICT con livello di affidabilità "elevato".

Preme inoltre precisare che tale tripartizione incide anche sull'individuazione dei certificatori e dei valutatori. Relativamente ai primi, l'art. 56 al comma 6 prevede che ove il sistema europeo di certificazione di cybersicurezza richieda un livello di affidabilità "elevato", «il certificato europeo di cybersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cybersicurezza» oppure, da un

117. Cfr. art. 52, par. 5, Regolamento (UE) 2019/881.
118. Cfr. art. 52, par. 6, Regolamento (UE) 2019/881.
119. Cfr. art. 52, par. 7, Regolamento (UE) 2019/881.

organismo di valutazione della conformità ma solo in presenza di determinate condizioni[120].

Inoltre, il comma 4 del medesimo disposto prevede che «in casi debitamente giustificati un sistema europeo di certificazione della cybersicurezza può prevedere che i certificati europei di cybersicurezza derivanti da tale sistema possano essere rilasciati unicamente da un ente pubblico», ossia un'autorità nazionale di certificazione della cybersicurezza, o un organismo pubblico accreditato come organismo di valutazione della conformità.

Tale disposizione è particolarmente indicativa. Come si apprende – "tra le righe" – dal citato Regolamento (UE) 765/2008, non tutti gli Stati membri e mondiali sono dotati di un organismo di certificazione della cybersicurezza governativo. Per alcuni contesti tale attività è perlopiù demandata anche ad organismi di valutazione della conformità di natura per lo più privata.

Per quanto riguarda i valutatori, all'art. 53 del *Cybersecurity Act* è stata introdotta l'autovalutazione della conformità, che consente, per i soli beni ICT che presentano un basso rischio e quindi corrispondenti al livello di affidabilità "di base", di affidare al fabbricante o al fornitore la responsabilità di valutare la conformità di tali beni, rilasciando poi la relativa dichiarazione UE di conformità (par. 2), ma a titolo volontario (par. 4).

4.1. Il quadro italiano. Il controllo sul procurement informatico alla luce della disciplina sul Perimetro di Sicurezza Nazionale Cibernetica

Il controllo sui prodotti ICT in Italia è stato disciplinato all'interno del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), istituito con d.l. 21 settembre 2019, n. 105, convertito con modificazioni in legge 18 novembre 2019 n. 133, e successivamente, dal d.lgs. 3 agosto 2022, n. 123, per quanto riguarda l'adeguamento dell'Italia al sistema di certificazione di cybersicurezza europeo (di cui si dirà al par. 4.2).

Relativamente al primo intervento, si tratta di una disciplina con la quale il legislatore italiano è intervenuto a protezione delle reti e delle risorse informatiche in uso presso le infrastrutture critiche, nonché le pubbliche amministrazioni di rilevanza nazionale, con un approccio sistematico e integrativo della disciplina NIS. Difatti, come è stato osservato, sono parte del PSNC «tutti quegli operatori pubblici o privati, che, seppur non ricompresi nell'ambito di applicazione della Direttiva NIS, risultino comunque essenziali per la sicurezza nazionale italiana […]»[121].

In particolare, l'art. 1 co. 1, del d.l. 21 settembre 2019, n. 105 dispone che l'obiettivo della normativa è di elevare i livelli 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 dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale».

Nel complesso, l'attuazione del PSNC consiste in un articolato programma la cui completa e concreta realizzazione è affidata ad una serie di regolamenti attuativi[122].

Con il decreto del Presidente del Consiglio dei ministri del 30 luglio 2020, n. 131, si è provveduto a definire le modalità e i criteri procedurali di individuazione dei soggetti afferenti al Perimetro,

120. Tali condizioni sono che deve esservi la «a) previa approvazione dell'autorità nazionale di certificazione della cybersicurezza per ogni singolo certificato europeo di cybersicurezza rilasciato da un organismo di valutazione della conformità; o b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cybersicurezza a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cybersicurezza».

121. Cfr. Mele 2020, p. 186. Nello specifico, confrontando le due citate discipline, il PSNC ricomprende anche quei soggetti attivi nei settori interno, difesa, spazio e aerospazio, telecomunicazioni, economia e finanza, servizi digitali, tecnologie critiche.

122. Per un quadro completo sui diversi provvedimenti che compongono la materia si invita a consultare il sito della Camera dei deputati, all'apposita sezione "Aree tematiche" relativa alla "Sicurezza cibernetica" (ultima consultazione il 12 novembre 2023).

affidando poi tale compito – come per la direttiva NIS – ad alcune amministrazioni centrali dello Stato. Si tratta di disposizioni con cui si sono quindi definiti i confini – o in tal caso i "perimetri" – applicativi della normativa a seconda dell'attività svolta dal soggetto di interesse.

A tal proposito, con l'art. 2 del citato d.P.C.M., si è innanzitutto definito un soggetto, esercente una «funzione essenziale dello Stato»: «laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti»[123], mentre un soggetto pubblico o privato presta un «servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato» laddove ponga in essere: «attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale»[124].

Relativamente alla riconduzione all'interno del Perimetro di diversi soggetti pubblici, pare utile evidenziare che alcuni di tali soggetti, originariamente esclusi all'interno della Direttiva NIS I, sono ora confluiti nell'ambito di applicazione della Direttiva (UE) 2022/2555 (anche nota come Direttiva NIS II). Nello specifico si tratta di soggetti «dell'amministrazione centrale qual[i] definit[i] da uno Stato membro conformemente al diritto nazionale»[125].

In linea generale, declinando ed estendendo gli obblighi di sicurezza contemplati dalla disciplina NIS (il riferimento è alla NIS I), il d.l. n. 105/2019 articola una disciplina che da una parte impone particolari obblighi verso i soggetti afferenti al Perimetro, amministrativamente e penalmente sanzionati, dall'altra contribuisce alla istituzione di organi componenti la nuova architettura nazionale di cybersicurezza per quanto riguarda il controllo sui beni ICT.

Tuttavia, l'aspetto di interesse in questa sede riguarda l'esercizio dei poteri di controllo sui beni ICT: accertamenti che vengono effettuati sia preliminarmente all'acquisto, sia una volta concluso il contratto.

Il d.l. 105/2019 affida l'esecuzione dei test sulle risorse informatiche in uso presso soggetti esercenti funzioni o servizi essenziali per lo Stato, al Centro di Valutazione e Certificazione nazionale (CVCN)[126]. Si tratta di un ente originariamente istituito presso l'Istituto Superiore delle Comunicazioni e Tecnologie Informatiche (ISCTI), del Ministero dello sviluppo economico, ed ora collocato presso l'Agenzia per la Cybersicurezza Nazionale (ACN)[127].

Con il d.P.R. 5 febbraio 2021, n. 54, emanato in attuazione dell'art. 1, comma 6, del d.l. 21 settembre 2019, n. 105, è stata dettagliata la disciplina sul punto. Nello specifico, oltre al CVCN, sono stati introdotti anche i Centri di Valutazione (CV) presso il Ministero dell'interno[128] e del Ministero della difesa (Ce.Va.), nonché i Laboratori accreditati in

123. Art. 2, lett. a), d.P.C.M. 30 luglio 2020, n. 131.

124. Art. 2, lett. b), d.P.C.M. 30 luglio 2020, n. 131.

125. Art. 3, par. 1, lett. d) della Direttiva 2022/2555, che rinvia all'art. 2, par. 2, lett. f), punto i) del medesimo provvedimento.

126. Si rinvia al sito ufficiale del CVCV presso l'Agenzia per la Cybersicurezza Nazionale.

127. Il trasferimento è avvenuto in virtù del d.l. 14 giugno 2021, n. 82 relativo a "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale". Per una disamina del provvedimento v. Parona 2021. Sia inoltre concesso rinviare a Serini 2022.

128. Nello specifico, l'organizzazione del Ministero dell'Interno è stata modificata con il DPR 231/2021 che, tra l'altro, disciplina la nuova Direzione centrale per la polizia scientifica e la sicurezza cibernetica. Mentre con il d.l. 34/2020 (cd. "decreto Rilancio", art. 240) è stata istituita la Direzione generale per lo sviluppo della prevenzione e tutela informatiche presso il Dipartimento della pubblica sicurezza del Ministero dell'interno.

prova (LAP), quali centri indipendenti dai soggetti inclusi nel Perimetro e dai fornitori, quali strutture accreditate dal CVCN conformemente alle procedure contemplate dal decreto del Presidente del Consiglio dei ministri del 18 maggio 2022, n. 92.

Come si apprende dalla lettera dell'art. 2 del d.P.R., con il decreto si sono disciplinate «a) le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte del CVCN e dei CV, ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri di cui alla lettera b) del presente comma, fatti salvi i casi di deroga di cui all'articolo 1, comma 6, lettera a), del decreto-legge; b) i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione di cui alla lettera a); c) le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi [rispetto ai soggetti afferenti al PSNC]».

Relativamente al profilo operativo, l'istituzione di tali Centri, frutto dell'esigenza di prevenire e attenuare i rischi derivanti da risorse informatiche vulnerabili, è stata definita da alcuni come un «modello derogatorio di procurement relativamente all'affidamento di forniture di beni, servizi ICT e sistemi […]» il quale ha imposto accurate verifiche tecnico-documentali preliminari, al termine del quale potranno essere disposte specifiche condizioni e test – di corretta implementazione e di intrusione – di hardware e software nel bando di gara e/o nel contratto[129]. L'art. 3 del citato d.P.R. n. 54 del 2021, relativo alla "comunicazione di affidamento" impone infatti ai soggetti afferenti al PSNC di comunicare al CVCN, o ai competenti Centri accreditati, l'intenzione di procedere all'affidamento di forniture di risorse informatiche «prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT di cui all'articolo 1, comma 6, lettera a), del decreto-legge [PSNC], anche nel caso in cui tali procedure siano espletate attraverso le centrali di committenza». Mentre il successivo art. 9 prevede che anche «successivamente all'aggiudicazione della gara o della stipula del contratto, [tali soggetti] comunica[no] al CVCN o ai CV, in via telematica, i riferimenti del fornitore e ogni elemento utile ad individuare in modo univoco l'oggetto di fornitura»[130].

Comunicato l'affidamento, la procedura di verifica e valutazione, il cui metodo è disciplinato all'art. 4, è articolata nelle seguenti fasi: *verifiche preliminari, individuazione di condizioni e test* (art. 5), ove il CVCN o i CV effettuano verifiche preliminari ed eventualmente richiedono al soggetto incluso nel Perimetro le informazioni necessarie per assicurare la collaborazione ai fini dell'individuazione delle condizioni per il fornitore e della tipologia di test di hardware e di software da eseguire; *preparazione all'esecuzione dei test* (art. 6), il CVCN e i CV verificano, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni; *esecuzione del test* (art. 7), il CVCN o i CV comunicano l'avvio dei test al soggetto incluso nel Perimetro e al fornitore che sarà eseguito presso i laboratori del CVCN, dei CV e dei LAP o, se necessario, presso il fornitore o il soggetto incluso nel Perimetro; *esito della valutazione e prescrizioni di utilizzo* (art. 8), ove il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei test e lo comunicano al soggetto incluso nel Perimetro e al fornitore.

Qualora il Centro si pronunci (entro 45/60 giorni) in senso negativo, questi potrà imporre ai bandi di gara e ai contratti clausole, anche sospensive o risolutive, volte al rispetto delle condizioni e dei test eventualmente disposti dallo stesso.

Preme precisare che tali atti del procedimento di verifica e valutazione «sono adottati nel rispetto dell'esigenza di tutela della sicurezza nazionale per le finalità di cui all'articolo 1, comma 1, del decreto-legge [PSNC]»[131].

Tra le altre ipotesi, le valutazioni possono infatti costituire un'importante fase preliminare anche per l'attivazione dei poteri speciali da parte del

129. Fiorentino 2020, p. 57.

130. Art. 5, co. 9, d.P.R. 54/2021.

131. Art. 4, d.P.R. 54/2021.

Governo (cc.dd. *golden powers*)[132] sui servizi di comunicazione a banda larga basati sulla tecnologia 5G (art. 3, d.l. 105/2019), il cui esercizio è possibile solo qualora, a seguito delle valutazioni svolte dal Centro, emergano «elementi indicanti fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano». Si precisa inoltre che l'art. 4-*bis* del l. 105/2019 interviene in materia di esercizio di poteri speciali del Governo, nei settori della difesa e sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, disciplinati nel d.l. 15 marzo 2012, n. 21, potenziando e ampliandone il loro campo applicativo[133].

4.2. Segue. Il decreto legislativo 3 agosto 2022, n. 123

L'ordinamento italiano si è adeguato al nuovo quadro europeo di certificazione della cybersicurezza, introdotto dal citato *Cybersecurity Act*, con il d.lgs. 3 agosto 2022, n. 123, con cui il Governo[134] ha dato attuazione alla delega di cui all'art. 18 della legge di delegazione europea 2019-2020 (l. 22 aprile 2021, n. 53).

Più precisamente, il provvedimento ha dato attuazione ad alcune disposizioni del titolo III del Regolamento, concernenti la certificazione della cybersicurezza dei beni ICT.

Innanzitutto, come già avvenuto sulla scorta del d.l. 14 giugno 2021, n. 82, il decreto legislativo ha riconosciuto l'Agenzia per la Cybersicurezza Nazionale (ACN) quale "Autorità Nazionale di Certificazione della Cybersicurezza", di cui all'art. 58 del *Cybersecurity Act*[135]. Si tratta di una attività che prima era di competenza dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) operante presso il Ministero dello sviluppo economico (MISE), ove era stato istituito, con il d.P.C.M. del 30 ottobre 2003, lo Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione a cui sovraintende l'Organismo di Certificazione della Sicurezza Informatica (OCSI), oggi anch'esso trasferito presso l'ACN[136].

In virtù di tale funzione, l'Agenzia ha competenze relative al rilascio dei certificati europei di cybersicurezza, quale attività "rigorosamente distinta" da quella di vigilanza. Tali competenze sono infatti affidate a due distinte divisioni dell'Agenzia[137].

Relativamente all'ultima attività, l'art. 5 del decreto legislativo, stabilisce che l'Agenzia svolge la funzione di vigilanza verso i fornitori e i fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità. Attività che può svolgere anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia, con le autorità di vigilanza degli altri Stati membri, e con le forze dell'ordine (soprattutto in sede ispettiva).

Il disposto prevede inoltre che nel caso in cui l'Agenzia, in esito alle attività di vigilanza, accerti l'emissione di un certificato non conforme, il certificato è revocato: a) se relativo a livelli di affidabilità "elevati"; b) per il livello di affidabilità "di base" o "sostanziale" nel caso in cui il certificato non conforme sia relativo ad un bene ICT che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale, o servizio di comunicazione elettronica, o alla salute o all'incolumità personale; c) se previsto espressamente dallo specifico sistema europeo di certificazione.

Relativamente al rilascio di certificati, conformemente alla lettera del *Cybersecurity Act*, l'art. 6 del d.lgs. 123/2022 affida all'ACN il rilascio dei certificati di cybersicurezza con livello di affidabilità

132. La valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, strumentale ai fini dell'esercizio dei poteri speciali è disciplinata all'art. 12 del d.P.R. 54/2021, rubricato "Casi particolari".

133. Mele 2020, p. 204 ss.

134. Sulla "Prevalenza dell'attività del Governo nella recezione della regolamentazione tecnica comunitaria" si rinvia a Iannuzzi 2006, p. 13.

135. Cfr. art. 4, d.lgs. n. 123/2022.

136. Sul punto si rinvia al sito ufficiale dell'OCSI presso l'Agenzia per la Cyberiscurezza Nazionale.

137. Sul punto si rinvia al d.P.C.M. 9 dicembre 2021, n. 223, "Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale".

"elevato", tramite l'Organismo di Certificazione della Sicurezza Informatica (OCSI). La disciplina nazionale prevede inoltre che l'ACN si può avvalere di esperti o di Laboratori di prova (LAP), abilitati dall'Agenzia ad operare per proprio conto e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

Il comma 2 stabilisce che ove uno specifico sistema di certificazione preveda il rilascio dei certificati con livello di affidabilità "sostanziale" o "di base" unicamente da parte di un organismo pubblico, l'Agenzia può emettere tali certificati attraverso l'OCSI. Tuttavia, il rilascio può avvenire anche ad opera di altro organismo di valutazione della conformità pubblico, comunque accreditato dall'organismo di accreditamento, monitorato e vigilato dall'Agenzia, e designato dalla stessa, salvo diverse disposizioni dello specifico sistema europeo di certificazione.

Altra funzione, che permette all'Agenzia di vigilare sugli organismi di valutazione, riguarda l'obbligo di cui all'art. 8 del d.lgs. dell'organismo di accreditamento nazionale (ossia Accredia[138]), di comunicare all'ACN ogni aggiornamento in merito agli organismi di valutazione della conformità accreditati quanto a nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento.

Infine, l'art. 9 dispone che, in assenza di un sistema europeo di certificazione, l'ACN potrà introdurre sistemi nazionali di certificazione per i beni ICT, previa consultazione dei portatori di interesse. Si ricorda tuttavia che, al fine di evitare la frammentazione del mercato interno dei sistemi di certificazione, in questo caso lo Stato italiano sarà tenuto ad informare la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersecurity.

5. Il *Cyber Resilience Act*. Il quadro dei controlli alla luce del recente trilogo tra i co-legislatori europei

All'istituzione del quadro unico armonizzato di certificazioni di cybersicurezza dei beni ICT, attuato con il *Cybersecurity Act*, ha fatto seguito l'istituzione di un quadro armonizzato di obblighi volti a mettere in cybersicurezza l'intera *supply chain* di produzione dei beni ICT.

Con la proposta di Regolamento relativa ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali che modifica il Regolamento (UE) 2019/1020 (anche nota come *Cyber Resilience Act* – CRA), possiamo dire che l'obiettivo di mettere in sicurezza il mercato unico digitale è in fase di completamento.

La proposta introduce infatti norme per l'immissione sul mercato di prodotti con elementi digitali, intesi come «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente»[139], al fine di armonizzare il mercato interno dei beni ICT relativamente ai requisiti di cybersicurezza[140].

Si precisa tuttavia che tale ampio ambito di applicazione non trova efficacia verso i prodotti con elementi digitali disciplinati dal Regolamento (UE) 2017/745, relativo ai dispositivi medici per uso umano e accessori per tali dispositivi, del Regolamento (UE) 2017/746, relativo ai dispositivi medicodiagnostici *in vitro* per uso umano e accessori per tali dispositivi, nonché ai prodotti con elementi digitali che siano stati certificati in conformità del Regolamento 2018/1139, relativo al livello elevato ed uniforme di sicurezza dell'aviazione civile, e ai prodotti a cui si applica il Regolamento (UE) 2019/2144, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli[141].

Nello specifico, la proposta disciplina i requisiti essenziali per la progettazione, lo sviluppo e la fabbricazione dei beni ICT rientranti nel suo campo d'applicazione, e gli obblighi per gli operatori economici relativi a tali beni, ed inoltre prevede norme in materia di vigilanza del mercato e loro relativa applicazione.

138. Sulle attività di Accredia nel contesto della cybersicurezza si invita a consultare la pagina ufficiale relativa agli atti del convegno dal titolo "Come gestire il rischio informatico? Il contributo dell'accreditamento e della certificazione alla cybersecurity nazionale", tenuto il 14 novembre 2022 presso Sapienza, Università di Roma.

139. Cfr. art. 3, par. 1, proposta CRA.

140. Chiara 2023, p. 151 ss., a cui si rinvia per una trattazione dettagliata della proposta CRA.

141. Cfr. art. 2, parr. 2 e 3, proposta CRA.

Per quel che interessa il presente contributo ci concentreremo sui primi aspetti, cercando di analizzare il rapporto tra le classi di rischio dei prodotti e i corrispondenti obblighi che gravano sui fabbricanti, rappresentanti autorizzati, importatori e distributori di prodotti con elementi digitali.

La particolarità della proposta di Regolamento è infatti quella di aver suddiviso i beni ICT in due categorie principali in base ai livelli di rischio formulati dalla Commissione e definiti all'interno degli allegati alla proposta[142]. La prima categoria comprende i prodotti "non critici" predefiniti, ossia hardware e software con un basso livello di criticità (ad esempio, hard disk, assistenti domestici intelligenti o giocattoli connessi).

L'art. 5 prevede che tali prodotti possano essere immessi sul mercato se il bene e i processi messi in atto dal fabbricante per la sua produzione sono conformi ai requisiti essenziali di cui all'allegato I, relativo ai "Requisiti essenziali di cybersicurezza", e «a condizione che siano correttamente installati, siano oggetto di un'adeguata manutenzione e siano utilizzati in maniera adeguata alla loro finalità prevista o in condizioni ragionevolmente prevedibili e, se opportuno, aggiornati»[143].

La seconda categoria include invece i "prodotti critici", disciplinati all'art. 6 ed elencati nell'allegato III. Tale categoria è ulteriormente suddivisa in due sottocategorie, la classe I relativa al "rischio inferiore", ove rientrano i prodotti con elementi digitali critici (ad esempio, reti private virtuali e router)[144] e la classe II per il "rischio elevato", ove troviamo i prodotti con elementi digitali altamente critici (ad esempio, sistemi operativi per computer fissi e telefoni cellulari o contatori intelligenti)[145].

In base al loro livello di rischio, i suddetti prodotti digitali sarebbero soggetti a procedure di valutazione della conformità meno o più stringenti per dimostrare la conformità agli obblighi di cybersicurezza stabiliti nella proposta di Regolamento. Premettiamo tuttavia che, tra i diversi operatori economici interessati dalla disciplina, l'onere di svolgere tale valutazione incombe solo sui fabbricanti di cui all'art. 10, par. 2 della proposta.

Tuttavia, considerato quanto già scritto a proposito dei prodotti "non critici", i fabbricanti di tali beni sono tenuti a dichiarare sotto la propria responsabilità che i dispositivi con elementi digitali da loro prodotti sono conformi a tutti i requisiti di sicurezza di cui all'allegato I (*self-assessment*).

Invece per i prodotti "critici", il processo per dimostrare la conformità varia a seconda della sottocategoria presa in considerazione. Per i prodotti critici di classe I (rischi inferiori), il produttore potrebbe ancora effettuare una valutazione autonoma sotto la propria responsabilità, a condizione che applichi al proprio prodotto gli attuali standard armonizzati di cibersicurezza, ad esempio, sviluppati da organizzazioni europee di normazione o schemi di certificazione di cibersicurezza nell'ambito del *Cybersecurity Act*. In assenza di tali standard e schemi per il prodotto in questione, o se il produttore non ha applicato o ha applicato solo in parte gli standard o gli schemi, il produttore dovrebbe sottoporsi a una valutazione di conformità effettuata da un terzo soggetto, ossia l'organismo di valutazione della conformità. Per i prodotti critici di classe II (rischio elevato), i produttori sarebbero soggetti a una valutazione di conformità di terze parti gestita da un organismo di valutazione della conformità.

Preme precisare che, al fine di facilitare la valutazione della conformità ai requisiti stabiliti, la proposta prevede una presunzione di conformità per i prodotti con elementi digitali che siano conformi alle norme armonizzate che traducono i requisiti essenziali della proposta in specifiche tecniche

142. Nel determinare i livelli di rischio la Commissione tiene conto di una serie di indici come la categoria del prodotto, ed in particolare se tale categoria di prodotti sia utilizzata dai soggetti essenziali di cui alla disciplina NIS, se sia una categoria di prodotti su cui detti soggetti fanno affidamento oppure possa avere un'importanza futura per le attività di tali soggetti, o sia pertinente per la resilienza dell'intera catena di approvvigionamento dei prodotti con elementi digitali contro eventi perturbatori.

143. Cfr. art. 5, proposta CRA.

144. Cfr. art. 3, n. 3, proposta CRA.

145. Cfr. art. 3, n. 4, proposta CRA.

dettagliate e che sono adottate conformemente al già ricordato Regolamento 1025/2012[146].

Altri obblighi che incombono sui fabbricanti riguardano la registrazione della documentazione tecnica e l'attenersi agli obblighi di notifica per le violazioni della cybersicurezza ai sensi dell'art. 11 della proposta (di cui si dirà dopo).

Gli importatori sono invece tenuti a mettere sul mercato solo prodotti digitali conformi ai requisiti essenziali di cybersicurezza e recanti la marcatura CE, mentre i distributori dovrebbero verificare che i prodotti digitali rechino la marcatura CE, ed hanno anche l'obbligo di accertarsi che i produttori e gli importatori abbiano adempiuto ai loro obblighi ai sensi della legge.

Al momento in cui si scrive, il testo della proposta è stato oggetto di discussione tra i co-legislatori europei che hanno raggiunto un accordo politico sul punto all'inizio di dicembre 2023. In attesa dell'approvazione del testo definitivo, per il momento riteniamo d'interesse evidenziare alcuni i punti critici sollevati lungo le fasi dell'iter.

Già durante la fase delle votazioni da parte delle Commissioni[147], il *TIC Council,* l'associazione internazionale che rappresenta aziende indipendenti specializzate in testing, ispezione e certificazione, ha criticato un punto nodale della proposta di Regolamento nella parte relativa alla procedura di valutazione della conformità che, come analizzato, differisce a seconda della classificazione del rischio del prodotto, prevedendo per i prodotti "non critici" una procedura di *self-assessment* da parte del fabbricante. Il gruppo di interesse ha infatti sottolineato che secondo le stime circa il 90% dei beni ICT rientrano in tale categoria, e pertanto gran parte delle responsabilità di cybersicurezza graverebbero proprio sui produttori privati, con il conseguente rischio che possano essere immessi sul mercato una certa quantità di dispositivi rischiosi per i consumatori[148]. Si è pertanto auspicato di includere anche tali beni tra quelli oggetto di controllo da parte delle competenti autorità pubbliche.

La *Computer & Communications Industry Association* (CCIA Europe), associazione dell'industria dei computer e delle comunicazioni, ha invece ritenuto eccessive le procedure di valutazione della conformità per i prodotti digitali, le quali potrebbero ostacolare lo sviluppo di nuove tecnologie e servizi[149].

Altre critiche sono state invece mosse dal mondo accademico. Tra queste, Mira Burri e Zaira Zihlmann, le quali ritengono che l'obiettivo dell'Unione europea di elevarsi a produttore di standard di cybersicurezza a livello globale potrebbe sortire l'effetto contrario, ossia di causare la frammentazione della governance globale dei dati[150].

Da settembre 2023, la proposta è passata all'esame congiunto della Commissione, del Parlamento europeo e del Consiglio (c.d. trilogo)[151]. Secondo quanto riportato dagli organi di stampa[152], tra i punti particolarmente dibattuti vi sono stati l'art. 11 relativo all'obbligo di notifica del produttore, e il campo di applicazione della disciplina.

Relativamente al primo, come si può apprendere dal testo dell'art. 11 par. 1 del progetto di Regolamento: «Il produttore deve notificare all'ENISA, senza ritardo e comunque entro 24 ore dal momento in cui ne viene a conoscenza, ogni vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali. […] L'ENISA deve, senza indugi, a meno di giustificati motivi connessi a rischi cibersicurezza, inoltrare la notifica al CSIRT designato per il coordinamento della divulgazione delle vulnerabilità in conformità con la [Direttiva NIS II], agli Stati membri interessati al momento

146. Cfr. considerando 15 proposta CRA.

147. Sul punto si rinvia al documento di "briefing" legislativo del Parlamento europeo, *EU cyber-resilience act*, del novembre 2023.

148. V. TIC Council 2022.

149. V. CCIA Europe 2022.

150. Burri-Zihlmann 2023.

151. Per maggiori dettagli, si rinvia alla pagina del Parlamento europeo dedicata all'osservatorio legislativo sul *Cyber Resilience Act,* 2022/0272(COD).

152. Per i temi discussi nei vari triloghi, si rinvia agli articoli di Euractiv firmati da Luca Bertuzzi, di cui in particolare: Bertuzzi 2023; Bertuzzi 2023a; Bertuzzi 2023b.

della ricezione e informare l'autorità di sorveglianza del mercato sulla vulnerabilità segnalata».

Le preoccupazioni sorte su questo punto hanno riguardato la nozione di «vulnerabilità attivamente sfruttata», introdotta per la prima volta nell'ordinamento europeo con la proposta CRA e definita come «una vulnerabilità per la quale esistono prove affidabili che l'esecuzione di codice dannoso è stata effettuata da un attore su un sistema senza il permesso del proprietario del sistema»[153]. Questa informazione sulla cybersicurezza è particolarmente sensibile poiché rappresenta una vulnerabilità difficile da sanare entro le ventiquattro ore richieste per la notifica, e quindi la sua divulgazione potrebbe costituire un potenziale pericolo se appresa da attori malevoli che potrebbero sfruttarla nuovamente.

Pertanto, rispetto alla formulazione originale dell'art. 11 della proposta, ove il compito di diffondere tali vulnerabilità era affidato all'ENISA, i governi degli Stati membri, temendo che tali vulnerabilità possano costituire rischi per la sicurezza e gli interessi nazionali, hanno proposto di affidare questa funzione di recepimento delle notifiche ai CSIRT nazionali[154].

L'emendamento ha tuttavia aperto ad un'ulteriore questione, anch'essa particolarmente discussa, riguardo alla possibilità per i CSIRT nazionali di ritardare discrezionalmente la trasmissione di tali informazioni per giustificati motivi di cibersicurezza, che possono includere ragioni di sicurezza nazionale e interesse pubblico, nonché ordine pubblico. Secondo alcuni dietro questa eccezione ci sarebbe l'interesse dagli Stati membri a sfruttare essi stessi le vulnerabilità così notificate ai propri CSIRTs per spiare bersagli per motivi di sicurezza nazionale[155].

Da quanto si apprende dall'ultimo trilogo il 30 novembre 2023[156], sembra che questo problema sia stato bilanciato giungendo a soluzioni restrittive che probabilmente faranno parte del testo finale del CRA[157]. Secondo tali indicazioni, il CSIRT nazionale avrà il potere di limitare la segnalazione se il prodotto coinvolto ha principalmente una penetrazione nel mercato nazionale e non comporta rischi significativi per gli altri paesi dell'UE. Inoltre, le autorità nazionali non saranno obbligate a rendere pubbliche le informazioni che ritengono essenziali per proteggere gli interessi fondamentali della sicurezza. Tuttavia, su proposta del Parlamento europeo, si è ottenuto che l'ENISA riceva comunque alcune informazioni per monitorare possibili rischi sistemici per il mercato unico.

Altro punto dibattuto, e connesso con il precedente, ha interessato il campo di applicazione della proposta rispetto ai fabbricanti. Secondo un documento fatto circolare dopo il trilogo, pare che la Commissione abbia proposto di considerare un produttore avere la sua sede principale nel Paese membro dell'Unione in cui sono prese prevalentemente ("*predominantly*") le decisioni relative alla cybersicurezza dei suoi prodotti con elementi digitali[158]. Nel caso in cui questo criterio non trovi efficacia, la sede principale dovrà essere considerata il Paese dell'Unione in cui l'azienda ha il maggior numero di dipendenti[159].

6. Considerazioni conclusive

Il *Cybersecurity Act* e la proposta di Regolamento *Cyber Resilience Act* si pongono l'obiettivo di rendere "cybersicuro" il mercato interno attraverso l'istituzione di sistemi di certificazione e sicurezza della catena di approvvigionamento dei beni ICT. Mentre le competenti autorità europee, in

153. Art. 3, n. 39, proposta CRA.

154. Le proposte del Consiglio europeo sul CRA possono essere consultate sul sito ufficiale alla pagina *Cyber resilience act: member states agree common position on security requirements for digital products* del 19 luglio 2023.

155. Bertuzzi 2023.

156. Si rinvia alla pagina del Consiglio, *Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products*, del 30 novembre 2023.

157. Bertuzzi 2023b.

158. Parte del documento è stato riportato da Euractiv. Il frammento interessato citato da Bertuzzi 2023 è «[a] manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken».

159. *Ibidem*.

particolare l'ENISA, svolgono un ruolo di supporto e promozione della certificazione europea di cybersicurezza, le autorità nazionali di certificazione sono responsabili della implementazione di tale sistema presso gli Stati membri tramite l'esercizio di poteri di vigilanza e sanzione.

Tuttavia, la questione che qui interessa maggiormente non attiene al sistema di controlli sui beni ICT affidato alla certificazione, ma a ciò che permette a tali beni di essere cybersicuri, ossia lo standard.

Come anticipato, le norme tecniche, nate come strumento privato per migliorare i processi produttivi, si sono rapidamente sviluppate come strumenti di intervento indiretto dei poteri pubblici nell'economia, per fini di interesse pubblico come la tutela ambientale, la qualità dei prodotti e la sicurezza.

In precedenza, relativamente agli standard di cybersicurezza si è fatto riferimento alla contrapposizione di modelli di normazione privata *state-centred/top-down* e *multistakeholder/bottom-up*, ove, per quanto riguarda questi ultimi, si è evidenziata la partecipazione sia delle rappresentanze civili e dell'industria, sia degli Stati.

La normazione europea è organizzata "da" e "per" i soggetti interessati sulla base della rappresentanza nazionale e l'iter di formazione di queste norme segue un processo ispirato ai principi riconosciuti dall'Organizzazione mondiale del commercio (OMC) nel settore della normazione, vale a dire, coerenza, trasparenza, apertura, consenso, applicazione volontaria, indipendenza da interessi particolari ed efficienza (c.d. "principi fondatori")[160].

In particolare, il processo di formazione delle "norme armonizzate" (vedi, *supra*, par. 3), disciplinato all'art. 10 del Regolamento 1025/2012, costituisce un esempio di co-regolazione: la Commissione stabilisce i requisiti relativi al contenuto che lo standard deve avere, l'organismo europeo di normazione, delegato a tal proposito in virtù della richiesta di standardizzare, qualora accetti, è vincolato al rispetto di tali prescrizioni.

Come è stato osservato, le parti interessate, quali ad esempio piccole e medie imprese, associazioni ambientaliste e dei consumatori, parti sociali, non sono direttamente coinvolte nel processo di formazione di tali norme, dato che solo i corpi nazionali hanno diritto di voto e di negoziare nella preparazione e nell'adozione degli standard europei[161]. Tali parti hanno infatti diretta rappresentanza all'interno delle organizzazioni europee di normazione e in quelle nazionali[162].

Tuttavia, come è stato osservato, il *Cybersecurity Act*, anche se fa riferimento a norme europee e internazionali, non è una legislazione che si conforma alla disciplina del Regolamento 1025/2012[163]. Infatti, i requisiti degli schemi di certificazione non sono stati definiti all'interno delle tre ESOs, ma all'interno del Gruppo Consultivo ENISA di cui all'art. 21 del *Cybersecurity Act*, composto da «esperti riconosciuti che rappresentano i pertinenti portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le PMI, gli operatori di servizi essenziali, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati in conformità della direttiva (UE) 2018/1972, delle organizzazioni europee di normazione nonché delle autorità di contrasto e delle autorità di controllo preposte alla protezione dei dati»[164].

A tal proposito, merita evidenziare che nella strategia europea per la standardizzazione *Una strategia dell'UE in materia di normazione. Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale* presentata il 2 febbraio 2022[165], è stato fissato l'obiettivo di favorire l'integrità, l'inclusività e l'accessibilità del sistema europeo di normazione attraverso principi di "buona governance".

160. Il considerando 2, Regolamento 1025/2012.

161. Hofmann 2016, p. 18.

162. *Ibidem*.

163. Kohler 2020, p. 9.

164. Art. 21, Regolamento (UE) 2019/881.

165. Commissione europea, Una strategia dell'UE in materia di normazione. *Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, 2 febbraio 2022, p. 4, COM(2022) 31.

Dal documento si apprende della necessità per l'Unione di «integrare i valori democratici fondamentali e gli interessi dell'UE e i principi ecologici e sociali» all'interno delle norme tecniche, «[a]d esempio, le norme in materia di cybersicurezza o resilienza delle infrastrutture critiche […] caratterizzate da una dimensione strategica», ormai non più limitate a trattare questioni relative alle sole componenti tecniche.

L'impressione pertanto è che l'Unione europea, con i citati interventi in materia di cybersicurezza, stia concentrando maggiore peso sul ruolo delle istituzioni pubbliche europee, piuttostoché, come in questo caso, sugli organismi di normazione di natura privata, al fine di sviluppare un sistema di normazione tecnica che sia rispettoso dei più ampi principi di democrazia e rappresentanza, oltreché dei "valori europei".

Tuttavia se da una parte questo sistema favorisce certamente l'armonizzazione delle norme tecniche a livello europeo tra tutti gli Stati membri, dall'altra, come già prospettato da alcuni[166], l'utilizzo della normazione tecnica come veicolo dei valori europei nel contesto globale potrebbe originare possibili frammentazioni nel settore. L'auspicio pertanto è che, come per il Regolamento generale sulla protezione dei dati personali (GDPR), l'"effetto Bruxelles"[167] delle politiche europee faccia effetto anche in questo caso.

Riferimenti bibliografici

P. Andreini (1995), *La normativa tecnica tra sfera pubblica e sfera privata*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di) (1995), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, il Mulino, 1995

J.P. Barlow (1996), *A Declaration of the Independence of Cyberspace*, 8 February 1996

M.E. Bartoloni (2021), *La regolazione privata nel sistema costituzionale dell'unione europea. Riflessioni sulla disciplina relativa al settore dell'innovazione*, in "Osservatorio sulle fonti", 2021, n. 3

K.P. Berger (1999), *The Creeping Codification of the Lex Mercatoria*, Kluwer Law International, 1999

V. Bertola, S. Quintarelli (2023), *Internet fatta a pezzi*, Bollati Boringhieri, 2023

L. Bertuzzi (2023), *EU Commission pitches double reporting of open security loopholes in cybersecurity law*, in "Euractiv", 15 November 2023

L. Bertuzzi (2023a), *EU policymakers prepare to close on cybersecurity law for connected devices*, in "Euractiv", 30 November 2023

L. Bertuzzi (2023b), *EU institutions finalise agreement on cybersecurity law for connected products*, in "Euractiv", 5 December 2023

A. Bradford (2019), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2019

M. Burri, Z. Zihlmann (2023), *The EU Cyber Resilience Act – An Appraisal and Contextualization*, in "Zeitschrift für Europarecht (EuZ)", 2023, n. 2

166. Burri-Zihlmann 2023.

167. Bradford 2019.

C. Caeiro, K. Jones, E. Taylor (2023), *Technical Standards and Human Rights: The Case of New IP*, in C. Sabatini (ed.), "Human Rights in a Changing World Order", Chatham House and Brookings Institution Press, 2023

G. Caia, F.A. Roversi Monaco (1995), *Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, in P. Andreini, G. Caia, G. Elias, F.A. Roversi Monaco (a cura di), "La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

B. Carotti (2016), *Il sistema di governo di Internet,* Giuffrè, 2016

CCIA Europe (2022), *New EU Cybersecurity Rules Are Well-intended, but Introduce Unnecessary Red Tape*, 15 September 2022

V.G. Cerf (2022), *Sulla governance di Internet*, in L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), "La Internet governance e le sfide della trasformazione digitale", Editoriale Scientifica, 2022

O.W. Cesarini (1929), *Il diritto dei privati*, Quodlibet, 1929

Z. Chen, C. Wang, G. Li, Z. Lou, S. Jiang, A. Galis (2020), *New IP Framework and Protocol for Future Applications*, University College, 2020

P.G. Chiara (2023), *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in "Rivista italiana di informatica e diritto", 2023, n. 1

P.G. Chiara (2022), *European Union – Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices*, in "European Data Protection Law Review", vol. 8, 2022

E. Chiti (2003), *La normalizzazione*, in S. Cassese (a cura di), "Trattato di diritto amministrativo", vol. IV, 2003

Commissione delle comunità europee (2009), *Libro bianco – Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE – Prospettive*, 3 luglio 2009

CSCG (2017), *Recommendation #2 – Definition of Cybersecurity*, ver. 01.08, 2017

W.J. Drake, V.G. Cerf, W. Kleinwächter (2016), *Internet fragmentation: An overview*, World Economic Forum, 2016

K. Eichensehr (2015), *The Cyber-Law of Nations*, in "The Georgetown Law Journal", vol. 103, 2015

S. Even, D. Siman-tov (2012), *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117, 2012

G. Finocchiaro (2001), *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in "Contratto e impresa", 2001, n. 2

L. Fiorentino (2020), *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea, L. Fiorentino (a cura di), "I 'poteri speciali' del Governo nei settori strategici", Editoriale Scientifica, 2020

F. Galgano (2016), *Lex mercatoria*, il Mulino, 2016

C. Gallotti (2019), *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001*, Lulu.com, 2019

W. Gibson (1984), *Neuromancer*, Ace books, 1984

M. Gigante (1997), *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in "Rivista italiana di diritto pubblico comunitario", 1997, n. 2

B. Goldman (1983), *Lex mercatoria*, Kluwer Law International, 1983

J. Goldsmith, T. Wu (2006), *Who controls the Internet? Illusion of a boardless world*, Oxford University Press, 2006

N. Greco (1999), *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale*, in Aa.Vv., "Crisi del diritto, produzione normativa e democrazia degli interessi", Edistudio, 1999

H.C.H. Hofmann (2016), *A European Regulatory Union – The Role of Agencies and Standards*, in P. Koutrakos, J. Snell (eds.), "Research Handbook on the EU's Internal Market", Elgar Publishing, University of Luxembourg Law Working Paper, 2016, n. 1

D.B. Hollis (2014), *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, in J.D. Ohlin, K. Govern, C. Finkelstein (eds.), "Cyberwar: Law & Ethics for Virtual Conflicts", Oxford University Press, 2014

A. Iannuzzi (2018), *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, 2018

A. Iannuzzi (2006), *Caratterizzazioni della normazione tecnica nell'ordinamento italiano. Il campo di analisi e di verifica della materia ambientale*, in "Studi parlamentari e di politica costituzionale", 2006, n. 151-152

S. Jiang (2019), *New IP Networking for Network 2030*, Fifth ITU Workshop on Network 2030, International Telecommunication Union, 2019

C. Joerges (1997), *Scientific expertise in Social Regulation and the European Court of Justice: Legal Frameworks for Denationalized Governance Structures*, in C. Joerges, K.-H. Ladeur, E. Vos (eds.), "Integrating Scientific Expertise into Regulatory Decision-Making. National traditions and European Innovation", Nomos, 1997

C. Joerges, H. Schepel, E. Vos (1999), *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the "New Approach"*, in "EUI Working Paper law", 1999, n. 9

O. Kanevskaia (2023), *The law and practice of global ICT standardization*, Cambridge University Press, 2023

N. Katagiri (2021), *Why international law and norms do little in preventing non-state cyber attacks*, in "Journal of Cybersecurity", vol. 7, 2021, n. 1

P. Khanna (2016), *Connectography. Le mappe del futuro ordine mondiale*, Fazi Editore, 2016

C. Kohler (2020), *The EU Cybersecurity Act and European standards: an introduction to the role of European standardization*, in " International Cybersecurity Law Review", vol. 1, 2020

F.D. Kramer (2009), *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in F.D. Kramer, S. Starr, L.K. Wentz (eds.), "Cyberpower and National Security", University of Nebraska Press, Potomac Books, 2009

D.T. Kuehl (2009), *From Cyberspace to Cyber-power: Defining the Problem*, in F.D. Kramer, S. Starr, L.K. Wentz (eds.), "Cyberpower and National Security", University of Nebraska Press, Potomac Books, 2009

J. Lanier (2017), *Dawn of the New Everything: Encounters with Reality and Virtual Reality*, Henry Holt and Co., 2017

L. Lessig (2006), *Code: Version 2.0*, Basic Books, 2006

M.C. Libicki (2009), *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009

D. Marrani (2020), *La cooperazione internazionale per la sicurezza e la stabilità del cyberspace*, Editoriale Scientifica, 2020

L. Martino (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica & Società", 2018, n. 1

W. Mattli, T. Büthe (2003), *Setting International Standards: Technological Rationality or Primacy of Power?*, in "World Politics", vol. 56, 2003, n. 1

M. Mayer, L. Martino, P. Mazurier, G. Tzvetkova (2014), *How would you define cyberspace?*, First Draft Pisa, Experimental online laboratory PhD in Politics, Human Rights and Sustainability, Scuola Superiore Sant'Anna, 19 May 2014

S. Mele (2020), *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano, S. Previti (a cura di), "Il diritto di Internet nell'era digitale", Giuffrè, 2020

H.J. Mertens (1996), *Lex Mercatoria: A Self-applying System Beyond National Law?*, in G. Teubner (ed.), "Global law without state", Dartmouth Publishing, 1996

A. Monti (2023), *Digital rights delusion: humans, machines and the technology of information*, Routlege, 2023

A. Monti (2023a), *Metaverso e convergenza tecnologica: aspetti (geo)politici, giuridici e regolamentari*, in G. Cassano, G. Scorza (a cura di), "Metaverso: diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini giuridica, 2023

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014

A. Oddenino (2018), *Digital standardization cybersecurity issues and international trade law*, in "Questions of International Law", vol. 5, 2018

L. Parona (2021), *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in "Giornale di diritto amministrativo", 2021, n. 6

S.Y. Peng (2018), *'Private' Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime*, in "Cornell International Law Journal", vol. 51, 2018, n. 2

O. Pollicino (2023), voce *Potere digitale*, in "Enciclopedia del diritto - Potere e Costituzione", V-2023

R. Radu, G. De Gregorio (2023), *The New Era of Internet Governance Technical Fragmentation and Digital Sovereignty Entanglements*, in F. Cristiano, B. van den Berg (eds.), "Hybridity, conflict, and Global Politics of Cybersecurity", Rowman & Littlefield Publishers, 2023

G.J. Rattray (2009), *An Environmental Approach to Understanding Cyberpower*, in "Cyberpower and National Security", in F.D. Kramer, S. Starr, L.K. Wentz (eds.), "Cyberpower and National Security", University of Nebraska Press, Potomac Books, 2009

M. Raymond, L. DeNardis (2015), *Multistakeholderism: anatomy of an inchoate global institution*, in "International Theory", vol. 7, 2015, n. 3

G.M. Ruotolo (2016), *Il sistema dei nomi di dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in "Il diritto dell'informazione e dell'informatica", 2016, n. 1

G.M. Ruotolo (2014), *Internet (diritto internazionale),* in "Enciclopedia del diritto – Annali", Giuffrè, 2014

D. Russell, G.T. Gangemi (1991), *Computer security basics*, O'Reilly & Associates, 1991

F. Salmoni (2002), *Le norme tecniche*, Giuffrè, 2002

M.N. Schmitt (2017) (general editor), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017

F. Serini (2023), *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in "MediaLaws", 2023, n. 3

F. Serini (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in "federalismi.it", 2022, n. 12

S.J. Shackelford, S. Russell, J. Haut (2016), *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks*, in "UC Davis Business Law Journal", vol. 16, 2016, n. 2

D.D. Stewart Ferguson (2022), *European Cybersecurity Certification Schemes and cybersecurity in the EU internal market*, in "International Cybersecurity Law Review", vol. 3, 2022

M.J. Teplinsky (2023), *A Review of NIST's Draft Cybersecurity Framework 2.0*, in "LawFare", 13 September 2023

G. Teubner (1996), *Global Bukowina: Legal Pluralism in the World-Society*, in G. Teubner (ed.), "Global law without state", Dartmouth Publishing, 1996

TIC Council (2022), *TIC Council Welcomes the European Commission's Proposal for a Cyber Resilience Act*, September 2022

G. Vesperini (1995), *Il controllo della «sicurezza» e della «qualità» dei prodotti industriali: due modelli e confronto*, in P. Andreini, G. Caia, G. Ellas, F.A. Roversi Monaco (a cura di), "Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali", il Mulino, 1995

World Trade Organization (2017), *Members debate cyber security and chemicals at technical barriers to trade committee*, 2017

J. Wouters (2023), *Corporations and the Making of Public Standards in International Law. The Case of China in the International Telecommunication Union*, in P. Delimatsis, S. Bijlmakers, M.K. Borowicz (eds.), "The Evolution of Transnational Rule-Makers through Crises", Cambridge University Press, 2023

A. Zei (2008), *Tecnica e diritto tra pubblico e privato*, Giuffrè, 2008