SAPIENZA
UNIVERSITÀ DI ROMA

DIPARTIMENTO DI
ECONOMIA E DIRITTO

DOTTORATO DI RICERCA IN DIRITTO PUBBLICO,
COMPARATO E INTERNAZIONALE

CURRICULUM DI
DIRITTO PUBBLICO DELL'ECONOMIA

CICLO XXXVI

Mercato, sicurezza e rischio informatico. Normazione e certificazione dei beni ICT per esigenze di cybersicurezza nel contesto europeo e nazionale

Docente tutor e relatore
Prof. Roberto Miccú

Candidato
Dott. Federico Serini

A.A. 2023/2024

SAPIENZA
UNIVERSITÀ DI ROMA

Mercato, sicurezza e rischio informatico. Normazione e certificazione dei beni ICT per esigenze di cybersicurezza nel contesto europeo e nazionale

Facoltà di Economia
Dipartimento di Scienze Politiche
Corso di Dottorato in Diritto pubblico, comparato e internazionale
Curriculum di Diritto pubblico dell'economia

Dott. Federico Serini
Matricola 1541023

Relatore
Prof. Roberto Miccú

A.A. 2023-2024

Questa ricerca è disponibile in open access come da Regolamento di Dottorato di Sapienza Università di Roma (R.D. 1150/2024). Tutti i diritti sono riservati. L'Autore è reperibile all'indirizzo mail: federico.serini@hotmail.com.

Alla mia famiglia

«E pensare che lo stesso fuoco che Prometeo sottrasse agli déi, accese il rogo di Giordano Bruno»

S.J. LEC, *Pensieri spettinati,* 1957

«Il geo-diritto si trova, dunque, all'interno d'una scissione dolorosa. [...] Da un lato, insomma, geo-diritto, ancora congiunto a geo-grafia, cioè a determinazioni spaziali di gruppi; dall'altro, geo-diritto, proteso a impossessarsi della geo-economia, e dunque contrastante o secondante la planetaria volontà di profitto. I due rami o volti del geo-diritto s'incontrano, o dovrebbero incontrarsi, nel *punto comune della decisione politica* a cui sempre spetta di dar risposta ai problemi dell'umano convivere»

N. IRTI, *Norma e luoghi*, 2001

INDICE

2. Alcune considerazioni generali sulla sicurezza in senso tradizionale
3. La sicurezza nella Costituzione italiana
   3.1 La sicurezza nazionale
   3.2 Ordine e sicurezza pubblica
4. La sicurezza nell'ordinamento europeo
   4.1. I concetti di ordine pubblico e sicurezza nazionale per l'ordinamento europeo
   4.2. La sicurezza come interesse collettivo europeo. SLSG e PSDC tra integrazione economica e politica
   4.3. L'esigenza di sicurezza degli Stati membri come limite alle libertà dell'Unione europea.
      a) La minaccia diretta all'interesse fondamentale della collettività
      b) Il rispetto del principio di proporzionalità
      c) Il doppio sindacato giurisdizionale in sede nazionale ed europea

CAPITOLO II
CYBERSICUREZZA E CYBERRESILIENZA TRA ORDINAMENTO EUROPEO E ITALIANO

1. Il quadro delle politiche e delle amministrazioni nel cyberspazio europeo tra sovranità tecnologica e sicurezza
   1.1 Il rafforzamento delle infrastrutture informatiche: tra soggetti critici e infrastrutture di Internet
      i) La sicurezza delle risorse informatiche infrastrutturali: la disciplina *Network and Information Security* (NIS)
      ii) La resilienza operativa digitale per il settore finanziario: il DORA
      iii) Dalle infrastrutture ai beni: il rafforzamento delle catene di approvvigionamento dei beni ICT
      iv) La prospettiva europea sulla sicurezza delle connessioni e dell'Internet globale
   1.2 La (cyber)consapevolezza situazionale europea e le relative amministrazioni
   1.3. La vulnerabilità umana e il rafforzamento delle competenze informatiche
2. Il d.L. 82/2021. L'architettura italiana di cybersicurezza
   2.1 Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)
   2.2 *Segue*. Oltre il segreto di Stato. Il controllo sul *procurement* informatico per fini di sicurezza e interesse nazionale
   2.3. *Segue*. L'estensione della sicurezza nazionale "statica" sui beni ICT: il caso delle TELCO e del 5G
3. La definizione di cybersicurezza tra norma tecnica e giuridica
   3.1. Il concetto giuridico di cybersicurezza europea: sicurezza del mercato unico e sicurezza dell'umano
   3.2. La cybersicurezza nazionale italiana
4. Il concetto di resilienza
5. Introduzione alla cyberresilienza
   5.1. La cyberresilienza europea
   5.2. La cyberresilienza nazionale
6. La terminologia del rischio informatico e le dimensioni della cybersicurezza europea
7. La privatizzazione della sicurezza
   7.1 *Segue*. Il ruolo dei privati nella normazione tecnica di sicurezza: il caso della cybersicurezza
   7.2 *Segue*. I partenariati pubblico-privati europei per lo scambio di informazioni di cybersicurezza
8. Gli interessi di rilevanza giuspubblicistica sottesi alla cybersicurezza: una relazione mediata tra sicurezza e tecnologie informatiche

9. Considerazioni conclusive sulla (cyber)sicurezza tra normativo e politico

PARTE III
LA CO-REGOLAZIONE DELLE CYBERSICUREZZE. LA NORMAZIONE TECNICA E LA CERTIFICAZIONE DI SICUREZZA DEI BENI, SERVIZI E PROCESSI ICT TRA ITALIA E UE

CAPITOLO I
LA NORMAZIONE E CERTIFICAZIONE TECNICA: ALCUNI ASPETTI GENERALI

1. Introduzione
2. La Normazione tecnica dalla prospettiva degli ordinamenti italiano ed europeo
   - 2.1. L'evoluzione storica della normazione tecnica
   - 2.2. La norma tecnica nella teoria generale del diritto
   - 2.3. La norma tecnica tra ordinamento giuridico e non giuridico
   - 2.4. Pubblico e privato nella produzione di norme tecniche
   - 2.5. Le norme tecniche volontarie pubblicizzate e l'incorporazione
   - 2.6. Le norme tecniche volontarie e il rinvio
     - 2.6.1. Gli organismi di normazione tecnica tra *munera publica* e natura privata
     - 2.6.2. Gli organismi di normazione nazionali
       - a) Il Comitato Elettrotecnico Italiano (CEI)
       - b) L'Ente Nazionale Italiano di Unificazione (UNI)
     - 2.6.3. Gli organismi di normazione internazionale
       - a) L'*International Telecommunication Union* (ITU)
       - b) L'*International Electrotechnical Commission* (IEC)
       - c) L'*International Organization for Standardization* (ISO)
   - 2.7 L'evoluzione delle norme (tecniche) armonizzate alla luce del diritto derivato
     - 2.7.1 *Segue*. Il Regolamento (UE) 1025/2012 sulla normazione europea
       - a) I principi generali della normazione e il processo di formazione delle norme armonizzate
       - b) partecipazione delle rappresentanze sociali al processo di normazione
       - c) L'individuazione delle specifiche tecniche delle ICT nelle procedure di appalto
       - d) La disciplina dell'attività della Commissione e dei comitati nella normazione europea
     - 2.7.2 *Segue*. La Direttiva (UE) 1535/2015 sulla procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione
     - 2.7.3 *Segue*. I recenti adattamenti e modifiche al Regolamento (UE) 1025/2012
       - a) Il Regolamento (UE) 2022/2480
       - b) Il Regolamento (UE) 2023/988
     - 2.7.4 Le norme (tecniche) armonizzate
     - 2.7.5 *Segue*. Il caso *James Elliot* sulle norme armonizzate
     - 2.7.6 *Segue*. Il caso *Stichting Rookpreventie* sull'accesso e opposizione alle norme volontarie (internazionali)
     - 2.7.7 *Segue*. Il caso *Public.Resource. Org Inc. et al.* sull'interesse pubblico all'accesso alle norme armonizzate
     - 2.7.8 *Segue*. Considerazioni sulla natura delle norme armonizzate alla luce degli approdi giurisprudenziali della Corte di giustizia

CAPITOLO II
QUALITÀ E SICUREZZA DELLE "COSE" NELLA NORMAZIONE TECNICA

CAPITOLO III
LA NORMAZIONE E CERTIFICAZIONE TECNICA DI CYBERSICUREZZA TRA UNIONE EUROPEA E ITALIA

INTRODUZIONE

Le risorse informatiche sono un elemento essenziale per le democrazie. Tali strumenti non rappresentano solo il mezzo che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi tramite la rete[1] ma, a livello tecnico, sono anche i parametri di configurazione e funzionamento di molte infrastrutture che erogano servizi e funzioni essenziali per la società e l'economia (c.d infrastrutture critiche) [2]. Si pensi agli apparati informatici in uso presso gli operatori attivi nei settori bancario e finanziario, energetico, dei trasporti, delle comunicazioni, quello sanitario nonché quelli in dotazione presso le pubbliche amministrazioni e le varie istituzioni statali.

Questi strumenti sono ormai indispensabili sia per lo Stato in sé, sia per le sue componenti, prime fra tutte gli individui e le imprese[3]. Ma, allo stesso tempo, sono anche responsabili di aver trasferito i rischi del cyberspazio nel mondo reale. La "rete globale" interconnessa si caratterizza infatti per essere un sistema non concepito per obbedire a criteri di sicurezza, quanto piuttosto a quelli di libero accesso, interoperabilità e libero scambio delle informazioni. Principi questi che si scontrano oggi con le possibilità di *dual use*[4] della rete e dei servizi informatici, tanto che Alcuni hanno avvertito che oggi «ogni società è tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso» e pertanto «più le società sono avanzate, più sono vulnerabili»[5].

Nonostante tale condizione - secondo cui "rischio informatico=rischio sociale" - porti in evidenza come la tutela e la garanzia dei diritti e delle libertà nell'attuale società tecnologica passi prima di tutto per la sicurezza delle reti e dei sistemi informatici[6], i poteri pubblici hanno volto l'attenzione verso questo fenomeno solo di recente (più o meno a partire dalla fine degli anni '90 del secolo scorso), a seguito della progressiva dipendenza degli Stati e delle infrastrutture all'informatica.

Non è un caso se le prime definizioni di cybersicurezza (*cybersecurity*), sicurezza informatica (*computer security*) e sicurezza delle informazioni (*information security*) hanno trovato formulazione

---

[1] V. FROSINI, *La democrazia nel XXI secolo* (1997), Macerata, Liberilibri, 2010, pp. 40-41.

[2] C. GALLOTTI, *I sistemi di gestione per la sicurezza delle informazioni La norma ISO/IEC 27001:2022 I controlli della ISO/IEC 27002:2022*, Lulu press, 2022.

[3] G. DE VERGOTTINI, *Sicurezza e i diritti fondamentali*, in L.E.R. VEGA, L. SCAFFARDI, I. SPIGNO, *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, Editoriale scientifica, 2021, p. 28.

[4] I prodotti *dual use* sono i prodotti, inclusi *software* e le tecnologie informatiche, che possono avere un utilizzo sia civile sia militare. Tali beni sono disciplinati dal regolamento (UE) 2021/821, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso.

[5] M.G. LOSANO, *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. FORNI, T. VETTOR (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017, p. 22. Sugli effetti delle forme di connettività non solo dovute alle tecnologie ICT v. A.L. BARABÀSI, *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, New York, Basic books, 2014. Analogamente v. anche P. KHANNA, *Connectography. Le mappe del futuro ordine mondiale*, Roma, Fazi, 2016.

[6] Cfr. M. DUNN CAVELTY, *Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities*, in *Science and Engineering Ethics,* vol. 20, 2014, p. 704.

all'interno di norme non giuridiche espressione del c.d. "diritto dei privati"[7], ossia le norme tecniche di settore[8].

La pretesa di sicurezza nel cyberspazio da parte degli Stati si scontra quindi con gli effetti derivanti da questo ritardo, da una parte dato dall'iniziale promozione dell'Internet quale motore di una nuova economia basata sull'autoregolazione e a cui gli Stati non hanno posto regole (neppure quelle che disciplinano la concorrenza); e dall'altra dovuto al fatto che l'oggetto della pretesa normativa, il cyberspazio per l'appunto, è un fenomeno globale privo di territorialità, e che ha rappresentato inizialmente un limite all'azione del potere pubblico che invece vanta «un'originaria necessità dei luoghi»[9].

Considerata quindi la difficoltà del diritto e del potere pubblico in generale nel regolare le nuove tecnologie e il cyberspazio, e data la pervasività della norma tecnica in questo settore, quale prodotto di un processo non giuridico-politico che conferisce particolare peso alle rappresentanze dei gruppi privati che operano nei settori delle ICTs, la domanda a cui si tenterà di dare risposta in questa ricerca, riprendendo quanto già dubitato da Ulrich Beck, è «[c]hi ha il diritto legittimo di prendere le decisioni in casi del genere? O, più in generale, le decisioni in merito a tecnologie pericolose come saranno in grado di venir legittimate in futuro?». Ossia specifichiamo noi: la cybersicurezza quale branca della sicurezza tradizionale è ancora assicurata dallo Stato con le norme giuridiche? che ruolo hanno le norme tecniche in questo settore? come sono formate? che rapporto hanno queste con le norme giuridiche dello Stato o dell'Unione europea? quali garanzie?

Come si comprenderà gli interrogativi sottendono alla più ampia riflessione sulla dicotomia potere pubblico-potere privato, spesso interpretata come evanescente nel cyberspazio, ponendo non pochi problemi nella collocazione del "politico" nell'attuale contesto.

In particolare, nel nostro caso, l'analisi intenderà concentrarsi su un particolare aspetto del potere pubblico che è quello della sicurezza, quale tipica espressione della sovranità statale ormai posta alla prova della modernità e del processo di globalizzazione che ne hanno cambiato la morfologia (per Alcuni da intendersi come evoluzione, per Altri come erosione). Per questo motivo la cybersicurezza, che rappresenta una nuova declinazione della sicurezza tradizionale nella società globale informatizzata, è sembrata essere un utile prospettiva di analisi di questo fenomeno.

Al fine di tentare di dare risposta a tali quesiti, la trattazione è stata articolata secondo uno schema frutto dell'esigenza di organizzare la riflessione su tre tematiche principali, rispettivamente argomentate nelle Parti I, II e III.

Nella prima sezione si è dato avvio alla ricerca contestualizzando il rapporto tra potere pubblico e privati nella regolazione del cyberspazio. Dopo aver fornito una sommaria ricostruzione di quest'ultimo concetto, estraneo al mondo del diritto, si sono ripercorse le fondamentali teorie che hanno animato il dibattito negli anni '90 circa i profili di fattibilità, nonché anche di opportunità e legittimità di una disciplina giuridica del cyberspazio. Ciò ha così permesso di approdare all'attuale

---

[7] Con la Raccomandazione ITU-T X.1205, del 18 aprile 2008, l'*International Telecommunication Union* (ITU) ha definito la cybersecurity come l'insieme degli strumenti politici, giuridici e tecnologici che hanno la finalità di proteggere il cyber environment e gli asset degli utenti dai cyber rischi, ed in particolare di garantire le tre priorità della riservatezza (*confidentiality*), integrità (*integrity*) e disponibilità (*availability*) degli stessi. Altra definizione è invece contenuta nella norma tecnica ISO/IEC 27032 ove la cybersicurezza è considerata come azione volta alla «preservation of confidentiality, integrity and availability of information in the Cyberspace».

[8] H. SCHEPEL, *The Constitution Of Private Governance: Product Standards In The Regulation Of Integrating Markets*, Londra, Hart Pub Ltd, 2005. In particolare sull'evoluzione storica della normazione tecnica nei settori della *computer* e *information security*, v. D. RUSSELL, G.T. GANGEMI, *Computer security basics*, Sebastopol, O'Reilly Media, 1991, p. 23.

[9] N. IRTI, *Norma e luoghi*, Roma-Bari, Laterza, 2006, p. 4.

dibattito che vede la contrapposizione di due modelli, da una parte quello di *multistakeholder governance,* e dall'altra il *multilateralism approach.*

Tale ricostruzione ci è stata utile per elaborare la presente proposta di studio che interessa la specifica esigenza di sicurezza nel cyberspazio assicurata per mezzo della normazione tecnica. Obiettivo di analisi che non poteva prescindere dall'ambivalente aspetto della cybersicurezza: dal punto di vista tecnico, dato dalle intrinseche ed originarie vulnerabilità delle reti e dei sistemi informatici; e dal punto di vista politico quale bilanciamento tra continuità del servizio di rete e del sistema informatico, libertà degli utenti e, per l'appunto, sicurezza.

Le evidenti difficoltà del potere politico e normativo di regolare questo spazio, non solo a livello locale da parte dei singoli Stati, ma anche a livello internazionale, ci hanno portato ad introdurre il concetto di cyberspazio "merceologico", quale proposta di interpretazione e scomposizione del cyberspazio inteso come una 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. L'intento è stato quello di legare questo concetto, spesso interpretato in termini astratti e distanti dal diritto, alla realtà concreta del mercato individuando un tratto comune in entrambi: 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.

Questo ci ha inoltre consentito di individuare la doppia anima delle norme tecniche nel contesto digitale: da una parte, a livello tecnico, quali strumenti che disciplinano il funzionamento delle reti e dei sistemi informatici (scomposti nel concetto di "beni ICT"), e dall'altra, dalla prospettiva del diritto pubblico dell'economia, quali strumenti che possono o meno costituire barriere al libero mercato, eventualmente anche come espressione di forme intervento pubblico in economia[10].

Così alla luce delle soluzioni tecno-giuridiche elaborate da Reidenberg e Lessig, ed in particolare il concetto di «*code*», la trattazione intende analizzare gli standard e i certificati di cybersicurezza negli ordinamenti europeo e italiano, proponendo uno studio sulle potenzialità della normazione tecnica non solo come strumento di mercato, ma anche come strumento che può concorrere a colmare il vuoto dato dal fallimento del diritto internazionale nella stabilità del cyberspazio[11], al fine di innalzare i livelli di sicurezza delle reti e dei sistemi informatici, se non a livello globale, per lo meno a livello europeo.

L'indagine ci ha così imposto di riflettere sui due macrotemi che sottendono l'intera riflessione: da una parte la cybersicurezza o, meglio, come vedremo, le "cybersicurezze" (a cui è dedicata la Parte II), dall'altra, la normazione e certificazione tecnica di cybersicurezza (Parte III). Argomenti specifici che non potevano ovviamente prescindere da un necessario inquadramento all'interno della dottrina generale sul punto.

In particolare, rispetto al primo (Parte II), in questa sede si tenterà di ricondurre, per quanto possibile, i concetti di cybersicurezza e cyberresilienza europea all'interno della più ampia riflessione sulla sicurezza in senso tradizionale, da una duplice prospettiva: dal generale al particolare, e viceversa, dal particolare al generale, al fine di meglio comprendere un tema di recente interesse per

---

[10] Cfr. M.R. MAURO, *Diritto internazionale dell'economia: teoria e prassi delle relazioni economiche internazionali*, Napoli, Edizioni scientifiche italiane, 2019, pp. 148 ss.

[11] N. KATAGIRI, *Why international law and norms do little in preventing non-state cyber attacks*, in *Journal of Cybersecurity*, Vol. 7, Issue 1, 2021, reperibile al link:<https://academic.oup.com/ cybersecurity/ article/7/1/ tyab009/ 6168044>.

il diritto, ed in particolare per la giuspubblicistica in generale, che vede tuttavia una certa rilevanza nei suoi aspetti tecnici e pratici.

Si tratta infatti di nozioni che trovano origine nella sicurezza informatica (*computer security*) e nella sicurezza delle informazioni (*information security*), regolate e definite nelle prime norme tecniche di settore. L'intento di detto studio sarà anche quello di cercare di conferire dignità giuridica a concetti di derivazione tecnica, tentando di cogliere il rapporto tra questo aspetto specialistico e quello giuridico.

Come intuibile, l'indagine non è priva di difficoltà, sia per l'ampiezza del concetto, sia per il suo inquadramento in termini giuridici. Se da una parte, analizzare la cybersicurezza e la cyberresilienza come nozioni slegate dalla sicurezza tradizionale porterebbe ad uno studio privo di riferimenti e mete, dall'altro, dobbiamo ammettere, che non esiste una nozione di sicurezza in termini universali. Si è così reso necessario svolgere alcune preliminari considerazioni sulla sicurezza in generale, prima ancora della relativa trattazione di questo concetto nell'ordinamento italiano ed europeo da una prospettiva di diritto costituzionale.

Analizzate le caratteristiche della sicurezza in generale - quelle che abbiamo reputato rilevanti per lo studio -, prima ancora di concentrare la trattazione sul significato dei concetti giuridici di cybersicurezza e cyberresilienza nei due livelli europeo e nazionale, si svolgerà una ricostruzione del quadro di governo sul punto, alla luce dei recenti interventi dei legislatori europeo e italiano, nonché dei documenti strategici in vigore.

La cybersicurezza non rappresenta solo una delle tante applicazioni della sicurezza in un determinato contesto (quello del cyberspazio), ma essa stessa al suo interno vede diverse sfaccettature, sia nella distinzione tra cybersicurezza e cyberresilienza, sia per la convivenza di attività di cybersicurezza pubblica e privata. Motivo che ci ha portato a far riferimento alle "sicurezze" nel titolo di questa Parte[12].

Al di là delle peculiarità del tema, la cybersicurezza è certamente un'esigenza a cui sottendono diversi interessi pubblici nel cyberspazio. Ciò apre la strada alla riflessione sulla normazione e certificazione tecnica, quindi strumenti di natura privata, per la garanzia di interessi pubblici (Parte III). Anche in questo caso, la specificità del tema ci porterà a svolgere una preliminare disamina di detto sistema sia nei suoi aspetti di teoria generale, sia in quelli applicativi avendo modo di analizzare sia la normazione tecnica (distinguendo le norme tecniche pubbliche, quelle volontarie e quelle armonizzate), e il relativo rapporto con l'ordinamento giuridico, sia i sistemi di accreditamento e certificazione, funzionali all'implementazione della prima, e ponendo attenzione anche agli organi che svolgono dette funzioni, nei tre livelli: internazionale, europeo, nazionale.

Dato l'oggetto della ricerca, si porrà particolare attenzione alla normazione europea, nello specifico relativamente alle c.d. norme armonizzate e il loro processo di formazione, oggetto di recenti attenzioni da parte del legislatore europeo sia nella sua disciplina generale, sia in riferimento al settore della cybersicurezza. Come si vedrà, anche alla luce degli orientamenti della Corte di giustizia al riguardo, ci si è concentrati sulla natura di tali norme e il loro rapporto con la norma giuridica e l'ordinamento in generale, nonché gli istituti di partecipazione delle rappresentanze sociali all'interno dei processi decisionali degli organismi di normazione.

[12] Cfr. C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova, Cedam, 2012, pp. 26, ove l'Autorevole dottrina evidenzia che oltre la concezione tradizionale di sicurezza pubblica si «comincia a registrare un'obiettiva distinzione tra sicurezza pubblica primaria ed una secondaria o sussidiaria o complementare».

La riflessione si concentrerà poi sulla normazione tecnica di sicurezza, quale espressione del processo di sicurezza privata già introdotto in precedenza (Parte III, Cap. II, 7), e che, sulla scorta delle riflessioni dell'Autorevole dottrina amministrativa italiana, ci ha consentito di andarne a rintracciare le sue origini nelle funzioni di polizia amministrativa risalenti allo Stato liberale.

Considerazioni che ci saranno utili per porre attenzione sul tema della standardizzazione di sicurezza delle "cose" al fine di poterle estendere anche ai beni ICT.

Infine, l'ultima parte della trattazione si concentrerà sulla standardizzazione e certificazione di cybersicurezza negli ordinamenti europeo e nazionale, tuttavia non prima di aver svolto alcune preliminari considerazioni sul più ampio tema della normazione tecnica nel settore delle ICTs, e sulla contrapposizione, a livello internazionale, tra modelli di *self* e *co-regulation*, che costituiscono il contesto entro il quale devono necessariamente essere collocate le due citate esperienze.

In particolare, la riflessione sarà condotta alla luce di quanto emerso dal "*Rolling Plan for ICT standardisation"* 2024, coprendo tre aspetti fondamentali dell'attuale quadro disciplinare europeo sul punto: la disciplina generale sulla certificazione europea, oggetto del Regolamento 2019/881 (anche noto come *Cybersecurity Act*), e la sua attuazione per mezzo del recente Regolamento 2024/482, attuativo del primo schema di certificazione europeo di cybersicurezza, l'*European Cybersecurity Scheme on Common Criteria* (EUCC), entrato in vigore il 31 gennaio 2024; la sicurezza delle catene di approvvigionamento dei beni ICT alla luce della proposta di Regolamento *Cyber Resilience Act*; ed infine, sarà analizzata la specializzazione dei tre organismi di normazione europei (CEN, CENELEC ed ETSI), ed anche quelli non europei, nella normazione della cybersicurezza.

Tali considerazioni sulla disciplina europea sul punto, ci consentiranno così di analizzare gli aspetti peculiari della regolazione italiana articolata tra alcune disposizioni del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e il Decreto legislativo del 3 agosto 2022 n. 123, avendo modo di analizzare gli effetti della regolazione di diritto derivato sull'architettura italiana in tema di certificazione.

PARTE I

LA *GOVERNANCE* DI SICUREZZA DEL CYBERSPAZIO

CAPITOLO I

PUBBLICO, PRIVATI E CYBERSPAZIO

SOMMARIO: 1. La nozione di cyberspazio - 2. Le teorie sulla regolazione del cyberspazio - 2.1 Cyber-anarchia e *self-regulation* degli utenti contro il potere pubblico (Barlow, Johnsone e Post) - 2.2 Il movimento anti-anarchico e l'applicazione del diritto internazionale (Wu e Goldsmith) - 2.3 Dalla norma giuridica alla legge naturale del cyberspazio: la *lex informatica* e il «*code*» (Reidenberg e Lessig) - 3. La regolazione globale del cyberspazio tra *multistakeholder governance* e *multilateralism approach*

1. La nozione di cyberspazio

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.

Uno dei creatori della Rete, Vinton Cerf, in occasione di un recente incontro organizzato dall'Istituto di Informatica Giuridica del Consiglio Nazionale delle Ricerche (CNR) sul tema della «Internet governance e le sfide della trasformazione digitale» ha infatti definito Internet come «il sistema di trasporto che sposta pacchetti di dati dal punto di origine alla destinazione. [...] 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].

Internet è quindi il servizio (costituito dall'insieme dei protocolli TCP/IP e UDP) che permette 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.

---

[1] Secondo lo studioso F. D. Kramer esistono 28 differenti definizioni del termine *cyberspace*. Cfr. F.D. KRAMER, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in F.D. KRAMER, S. STARR, L.K. WENTZ, *Cyberpower and National Security*, National Defense University Press, Washington (D.C.), 2009.

[2] V.G. CERF, *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, Napoli, 2022, p. 18, reperibile al link del sito della Rivista Italiana di Informatica e diritto:<https://www.rivistaitalianadiinformatica ediritto.it/ index.php/RIID/ issue/view/8>. L'incontro tenutosi il 19 gennaio 2023 presso la sala convegni del CNR di Roma può essere visualizzato al link video:<https://www.youtube.com/watch?v=ykJNJ1S8I5Y>

[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 B. CAROTTI, *Il sistema di governo di Internet*, Giuffrè, Milano, 2016, p. XIII, ove l'A. definisce Internet come «una tecnica di trasmissione di dati».

[4] Sul punto si faccia riferimento alla definizione di Internet 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 report del Congresso del 9 dicembre 2022 reperibile al link:<https://sgp.fas.org/crs/natsec/IF10537.pdf>.

Cerchiamo quindi di capire cosa si intenda per "cyberspazio". Precisiamo innanzitutto che non si tratta di un concetto giuridico, sebbene ormai diffusamente impiegato all'interno di leggi e regolamenti[5].

Anche l'etimologia della parola cyberspazio è ambigua. Secondo la letteratura il lemma "cyber" «è un confisso ricavato dal sostantivo inglese cybernetics, cibernetica, parola derivata dal greco dove κυβερνήτης (*kybernetes*) aveva il significato letterale di 'timoniere, pilota di una nave' e per estensione 'colui che guida e governa una città o uno Stato'»[6].

Come noto, il primo utilizzo del termine lo si trova in un romanzo di un genere letterario che stava prendendo piede negli anni '80 del secolo scorso, il *cyberpunk*. Nel *Neuromancer*, lo scrittore William Gibson ambienta il suo romanzo in una realtà futuristica e distopica dove 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[7]. Alcuni Autori hanno invece descritto il cyberspazio come una «realtà virtuale»[8], Altri come una rete internazionale di computers costituente a tutti gli effetti un «*electronic frontier*»[9].

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 alcuna definizione, e limitandosi solo a definire i comportamenti degli Stati in questo "ambiente"[10]; nell'ambito militare il concetto assume una puntuale 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"[11].

---

[5] Sugli effetti dell'utilizzo del termine cyberspazio a livello giuridico si rinvia a A. MONTI, *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, Pisa, 2023, 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 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 A. MONTI, *Digital rights delusion : humans, machines and the technology of information*, Routlege, Londra, 2023.

[6] Accademia della Crusca on line, reperibile al link:<https://accademiadellacrusca.it/ it/consulenza/cyber/1417>.

[7] 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» (W. GIBSON, *Il Neuromante (1986)*, Ace book, 2018, p. 54).

[8] 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. J. LANIER, *Dawn of the New Everything: Encounters with Reality and Virtual Reality*, Henry Holt and Company, New York, 2017, p. 3.

[9] V. J. L. GOLDSMITH, T. WU, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford, Oxford University Press, 2006, p. 17 a proposito di Jhon Perry Barlow.

[10] D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità del cyberspace*, Napoli, Editoriale scientifica, 2020, pp. 49 ss.

[11] Nel *Warsaw Summit Commniquè* del 9 luglio 2016, l'organizzazione dell'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

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 land, at sea, in the air, and in space (henceforth, "the physical spheres")[12].

Tale ricostruzione ci permette di individuare la caratteristica fondamentale del cyberspazio data dalla convivenza di elementi materiali[13] con elementi immateriali, e soprattutto dalla presenza di una dimensione sociale di livello globale: peculiarità queste che hanno dato vita ai problematici dibattiti della dottrina, soprattutto quella di diritto internazionale sia pubblico, sia privato[14], relativamente all'esercizio della sovranità degli Stati in questo spazio, che saranno sommariamente delineati nel prosieguo.

2. Le teorie sulla regolazione del cyberspazio

Il cyberspazio - così come il servizio Internet in esso ricompreso - è un elemento che ha la capacità di incidere sugli elementi dello Stato (popolo, sovranità, territorio). Si comprende pertanto come

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» (D.T. KUEHL, *From Cyberspace to Cyber-power: Defining the Problem*, in F.D. KRAMER, S.H. STARR, L.K. WENTZ, *Cyberpower and National Security*, Potomac Books Inc, 2009, pp. 26-28). Lo stesso anno, Martin C. Libicki definisce il cyberspazio individuando tre livelli: fisico, sintattico e semantico M.C. LIBICKI, *Cyberdeterrence e cyberwar*, Santa Monica, RAND Corporation, 2009.

[12] Cfr. S. EVEN, D. SIMAN-TOV, *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv, Memorandum, 2012, n. 117, 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), nel *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, M.N. SCHMITT (General editor), Cambridge, 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 consists of the connection that exists 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».

[13] Cfr. 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». Si rinvia al link:<https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>.

[14] Cfr. J.G. CASTEL, *The Internet in Light of Traditional Public and Private International Law Principles and Rules Applied in Canada*, in *Canadian Yearbook of International Law*, n. 39, 2001, pp. 3-68, reperibile al link:<https://digitalcommons.osgoode.yorku.ca/scholarly_works/1360/>. Per quanto riguarda la prospettiva di diritto internazionale privato si rinvia ai diversi studi di Dan Jerker B. Svantesson, tra cui D.J.B. SVANTESSON, *Private international law and the Internet*, Alphen aan der Rijn, Wolters Kluwer, 2021; ID, *Solving the internet jurisdiction puzzle*, New York, Oxford University Press, 2017; ID, *A legal method for solving issues of Internet regulation; Applied to the regulation of cross-border privacy issues*, in *EUI Working Papers*, n. 18, 2010, reperibile al link:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1785421>.

questo elemento sia di inevitabile interesse per gli ordinamenti che lo percepiscono come un fenomeno che incide nelle loro realtà e che quindi necessita di essere normato.

Dalla prospettiva giuridica, la regolazione del cyberspazio si caratterizza come un'esigenza avvertita solo di recente se si considera che «[t]he concept of regulation the Net […] did not exist prior to the 1990s because "the Net" did not yet exist as a society-wide communications medium»[15]. Difatti è a partire da questo periodo, a seguito della progressiva diffusione dell'informatica nel mercato, e quindi presso il pubblico, che la dottrina ha iniziato ad interrogarsi sulla disciplina giuridica del cyberspazio.

Il dibattito ha attraversato diversi periodi, animati da critiche concernenti non solo i profili della fattibilità, ma anche dell'opportunità e della legittimità di una disciplina giuridica di questo "nuovo spazio". Questioni che costituiscono ancora oggi un vero e proprio "dilemma"[16] per il diritto, soprattutto dalla prospettiva giuspubblicistica non solo interna, ma anche europea e internazionale.

Riprendendo i termini del dibattito della dottrina giuridica dei primi anni '90 del secolo scorso, è possibile individuare tre tesi di fondo che rispecchiano il movimento di idee e filosofie che ha caratterizzato la discussione sulla regolazione di Internet:

- l'idea cyberlibertaria, posta a rifiuto dell'introduzione di regole nel cyberspazio, non solo in quanto spazio privo di confini territoriali, quindi diverso dagli spazi reali, ma anche perché interpretato come ordinamento regolato dalle sole norme da esso prodotte tramite gli utenti della Rete (o c.d. *self-regulation*);
- posizione contrapposta alla prima, riteneva invece applicabile il diritto vigente, sia esso statale o convenzionale, al cyberspazio in quanto interpretato come dimensione non dissimile da quella degli spazi reali, soprattutto in considerazione della parte fisica che lo compone, inevitabilmente collocata nel territorio di uno Stato;
- la posizione tecno-giuridica, che ha spostato la riflessione sulle "fonti" che regolano il cyberspazio e il relativo rapporto con il potere politico.

2.1 Cyber-anarchia e *self-regulation* degli utenti contro il potere pubblico (Barlow, Johnson e Post)

Tra gli esponenti, nonché anche iniziatori, del movimento cyber-anarchico (secondo alcuni cyber-libertario) troviamo certamento John Perry Barlow, uno dei fondatori dell'*Electronic Frontier Foundation* (EFF), la cui Dichiarazione di indipendenza del cyberspazio firmata Davos 1996, rappresenta il baluardo del *cyberlibertarianism* che si opponeva, «In nome del futuro»[17] all'intervento dei «Governi del Mondo industriale, […] stanchi giganti di carne ed acciaio»[18] criticando l'assenza di sovranità dei pubblici poteri in questa nuova dimensione, il cui tratto caratterizzante è dato dalla capacità di far incontrare, seppur virtualmente, persone di tutto il mondo purché dotate di strumenti di connessione.

---

[15] Y. BENKLER, *Symposium Overview: Part Iv: How (IF At All) To Regulate The Internet: Net Regulation: Taking Stock And Looking Forward*, in *University of Colorado Law Review*, vol. 71. 2000, p. 1205.

[16] O. POLLICINO, M. BASSINI, G. DE GREGORIO, *Internet law and protection of fundamental rights*, Milano, Bocconi University Press, 2022, pp. 4 ss.

[17] J.P. BARLOW, *A Declaration of the Independence of Cyberspace*, 8 febbraio 1996. Il testo della dichiarazione è disponibile sul sito dell'EFF al link: <https://www.eff. org/it/cyberspace -independ ence>.

[18] *Ibidem.*

Si affermava quindi una disciplina normativa del cyberspazio che negava quella dei poteri pubblici del mondo fisico in quanto spazio sociale globale che «cresce spontaneamente attraverso le azioni collettive» e regolato da una cultura, etica e codici non scritti che secondo lo scrittore avrebbero fornito a questa cyebr-società «un ordine maggiore di quanto potrebbe essere ottenuto con le […] imposizioni» dei governi: pertanto il cyberspazio era descritto come una dimensione capace di autoregolarsi.

La proclamazione di Barlow può essere compresa se contestualizzata alla luce dei cambiamenti apportati dal passaggio dall'Internet degli albori - che ha rappresentato un fenomeno privo di interesse per i governi - a quello della diffusione dell'informatica presso il pubblico; fenomeno che ha destato l'interesse dei pubblici poteri.

L'autoregolazione ha infatti caratterizzato tutta la prima fase di Internet. Il motivo può essere ricondotto al fatto che in questo periodo la rete era utilizzata da un ristretto numero di soggetti, spesso coinvolti nella sua stessa costruzione[19] ove «[l]'autorità sembrava spettare a chi, da un lato possedesse superiori competenze tecniche e scientifiche, e dall'altro fosse disponibile a impiegare queste competenze in sviluppi innovativi, cui la comunità degli utenti era invitata a partecipare»[20]. Vi era infatti l'autorità «tecnica e morale» dei padri fondatori della rete (tra cui, Vinton Cerf, Robert Kahn e Jon Postel), tuttavia il coordinamento delle iniziative individuali era dettato da strumenti che, seppur non giuridicamente vincolanti, avevano una forza *de facto* vincolante: ossia gli standard di comunicazione (c.d. protocolli) e le norme sociali della rete (c.d. *Netiquette*).

Ciò che interessa in questa sede è la modalità di formazione di tali norme di *soft law* dell'Internet originario. Per quanto riguarda gli standard, la loro adozione avveniva, e avviene tutt'ora, da parte di comitati esperti imparziali (come l'IETF - *Internet Engineering Task*) che, a seguito di dibattiti nella comunità di Internet, valutano lo standard sulla base della sua validità tecnica, avendo poi riguardo di condividerlo e facendo in modo che ogni sviluppatore di *software* lo adotti, nell'aspettativa che anche gli altri sviluppatori facciano lo stesso[21].

---

[19] G: SARTOR, *Internet e il diritto,* in *Temi di diritto dell'informatica*, Giappichelli, Torino, 2011, pp. 8-10. In particolare l' A. richiama lo studio di Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford, 2002, secondo cui lo sviluppo della rete è stato determinato dall'incontro di quattro ispirazioni ideali: «la cultura tecnico-meritocratica, caratterizzata dai valori della scoperta tecnologica. della competenza e della condivisione della conoscenza; la cultura hacker, che unisce ai valori tecnico-meritocratici gli aspetti della creatività e della cooperazione; la cultura virtual-comunitaria, caratterizzata dei valori della libertà di comunicazione, associazione e auto-organizzazione; la cultura imprenditoriale, basata sui valori del danaro, del lavoro e del consumo».

[20] *Ibidem.*

[21] L'organizzazione tecnica della Rete e la determinazione dei relativi standard è affidata a tre organismi: L'*Internet Engineering Task Force* (IETF), il *World Wide Web Consortium* (W3C) e l'*Internet Corporation for Assigned Names and Numbers* (ICANN).

L'IETF risale al 1986 ed ha come obiettivo quello di assicurare la promozione degli standard e dei protocolli che assicurano l'interoperabilità delle reti. Si tratta di un'organizzazione indipendente, sostenuta dall'ISoC (I*nternet Society*), composta da fornitori di servizi e di utilizzatori, di produttori di *computers*, di ricercatori e altri soggetti interessati.

Il W3C è stato creato da Tim Berners Lee, l'inventore del primo *server*, del primo *browser* e del *World Wide Web*. Fondato nel 1994 presso il Mit (*Massachusetts Institute of Technology*) di Cambridge, in collaborazione con il CERN di Ginevra, attualmente vede la cooperazione di altri istituti come l'*Institute national de Recherche en Informatique et en Automatique* in Francia e della *Keio University* in Giappone. È anch'esso un organo di regolamentazione tecnica della Rete che ha prodotto diverse specifiche tecniche relative all'infrastruttura del Web, specialmente nel settore dell'architettura della Rete (e delle tecnologie sottostanti), della formattazione dei documenti, degli strumenti che facilitano tutte le forme di interazione.

L'ICANN è un'organizzazione senza scopo di lucro nata negli Stati Uniti nel 1998. Gestisce a livello internazionale e centralizzato l'assegnazione dei nomi di dominio. Si articola in tre divisioni che gestiscono l'allocazione dello spazio degli indirizzi IP, l'assegnazione dei parametri inclusi nei protocolli, la gestione del sistema dei nomi di dominio e dei relativi server (*root server*).

Relativamente alle norme sociali, queste possono essere qualificate come le "consuetudini" di Internet. Ossia modelli di comportamento non scritti, accettati degli utilizzatori e ripetuti nel tempo, la cui violazione comporta sanzioni informali, quali il giudizio negativo, la stigmatizzazione o anche l'allontanamento del violatore.

Il movimento *cyberlibertarianism* trovò sostenitori anche nel mondo del diritto tra i giuristi che negavano la sovranità statale e la giurisdizione territoriale nel cyberspazio. Tra questi, meritano attenzione la tesi avanzate da David Johnson e David Post, i quali, in un articolo del 1996 dal titolo "*Law and Borders - The Rise of Law in Cyberspace*", definirono il cyberspazio come un insieme di comunicazioni globali basate su computer che attraversano i confini territoriali che creano un nuovo ambito di attività umana e minano la fattibilità e la legittimità delle leggi basate su confini geografici[22].

Sottoporre la Rete al diritto degli Stati avrebbe infatti causato conflitti tra le differenti regolazioni nazionali coinvolte nella normazione di una determinata attività nel cyberspazio portando ad effetti di c.d. *spill over*: ossia ad una incertezza nella individuazione della legge applicabile e del foro competente secondo i consueti criteri del diritto internazionale privato.

Secondo tale dottrina il cyberspazio rappresentava un luogo distinto dal mondo fisico (il «"real world" of atoms»), tale per cui la sua unica forma di governo non poteva che essere affidata a un nuovo sistema di regole dettato dagli utilizzatori - per l'appunto *self-regulation* - che avrebbe definito la personalità giuridica e il diritto di proprietà, nonché sarebbe stato utile per la risoluzione di controversie, e avrebbe definito i valori fondamentali relativi alla conversazione *on line* dei partecipanti[23].

2.2 Il movimento anti-anarchico e l'applicazione del diritto internazionale (Wu e Goldsmith)

Al *cyberlibertarianism* degli scettici alla regolazione pubblica del cyberspazio si oppose il movimento contrario di coloro che ritenevano la regolazione del cyberspazio da parte degli Stati fattibile e legittima[24].

Tra questi, pare utile porre attenzione alla tesi di Jack Goldsmith, il quale, nel 1999, in un articolo dall'eloquente titolo "*Against Cyberanarchy*", ha confutato quanto sostenuto dai "*regulation skeptics*" criticando le argomentazioni di Johnson e Post[25].

---

[22] D. JOHNSON, D. POST, *Law and Borders - the Rise of Law in Cyberspace*, in *Stanford Law Review*, vol. 48, 1996, p. 1367.

[23] *Ibidem.*

[24] Sul punto si faccia riferimento agli scritti di T. WU, *Cyberspace sovereignty? - The Internet and the International system*, in *Harvard Journal of Law & Technology*, vol. 10, n. 3, 1997 e J. L. GOLDSMITH, *Against Cyberanarchy*, in *University of Chicago Law Occasional Paper*, vol. 65, n. 40, 1999, reperibile al link:<https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1001 &context=occasional_papers>.

[25] J.L. GOLDSMITH, *Against Cyberanarchy ...op.cit.*, p. 1, ove scrive che «[t]he regulation skeptics make both descriptive and normative claims. On the descriptive side, they claim that the application of geographically based conceptions of legal regulation and choice of law to a-geographical cyberspace activity either makes no sense or leads to hopeless confusion. On the normative side, they argue that because cyberspace transactions occur "simultaneously and equally" in all national jurisdictions, regulation of the flow of this information by any particular national jurisdiction illegitimately produces significant negative spillover effects in other jurisdictions. They also claim that the architecture of cyberspace precludes notice of governing law that is crucial to the law's legitimacy. In contrast, they argue, cyberspace participants are much better positioned than national regulators to design comprehensive legal rules that would both internalize the costs of cyberspace activity and give proper notice to cyberspace participants. The regulation skeptics conclude from these arguments that national regulators should "defer to the self-regulatory efforts of Cyberspace participants"».

Secondo Goldsmith, i cyber-libertari commettono tre errori[26]. Innanzitutto, questi esagerano le differenze tra le transazioni che avvengono nel cyberspazio e quelle che avvengono nel mondo fisico tra gli Stati. A ben vedere «[e]ntrambe coinvolgono persone nello spazio reale in una giurisdizione territoriale che effettua transazioni con persone nello spazio reale in un'altra giurisdizione territoriale in modo tale da causare talvolta danni nel mondo reale. In entrambi i contesti, lo Stato in cui si verificano i danni ha un interesse legittimo a regolare l'attività che produce tali danni»[27].

In secondo luogo, gli scettici non tengono conto della distinzione tra le regole frutto dell'autonomia privata (nel testo "*default laws*", che potremmo ricondurre al diritto privato e al "diritto dei privati" di cui in Pt. III, Cap. I, 2), e le leggi dello Stato, ossia "*mandatory laws*". Goldsmith sostieneva infatti che l'autoregolazione ha senso in relazione alle prime che, per definizione, le parti private possono modificare per soddisfare le proprie esigenze. Ma ha molto meno senso invece in relazione alle prescrizioni obbligatorie dello Stato che, per motivi paternalistici o al fine di proteggere terzi, pongono limiti all'ordinamento legale privato.

Infine, gli scettici sottovalutano il potenziale dei tradizionali strumenti legali utili alla risoluzione di problemi regolatori multigiurisdizionali che possono rilevare nel cyberspazio. Le transazioni in questo ambiente non giustificano una maggiore deferenza da parte dei regolatori nazionali e non sono significativamente meno resistenti agli strumenti del conflitto di leggi rispetto ad altre transazioni transnazionali.

Goldsmith concluse la sua critica evidenziando che «[n]on esiste un argomento normativo generale che giustifichi l'immunizzazione delle attività nel cyberspazio dalla regolamentazione territoriale. E c'è ogni ragione per credere che le nazioni possano esercitare l'autorità territoriale per ottenere un significativo controllo regolatorio sulle transazioni nel cyberspazio»[28].

Secondo questa tesi pertanto la regolazione del cyberspazio sarebbe possibile in virtù di un'azione di armonizzazione dei vari ordinamenti statali per mezzo del diritto internazionale[29]. Gli effetti di *spill over* sarebbero infatti ridimensionati da una compiuta regolamentazione giuridica di Internet la quale andrebbe ad affidare al diritto internazionale privato le questioni attinenti alla gestione della rete come infrastruttura, e al diritto internazionale pubblico, l'individuazione «mediante coordinamento dei vari ordinamenti nazionali, della giurisdizione nazionale competente a dirimere le controversie che hanno luogo *on-line* e il relativo diritto applicabile»[30].

2.3 Dalla norma giuridica alla legge naturale del cyberspazio: la *lex informatica* e il «*code*» (Reidenberg e Lessig)

---

[26] Sul punto v. anche O. POLLICINO, M. BASSINI, G. DE GREGORIO, *op. cit.*, pp. 7 ss

[27] J.L. GOLDSMITH, *op. cit.,* p. 2.

[28] J.L. GOLDSMITH, *op. cit.,* p. 37. In Italia, tra i sostenitori della tesi dell'applicazione ad Internet del diritto vigente può essere ricompreso l'illustre dottrina di Natalino Irti, il quale in N. IRTI, *Norma e luoghi: problemi di geo-diritto*, Roma, Laterza, 2005, pp. 60 ss., ove scrive «[l]a *Globalisierung* sembra raggiungere il grado più alto nella rete telematica. Dove certo sono individuabili i luoghi dei singoli computes, disseminati sulla superficie terrestre; e così i luoghi e i nomi degli innumerevoli "utenti". Ma dove il contenuto, uditivo e visivo, non ha posizione nello spazio. Esso costituisce e determina il proprio "spazio": lo spazio telematico, che è un non-luogo, poiché i "luoghi" appartengono a terra mare aria [...]. La perdita dei luoghi non consente l'immediata individuazione del diritto applicabile. *Il dove giuridico attende nuovi criteri.* Lo spazio telematico sciolto da agganci terrestri, si apre a tutte le soluzioni dell'artificialità».

[29] Interpretazione di G.M. RUOTOLO, *Internet (dir. internaz.)*, in *Enciclopedia del diritto – Annali*, Milano, 2014, p. 548.

[30] *Ibidem.*

Tra i due contrapposti orientamenti si sono inserite le tesi di Joel Reidenberg e Lawrence Lessig[31] che, fuori dalla prospettiva di applicazione del diritto internazionale, si posero in critica delle teorie libertarie, intuendo come il cyberspazio non rappresenti una dimensione di assoluta e incondizionata libertà, ma anzi al suo interno è possibile individuare diverse "*default rules*", questa volta intese come regole derivanti dalla sua intrinseca natura, quali le capacità tecnologiche e i sistemi di configurazione del cyberspazio che impongono regole agli utenti.

A nostro modo di vedere, il tratto innovativo delle teorie dei due giuristi è stato quello di aver investigato da una prospettiva tecno-giuridica la *self-regulation* degli utenti del cyberspazio proclamata dal movimento cyberlibertario, individuandone una fonte che limita di fatto le libertà degli utilizzatori.

Nello specifico, secondo Reidenmberg:

> *[t]echnological architectures may prohibit certain actions on the network, such as access without security clearances, or may impose certain flows, such as mandatory address routing data for electronic messages*[32].

Allo stesso modo Lessig scrive che:

> [l]ife in cyberspace is regulated primarily through the code of cyberpsace […]. Regulated in the sense that bars on a prison regulate the movement of a prisoner, or regulated in the sense that stairs regulate the access of the disabled[33].

Secondo gli Autori nel cyberspazio sussistono regole che, diversamente da quelle che orientano il comportamento dei soggetti nel mondo fisico, non trovano la loro origine nelle fonti del diritto statuale ma nel «tecnologo sviluppatore e [nel] processo sociale attraverso il quale si evolvono le consuetudini»[34], e costituiscono l'unica fonte capace di trovare applicazione nel cyberspazio.

Mutuando dalla "*lex mercatoria*"[35], Reidenberg riteneva che tali regole costituissero l'espressione di un nuovo diritto comune - rinominato per l'appunto "*lex informatica*" - fondato sulle regole (informatiche) elaborate sia dagli utenti, sia dagli sviluppatori.

Medesima tesi è anche quella di Lessig il quale tuttavia ha specificato che il mezzo di costrizione dei comportamenti umani nel cyberspazio è il «*code*», ossia l'insieme di *hardware* e *software* che

---

[31] J.R. REIDENBERG, *Lex informatica: The formulation of information policy rules thruogh technology*, in *Texas Law Review*, 76, 3, 1998, pp. 553-593; L. LESSIG, *Code: and other laws of cyberspace*, Basic books, 1999; ID, *Code. Versione 2.0*, Basic books, New York, 2006. Sul versante delle scienze dei media v. W.J. MITCHELL, *City of bits. Space, place and Infobahn*, MIT Press, 1996.

[32] J.R. REIDENBERG, *op. cit.*, p. 568.

[33] *Ivi*, p. 83.

[34] *Ivi*, p. 571.

[35] Sulla critica al richiamo della *lex mercatoria* per proporre un diritto comune del cyberspazio v. G. FINOCCHIARO, *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, vol. 17, 2001, pp. 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. K.P. BERGER, *The Creeping Codification of the Lex Mercatoria*, Kluwe law, London, 1999; F. GALGANO, *Lex mercatoria*, Il Mulino, Bologna, 2016; B. GOLDMAN, *Lex mercatoria,* Kluwer Law International, 1983; G. TEUBNER, *Global Bukowina: Legal Pluralism in the World-Society*, in G. TEUBNER (a cura di), *Global law without state*, Aldershot ,Dartsmouth, 1996, pp. 3-28; H.J. MERTENS, *Lex Mercatoria: A Self-applying System Beyond National Law?*, in G. TEUBNER (a cura di), *Global law without state*, Aldershot ,Dartsmouth, 1996, pp. 31 ss.

consentono l'esistenza del cyberspazio[36], e ponendo l'attenzione sul «how different "code" regulates»[37].

Diversamente dalle tesi libertarie e anti-anarchiche dell'Internet che negano o tentano di applicare i principi del diritto "classico" al cyberspazio, l'intuizione dei due Autori è stata quella di individuare - attraverso l'attenta osservazione dei processi logici che regolano la rete - un valido "appiglio" tecno-giuridico attraverso il quale i poteri pubblici avrebbero potuto orientare indirettamente le attività nel cyberspazio (o meglio la "società informazionale"), ponendo nuovamente il potere politico pubblico al centro delle soluzioni.

Difatti, secondo tali ricostruzioni, se i tecnologi informatici progettano le caratteristiche di base dell'infrastruttura che crea ed attua le impostazioni predefinite della rete, che limitano di fatto le azioni degli utilizzatori nel cyberspazio, gli Stati possono regolare indirettamente i comportamenti umani nel cyberspazio influenzando le decisioni prese dai tecnologi attraverso leggi che impongano restrizioni sulle scelte che questi prendono[38].

Nello specifico il diritto ha una doppia valenza in questo ambito. Da una parte troviamo l'introduzione di norme giuridiche, che trovano applicazione sugli utenti e possono vietare determinati comportamenti, ad esempio attraverso la criminalizzazione di determinate condotte perpetrate attraverso la rete (*cybercrime*), o contro l'infrastruttura fisiche della rete (*computer crimes*), quindi qualificate come fattispecie di reato[39]; dall'altra invece il *code*, il quale può essere regolato dai governi incidendo sugli sviluppatori al fine di plasmare la rete secondo il volere dal decisore politico.

I due Autori pervengono alle medesime conclusioni secondo cui l'instradamento della *lex Informatica,* o del *code*, richiede un «cambiamento nel *focus* dell'azione governativa», che si sposti dalla regolamentazione diretta a quella indiretta, tale che queste fonti intermedie dovrebbero essere annoverate tra gli strumenti posti a disposizione dei governi «as an effective substitute for law where self-executing, customized rules are desirable»[40].

L'assunto ci è particolarmente utile poiché, come argomenteremo più avanti (Pt. II, Cap. II, 8), la sicurezza nel cyberspazio è una sicurezza mediata, ossia che ha ad oggetto la messa in sicurezza degli *hardware* e *software*, al fine di garantire indirettamente diversi obiettivi (sicurezza nazionale, sicurezza europea, nonché la sicurezza umana). Tuttavia, diversamente da alcune interpretazioni, che ritengono queste azioni di sicurezza affidate a dispositivi tecnologici, precisiamo che semmai tale "delega" di sicurezza non è verso l'oggetto (sia esso un dispositivo, algoritmo, ecc), ma verso i soggetti che li pensano, progettano, sviluppano su richiesta di qualcuno, siano essi soggetti pubblici o privati.

Pertanto riteniamo che le intuizioni di Reidenberg e Lessig siano valide tutt'oggi per evitare interpretazioni distopiche e strabiche nello studio del progresso tecnologico, che altrimenti porterebbero a ridurre il tutto al terrore di una nuova tecnosorveglianza verso cui i sorvegliati nulla

---

[36] L. LESSIG, *Code. Versione 2.0*, Basic books, New York, 2006, p. 5.

[37] *Ibidem.*

[38] L. LESSIG, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, in *Common Law Conspectus*, n. 5, 1997, reperibile al link:<https://scholarship.law.edu/commlaw/vol5/iss2/5/>.

[39] Una certa dottrina italiana ha distinto i due concetti secondo cui i *computer crimes* sono i reati compiuti per mezzo dei sistemi informatici e telematici, mentre i *cybercrimes* sono i reati contro i medesimi sistemi. Le due figure possono pertanto coincidere o meno. Cfr. S. SBORDONI, *Web, libertà e Diritto. Aspetti di diritto positivo nella comunità virtuale*, Roma, Istituto poligrafico e Zecca dello Stato, 2014, p. 3. Così anche V. CONTRAFFATTO, *I reati informatici*, Frosinone, Key editore, 2017, p. 11.

[40] J.R. REIDENBERG, *op. cit.*, p. 585-586.

possono, e quindi alla paralisi della funzione del diritto a tutela dei diritti e delle libertà sociale ed anche economiche (v. Pt. III, Cap. I, 1).

3. La regolazione globale del cyberspazio tra *multistakeholder governance* e *multilateralism approach*

La breve analisi degli orientamenti dottrinali sulla regolazione del cyberspazio dei primi anni '90 del secolo scorso ci ha permesso di contestualizzare le questioni culturali e giuridiche sottese al tema, ma tale ricostruzione deve tener conto di un elemento fondamentale. Sebbene l'ideale cyberlibertario della creazione di uno spazio fuori dalla giurisdizione dei poteri dei governi non abbia trovato riscontro nei successivi sviluppi di Internet, resta il fatto che la Rete è nata e funziona, in parte, sulla scorta di regole autoprodotte dalla sua stessa comunità degli albori che ha dettato i principi di apertura e libero accesso verso tutti.

Come anticipato, i primi decenni della creazione di Internet (1970-1999) sono stati caratterizzati dall'assenza di vincoli da parte degli Stati. In 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 - curiosamente - da una parte ha dato inizio all'uso commerciale di Internet[41], 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, stante l'affermazione dei grandi gruppi privati attivi nel mercato delle ICTs[42].

Nell'ultimo ventennio la crescente consapevolezza dei rischi della rete ha tuttavia portato i governi a volgere l'attenzione verso il cyberspazio dimostrando «non solo di [poterlo] regolamentare ma anche "iper-regolare"»[43].

La questione che ci si pone quindi oggi è in che maniera gli Stati, il cui intervento è successivo nel tempo, intendano regolare il cyberspazio, ora inteso come spazio regolato primariamente da forme di *self regulation*, prima degli stessi utenti, poi dei grandi gruppi privati.

A nostro modo di vedere il tema involge due questioni: la prima può essere ricondotta all'interno della più ampia discussione sulla sovranità statale alla prova della globalizzazione, quale processo che ha profondamente trasformato la società e le sue istituzioni[44]; la seconda, riguarda la modalità di esercizio di detto potere nel cyberspazio in maniera tale da non modificare o negare i principi di apertura e libertà che lo caratterizzano sin dalle origini (*infra* Cap. II, 2).

---

[41] J. L. GOLDSMITH, T. WU, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford, Oxford University Press, 2006.

[42] *Ibidem.*

[43] O. POLLICINO, *Potere digitale*, Estratto da I Tematici, V-2023, Potere e Costituzione, in *Enc. dir.,* 2023, p. 415.

[44] Sul rapporto tra sovranità statale e processo di globalizzazione si rinvia a AA.VV., *Costituzionalismo e globalizzazione*, *Atti del XXVII Convegno annuale, Salerno, 22-24 novembre 2012*, Jovene, Napoli 2014; G. DE VERGOTTINI, *La persistente sovranità*, in *Recte sapere. Studi in onore di Giuseppe Dalla Torre*, Torino, 2014, p.1373 ss., pubblicato altresì in *Consulta online*, reperibile al link:<https://giurcost.org/contents/ giurcost/studi/ devergottini2.pdf>; E. DENNINGER, *Sovranità dello Stato e tutela dei diritti fondamentali nel confronto dialettico tra autodeterminazione nazionale e intreccio globale*, in *Dirittifondamentali.it*, 29 giugno 2016, reperibile al link:<https://dirittifondamentali.it/wp-content/uploads/2019/04/1_2016-denninger_sovranit %C3%A0-dello-stato- e-tutela-dei-diritti-fondamentali.pdf>; E. CANNIZZARO, *La sovranità oltre lo Stato*, Il Mulino, Bologna, 2020.

Per ora ci soffermeremo sulla prima questione. Come emerso dal breve quadro sulle tesi relative alla regolazione, il cyberspazio costituisce di fatto un limite per l'esercizio dei poteri pubblici sovrani, da sempre legati all'elemento materiale della territorialità[45].

A tal proposito, una certa dottrina di diritto internazionale pubblico ritiene che la concezione spazial-tridimensionale dello Stato che, oltre al territorio, comprende anche i c.d. spazi soprastanti come lo spazio aereo, sottostanti come il sottosuolo e adiacenti come lo spazio marino, sia stata da tempo superata[46]. Tale orientamento distingue infatti due piani spaziali: quello del territorio, sul quale lo Stato esercita la sua normale funzione nell'ambito dell'organizzazione sovrana; e quello degli altri spazi (per l'appunto sovrastanti, sottostanti o adiacenti) che, in quanto posizioni differenti da quella territoriale propriamente detta, in essi «si ha solo un'irradiazione della vita e degli interessi della comunità stanziata sul territorio ed in funzione di questa, ma solo in funzione di questa, un'irradiazione della potestà di governo dello Stato territoriale»[47].

Tralasciando l'applicazione di simile teoria anche alla realtà del cyberspazio - ritenuta possibile secondo alcune recenti ricostruzioni data la duplicità del criterio territoriale e quello funzionale[48] - e quindi del potere di un singolo Stato su "una porzione" del cyberspazio, resta tuttavia il dilemma della regolazione del cyberspazio nel suo complesso, quale realtà globale aperta e accessibile a tutti.

Il dato certo 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[49].

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[50], sia perché, malgrado il tentativo di approdare verso un modello in cui tutte le parti interessate, compresi

---

[45] C. MORTATI, *Istituzioni di diritto pubblico*, Cedam, Padova, 1962, p. 104, ove l'A. scrive «il territorio è [...] elemento dello stato in quanto contribuisce a farlo essere quello che è, a dargli una sua individualità, insieme al popolo che lo abita ma senza confondersi con questo, venendo ad assumere una posizione analoga a quella del corpo per la persona umana». Cfr. M. D'ALBERTI, *Poteri pubblici, mercati e globalizzazione*, Bologna, 2008, p. 8. Analogamente alla questione che investe la regolazione dello spazio cibernetico, l'A., affrontando il tema del potere statale ai tempi della globalizzazione economica, nota che «la finanza globale o i mercati sovranazionali delle comunicazioni elettroniche sono sottratti a qualunque tipo di controllo o di disciplina autoritativa», poiché «venendo meno l'ancoraggio al territorio, il potere degli Stati è incapace di farsi valere».

[46] Cfr. U. LAENZA, *Fenomeni di contiguità aerea nel Diritto internazionale*, Napoli, 1961, Capo VI, pp. 173 ss.

[47] U. LAENZA, *Il diritto degli spazi internazionali. Parte prima. La tradizione*, Torino, 1999, p. 25.

[48] D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità nel cyberspace*, Editoriale scientifica, Napoli, 2020, pp. 17-18.

[49] Cfr. D.B. HOLLIS, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, in J.D. OHLIN, K. GOVERN, C. FINKELSTEIN (a cura di), *Cyberwar: Law & Ethics for Virtual Conflicts,* Oxford, Oxford University Press, 2014, p. 11, reperibile al link: https:<//ssrn.com/abstract=2424230>.

[50] G.M. RUOTOLO, *Internet* (diritto internazionale) in *Enciclopedia del diritto* – Annali, Milano, 2104, p. 549.

i Governi, partecipino in condizioni di parità[51], gli USA continuano a gestire unilateralmente detto sistema[52].

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[53]. Considerata l'incertezza dei rapporti tra i poteri sovrani e il cyberspazio[54], e nell'assenza di un «founding international constitutional moment»[55], gli Stati stanno tentando di plasmare Internet e il cyberspazio secondo propri orientamenti ideologici e interpretativi[56].

Dall'osservazione delle pratiche internazionali emerge la contrapposizione di due approcci: quello multilaterale, e quello di *governance multistakeholder*.

In linea generale la distinzione tra i due approcci è che mentre il primo, quale metodo in uso nelle organizzazioni internazionali tradizionali, prevede la sola partecipazione degli Stati (*state based model*), il secondo coinvolge anche altri soggetti di non secondaria rilevanza nella regolazione di Internet, ossia le rappresentanze della società civile, e gli attori privati.

Considerato che non vi è univoca interpretazione del concetto di *governance*[57], per quanto riguarda Internet pare utile richiamare la definizione emersa all'interno del *World Summit on the Information Society* (WSIS) del 2003 tenuto a Ginevra. Kofi Annan, allora Segretario generale delle Nazioni Unite, nel 2005 istituì il *Working Group on Internet Governance* (WGIG) in risposta alle questioni sul controllo di Internet rimaste irrisolte al precedente WSIS. Il gruppo di lavoro, che comprendeva 40 partecipanti provenienti dai governi, dal settore privato e dalla società civile, incaricato di sviluppare una definizione di *governance* di Internet, trovò raccordo nella seguente formulazione secondo cui:

---

[51] 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 epsresso 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 G.M. RUOTOLO, *Il sistema dei nomi di dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in *Il diritto dell'informazione e dell'informatica,* 2016, p. 38.

[52] *Ibidem.*

[53] J. GOLDSMITH, T. WU, *Who controls the Internet?: Illusion of a boardless world*, New York, Oxford University Press, 2006, p. 164.

[54] L. LESSIG, *Code. Versione 2.0* …, p. 302.

[55] *Ibidem.*

[56] K. EICHENSEHR, *The Cyber-Law of Nations*, in *The Georgetown law journal*, vol. 103, 2015, p. 329, reperibile al link:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447683>.

[57] Date le diverse accezzioni del termine, riteniamo utile far riferimento alla definizione formulata in Treccani, voce *governance* (dir. cost), reperibile al link:<https://www.treccani.it/enciclopedia/governance-dir-cost_%28Diritto -on-line%29/>, ove viene precisato che «[l]'utilizzo del termine si è affermato partendo da ambiti specialistici e sta ad indicare una modalità di decisione a carattere sempre più generalista; si tratta di nozione indispensabile quale elemento di analisi e comprensione delle dinamiche decisorie a partire da quelle sovranazionali. Viene evocato un sistema decisionale che mette insieme attori pubblici e privati, istituzioni politiche e finanziarie, stravolgendo i tradizionali meccanismi ordinati dalle costituzioni nazionali».

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet[58].

Modello ritenuto il più confacente anche da uno dei creatori della rete, Vinton Cerf, che in occasione di un recente incontro organizzato dall'Istituto italiano di Informatica Giuridica del CNR sulla «Internet governance e le sfide della trasformazione digitale» ha ribadito che:

> [l]'approccio "multistakeholder" per lo sviluppo delle policy di Internet – che coinvolge i governi, la società civile, le comunità scientifiche, le organizzazioni degli standard e il settore privato – rimane la migliore soluzione auspicabile che permette di tenere conto dei vari punti di vista – nella definizione delle policy, dei regolamenti e dei metodi di applicazione delle norme – e di verificare le potenziali ricadute nei vari settori[59].

Le divergenze tra i due modelli possono essere colte dall'esperienza del *World Conference on International Telecommunications* (WCIT) tenutosi a Dubai nel Dicembre 2012. L'obiettivo dell'incontro era quella di applicare ad Internet le condizioni dei servizi di telecomunicazione previsti nelle *International Telecommunication Regulations* (ITRs) elaborate dall'*Unione Internazionale delle Telecomunicazioni* (ITU)[60] nel 1988 sul principio del «chi trasmette paga»[61]. 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

---

[58] Working Group on Internet Governance, *Report of the Working Group on Internet Governance*, 2005, p. 4, reperibile al link:<http://www.wgig.org/WGIG-Report.html>.

[59] V.G. CERF, *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, Napoli, 2022, p. 21, reperibile al link del sito della Rivista Italiana di Informatica Giuridica:<https:// www.rivistaitalianadiinformaticaediritto.it/ index.php/ RIID/issue/view/8>. Il video della manifestazione che si è tenuta presso la sede del CNR di Roma può essere visualizzato al link:<https://www.youtube.com/watch?v=ykJNJ1S8I5Y>.

[60] Cfr. J. WOUTERS, *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, *The Evolution of Transnational Rule-Makers through Crises*, Cambridge, Cambridge University Press, 2023, p. 67-68, disponibile in open access al link:<https://www.cambridge .org/core/books/evolution-of-transnational-rulemakers-through-crises/ 64FD7201F60B95B784D E1FCF684C778A>. L'ITU è una delle più antiche agenzie di regolamentazione globale. Fondata originariamente come *Unione Telegrafica Internazionale* nel 1865 per promuovere la cooperazione tra le organizzazioni internazionali, l'ITU ha contribuito per oltre 150 anni alla connettività, all'interoperabilità e alla standardizzazione delle telecomunicazioni, dall'uso del codice Morse fino alle comunicazioni satellitari. Come agenzia specializzata delle Nazioni Unite dal 1947, si è evoluta in una piattaforma unica per la collaborazione tra pubblico e privato a livello globale e ha abbracciato saldamente il settore delle imprese e altre parti interessate. Dal sito web si apprende che «i suoi membri globali includono 193 Stati membri oltre a circa 900 aziende, università e organizzazioni internazionali e regionali». Più precisamente, ci sono due tipi di membri: 193 Stati membri Stati membri e i 900 "membri del settore". Dal 1994, i membri del settore possono partecipare formalmente ai processi decisionali dell'ITU e dal 1998 sono stati riconosciuti come aventi diritti formali di partecipazione ai sensi della Costituzione dell'Agenzia. L'ITU ha tre settori: Radiocomunicazione (ITU-R), Standardizzazione delle telecomunicazioni (ITU-T) e Sviluppo delle telecomunicazioni (ITU-D). Le aziende o le organizzazioni possono diventare membri di uno o più settori e possono aderire come Membro del Settore o come Associato. Ebbene, gran parte della dinamica normativa dell'ITU ha inizio nei "Gruppi di studio", che vengono rinnovati ogni quattro anni. Ognuno di questi gruppi di studio, a cui partecipano "migliaia di esperti in rappresentanza del governo, dell'industria e del mondo accademico", è responsabile dell'avanzamento dei lavori dell'Agenzia in un campo specifico del mandato dell'organizzazione: essi sviluppano le basi tecniche per gli accordi, gli standard e i rapporti dell'ITU. I mandati e i gruppi dirigenti dei Gruppi di studio di ciascun settore sono decisi dai rispettivi organi direttivi del settore, ossia l'Assemblea delle radiocomunicazioni (RA), l'Assemblea mondiale di standardizzazione delle telecomunicazioni (WTSA) e la Conferenza mondiale per lo sviluppo delle telecomunicazioni (WTDC). È stato osservato dai membri delle delegazioni all'ITU che gli standard dell'ITU - che in genere richiedono circa due anni per essere sviluppati - «are increasingly written by companies, rather than governments».

[61] Sul punto si rinvia a G.M. RUOTOLO, *Internet* (diritto internazionale) … *op. cit.*, p. 554.

un'organizzazione internazionale di stampo classico al fine di aumentare la rilevanza dei governi nella gestione della Rete[62].

Nel 2011 la rappresentanza russa ha dichiarato che l'obiettivo della Russia è quello di «establish 'international control over the Internet' through the [ITU]»[63] compreso il sistema dei nomi di dominio[64]. La proposta ha suscitato l'opposizione di attori privati come Google, della società civile, nonché degli Stati Uniti e dell'Unione europea sostenitori del modello di governance *multistakeholder.*

Come evidenziato dal Funzionario del Dipartimento di Stato degli Stati Uniti, il controllo centralizzato di Internet attraverso una forma di governo *top-down* «would put political dealmakers rather than innovators and experts in charge of the future of the Internet», causando di conseguenza effetti sia sul piano economico, quali il rallentamento dell'innovazione, l'ostacolo allo sviluppo economico globale, nonché, soprattutto, sul piano sociale, dato il rischio di dar vita ad un sistema di controllo sulle attività delle persone in Rete senza precedenti[65].

Il WCIT-12 si concluse con il non raggiungimento dei consensi nè sull'opportunità di applicare gli ITRs ad Internet, nè sulle proposte di governo multilaterale della Rete. Tuttavia quest'ultimo invito è stato riproposto in tempi recenti da parte della Cina sotto altre forme.

Nel settembre 2019, Huawei, China Mobile Communications Corporation, China Unicom, e il Ministero cinese dell'industria e delle tecnologie dell'informazione hanno proposto in seno al *Telecommunication Standardization Advisory Group* (TSAG) dell'ITU di studiare la creazione di una nuova architettura di Rete che possa far fronte ai futuri sviluppi delle tecnologie informatiche[66]. 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[67], facendo richiesta ai Gruppi di Studio del *Telecommunication Standardization Sector (ITU-T) Study Group* di avviare ricerche a lungo termine nel periodo allora in corso (2017–2020) e nel successivo (2021–2025).

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 come l'*Internet Engineering Task Force* (IETF)[68]. Dello

---

[62] *Ibidem.*

[63] Centre for Democracy & Technology, *ITU move to expand powers threatens the Internet: civil society should have voice in ITU Internet debate*, 12 marzo 2012, p. 3, reperibile al link:<https://cdt.org/wp-content/uploads/pdfs/ CDT-ITU_WCIT12_background.pdf> .

[64] Nello specifico la Russia propose che «[m]ember States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of basic Internet infrastructure» (art. 3A.2). Si rinvia a Russian Federation, *Proposals for the Work of the Conference*, reperibile al link:<https://www.itu.int/md/ S12-WCIT12-C-0044/en>.

[65] v. *International Proposals to Regulate the Internet: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce*, 112th Cong. 24 (2012) (statement of Ambassador Philip Verveer, Deputy Assistant Secretary of State and United States Coordinator for International Communications and Information Policy), p. 42, disponibile al link:<http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg79558/pdf/CHRG-112hhrg79558.pdf>.

[66] Z. CHEN, C. WANG, G. LI, Z. LOU, S. JIANG, *New IP Framework and Protocol for Future Applications*, University college, Londono, 2020, reperibile al link:<https://discovery.ucl.ac.uk/id/eprint/10109959/1/201791_1_ CameraReady .pdf>.

[67] Sulle caratteristiche del nuovo protocollo proposto si rinvia a S. JIANG, *New IP Networking for Network 2030*, Fifth ITU Workshop on Network 2030, International Telecommunication Union, ottobre, 2019, reperibile al link:<https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf>.

[68] Sugli aspetti di dettaglio si rinvia a J. WOUTERS, *Corporations and the Making of Public Standards …op.cit.,* p. 71; nonché a R. RADU, G. DE GREGORIO, *The New Era of Internet Governance Technical Fragmentation and Digital Sovereignty Entanglements*, in F. CRISTIANO, B.BERG, *Hybridity, conflict, and Global Politics of Cybersecurity*, Rowman

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[69].

Sebbene la proposta cinese sia stata 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, 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 alla inadeguata sede della presentazione della proposta. Brevemente si precisa che mentre nell'IETF il processo decisionale è trasparente, *bottom-up* 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 Stati membri sono gli unici partecipanti ad avere l'ultima parola sull'approvazione della proposta, o esprimere un voto, quando non c'è consenso[70].

Altra questione attiene all'oggetto della proposta - per l'appunto il protocollo IP - il quale dimostra il valore politico degli standard e degli organismi di standardizzazione che li elaborano. I processi decisionali di tali enti, percepiti come neutrali, incorporano implicitamente dei valori che ne attribuiscono inevitabilmente valore politico[71].

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[72].

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[73].

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 cybersicurezza per il decennio digitale presentata nel dicembre 2020 è un esempio di tale inedito uso delle norme tecniche[74]. 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:

& Littlefield, 2023, pp. 15 ss., disponibile in open access al link:<https://www.uu.nl/en/publication/ hybridity-conflict-and-the-global-politics-of-cybersecurity>.

[69] *Ibidem*.

[70] *Ibidem*.

[71] W. MATTLI, T. BÜTHE, *Setting International Standards: Technological Rationality or Primacy of Power?*, in *World Politics*, vol. 56 , n. 1 , 2003 , pp. 1 - 42 reperibile al link:<https://www.cambridge.org/ core/journals/world-politics/ article/ abs/setting-international- stand ards-technological-rationality- or-primacy-of-power/ 950CCFEEFE34 691BF6E2584141B0023A>.

[72] C. CAIERO, K. JONES, E. TAYLOR, *Technical Standards and Human Rights: The Case of New IP*, in C. SABATINI (a cura di), *Human Rights in a Changing World Order*, Londra, Chatham House and Brookings Institution Press, 2023, p. 186, disponibile al link:<https://www.chathamhouse.org/2022/ 10/reclaiming-human-rights-changing-world-order>. Si rinvia al citato contributo soprattutto per quanto riguarda l'analisi dell'impatto della proposta cinese sui diritti umani.

[73] W. MATTLI, T. BÜTHE, *Setting International Standards …op. cit.*

[74] Commissione europea, *Comunicazione congiunta al parlamento europeo e al consiglio. La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020) 18 final.

> Shaping international standards in 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[75].

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[76].

[75] *Ivi*, p. 20.

[76] M. RAYMOND, L. DENARDIS, *Multistakeholderism: anatomy of an inchoate global institution*, in International Theory, 2015, pp. 572–616, reperibile al link:<https:// www. cambridge.org/ core/journals/international-theory/ article/multistakeholderism-anatomy-of-an-inchoate-global -institution/B69E6361B5965C98CFD400F75AA8DC53>.

CAPITOLO II

REGOLARE PER MEZZO DELLA TECNICA:
UNA PROPOSTA DI STUDIO E ITINERARIO DELLA RICERCA

SOMMARIO: 1. L'insicurezza infrastrutturale delle reti: alle origini del rischio informatico e dell'esigenza di cybersicurezza - 2. La stabilità del cyberspazio: un bilanciamento tra continuità del servizio, libertà degli utenti e sicurezza - 3. Prospettiva di studio: il cyberspazio merceologico tra mercato e beni ICT - 4. La tutela dei diritti e delle libertà attraverso il «*code*» e la via europea

1. L'insicurezza infrastrutturale delle reti: alle origini del rischio informatico e dell'esigenza di cybersicurezza

Il progresso e l'espansione verso confini inesplorati hanno tipicamente imposto all'uomo di fare i conti con eventi futuri e imprevedibili che lo hanno portato a tenere in debita considerazione il "fattore rischio", ossia la prospettazione di un futuro danno. Simili valutazioni, dettate dalla paura, hanno condizionato la libertà dell'agire umano sia nelle scelte individuali, sia in quelle collettive, al fine di preservare la vita e i propri interessi di fronte all'incertezza dell'ignoto[1].

Con questo non vogliamo sostenere tesi che interpretano il rischio solo nel suo aspetto negativo, dato che vi è anche la dimensione di rischio-opportunità[2], tuttavia il processo di creazione del cyberspazio sembra non esser stato accompagnato dalle considerazioni circa i possibili pericoli che ne sarebbero potuti derivare.

A tal proposito, i primi decenni dalla creazione di Internet sono stati caratterizzati dall'assenza di vincoli da parte degli Stati. Diversamente dalla telefonia, dove l'intervento statale è stato determinante per lo sviluppo delle infrastrutture, la diffusione della telematica non ha richiesto grandi investimenti e si è potuta quindi sviluppare autonomamente e senza schemi o piani predeterminati.

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 ha dato inizio all'uso commerciale di Internet[3], e segnato il fallimento del movimento libertario della Rete che auspicava la creazione di uno spazio fuori dalla giurisdizione dei poteri dei governi[4].

Le origini del rischio informatico possono essere individuate in questo passaggio che ha portato alla diffusione delle reti e delle tecnologie informatiche presso il pubblico, senza tuttavia fare i conti

[1] Sul punto v. A. GIDDENS, *Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita*, Bologna, 2000, p. 36 ss., ove l'A. scrive che «l'idea di rischio emerge nei secoli XVI e XVII, coniata per la prima volta dagli esploratori occidentali che si avventurarono per il mondo: la parola "rischio" sembra infatti derivare dallo spagnolo o dal portoghese, lingue nell'ambito delle quali era impiegata per indicare la navigazione in acque ignote, non segnate sulle carte». Si tratta pertanto di una nozione che «rivela chiaramente i suoi legami con la società moderna, e rimarca significative differenze con il mondo premoderno: [ove] il rischio prende il posto del fato o della divinazione per evitare l'ira degli dei» (R. BRADIMARTE, *Rischio*, in R. BRADIMARTE, P. CHIANTERA-STRUTTE, P. DI VITTORIO, O. MARZOCCA, O. ROMANO, A. RUSSO, A. SIMONE (a cura di), *Lessico di biopolitica*, Manifestolibri, Roma, 2006, p. 262)

[2] A. GIDDENS, *Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita*, Bologna, Il Mulino, 2000, p.38, ove l'A. scrive che «[...] una positiva assunzione di rischio sta alla base di quell'energia che crea la ricchezza in un'economia moderna».

[3] J. L. GOLDSMITH, T. WU, *Who Controls the Internet? ...op. cit.*

[4] J.P. BARLOW, *A Declaration of the Independence of Cyberspace*, 8 febbraio 1996. Il testo della dichiarazione è disponibile sul sito dell'*Electronic Frontier Foundation* (EFF).

con il pregresso di idee e filosofie che era alla base del servizio che ha permesso a tali beni e infrastrutture di poter comunicare tra loro.

Internet rappresenta la prima convergenza tra le tecnologie computazionali e quelle comunicative il che pone in evidenza i due elementi infrastrutturali che la caratterizzano: la ridondanza delle reti e l'utilizzo del protocollo di trasmissione dei dati a pacchetto (anche noto come TCP/IP[5]).

Invero ancor prima di Internet i continenti erano già attraversati da vaste reti di comunicazione, si pensi alle reti telegrafiche (1844) e quelle dei primi telefoni (1876). Le connessioni delle macchine computazionali avvennero negli Stati Uniti, subito dopo la Seconda Guerra Mondiale, all'interno delle accademie. Tuttavia, questa prima rete aveva una struttura centralizzata, e cioè ogni macchina era connessa ad una macchina centrale che era l'unica a poter ricevere, creare e distribuire informazioni alle macchine periferiche[6].

Come intuibile questa architettura comunicativa presentava due tipi di problemi: la lunghezza in termini di percorso che doveva compiere un'informazione per poter essere trasmessa; e soprattutto, l'estrema vulnerabilità: la compromissione del nodo centrale[7] avrebbe comportato la paralisi dell'intero sistema.

Tale debolezza aveva rilievo non solo per il mondo accademico, dato che tale struttura non agevolava certamente il lavoro dei ricercatori statunitensi che spesso erano costretti a viaggiare verso le università ove erano disposti i computer centrali per svolgere le proprie ricerche o inviare a più colleghi i loro risultati, ma anche per il mondo militare.

La competizione tecnologica tra Stati Uniti e Russia che caratterizzò il periodo della Guerra fredda portò i primi, soprattutto a seguito del lancio in orbita del satellite Sputnik, ad avviare ricerche sulle possibili forme di comunicazione utili di *escalation* nucleare.

Dietro il sostegno governativo nacque così l'*Advanced Research Projects Agency* (ARPA), una struttura interna al Dipartimento della Difesa degli Stati Uniti (DoD), che diede vita ad ARPAnet, il primo archetipo di rete oggi comunemente utilizzata. Teorizzata sulle intuizioni di J.C.R. Licklider, Paul Baran, e Leonard Kleinrock, la nuova rete si basava su un'architettura non più "centralizzata" ma "distribuita" ispirata al funzionamento delle connessioni neurali del cervello umano: le funzioni di una parte danneggiata possono essere rimpiazzate da una nuova connessione realizzata con i

---

[5] Le regole che sono alla base del funzionamento della comunicazione del servizio Internet prendono il nome di protocolli di rete [e hanno avuto origine dalle intuizioni dei tre informatici Vinton Cerf, Robert Kahn, e Jon Postel. A livello tecnico la loro funzione è quella di coordinare la trasmissione dei messaggi tra i diversi computer. Nello specifico il protocollo TCP/IP (*Transport Control Protocol/ Internet Protocol*), come intuibile dal nome è composto a sua volta da altri due protocolli rispettivamente responsabili: il *Transmission Control Protocol* (TCP) del sezionamento all'origine dei messaggi in diversi pacchetti, per poi ricomporli in unità una volta arrivati a destinazione; l'*Internet Protocol* (IP) dell'indirizzamento delle singole porzioni di dati attraverso i nodi multipli e *networks* spesso funzionanti sulla base di standard diversi.

[6] La nascita di Internet è fatta convenzionalmente risalire al 29 ottobre 1969, data in cui vennero messi in comunicazione i computers dell'Università della California in Los Angeles, e quello dello *Stanford Research Institute*. L'esperimento consisteva nell'inviare un messaggio da un'Università all'altra per via telematica e fu un successo, sebbene si concluse con il *crash* delle due macchine. Dall'Università della California sarebbe dovuto partire un messaggio il cui contenuto erano le parole "*log in*" diretto al computer dell'Università di Stanford. Tuttavia, dopo aver scritto le prime due lettere, il computer mittente si bloccò improvvisamente, così il primo messaggio inviato tramite Internet furono le due lettere "*lo*".

[7] Il "nodo" è un concetto ripreso dalla "Teoria dei grafi", una branca della Matematica che permette di descrivere insiemi di oggetti e le loro relazioni all'interno di una rete (o meglio secondo il gergo di questa disciplina, un "grafo"). Il grafo è un oggetto matematico costituito da due elementi: l'arco, ossia il collegamento, e il nodo, il punto che viene collegato ad un altro grazie all'arco. Tale teoria trova applicazione in diversi contesti disciplinari come le reti di rapporti sociali, le connessioni fisiche o anche quelle logiche come nel caso delle connessioni informatiche. Sulla Teoria dei grafi v. A.L. BARABÁSI, *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, New York, 2014.

neuroni intatti. Ciò fu possibile grazie ai due principi che avevano ispirato il progetto, ossia la molteplicità e la ridondanza dei collegamenti che permetteva ad ogni nodo di ricevere, creare e trasferire informazioni[8].

Se la molteplicità e la ridondanza dei collegamenti sono stati gli elementi fondanti ARPAnet, il protocollo di trasmissione a pacchetto TCP/IP lo è stato per l'Internet. Sul finire della guerra fredda la rete ARPAnet, fino ad allora utilizzata solo nel contesto militare e quello accademico, venne diffusa presso il pubblico. Altri Paesi imitarono il progetto di rete utilizzando tuttavia tecnologie e protocolli diversi, dando così vita ad una serie di reti continentali non collegate tra loro[9]. L'invenzione del protocollo TCP/IP ebbe l'effetto di collegare queste diverse reti e dare vita all'Internet – anche noto per l'appunto – come la "rete delle reti" ossia il servizio universale che ha permesso di mettere in comunicazione le diverse reti continentali.

Le precisazioni di carattere storico e tecnico fin qui esposte non hanno solo una valenza teorica, ma, permettono di comprendere il fenomeno del rischio informatico legato all'intrinseca insicurezza della rete. Difatti l'idea che portò alla creazione di ARPAnet era quella di creare una rete locale "fra amici"[10]: ossia uno spazio privo di regole – se non quelle tecniche che ne regolavano il suo funzionamento – al fine di fornire un servizio "aperto" che agevolasse le comunicazioni tra soggetti che intendevano collaborare tra loro, trascurandone così la sicurezza interna, cosicché la rete non è stata «concepita obbedendo a criteri di sicurezza ma, al contrario, per garantire l'accesso e facilitare lo scambio di informazioni»[11].

Le reti e le risorse informatiche sono quindi caratterizzate da debolezze tecniche[12] e strutturali intrinseche che le rendono particolarmente vulnerabili a categorie di rischio riconducibili alle azioni malevole dell'uomo (il c.d. rischio antropico), come l'attacco informatico, ma anche il non corretto utilizzo dell'informatica o il mero errore umano[13]. Non solo, in quanto elementi anche materiali, al pari di tutti i beni fisici, sono soggette anche alle minacce non antropiche degli eventi naturali come alluvioni, incendi o terremoti, che possono abbattersi su di queste.

---

[8] P. BARAN, *On distributed communications: Introduction to distributed communications networks*, RAND Corp., Santa Monica (CA), 1964, reperibile al link:<https://www.rand.org/content/dam/ rand/pubs/research_memoranda/ 2006/RM3420.pdf>. Si consideri tuttavia anche il contributo di J.C.R. LICKLIDER, W.E. CLARK, *On-Line Man-Computer Communication*, Cambridge, Massachussetts, 1962.

[9] È ad esempio il caso della rete francese Minitel sviluppata nel 1981 come alternativa alla rete ARPAnet.

[10] L'espressione è di J. Palfrey.

[11] G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003, p. 332; v. anche C. GIUSTOZZI, *Cos'è il "rischio cyber" e perché ce ne dobbiamo preoccupare*, in F. RUGGE, S. DOMINIONI (a cura di), *La gestione dei rischi nello spazio cibernetico*, Dossier ISPI, 2019, p. 3. È prova di tale impostazione ideologica il funzionamento del protocollo TCP/IP creato dall'informatico Jon Bruce Postel ispirandosi ai principi delle comuni hippie. Da cui la legge di Postel che postula: "*be conservative in what you do, be liberal in what you accept from others*" di al presente Capitolo *infra* 5.

[12] Precisiamo che la letteratura tecnica distingue due nozioni, quali quelle di "vulnerabilità informatica" e di "debolezza informatica". Per vulnerabilità informatica è generalmente intesa la falla nel *design*, nell'implementazione o nella configurazione di un sistema informatico, un'applicazione *software* o un componente *hardware*. Queste vulnerabilità possono derivare da errori di programmazione, mancanza di aggiornamenti di sicurezza, configurazioni errate o altre carenze nella progettazione e nella gestione di sistemi informatici, e forniscono agli attaccanti la possibilità di sfruttarle per ottenere accesso non autorizzato o causare danni. Le debolezze informatiche si riferiscono invece a difetti o carenze intrinseche nei sistemi informatici o nei *software*. A differenza delle vulnerabilità, le debolezze non sono necessariamente il risultato di errori od omissioni umane, ma piuttosto possono essere parte integrante del sistema o del *software* stesso.

[13] Si rinvia al considerando 8 del Regolamento (UE) 2019/881 - c.d Cybersecurity Act - a proposito dell'igiene informatica. «[l]a cybersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'"igiene informatica", vale a dire semplici misure di routine che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche».

In entrambe le ipotesi la diffusione dell'informatica presso la società rende evidente come tali rischi - che per l'appunto definiremo informatici - possano indirettamente impattare sui diritti e le libertà dei singoli nelle società industrializzate.

Tuttavia, solo nell'ultimo ventennio, la crescente consapevolezza sui rischi della rete ha portato i poteri pubblici a volgere l'attenzione verso il cyberspazio con una sempre maggiori interventi legislativi di settore. Ma, come sarà argomentato in questo lavoro, i primi rimedi di cybersicurezza, o meglio di sicurezza informatica (*computer security*) e di sicurezza delle informazioni (*information security*), sono stati sperimentati e sviluppati dagli esperti di settore e dalle imprese per mezzo della normazione tecnica variamente prodotta da consorzi od organismi di normazione veri e propri (Pt. III, Cap. III, 1).

2. La stabilità del cyberspazio: un bilanciamento tra continuità del servizio, libertà degli utenti e sicurezza

«Be conservative in what you do, be liberal in what you accept from others». Nel 1980, con questo postulato l'informatico statunitense Jon Postel, uno dei creatori di Internet, dettava il principio di robustezza delle reti, anche noto in informatica come legge di Postel[14].

L'enunciato è particolarmente significativo in quanto sintetizza bene l'idea che ha portato alla creazione di Internet ai suoi albori, il cui valore è tuttavia ancora attuale. Si tratta infatti di uno dei principi che regolano la progettazione della trasmissione dei dati a pacchetto, che caratterizza per l'appunto il servizio Internet come lo conosciamo oggi, prevedendo che quando si inviano dati o si sviluppano nuovi protocolli e applicazioni per Internet, si dovrebbe farlo in modo conservativo, cioè seguendo rigorosamente gli standard e le specifiche esistenti. Dall'altro, quando si ricevono dati o si accettano connessioni, si dovrebbe essere più flessibili e tolleranti verso eventuali errori o variazioni dai protocolli standard.

L'assunto ci è utile per due ragioni. Innanzitutto testimonia quanto già argomentato nel precedente paragrafo: ossia che l'Internet degli albori, così come quello odierno, è direttamente influenzato dagli standard di funzionamento. Inoltre il postulato rende evidente la natura "aperta" e vulnerabile delle reti, orientate a preservare il libero flusso delle informazioni.

Derivati della legge di Postel sono infatti i due principi di libero accesso e neutralità[15]. Principi che permettono non solo l'utilizzo di Internet, quale servizio universale[16], ma allo stesso tempo costituiscono anche i criteri di funzionamento dell'infrastruttura stessa.

---

[14] Si rinvia alla RFC 761 (acronimo di "*request of comments*", si tratta di un'espressione utilizzata in telecomunicazioni e informatica indicante un documento pubblicato dalla *Internet Engineering Task Force*, che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico o, più nello specifico, di Internet) al link: https://www.rfc-editor.org/rfc/rfc793.

[15] Per un esempio di definizione di neutralità della rete v. AGCOM, *Internet Aperta/Neutralità della rete*, reperibile al link:<https://www.agcom.it/ internet-aperta/neutralita-della-rete# :~:text=In% 20base%20al% 20principio%20di,dal% 20 mittente% 20e%20dal% 20destinatario>, «La neutralità della rete è il principio per il quale le informazioni e contenuti scambiati attraverso la rete devono essere trattati in modo non discriminatorio, indipendentemente dal contenuto, dall'applicazione, dal servizio, dal terminale, nonché dal mittente e dal destinatario». Per una panoramica sulla definizione del principio della neutralità della rete, si veda veda P. DE FILIPPI, L. BELLI, *Network Neutrality: An Unfinished Debate* in L. BELLI, P. DE FILIPPI (a cura di), *Network Neutrality: an Ongoing Regulatory Debate*, 2014.

[16] Su Internet come patrimonio comune dell'umanità . G.M. RUOTOLO, *Internet (dir. internaz.)*, in *Enciclopedia del diritto – Annali*, Milano, 2104, pp. 556 ss.; A. SEGURA SERRANO, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, vol. 10, The Hague: Brill, 2006, pp. 191-272; SPANG-HASSEN, *Public International Computer Network Law Issues*, Djoef Publishing, Copenhagen, 2006.

Vi è quindi un punto di contatto tra le regole che disciplinano il funzionamento e l'esistenza della Rete (secondo l'accezione per cui è stata pensata sin dai suoi albori), e la tutela dei diritti umani in Rete[17], tra cui il diritto di accesso alla stessa.

A bene vedere secondo Alcuni il diritto di accesso non è un diritto umano a sé stante, ma piuttosto è uno strumento di esercizio di altri diritti[18].

Al di là delle diverse interpretazioni, se l'accesso abbia valore meramente strumentale, o sia un una libertà o diritto sociale[19], il dato certo è che la rete è indubbiamente uno strumento che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi per mezzo di essa e dei suoi diversi servizi[20].

La precisazione è d'obbligo poiché, come si comprenderà, parlare di "*governance* della sicurezza nel cyberspazio", significa innanzitutto chiedersi in quali rapporti si pone l'esigenza di sicurezza rispetto alle libertà della Rete, e da quale punto di vista ci poniamo[21].

Si assiste spesso ad azioni che hanno l'effetto di rompere questo legame e frammentare la Rete, o il cyberspazio[22]. 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[23].

In tutte le ipotesi emerge come queste azioni possano essere perpetrate tanto da poteri pubblici che da attori privati. Relativamente ai primi, ne sono un esempio le pratiche di *zoning*, ossia la creazione di percorsi di rete alternativi a quello ordinario (l'Internet o cyberspazio globale), che se portate all'eccesso possono essere l'origine di un processo di balcanizzazione della Rete[24], e quindi alla creazione di tante sotto-Reti che hanno adottato criteri logici e di funzionamento diversi.

---

[17] Cfr. art. 1 della Dichiarazione di Paragi adottata in seno al *World Summit on Information Society* (WSIS) nel 2003 pone come obiettivo la costruzione di una società dell'informazione a dimensione umana, aperta e caratterizzata dalla piena condivisibilità della medesima, individuando pertanto un legame con la dimensione della tutela dei diritti umani. Sul punto v. A. ODDENINO, *La governance di Internet fra autoregolamentazione, sovranità statale e diritto internazionale*, Giappichelli, Torino, 2008, pp. 151 e ss.

[18] V.C. CERF, *Internet Access Is Not a Human Right*, in *The New York Times*, 4 gennaio 2012, reperibile al link:<https ://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html>.

[19] Per una efficace panoramica sull'accesso ad Internet e le relative implicazioni nel contesto nazionale ed internazionale si rinvia a P. PASSAGLIA, *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in *MediaLaws*, n. 3, 2021, reperibile al link:<https://www. medialaws.eu/wp-content/uploads/2021/10/3-21-Passaglia. pdf>.

[20] Cfr. V. FROSINI, *La democrazia nel XXI secolo* (1997), Macerata, Liberilibri, 2010, pp. 40-41.

[21] Come vedremo la sicurezza è un concetto politico e relativo, Pt. II, Cap. I, 2.

[22] In quest'ultimo caso sia concesso rinviare a F. SERINI, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in *Rivista Italiana di Informatica e Diritto*, fasc. 2, 2023, reperibile al link:<https://doi.org/10.32091/RIID0123>.

[23] W.J. DRAKE, V.G. CERF, W. KLEINWACHTER, *Internet fragmentation: An overview. Davos: World Economic Forum*, 2016, p. 4. Il contributo nasce dall'esigenza di chiarire l'argomento in questione al fine di facilitare il confronto in senso al *World Economic Forum's multi-year Future of the Internet Initiative* (FII) dato che il concetto di "frammentazione" non ha univoco significato:«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).

[24] Cfr. A. ODDENINO, *La governance di Internet fra autoregolamentazione ...op.cit.,* p. 74. A tal proposito è nota la "Great Firewall" adottata dal governo cinese, sul punto v. X. WANG, *The Great Firewall of China and Its Implications*

Tra i casi che invece possono essere annoverati alle azioni di frammentazione dei privati possiamo invece far riferimento alle pratiche di *vendor lock-in* attraverso la creazione di specifiche tecniche (standard), che possono dare vita a vere e proprie guerre di standards per il dominio sui mercati[25], o anche essere guidate da fini e obiettivi politici estranei alle logiche di mercato[26].

Tuttavia sono possibili azioni che interferiscono sui diritti e libertà dei soggetti interconnessi anche senza ricorrere a strumenti che hanno l'effetto di frammentare la Rete, come nel caso del filtraggio e il controllo dei contenuti.

In tutti questi casi si tratta di attività poste in essere per ragioni di sicurezza interna di singoli Paesi ma che possono incidere su un servizio universale come l'Internet o su soggetti che risiedono al di fuori di essi.

Come osservato da Alcuni in considerazione della Dichiarazione universale dei diritti umani, in particolare gli artt. 19 e 29, emerge con chiarezza che «sono i governi a determinare cosa è contro la sicurezza nazionale e l'ordine pubblico nelle rispettive società [cosicché] un combattente per la libertà agli occhi di un governo potrebbe essere considerato un terrorista agli occhi di un altro paese»[27].

Da ciò è possibile dedurre come il bilanciamento tra uno strumento di libertà e globale come il servizio Internet e le ragioni di sicurezza interna degli Stati, possa variare da ordinamento a ordinamento a seconda della forma di Stato vigente, tra soluzioni che vanno dalla netta chiusura al controllo, ad altre che invece privilegiano la proporzionalità.

Tuttavia non solo i poteri pubblici hanno rilevanza in questo contesto. Ulteriore protagonista sono anche i privati che producono beni o erogano servizi ICT i quali possono anche produrre beni e servizi sul mercato ispirati a principi non necessariamente coincidenti con quelli di uno Stato. Si faccia riferimento al recente caso posto in evidenza dalla stampa internazionale secondo cui Apple avrebbe avrebbe notificato a giornalisti indipendenti indiani e politici dell'opposizione che il governo potrebbero aver cercato di violare i loro iPhone[28].

3. Prospettiva di studio: il cyberspazio merceologico tra mercato e beni ICT

Abbiamo introdotto la nozione di cyberspazio individuando un tratto comune alle diverse formulazioni dei primi anni 2000 nella individuazione dei livelli dello spazio cybernetico, anche noti come stratificazioni del cyberspazio, quali quello fisico, logico e umano.

Recenti studi, ritenendo ormai obsoleta tale impostazione statica[29], hanno formulato definizioni orientate ad esaltare il profilo dinamico del cyberspazio («la natura dromologica [...] dell'ambiente

---

for Political Information Systems, 2019, reperibile al link:<https://papers.ssrn.com/ sol3/papers.cfm?abstract_ id= 342 5612>.

[25] C. SHAPIRO, H.R. VARIAN, *The Art of Standards Wars*, in *California Management Review*, vol. 41, n. 2, 1999, pp. 8-32, reperibile al link:<https://doi.org/10.2307/41165984>.

[26] Nel caso della creazione di barriere commerciali nel settore delle ICTs per ragioni di sicurezza interna v. S. PENG, *Standards as a Means to Technological Leadership? China's ICT Standards in the Context of the International Economic Order*, in L. TOOHEY et al. (a cura di), *China In The International Economic Order: New Directions And Changing Paradigms*, Cambridge University Press, 2015, pp. 128-150 reperibile al link:<https:// ssrn.com/ abstract=3952315>.

[27] W.J. DRAKE, V.G. CERF, W. KLEINWACHTER, *Internet fragmentation …op.cit.,* p. 32.

[28] G. SHIH, J. MENN, *India targets Apple over its phone hacking notifications*, in *The Washington Post*, 27 dicembre 2023, reperibile al link:<https://www.washingtonpost.com/world/2023/12/27/ india-apple-iphone-hacking/>.

[29] G.J. RATTRAY, *An Environmental Approach to Understanding Cyberpower*, in "Cyberpower and National Security", in F.D. KRAMER, S. STARR, L.K. WENTZ (acura di), *Cyberpower and National Security*, National Defense University Press, Washington (D.C.), 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

cibernetico»), caratterizzato da due elementi: la velocità di propagazione e l'abbattimento dei confini[30]. Come scrive Luigi Martino, simili caratteristiche «insieme all'economicità dei mezzi, condiziona il rapporto di reciprocità tra territorio, interazioni sociali e dinamiche politiche»[31].

Aderendo a tale tesi, nel presente contributo si propone una scomposizione e reinterpretazione del cyberspazio come insieme di "merci"[32] - 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 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[33].

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 (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;

---

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».

[30] L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, fasc. 1, gennaio-aprile, 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*, *Uncertainity*, *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 M. MAYER, L. MARTINO, P. MAZURIER, G. TZVETKOVA, *How would you define cyberspace?*, First Draft Pisa, 19.05.2014, Experimental online laboratory PhD in Politics, Human Rights and Sustainability, Scuola Superiore Sant'Anna.

[31] L. MARTINO, *La quinta dimensione della conflittualità …op.cit.,* p. 66.

[32] Cfr. G. FINOCCHIARO, *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, vol. 17, 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».

[33] 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».

«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 («beni con elementi digitali»);

mentre ai nn. 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[34] 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[35], 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 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 dalla prospettiva degli ordinamenti europeo e degli Stati membri, che l'infrastruttura logica e materiale del cyberspazio possa essere interpretata

[34] Cfr. considerando 15, della proposta CRA.

[35] P.G. CHIARA, *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.

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 rispondono a regole simili[36]. 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[37], 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[38].

Il concetto di cyberspazio "merceologico" ci pare quindi utile poiché ci consente innanzitutto di individuare una connessione tra questa dimensione e il mercato, e quindi anche di poter ragionare sulla possibile regolazione del cyberspazio (per lo meno a livello europeo) per mezzo di un'azione sulle fonti che caratterizzano le relazioni commerciali, tra cui la certificazione e normazione tecnica, già note nel diritto internazionale dell'economia come "ostacoli tecnici al mercato"[39].

Tuttavia, nel nostro specifico caso si avrà modo di riflettere su tali strumenti, di natura non giuridica e prodotti attraverso alternative forme di aggregazione degli interessi di natura privata, non dalla prospettiva di diritto commerciale, ma costituzionale, al fine di studiare il loro impatto sui diritti e le libertà nel contesto della cybersicurezza.

4. La tutela dei diritti e delle libertà attraverso il «*code*» e la via europea

Gli standard che si riferiscono ai beni ICT sono 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 di tali beni nel mercato ed allo stesso tempo essere portatori di indubbi

---

[36] Precisiamo tuttavia che non intendiamo assimiliare la *lex informatica* alla *lex mercatoria*. Sul punto si rinvia a G. FINOCCHIARO, *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, vol. 17, 2001, pp. 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 maenirea univoca, questione che ha dato motivo di aprire un dibattito sul suo significato. A tal proposito v. K.P. BERGER, *The Creeping Codification of the Lex Mercatoria*, Kluwe law, London, 1999; F. GALGANO, *Lex mercatoria*, Il Mulino, Bologna, 2016; B. GOLDMAN, *Lex mercatoria,* Kluwer Law International, 1983; G. TEUBNER, *Global Bukowina: Legal Pluralism in the World-Society*, in G. TEUBNER (a cura di), *Global law without state*, Aldershot ,Dartsmouth, 1996, pp. 3-28; H.J. MERTENS, *Lex Mercatoria: A Self-applying System Beyond National Law?*, in G. TEUBNER (a cura di), *Global law without state*, Aldershot ,Dartsmouth, 1996, pp. 31 ss.

[37] COM (2015) 192 final, *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".

[38] 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.

[39] Il riferimento è ai c.d. *Technical Barriers to Trade (TBT) Agreement*, il quale mira a garantire che le normative tecniche, gli standard e le procedure di valutazione della conformità non siano discriminatorie e non creino ostacoli ingiustificati al commercio. Allo stesso tempo, riconosce il diritto dei membri dell'OMC di adottare misure per raggiungere obiettivi politici legittimi, come la tutela della salute umana e della sicurezza, o la protezione dell'ambiente. L'Accordo TBT incoraggia fortemente i membri a basare le loro misure sugli standard internazionali come mezzo per facilitare il commercio. Attraverso le disposizioni sulla trasparenza, mira anche a creare un ambiente commerciale prevedibile. Dal sito OMC di cui al link:<https:// www.wto.org/ english/ tratop_e/tbt_e/tbt_e.htm>.

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[40]. Diversamente, la moltiplicazione di norme tecniche e certificazioni diverse tra loro, se non addirittura incompatibili, ha l'effetto di creare barriere nel mercato[41], nonché di incidere negativamente sulla interoperabilità tecnica e sulla sicurezza dei sistemi[42] dal quale potrebbe derivare una inevitabile frammentazione del cyberspazio.

Questa prospettiva, che potremmo definire cyberspazio-mercato, non ci consente tuttavia di cogliere una potenzialità della normazione tecnica, nascosta dalla sua apparente neutralità.

Innanzitutto, come già argomentato, l'intuizione di Reidenberg e Lessig è stata quello di individuare - attraverso l'attenta osservazione dei processi logici che regolano la rete - un valido "appiglio" tecno-giuridico attraverso il quale i poteri pubblici avrebbero potuto orientare indirettamente le attività nel cyberspazio (o meglio la "società informazionale"), ponendo nuovamente il potere politico pubblico al centro delle soluzioni.

Difatti, secondo tali ricostruzioni, se i tecnologi informatici progettano le caratteristiche di base dell'infrastruttura che crea ed attua le impostazioni predefinite della rete, che limitano di fatto le azioni degli utilizzatori nel cyberspazio, gli Stati possono regolare indirettamente i comportamenti umani nel cyberspazio influenzando a monte le decisioni prese dai tecnologi attraverso leggi che impongono restrizioni sulle scelte che questi prendono[43].

Si è anche avuto modo di osservare, relativamente alla proposta della Cina di sviluppare un nuovo protocollo IP, quindi uno standard, come nella normazione tecnica l'elemento tecnico ed economico non prescindono da quello politico, mostrando quindi come i processi di standardizzazione possono consentire agli Stati di inserire i propri principi ideologici nella progettazione e nella architettura delle nuove tecnologie con modalità inedite[44].

Possiamo pertanto individuare tre "anime" delle norme tecniche nel contesto digitale: a livello tecnico, sono strumenti che disciplinano il funzionamento delle reti e dei sistemi informatici (scomposti nel concetto di "beni ICT"), a livello economico, sono strumenti che possono o meno costituire barriere al libero mercato, ed infine a livello giuridico-politico, possono farsi portatrici di valori e principi di determinati ordinamenti.

La presente proposta di studio intende avviare la riflessione sulla standardizzazione e certificazione di cybersicurezza a partire dall'obiettivo dell'Unione europea, "Leadership on standards, norms and frameworks in cyberspace" che compone uno dei punti della attuale Strategia europea di cybersicurezza per il decennio digitale presentata nel dicembre 2020[45].

---

[40] N. KATAGIRI, *Why international law and norms do little in preventing non-state cyber attacks*, in *Journal of Cybersecurity*, Vol. 7, Issue 1, 2021, reperibile al link:<https:// academic.oup.com/ cybersecurity/ article/7/1/ tyab009/ 6168044>.

[41] WORLD TRADE ORGANIZATION, *Members debate cyber security and chemicals at technical barriers to trade committee*, 2017.

[42] A. ODDENINO, *Digital standardization cybersecurity issues and international trade law*, in "Questions of International Law", 2018, pp. 31-51.

[43] L. LESSIG, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, in *Common Law Conspectus*, n. 5, 1997, reperibile al link:<https:// scholarship.law.edu/ commlaw/vol5/iss2/5/>.

[44] W. MATTLI, T. BÜTHE, *Setting International Standards …op. cit.*

[45] Commissione europea, *Comunicazione congiunta al parlamento europeo e al consiglio. La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020) 18 final.

Dal documento si apprende infatti che a fronte del dato che «[l]a normazione internazionale è sempre più utilizzata dai paesi terzi per far progredire la loro agenda politica e ideologica, che spesso non corrisponde ai valori dell'UE», l'Unione si impegna a formulare:

> norme internazionali nei settori delle tecnologie emergenti e dell'architettura di base di Internet in linea con i valori dell'UE [al fine di] garantire che Internet rimanga globale e aperta, che le tecnologie siano antropocentriche, attente alla riservatezza, e che il loro uso sia legale, sicuro ed etico. Nell'ambito della sua prossima strategia di normazione, l'UE dovrebbe definire i suoi obiettivi per la normazione internazionale e condurre un'azione proattiva e coordinata per promuoverli a livello internazionale. Si dovrebbe cercare una cooperazione più forte e una condivisione degli oneri con i partner che condividono le stesse idee e con i portatori di interessi europei.[46].

[46] *Ivi*, p. 20.

PARTE II

LE SICUREZZE DEL CYBERSPAZIO. UNA PROPOSTA DI ANALISI DEI CONCETTI GIURIDICI DI "CYBERSICUREZZA" E "CYBERRESILIENZA" NEL DIRITTO EUROPEO E NAZIONALE ALLA LUCE DELLA SICUREZZA IN SENSO TRADIZIONALE

CAPITOLO I

LA SICUREZZA IN SENSO TRADIZIONALE: UN INQUADRAMENTO GENERALE

SOMMARIO: 1. Premessa di studio sui concetti giuridici di cybersicurezza e cyberesilienza: un nuovo "diritto dei cavalli"? - 2. Alcune considerazioni generali sulla sicurezza in senso tradizionale - 3. La sicurezza nella Costituzione italiana - 3.1 La sicurezza nazionale - 3.2 Ordine e sicurezza pubblica - 4. La sicurezza nell'ordinamento europeo - 4.1. I concetti di ordine pubblico e sicurezza nazionale per l'ordinamento europeo - 4.2. La sicurezza come interesse collettivo europeo. SLSG e PSDC tra integrazione economica e politica - 4.3. L'esigenza di sicurezza degli Stati membri come limite alle libertà dell'Unione europea - *a) La minaccia diretta all'interesse fondamentale della collettività - b) Il rispetto del principio di proporzionalità - c) Il doppio sindacato giurisdizionale in sede nazionale ed europea*

1. Premessa di studio sui concetti giuridici di cybersicurezza e cyberresilienza: un nuovo "diritto dei cavalli"?

Negli stessi anni in cui era in corso il dibattito tra "*regulation skeptics*" e "*non regultation skeptics*", già sommariamente tratteggiato in precedenza (Parte I, Cap. I, 2), troviamo anche un ulteriore filone di discussione tra chi riteneva necessario introdurre una nuova branca del diritto attenta a studiare il cyberspazio e chi ne era contrario.

Tra quest'ultimi vi è il giudice Frank Easterbrooks che, in un discorso tenuto presso l'Università di Chicago nel 1996, fece ricorso alla metafora della «*law of the horse*»[1] per argomentare la sua idea di inutilità di una branca del diritto specializzata nel cyberspazio, la c.d. *cyberlaw*. Ricordando gli insegnamenti del decano Gerhard Casper, il giudice affermò che «il miglior modo per apprendere il diritto applicabile a specifici settori è quello di studiare le regole generali»[2]. In caso contrario, si andrebbe incontro ad un pericoloso rischio di dilettantismo multidisciplinare che porterebbe il "cieco" - ossia lo studioso specializzato in un solo settore - ad essere un pessimo pioniere[3]. Difatti secondo Easterbrooks, la *cyberlaw*, al pari della *law of the horse*, non avrebbe alcuna utilità dato che questa non «illuminerebbe l'intero ordinamento»[4].

Enunciazioni che non furono scevre di critica da parte di chi, come Lawrence Lessig, riteneva invece che la *cyberlaw*, diversamente da qualsiasi altra specializzazione del diritto, potrebbe invece

[1] F. ESTERBROOK, *Cyberspace and the Law of the Horse*, University of Chicago Legal Forum, 1996, pp. 207 ss., reperibile al link:<https://chicagounbound.uchicago.edu/uclf/vol1996/iss1/7/>.
[2] *Ivi.*
[3] Cfr. *Ivi.*
[4] *Ivi.*

"illuminare" l'ordinamento offrendo l'occasione di riflettere «sugli strumenti che una società ha a disposizione per imporre vincoli al comportamento»[5].

Secondo nostro parere, le argomentazioni di Lessig sono ragionevoli e non escludono affatto il necessario studio della teoria generale del diritto nonché soprattutto dei valori e principi costituzionali di un ordinamento. Anzi, tenendo conto del dato pratico, ossia il citato «*code*» quale limite alla legge giuridica (in questo caso possiamo considerarlo a tutti gli effetti come una norma tecnica), la *cyberlaw* consente di studiare i possibili fattori che influenzano il codice e, sulla scorta di ciò, come orientare il codice al rispetto dei diritti e delle libertà.

Ad ogni modo, al di là delle specializzazioni del diritto nel settore delle ICT (oltre al Diritto delle tecnologie e dell'informazione, si pensi anche all'informatica giuridica), l'obiettivo del presente studio è quello di analizzare la trasformazione del Diritto (dello Stato) dalla privilegiata prospettiva della sicurezza, quale altra faccia della sovranità[6].

Prima di affrontare la trattazione della normazione e certificazione tecnica di cybersicurezza (Parte III), in questa sede tenteremo così di studiare i concetti di cybersicurezza e cyberresilienza e lo faremo cercando di ricondurli, per quanto possibile, all'interno della più ampia riflessione sulla sicurezza in senso tradizionale. Inoltre, a riprova dell'importanza del dato pratico, faremo tesoro della lezione di altra Autorevole dottrina, affinché anche gli aspetti pratico-tecnici della materia siano presi in considerazione[7]. Una duplice prospettiva, quella dal generale al particolare, e viceversa, dal particolare al generale, di cui ci serviremo per tentare di meglio comprendere un tema di recente interesse per il diritto, ed in particolare per la giuspubblicistica in generale.

L'intento è quello di cercare di conferire dignità giuridica ad un concetto, quello di cybersicurezza, troppo spesso interpretato, e quindi studiato, sulla scorta di stereotipi e di sensazionalismi - come del resto per gran parte delle questioni che riguardano le nuove tecnologie dell'informazione e informatiche[8] - che hanno l'effetto di rendere il tema estraneo, o comunque distante al diritto rendendo difficile ragionare sulle questioni fondamentali che interessano l'ordinamento, primo fra tutti la tutela dei diritti e delle libertà.

Come intuibile, l'indagine non è priva di difficoltà, sia per l'ampiezza del concetto, sia per il suo inquadramento in termini giuridici. Se da una parte, analizzare la cybersicurezza e la cyberresilienza

---

[5] L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, n. 2, 1999, pp. 501 ss., reperibile al link:<https://doi.org/10.2307/1342331>.

[6] Per un primo studio sul punto v. M. LOSANO, *Il Diritto pubblico dell'informatica. Corso di informatica giuridica*, Torino, Einaudi, 1986.

[7] C. MOSCA, *Valori, modelli e prassi istituzionali*, Napoli, Editoriale scientifica, 2021, p. 4, ove l'A. scrive che «[u]na teoria generale della sicurezza deve, dunque, essere una rappresentazione che spieghi razionalmente il fenomeno studiato, attingendo alla prassi con l'ambizione di riuscire a ricavarne, attraverso uno sforzo classificatorio e con la soluzione di eventuali apparenti antinomie, osservazioni che, individuando i modelli concreti d'interazione istituzionale designati da norme e regole, possano assumere validità generale».

[8] Sugli effetti dell'utilizzo del termine cyberspazio a livello giuridico si rinvia a A. MONTI, *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, Pisa, 2023, 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 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 A. MONTI, *Digital rights delusion : humans, machines and the technology of information*, Routlege, Londra, 2023.

come nozioni slegate dalla sicurezza tradizionale porterebbe ad uno studio privo di riferimenti e mete, dall'altro, dobbiamo ammettere, che non esiste una nozione di sicurezza in termini universali.

Come noto, la sicurezza è una nozione sfuggente, di difficile definizione, dato che questa può acquistare differenti significati in base ai differenti contesti e al momento storico di riferimento[9], se non addirittura variare in base alle diverse sensibilità da persona a persona[10].

In particolare, come si avrà modo di osservare nel proseguo, nello specifico caso della cybersicurezza, questa non rappresenta solo una delle tante applicazioni della sicurezza in un determinato contesto (quello del cyberspazio), ma essa stessa al suo interno vede diverse sfaccettature, sia nella distinzione tra cybersicurezza e cyberresilienza, sia per la convivenza di attività di cybersicurezza pubblica e privata. Motivo che ci ha portato a far riferimento alle "sicurezze" nel titolo di questa Parte[11].

Si consideri inoltre che le "sicurezze" del cyberspazio sono espressione di esigenze securitarie scaturite da minacce globali che elevano la cybersicurezza ad interesse non solo nazionale ed europeo, ma anche internazionale, conferendone particolare rilievo nel più ampio multilivello degli ordinamenti.

A tal proposito specifichiamo che nella presente trattazione cercheremo di ricondurre i due citati concetti all'interno di una "sistematica"[12] della sicurezza, o perlomeno nell'alveo interpretativo dei canoni della sicurezza in senso tradizionale, alla luce degli ordinamenti nazionale ed europeo, e solo ove necessario faremo richiami alla disciplina di diritto internazionale.

2. Alcune considerazioni generali sulla sicurezza in senso tradizionale

L'etimologia latina del termine "sicurezza", ossia la *securitas*, rinvia alla condizione del singolo nella società di poter svolgere le proprie occupazioni abituali "senza preoccupazioni" - "*sine" "cura"* per l'appunto - rispetto ad eventi imprevedibili provenienti da fonti più o meno conosciute, ovvero dalle conseguenze dei suoi stessi comportamenti e quindi dalla possibilità di calcolare e prevedere le conseguenze delle sue stesse azioni[13].

Autorevole dottrina ha definito la sicurezza come quella «condizione di chi e di ciò che è esente da pericoli o tutelato da possibili pericoli», che consente ai consociati di sentirsi «liberi di agire con certezza e libertà»[14].

---

[9] Sul punto diffusamente v. E. ROTHSCHILD, *What is security?*, in *Daedalus*, vol. 124, n. 3, 1995, pp. 53-98, reperibile al link: <http://www.jstor.org/stable/20027310>.

[10] Cfr. A. STERPA, *La sicurezza dal punto di vista della Costituzione*, in C. BASSU, G. PISTORIO, A. STERPA, *Diritto pubblico della sicurezza*, Napoli, Editoriale scientifica, 2023, p. 12.

[11] Cfr. C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova, Cedam, 2012, pp. 26, ove l'Autorevole dottrina evidenzia che oltre la concezione tradizionale di sicurezza pubblica si «comincia a registrare un'obiettiva distinzione tra sicurezza pubblica primaria ed una secondaria o sussidiaria o complementare».

[12] N. IRTI, *L'età della decodificazione* [1989], Milano, Giuffrè, 1999, p. 170, ove l'A. descrive la disputa tra sistematici ed esegeti come uno «schermo di una lontananza più radicale e profonda» data dal fatto che «[c]i sono uomini, che ancora credono nell'armonia delle cose (armonia, costruita dalla sapienza di una divinità o della terrena perizia dei legislatori), e rifiutano di vedere la realtà come un intricato e buio groviglio. E ci sono invece uomini che - per usare un prezioso e finissimo titolo di Pietro Citati - scorgono tutt'intorno i "frantumi del mondo", e si piegano su di essi, e li interrogano, e cercano così di assolvere l'umile ed umano dovere del capire».

[13] E. NOCIFORA, *Sociologia della sicurezza, rischio e legalità democratica*, in AA.VV., *Sicurezza e democrazia*, Scriptaweb, Napoli, 2010, pp. 102-103.

[14] C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Cedam, Padova, 2012, p. 21.

Riprenderemo successivamente questo assunto, ma per il momento riteniamo utile evidenziare una prima distinzione tra la sicurezza oggettiva, ossia la sicurezza come "condizione" (di chi o di ciò che è esente o tutelato da possibili pericoli), e la sicurezza soggettiva, ossia la percezione dei consociati di sentirsi protetti.

La sicurezza è infatti prima di tutto un'esigenza umana che rientra nella sfera delle percezioni dell'individuo, e «la percezione è influenzata non tanto dalla situazione oggettiva quanto dal bisogno di equilibrio interiore»[15]. Questa, pertanto, può variare da persona a persona, nonché da cultura a cultura, e quindi da ordinamento a ordinamento.

A tal proposito, si consideri ad esempio che diversamente dall'italiano e dal tedesco, nalla ligua francese e inglese al concetto di sicurezza corrispondono due distinte nozioni.

In francese, con il termine *sureté* si fa riferimento a «pericoli o rischi proveninenti da azioni che intendono nuocere», mentre la *securité* «rinvia [...] a quei rischi che possono danneggiare persone e cose, ma che derivano da fatti accidentali (tecnici, fisici, chimici, sanitari o ambientali che siano)»[16]. In inglese la distinzione è invece tra il concetto di *security* e *safety*, sulle cui definizioni vi sono diverse interpretazioni[17]. A nostro parere, riteniamo utile rinviare alla distinzione secondo cui con il termine *safety* si è soliti far riferimento all'essere protetti da danni causati da atti non intenzionali, mentre per *security* il riferimento è alla protezione da azioni o comportamenti umani intenzionali[18].

Al di là delle diverse accezioni linguistiche e dell'etimologia del termine, resta il dilemma della definizione in termini giuridici di tale concetto[19].

Problema avvertito in realtà anche da una branca di studio delle relazioni internazionali, i c.d. studi sulla sicurezza (*security studies*)[20] che, nonostante abbiano il pregio di fornire una panoramica delle diverse prospettive teoriche con il quale è stata studiata e interpretata la sicurezza nel tempo, sono anche queste alla ricerca di una definizione sul punto[21].

Oltre la variabile storica e culturale, si consideri inoltre il carattere trasversale del concetto, il quale si è evoluto nel tempo sino a ricomprendere oggi un ampio spettro di ambiti. Si è passati infatti dalla tipica sicurezza (militare) dello Stato, alla sicurezza del singolo, sia come tale, sia come parte delle organizzazioni sociali, o fuori da esse (si pensi agli apolidi e agli immigrati), nonché alla

---

[15] W. SOFSKY, *Rischio e sicurezza*, Torino, Einaudi, 2005, p. 22.

[16] R. URSI, *La sicurezza pubblica*, Il Mulino, Bologna, 2022, p. 16.

[17] J. WALDRON, *Safety and security*, in E. REED, M. DUMPER (a cura di), *Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspectives*, Cambridge, Cambridge University Press, 2012, pp. 13-34; M. DURANTE, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in D. BERKICH, M. D'ALFONSO (a cura di), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence. Philosophical Studies Series*, Springer, Cham, vol 134, 2019.

[18] R. URSI, *op. cit.*, p. 16.

[19] O LEPSIUS, *Liberty, Security, and Terrorism: The Legal Position in Germany*, in *German Law Journal*, n. 5, 2004, reperibile al link:<https://germanlawjournal.com/ wp- content/uploads/glj_vol_05_no_05_lepsius.pdf>, ove l'A. scrive «To speak of "balancing" freedom against security is thus misleading. Security has become ambiguous in its meaning […] If a legal system wants to realize the "idea of security", it has to further define and outline this hyper-positive idea on a lower, more tangible, level […] The dangers of such an approach, where precise definitions of "security" and "danger" are neglected in favor of a diffuse scenario of threat, risks and networks, lie in the loss of individual freedom and, more importantly, in a loss of legal rationality» (pp. 459-460).

[20] Si tratta di una disciplina "giovane", che rientra negli studi sulle relazioni internazionali, e che si è originata durante il periodo della guerra fredda. Per ulteriori si rinvia alla pagina JStore, al link:<https://daily.jstor.org/ security-studies - foundations-and-key-concepts/>.

[21] R. POWELL, *Rights as Security: The Theoretical Basis of Security of Person*, Oxford online edn, Oxford Academic, 2019, in particolare si rivia al capitolo *Attempts to Define Security*, reperibila al link:<https://academic.oup. com/ book/ 35225/ chapter-abstract/299742504?redirectedFrom=fulltext>.

sicurezza di particolari campi di interesse riconducibili indirettamente alla sicurezza dello Stato o dell'uomo (es. ambiente, alimentare, dei prodotti, ecc.), mostrando i diversi aspetti applicativi e settoriali della nozione.

Come è stato osservato la sicurezza è un concetto relazionale che assume significato concreto solo quando utilizzato congiuntamente a specifici oggetti ritenuti meritevoli di protezione dagli ordinamenti (es. la sicurezza alimentare è diversa dalla sicurezza strategica dello Stato, ma allo stesso tempo ne può dipendere), così che «[s]ince security has no inherent meaning outside its relations with other concepts, there is no one 'security' but multiple securities»[22].

La studio della sicurezza riscontra quindi un preliminare ostacolo a livello concettuale dato da due opposti problemi. Il primo, relativo all'impossibilità di addivenire ad una definizione universale di sicurezza tale da ricomprendere tutte le sue sfaccettature multidisciplinari e interpretative; l'altro relativo alla necessità di inquadrare lo studio delle discipline settoriali della sicurezza (es. nel nostro caso la cybersicurezza) all'interno del più ampio quadro della sicurezza in generale, quale concetto relativo e mutevole come poc'anzi osservato.

La sicurezza è una nozione correlata ad un altro concetto quale quello di sovranità statale[23], dal quale deriva la sua connotazione ampia[24] e politica[25]. Alla luce di ciò, studiare la sicurezza impone quindi innanzitutto la necessità per l'osservatore di porsi da una determinata prospettiva (temporale, disciplinare e politica) per comprendere tale concetto nelle sue diverse dimensioni.

La presente trattazione intende analizzare le "sicurezze" del cyberspazio alla luce del concetto di sicurezza in senso tradizionale negli ordinamenti europeo e nazionale da una prospettiva di diritto costituzionale. A tal fine, riteniamo tuttavia di non poterci arrestare alla sola concezione odierna di sicurezza in senso giuridico, dato che è possibile rinvenire in questa il portato di diverse visioni securitarie che hanno caratterizzato gli ordinamenti liberaldemocratici nel tempo e che ci portano a dover far riferimento anche a parte degli assunti delle scienze sociali e delle relazioni internazionali.

---

[22] M. BOURNE, *Understanding security*, Macmillan Publishing, Londra, 2014, pp. 3-4. Sulla critica alla mancata definizione del concetto di sicurezza in termini giuridici v. O LEPSIUS, *Liberty, Security, and Terrorism: The Legal Position in Germany*, in German Law Journal, n. 5, 2004, reperibile al link:<https://germanlawjournal.com/ wp-content/uploads/glj_vol_05_no_05_lepsius.pdf>, ove l'A. scrive «To speak of "balancing" freedom against security is thus misleading. Security has become ambiguous in its meaning […] If a legal system wants to realize the "idea of security", it has to further define and outline this hyper-positive idea on a lower, more tangible, level […] The dangers of such an approach, where precise definitions of "security" and "danger" are neglected in favor of a diffuse scenario of threat, risks and networks, lie in the loss of individual freedom and, more importantly, in a loss of legal rationality» (pp. 459-460).

[23] Sull'evoluzione storica del concetto di sovranità v. M. GALIZIA, *La teoria della sovranità dal Medio Evo alla rivoluzione francese*, Milano, 1951; G. CHIARELLI, *Sovranità*, in *Noviss. dig. it.*, XVII, Torino, 1970, p. 1043 ss., N. MATTEUCCI, *Sovranità*, in N. BOBBIO, N. MATTEUCCI, G. PASQUINO, *Dizionario di politica*, Torino, 1990, p. 909 ss. Nonché v. anche E. CORTESE, *Sovranità (storia)*, in *Enc. dir.*, XLIII, Milano, 1990, p. 205 ss., G. SILVESTRI, *La parabola della sovranità. Ascesa declino e trasfigurazione di un concetto*, in *Riv. dir. cost.*, 1996; L. VENTURA, *Stato e sovranità: profili essenziali*, Torino : Giappichelli, 2010; E. CANNIZZARO, *La sovranità oltre lo Stato*, Bologna, 1 Mulino, 2020; F. TUCCARI, G. BORGOGNONE, *La sovranità: trasformazioni e crisi in età contemporanea*, Roma, Carocci, 2021;

[24] Sull'impossibilità di un concetto generale di sicurezza cfr. B. BUZAN, *New Patterns of Global Security in the Twenty-First Century*, in *International Affairs (Royal Institute of International Affairs 1944-)*, vol. 67, n. 3, 1991, pp. 431–51, reperibile al link:<https://academic.oup.com/ia/article-abstract/67/3/431/2406749>.

[25] Sulla natura politologica del concetto di sicurezza cfr. B. BUZAN, *Rethinking Security after the Cold War*, in *Cooperation and Conflict*, vol. 32, n. 1, 1997, pp. 5–28; K. BOOTH, *Theory of word security*, Cambridge university press, Cambridge, 2007, pp. 109 ss., ove l'A. descrive la sicurezza come "*derivative concept*" delle scienze e filosofie politiche. V. anche T. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Libreria Bonomo Editore, Bologna, 2010, ove a proposito della «sicurezza come condizione di ogni ordinamento giuridico», l'A. osserva che «[d]a questo punto di vista, però, la sicurezza risulta un dato sostanzialmente filosofico, che accompagna la nascita del fenomeno giuridico. Non esiste, quindi, una sua valenza propriamente prescrittiva» (p. 23).

Parte delle trattazioni giuridiche sulla sicurezza sono solite iniziare lo studio di tale concetto dall'analisi della sua evoluzione storica nelle diverse forme della statualità: stato moderno (o assoluto), stato liberale, stato sociale[26].

Analogamente, la letteratura delle relazioni internazionali ha organizzato una panoramica delle diverse prospettive teoriche con il quale è stata studiata e interpretata la sicurezza al fine di fornire una base per la conduzione dei ricordati *security studies*. Le trattazioni più recenti sono concordi nell'individuare almeno cinque approcci teorici comuni, distinti in tradizionali (quale l'approccio realista, liberista e costruttivista), e critici (quale la teoria critica e quella della securitizzazione della scuola di Copenaghen)[27]. Un fattore comune con gli studi giuspubblicistici è certamente dato dal concetto di sovranità statale che interessa entrambe le materie, ma lo sono anche la gestione delle situazioni di crisi o emergenziali che possono comportare la dichiarazione di stati di emergenza o l'adozione di misure straordinarie. Precisiamo tuttavia, in accordo con quanto recentemente osservato, che gli approcci condotti dai *security studies* pongono particolare attenzione alle relazioni tra gli Stati, da una visione perlopiù di sicurezza militare degli stessi, piuttosto che sugli individui (se non relativamente alla protezione dei diritti umani)[28], non ponendo quindi attenzione al rapporto governanti-governati, o autorità-libertà, nel contesto della sicurezza che è invece uno dei tratti di tipico interesse per lo studio della sicurezza dalla prospettiva giuridica.

Una certa dottrina giuridica[29] haproposto uno studio del rapporto tra la sicurezza e l'ordinamento giuridico[30] alla luce della teoria della securitizzazione dei *security studies*[31], teorizzando il concetto di sicurezza o, meglio, delle sicurezze, «as a mindsets», ossia come «a specific way of thinking about security», con l'intento di comprendere «come pensiamo e parliamo della sicurezza, come la problematizziamo e come affrontiamo e risolviamo i problemi legati alla sicurezza»[32]. Nello

---

[26] Cfr. T. GIUPPONI, *Le dimensioni costituzionali della sicurezza …op. cit.*; R. URSI, *La sicurezza pubblica*, Bologna, Il Mulino, 2022; F. CARINGELLA, A. IANNUZZI, L. LEVITA (diretto da), *Manuale di pubblica sicurezza*, Roma, Dike, 2013.

[27] La suddetta suddivisione è colta da P.D. WILLIAMS, M. MCDONALD, *Security studies: an introduction*, London-New York, Routledge, 2018 secondo cui, oltre a quelli citati, tra gli approcci critici sono ricondotti anche quello femminista, poststrutturalista e postcolonialista. Cfr. A. COLLINS, *Contemporary Security Studies*, Oxford, Oxford University Press, 2022, che oltre quelli citati, individua anche gli approcci "historical materialism", "peace studies", e "populear culture"; M. DUNN CAVELTY, THIERRY BALZACQ, *Routledge handbook of security studies*, London, New York, Routledge, 2017, ove gli AA. classificano tra gli approcci teorici, oltre i citati, anche quello della politica economica internazionale, quello della "English school", della sicurezza umana, del rapporto tra sicurezza e rischio e della «security as a practice». Altri studi si concentrano invece sull'analisi dei soli approcci critici sul punto v. C. PEOPLES, N. VAUGHAN-WILLIAMS, *Critical security studies: an introduction*, London, New York, Routledge, 2021.

[28] R. POWELL, *Rights as Security …op. cit.* Sul punto v. anche B. LÜTHI, *Perspectives on Security in Twentieth-Century Europe and the World*, in *Contemporary European History*, vol. 20, no. 2, 2011, pp. 207–14, reperibile al link:<https://www.jstor.org/stable/41238353>.

[29] Cfr. J. KREMER, *Exception, protection and securitization: security mindsets in law*, in M. FICHERA, J. KREMER (a cura di), *Law and security in Europe: Reconsidering the security constitution*, Intersentia, Cambridge, 2013.

[30] M. FICHERA, J. KREMER, *Introduction*, in M. FICHERA, J. KREMER (a cura di), *Law and security in Europe …op. cit.,* p. 1, ove gli AA., scrivono «Hence, secuirty is a manifold and complicated concept. Especially when analysed within the social realm, a whole range of theories and philosophies apply. In that sense, the aim of this book cannot be that of understanding security in a comprehensive way in social theory. Instead, this book focuses on the relationship between security and law».

[31] Brevemente e in maniera non esaustiva, l'approccio costruttivista enfatizza il carattere sociale e contestuale della securitizzazione, mostrando come le minacce vengano costruite e interpretate attraverso interazioni umane e processi di significato. La securitizzazione può essere vista come una manifestazione pratica dell'approccio costruttivista nella quale le rappresentazioni della sicurezza influenzano le decisioni politiche e le risposte istituzionali.

[32] Cfr. J. KREMER, *Exception, protection and securitization …op.cit.,* pp. 8 ss. L'A precisa che l'idea dei "security mindsets" combina tre concetti, quali quello elaborato da B. SCHNEIER, *Inside the Twisted Mind of the Security Professional*, in *Wired*, 20 marzo 2000, reperibile al link:<https://www.wired.com/2008/03/ securitymatters-0320/>

specifico sono distinti tre *security mindsets*: il *traditional security mindset*, il *liberal or expanded security mindset* e il *constructivist security mindset*[33].

Tale studio ci pare utile ai fini della presente ricerca, non tanto per il contenuto dei singoli *mindset*, per via dei limiti appena ricordati dei *security studies*, quanto per l'applicazione della teoria costruttivista (o della securitizzazione) dal punto di vista giuridico.

Prima riteniamo però opportuno partire da alcune considerazioni generali. L'evoluzione storica del concetto di sicurezza nel costituzionalismo moderno ha posto il monopolio della forza e la garanzia di sicurezza nelle mani dello Stato che la garantisce sia per preservare sé stesso dalle minacce esterne (sicurezza dello Stato apparato - sicurezza nazionale), sia per tutelare i propri cittadini, nel senso di Stato collettività (ordine pubblico). Tuttavia, se nello Stato moderno assoluto, di Thomas Hobbes l'individuo è tutelato dalla violenza degli altri individui[34], questi era tuttavia sfornito di rimedi contro la violenza o la prevaricazione del pubblico potere. Con il costituzionalismo liberale l'agire pubblico è stato sottoposto alla legge, quale espressione delle rappresentanze politiche dei cittadini, che limita l'arbitrarietà del potere pubblico tenuto a rispettare la sfera intangibile delle persone al fine di garantirne le libertà (c.d. libertà negative).

Alla luce di ciò possiamo trarre alcune preliminari conclusioni. La prima è che la sicurezza è un bisogno primario la cui soddisfazione non è rimessa ai singoli individui, pensati come incapaci di garantirla, ma è stata da questi affidata, secondo i teorici contrattualisti, allo Stato[35]. In questo senso la sicurezza è quindi strumento di tutela dei diritti.

(ultima consultazione 29.12.23), il quale propone un approccio dal punto di vista dei professionisti della sicurezza, e quindi funzionale alle scoperta delle vulnerabilità e debolezze dei sistemi (nel caso di specie dei sistemi informatici), quello elaborato da K. TUORI, *A European Security Constitution?*, in D. JENKINS, A. JACOBSEN, A. HENRIKSEN (a cura di), *The Long Decade: How 9/11 Changed the Law,* New York, Oxford Academic, 2014, reperibil al link:<https://academic.oup.com/book/12628/chapter- abstract/ 162545165?redirectedFrom=fulltext>, a proposito del concetto di "*hidden societal theory"*, ed infine il concetto di sicurezza elaborato dalla teoria della sicuritizzazione della scuola di Copenaghen.

[33] Il primo appriccio, anche noto come "realista" nella teoria classica delle relazioni internazionali, enfatizza la centralità degli Stati come attori principali, guidati da interessi nazionali e dallo spirito di sopravvivenza, e vede la forza militare come un mezzo per garantire la sicurezza e la stabilità. Questo paradigma coincide con il concetto di sicurezza tipico dello Stato moderno, profondamente connesso con l'affermazione della sovranità statuale. Come teorizzato da Thomas Hobbes nel *Leviathan,* il fine di garantire la sicurezza dei sudditi e la difesa dagli attacchi dei nemici esterni, ha giustificato la progressiva concentrazione dei poteri nelle mani del monarca attraverso il *pactum subiections* dei propri sudditi che consì hanno conferiscono il monopolio della forza al sovrano#. Pertanto in questi termini la sicurezza realista è la sicurezza (militare) dello Stato (o sicurezza nazionale) che legittima qualsiasi comportamento dello stesso, anche nell'uso della forza. Ve ne è traccia nella consuetudine internazionale relativa all'esercizio dell'autodifesa degli Stati a difesa di un attacco armato. Il corollario di una simile interpretazione è il *secuirty dilemma* descritto da John Herz ossia «una condizione sociale in cui ogni attore o entità si sforza di ottenere maggiore sicurezza espandendo i propri poteri con l'effetto che anche le altre entità, temendo per la propria sicurezza, cercano di espandere i propri poteri» (J. KREMER, *Exception, protection and securitization …op.cit.,* pp. 11 ss). Diversamente il concetto di sicurezza nel *liberal mindset*, non riguarda i soli profili della sicurezza dello Stato in , ma si espande oltre investendo anche altre dimensioni quali quella psicologica, sociologica ed economica. Contrariamente alla visione realista, quella liberale è favorevole alla cooperazione internazionale, alle creazione di istituzioni internazionali e alla diffusione dei valori democratici e della protezione dei diritti umani come fattori che contribuiscono alla sicurezza globale. Gli sforzi nella ricerca della cooperazione internazionale sono un esempio odierno di tale approccio. Per quanto riguarda l'approccio costruttivista della securituzzazione sarà ogetto di analisi nella trattazione.

[34] T. HOBBES, *Leviatano* (1651), con saggio introduttivo di C. GALLI, Rizzoli, 2011, pp. 177 ss. «[...] La moltitudine così unita in una persona viene chiamata uno Stato, in latino *Civitas*. Questa è la generazione di quel grande Leviatano...al quale dobbiamo la nostra pace e la nostra difesa [...] in esso consiste l'essenza dello Stato, che è una persona dei cui atti ogni membro di una grande moltitudine, con patti reciproci, l'uno nei confronti dell'altro e viceversa, si è fatto autore, affinchè possa usare la forza e i mezzi di tutti, come penserà sia vantaggioso per la loro pace e la comune difesa [...]».

[35] Sul punto v. T. HOBBES, *De Cive* (1642), a cura di T. MAGRI, Roma, Editori Riuniti, 2014; J. LOCKE, *Secondo Trattato sul Governo* (1689), Milano, Mondadori, 2018.

L'altro assunto è che tale azione di sicurezza del potere pubblico comporta una limitazione dei diritti e delle libertà dell'individuo (sicurezza come limite). Tuttavia, il potere pubblico è a sua volta limitata dall'obbligo di rispettare la legge, e dal principio di proporzionalità, elementi questi che costituiscono parametro del sindacato da parte di un giudice.

È proprio attraverso questo sistema di bilanciamento che negli ordinamenti costituzionali di impronta liberale, l'azione di sicurezza è funzionale alla garanzia delle libertà. Come precisato da Autorevole dottrina, la sicurezza è infatti quella «condizione di chi e di ciò che è esente da pericoli o tutelato da possibili pericoli», che consente ai consociati di sentirsi «liberi di agire con certezza e libertà»[36].

Alla luce di ciò, secondo una prima accezione, la sicurezza tradizionale moderna si esprimerebbe quindi come sicurezza giuridica, ossia sicurezza ottenuta attraverso il diritto, il quale costituisce la base legittimante l'azione del potere pubblico ed allo stesso tempo anche il suo limite (sicurezza giuridica rispetto al potere)[37]. La validità dell'azione pubblica per fini di sicurezza scaturisce infatti dalla sua conformità alla legge, che vede nel popolo sovrano il suo creatore per mezzo dei rappresentanti politici, i quali sono tenuti a rispettare i procedimenti di creazione normativa.

Altro profilo della sicurezza giuridica interessa tuttavia anche il diritto stesso («sicurezza nel diritto»), ed è volta a conferire certezza normativa al fine di evitare che l'arbitrio (sicurezza giuridica in relazione al diritto)[38]. In questo caso si fa riferimento al complesso di fonti, che vincolano gli operatori giuridici, e che riguardano la creazione e abrogazione delle norme, la loro applicazione e interpretazione, nel loro mantenimento e nella loro garanzia.

In questi termini la sicurezza assume quindi una dimensione normativa di ispirazione kelseniana ove la validità dell'azione del pubblico potere per fini di sicurezza, espressa per mezzo della norma, deriva dall'appartenenza di questa alla norma fondamentale (*Grundnorm*) che costituisce l'ordinamento giuridico[39], ossia oggi la Carta costituzionale.

Come è stato osservato, una simile interpretazione non lascerebbe «nessuno spazio a suggestioni connesse alla presunta (o meno) conformità della stessa alla realtà dei fatti o a determinati valori»[40]. Ecco che quindi oltre all'aspetto di conformità formale dell'azione pubblica all'ordinamento, emerge anche il profilo decisionale, relativo alla scelta del decisore politico per motivi di sicurezza relativa non solo allo strumento più opportuno, ma anche al bilanciamento degli interessi che determinano il contenuto della decisione e, ancora prima, al "se" intervenire.

Quest'ultimi aspetti sono stati oggetto di analisi nei *security studies* nello specifico approccio della "scuola di Copenaghen" che ha contribuito al dibattito sull'ampliamento del concetto di sicurezza e alla definizione del processo si securitizzazione, ossia la costruzione e identificazione delle minacce alla sicurezza, intese secondo questa teoria come minacce esistenziali alla sopravvivenza dello Stato nelle sue diverse articolazioni (*rectius* "settori" secondo tale teoria).

Si tratta di un'elaborazione che rifiuta la dimensione oggettiva della sicurezza, sostenendo piuttosto l'intersoggettività del concetto, dato che per la scuola di Copenaghen «l'attore

---

[36] C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Cedam, Padova, 2012, p. 21.

[37] G. PECES-BARBA, *Teoria dei diritti fondamentali*, Milano, Giuffrè, 1993, pp. 226 ss. Sul punto si rinvia anche a G. PISTORIO, *La sicurezza giuridica: profili attuali di un problema antico*, Napoli, Editoriale Scientifica, 2021, per aver analizzato la sicurezza secondo le coordinate della sicurezza "attravero" il diritto, e la sicurezza "nel" diritto.

[38] *Ivi*, pp. 231 ss.

[39] H. KELSEN, *Lineamenti di dottrina pura del diritto* (1934), Torino, Einaudi, 2000, p. 95.

[40] T. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Bologna, Libreria Bonomo Editore, 2010, pp. 21 ss.

securitizzante, presentando la questione in termini di minaccia esistenziale, riesce a far accettare e legittimare l'adozione di misure eccezionali e urgenti»[41] all'"*audience*" ossia l'opinione pubblica, alla classe politica e militare[42].

Le minacce esistenziali possono tuttavia essere comprese solo in relazione ai diversi settori nei quali si articola la sicurezza, individuati in quelli militare, ambientale, economico, societario e politico. Mentre l'identificazione di ciò che è rilevante per la sicurezza in ogni settore è data da uno spettro che va dal non politicizzato (il problema non è di interesse nel dibattito pubblico e non è considerato nei processi decisionali), a politicizzato (il tema è parte dell'agenda politica ed è gestito nei processi politici), a securitizzato (il problema politicizzato è presentato come minaccia esistenziale che richiede quindi misure eccezionali)[43]. Sinteticamente, la securitizzazione descrive quindi il processo che «porta una questione oltre la normale politicizzazione nell'ambito dell'eccezionalità»[44]. Pertanto in questi termini la sicurezza è interpretata come un costrutto, un prodotto di tale processo.

La connessione con il pensiero di Cal Schmitt è evidente[45]. Come noto, per Schmitt lo stato d'eccezione ha una dimensione straordinaria dato che la decisione del sovrano su di esso è «eminente» non potendo la legge normalmente vigente «comprendere un'eccezione assoluta e non [potendo] neppure dare fondamento pacificamente alla decisione che si trova di fronte ad un vero e proprio caso di eccezione»[46]. In questo frangente emergenziale l'autoconservazione dello Stato dimostra quindi di essere superiore alla validità della norma giuridica, provvedendo a sospendere il diritto[47]. Tuttavia precisa Schmitt, l'eccezione resta comunque accessibile alla conoscenza giuridica, poiché sia la norma, sia la decisione «permangono nell'ambito del dato giuridico»[48].

Difatti non è possibile affermare che l'eccezione non abbia alcun significato giuridico dato che, per essere accettabili, le limitazioni dei diritti di libertà devono avvenire in modo da non compromettere i principi garantisti propri delle costituzioni. Si faccia riferimento ai regimi emergenziali (come ad esempio il terrorismo) i quali possono comportare il rischio di adottore misure, più o meno organiche e più o meno protratte nel tempo che, sebbene abbiano il fine di garantire sicurezza proteggendo le libertà, «si [pongono] in una inconciliabile contraddizione con le stesse»[49].

Diversamente dai *security studies* che, come già evidenziato, non colgono la dialettica autorità-libertà propria dei rapporti interni tra governanti e governati, la dottrina giuridica ha invece rilevato come anche in situazioni emergenziali lo Stato è chiamato a dover bilanciare l'esigenza di proteggere l'ordinamento dalle minaccie con l'esigenza di garantire la tutela dei diritti fondamentali

---

[41] B. BUZAN, O. WAEVER, J. DE WILDE, *Security: a new framework for analysis*, London, Lynne Rienner, 1998, p. 25, reperibile al link:<https://www.academia.edu/39047709/ Buzan_Waever_and_De_Wilde_1998_Security _A_New_ Framework_For_Analysis>.

[42] *Ibidem.*

[43] *Ivi,* pp. 23-24.

[44] J. KREMER, *Exception, protection and securitization …op.cit.,* p. 19.

[45] A bene vedere, non è passata inosservata neppure agli studiosi delle relazioni internazionali v. M.C. WILLIAMS, *Words, Images, Enemies: Securitization and International Politics*, in *International Studies Quarterly*, vol. 47, n. 4, 2003, pp. 511–31, reperibile al link:<https://www.jstor.org/ stable/3693634>.

[46] C. SCHMITT, *Teologia politica* (1922), in *Le categorie del politico*, Bologna, Il Mulino, 2013 p. 33.

[47] *Ivi*, p. 39.

[48] *Ibidem.*

[49] G. DE VERGOTTINI, *Nuovi conflitti e sfide alla democrazia*, in L. FORNI, T. VETTOR, *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017, p. 40.

dell'essere umano da una eccessiva limitazione derivante dall'applicazione delle misure emergenziali[50]. Motivo che porta ad adottare tali misure solo quando queste siano previste dalla legge, in maniera proporzionale al pericolo e vigenti per il periodo di tempo strettamente necessario a far fronte all'emergenza al fine di limitare il possibile eccesso del politico sul giuridico.

La visione normativista kelseniana, e quella decisionista di matrice schmittiana, ci restituiscono così le due dimensioni dell'esigenza di sicurezza che sono quella ordinaria, quando l'eccezione è prevista dallo stesso ordinamento attraverso limitazioni e deroghe imposte da una norma, ovvero straordinaria, quando l'eccezione non può essere contemplata dalla norma e sul quale la decisione non può che essere presa dal decisore politico (o il sovrano schmittiano), comunque nel rispetto delle garanzie costituzionali. Opposte accezioni secondo cui la prima giustifica l'azione di sicurezza secondo le norme, l'altra, invece, secondo i fatti che richiedono misure eccezionali.

Nelle costituzioni delle democrazie liberali attuali pare potersi scorgere una sintesi di questi due orientamenti, più o meno calibrata su un polo o sull'altro a seconda degli ordinamenti considerati[51].

Si ritiene infatti che il ricorso a misure restrittive delle libertà sia sempre possibile in presenza di un fondamento normativo che le preveda, nei soli casi necessari e inevitabili, con provvedimenti proporzionati al pericolo e scaturenti da un giudizio di bilanciamento fra sicurezza e libertà sottoponibile al controllo Parlamentare e dei Giudici[52].

Tuttavia osservando la gestione degli stati d'emergenza, si registra la tendenziale diffidenza delle democrazie liberali alla gestione di tali situazioni con misure eccezionali che ha portato alla pratica della «normalizzazione dell'emergenza»[53], ossia all'utilizzo di strumenti ordinari anche quando le loro costituzioni prevedono la possibilità di formalizzare la crisi introducendo lo stato d'emergenza, segnando così il «tendenziale superamento della distinzione fra diritto normale e diritto eccezionale»[54]. Si tratta di una prassi che deve essere contestualizzata e interpretata rispetto al fenomeno terroristico, o ai fenomeni di rischio in generale. Lo Stato d'eccezione, ossia la sospensione delle garanzie costituzionali, trae infatti origine dall'esigenza di consentire alle democrazie di sopravvivere nei casi di guerra. Il problema dato dalle attuali esigenze di sicurezza è che mentre nei casi di guerra le restrizioni sono limitate alla durata del conflitto. Diversamente, l'indeterminatezza dei periodi di pace e guerra propria delle minacce ibride, ossia conflitti asimmetrici ove sono utilizzati mezzi e metodi non convenzionali[55], rischia di rendere tali restrizioni permanenti poiché permanente è lo stato di paura indotto da tali minacce[56].

---

[50] Cfr. C. BASSU, *I diritti umani e le nuove sfide alla sicurezza*, in L. FORNI, T. VETTOR, *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017, p. 117 ss, reperibile anche in *Forum di quaderni costituzionali*, 27 marzo 2017, al link:<https://www.forumcostituzionale.it/ wordpress/wp-content/uploads/2016/06/bassu.pdf>.

[51] *Ivi*, pp. 124 ss., ove l'A. conduce un'indagine comparatistica sul punto

[52] G. DE VERGOTTINI, *Sicurezza e diritti fondamentali*, in L.E.R. VEGA, L. SCAFFARDI, I. SPIGNO, *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, Editoriale scientifica, 2021, p. 22.

[53] G. DE VERGOTTINI, *Guerra e costituzione. Nuovi conflitti e sfide alla democrazia*, Milano, Il Mulino, 2004, p. 201. Sul punto v. anche C. BASSU, *I diritti umani e le nuove sfide alla sicurezza …op. cit.,* p. 123.

[54] *Ibidem*. Sul punto v. anche G. AGAMBEN, *Stato di eccezione: Homo sacer, II, 1*, Torino, Bollati boringhieri, 2003.

[55] Sui concetti di guerra asimmetrica ibrida si rivia a F. HOFFMAN, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007, reperibile al link:<https://www.potomacinstitute.org/images/ stories/publications/potomac_hybridwar_0108.pdf>; M. BRESSAN, G. CUZZELLI, *Da Clausewitz a Putin: la guerra nel XXI secolo*, Milano, Ledizioni, 2022.

[56] P. CIARLO, *Sicurezza e Stato di diritto*, in V. BALDINI (a cura di), *Sicurezza e Stato di diritto: problematiche costituzionali*, Cassino, Edizioni dell'Università degli Studi di Cassino, 2005, p. 20. Sul rapporto sicurezza e paura v. anche E. DENNINGER, *Dallo "Stato di diritto" allo "Stato di prevenzione"*, nella medesima opera, ove l'A. richiamando W. SOFOSKY, *Elemente des Terros*, in H. HOFFMANN, W.F. SCHOELLER (a cura di), *Wendepunkt 11. September 2001: Terror, Islam und Demokratie*, Amsterdam, DuMont Buchverlag, 2001, pp. 27 ss. scrive a proposito del concetto di

Tralasciando la distinzione tra l'esigenza di sicurezza ordinaria (riconducibile alla tutela dell'ordine pubblico) e straordinaria (riconducibile alla sicurezza dello Stato), riteniamo che la teoria della securitizzazione abbia il pregio di porre attenzione sul momento in cui l'esigenza di sicurezza oltre ad essere avvertita, viene anche evocata ("*uttering*") dal decisore politico per far fronte alle minacce che di volta in volta si presentano per lo Stato e per i cittadini[57].

L'identificazione della minaccia porta inevitabilmente a riflettere su quali paure possano essere ritenute meritevoli di attenzione da parte del decisore. Come è stato intuito, la sicurezza, nella sua dimensione soggettiva, può infatti essere considerata come un «"contenitore giuridico aperto"» che non può tuttavia, sul piano oggettivo, «tradurre in norma giuridica ogni pretesa di protezione che emerge dalla comunità di individui»[58]. Se portata alle estreme conseguenze, una simile azione priverebbe infatti gli individui di compiere scelte proprie e quindi del loro libero arbitrio[59].

Pertanto la gestione delle "paure" da parte del decisore politico lo espone ad un difficile bilanciamento tra l'esigenza di garantire la sicurezza collettiva ossia «tutto quello che garantisce la ordinata convivenza di una comunità e dei suoi individui»[60], e la sicurezza individuale intesa come «garanzia dell'incolumità dell'individuo quale presupposto all'esercizio della sua libertà»[61], ove la libertà dello stesso è il bene oggetto di tutela.

Si tratta di due eccezioni della sicurezza che possiamo interpretare - mutuando dalla distinzione di Isahia Berlin tra libertà positiva e negativa[62] - alla luce dei concetti di sicurezza positiva e sicurezza negativa[63]. Divisione riconducibile al passaggio dallo Stato liberale a quello sociale.

In quest'ultima forma, trova origine il concetto di sicurezza collettiva quale espressione dell'assunzione da parte dello Stato e della pubblica amministrazione di compiti volti ad assistere gli invididui nei loro bisogni, garantendo dignità e integrazione sociale. Secondo Alcun è in questo periodo che si afferma la «sicurezza dei diritti»[64], quale espressioone della accessione positiva della sicurezza, come riconoscimento dei bisogni e funzionale alla partecipazione alla vita sociale (sicurezza *di*/sicurezza in senso lato).

Diversamente, la sicurezza che troviamo nello Stato liberale, si esprime nella sua accezione negativa, il «diritto alla sicurezza», come forma di protezione dalle aggressioni e quindi dalle paure (sicurezza *da*/sicurezza in senso stretto).

"terrore selettivo" «è un meccanismo per la differenziazione sociale della paura. Separa quelli che devono temere per la loro vita da quelli che ancora possono godersi una certa sicurezza. Invece, il terrore generale prende di mira tutti. Cerca di paralizzare nell'angoscia la società intera, cerca di togliere allo stato la sua legittimità di base».

[57] B. BUZAN, O. WAEVER, J. DE WILDE, *Security …op.cit.* p. 24.

[58] A. STERPA, *La sicurezza dal punto di vista della Costituzione*, in C. BASSU, G. PISTORIO, A. STERPA, *Diritto pubblico della sicurezza*, Napoli, Editoriale scientifica, 2023, pp. 14 ss.

[59] *Ibidem*.

[60] T. GIUPPONI, *Le dimensioni costituzionali della sicurezza … op. cit*., p. 11.

[61] A. STERPA, *La libertà dalla paura - una lettura costituzionale della sicurezza*, Napoli, Editoriale scientifica, 2019, p.16.

[62] I. BERLIN, *Quattro saggi sulla libertà* (1969), Milano, Feltrinelli, 1989.

[63] P. CERI, *La società vulnerabile. Quale sicurezza, quale libertà*, Roma-Bari, Laterza, 2003, pp. 52 ss.

[64] A. BARATTA, *Diritto alla sicurezza o sicurezza dei diritti?*, in *Democrazia e diritto*, n. 2, 2000, pp. 19 ss.

In conclusione, considerate le diverse articolazioni del concetto che abbiamo cercato di tratteggiare alla luce della sua evoluzione storica, tralasciando se sia un principio[65], un valore[66] o un diritto[67], nella presente trattazione ci concentreremo su alcuni concetti di sicurezza a livello interno ed europeo, tentando di cogliere il rapporto autorità-libertà quale riflessione che sarà replicata anche a proposito delle "cybersicurezze" di cui al Cap. II

3. Aspetti generali sulle dimensioni della sicurezza nella Costituzione italiana

La Costituzione italiana non definisce il concetto di sicurezza, sebbene questo sia espressamente inserito in diverse disposizioni del testo già nella sua versione del 1948, tra i diritti e i doveri, e ne sia stata poi accresciuta la sua presenza a seguito della riforma avvenuta con la Legge costituzionale n. 3 del 2001 che ha apportato modifiche al Titolo V della seconda parte del testo[68].

Da una prospettiva sistematica è possibile cogliere la duplice funzione di questo concetto all'interno della Carta. Da una parte, come elemento che limita le libertà (artt. 13, 16, 17, 25, 41) o fondamento dei doveri dei cittadini (di difesa e fedeltà, artt. 52, 54), dall'altra, come compito normativo dei pubblici poteri, in sede di materia e riparto dei compiti a livello di governo (artt. 117, 118, 120 e 126 Cost), e compito amministrativo di protezione[69].

La legislazione primaria settoriale ha poi portato a diverse nozioni di sicurezza, che si differenziano in relazione all'aggettivo o al sostantivo che qualifica o definisce quest'ultima (es. sicurezza alimentare, del lavoro, della navigazione, ecc.).

Per quel che qui interessa, ci soffermeremo su due particolari dimensioni costituzionali del concetto di sicurezza che sono quelle di "sicurezza nazionale" e "ordine pubblico", che, sebbene siano strettamente correlate, riteniamo meritevoli di una trattazione distinta[70].

L'obiettivo sarà, per quanto possibile quello di capire il significato giuridico della sicurezza nazionale e ordine pubbliche alla luce delle nuove esigenze dettate soprattutto dall'informatizzazione della società.

---

[65] Sulla sicurezza come principio v. K. LACHMAYER, *A Comparative Analysis of Security as an Element of Constitutional Design: Is Global Terrorism Changing the Conditions of International Constitutional Law?*, Online Paper submitted at the VII World Conference of the International Association of Constitutional Law – Workshop 8: Constitutions and Global Terrorism 2007, pp. 7-8, reperibile al link:<https://www.lachmayer.eu/wp-content/uploads/2014/05/2007_A-Comparative-Analysis-of-Security. pdf>.

[66] Sulla sicurezza come principio v. G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi Costituzionali*, n. 1, 2008, pp. 31 ss.

[67] Sulla sicurezza come diritto G. DE VERGOTTINI, *Il bilanciamento tra sicurezza e libertà civili nella stagione del terrorismo*, in AA.VV., *Sicurezza: le nuove frontiere*, Franco Angeli, Milano, 2005, p. 110; P. TORRETTA, *Diritto alla sicurezza e altri diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Giuffrè, Milano, 2003, pp. 451 ss.; C. MOSCA, *La sicurezza come diritto di libertà …op. cit.*

[68] Sul punto v. B. CARAVITA, *Sicurezza e sicurezze nelle politiche regionali*, in *federalismi.it*, n. 25, 2004, reperibile al link:<https://www.federalismi.it/nv14/editoriale.cfm?eid=44>.

[69] Sulla a funzione di polizia di sicurezza come funzione amministrativa e i suoi relativi poteri si rinvia a R. URSI, *La sicurezza pubblica*, Bologna, Il Mulino, 2022.

[70] Relativamente al concetto di "interesse nazionale" si rinvia per uno studio dalla prospettiva politica a V.E. PARISI, *Interesse nazionale e globalizzazione: i regimi democratici nelle trasformazioni del sistema post-westfaliano*, Milano, Jaca book, 1998; A. ARESU, L. GORI, *L'interesse nazionale: la bussola dell'Italia*, Bologna, Il mulino, 2018, nonché dalla prospettiva giuridica A. CORNELI, *I Servizi d'intelligence e l'interesse nazionale*, in *Per Aspera Ad Veritatem*, n.7, 1997; reperibile presso il sito della rivista Gnosis; B. CARAVITA, *In tema di "interesse nazionale" e riforme istituzionali*, in *federalismi.it*, n. 6, 2003.

3.1. La sicurezza nazionale

Il concetto giuridico di sicurezza nazionale nasce negli Stati Uniti e si afferma durante il periodo della guerra fredda[71]. Come anticipato già per la sicurezza in generale, non è ipotizzabile una definizione in termini esclusivamente giuridici del concetto in questione poiché il suo profilo essenziale è nell'esercizio di un potere politico, e in quanto tale la sua natura è relativa, da ordinamento a ordinamento, e in relazione ad una determinata fase storica. Gli studiosi di diverse discipline ne hanno negato il suo significato giuridico poiché per Alcuni si tratterebbe di un concetto connotato da soli elementi ideologici e morali, quindi politici[72], mentre per Altri il concetto avrebbe natura geopolitica e quindi sarebbe difficile da perimetrare in ragione della fluidità dello scenario che obbliga a scelte dettate dalla contingenza[73].

Non resta quindi che cercare di individuare i contorni e il nucleo essenziale di tale concetto mutevole. Nella letteratura giuridica d'oltreoceano[74] e in quella dei *security studies*[75] non sono mancate analisi che hanno delimitato i settori in cui tale concetto interviene, come la difesa delle pratiche democratiche contro ogni influenza esterna, la difesa dell'indipendenza della nazione e del territorio contro attacchi militari, il mantenimento dei *core-values* della società e la salvaguardia delle libertà delle popolazioni da minacce esistenziali.

A livello giuridico, tra le fonti sovranazionali la sicurezza nazionale è espressamente citata nella Carta dei diritti fondamentali dell'Unione europea (art. 8)[76], nella Convenzione per la salvaguardia

---

[71] M. VALENTINI, *Alta direzione, coordinamento e responsabilità politica*, in C. MOSCA, G. SCANDONE, S. GAMBACURTA, M. VALENTINI, *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)*, Milano, Giuffrè, 2008, pp. 56 ss. V. anche M.P. LEFFLER, *National Security*, in *The Journal of American History*, vol. 77, n. 1, 1990, pp. 143–52, reperibile al link:<https://www.jstor.org/stable/ 207 8646>. Per una diffusa trattazione sulle orgini del concetto di sicurezza nazionale e il rapporto con il diritto e le nuove tecnologie v. A. MONTI, *National security in the new world order. Government and the technology information*, New York, Routledge, 2022.

[72] B. BUZAN, *Rethinking Security after the Cold War …op.cit.*

[73] C. JEAN, *La politica di sicurezza dell'Italia*, in *Gnosis*, n. 4, 2014.

[74] L. LUSTGARTEN, I. LEIGH, *In From the Cold: National Security and Parliamentary Democracy*, Oxford, Oxford University Press, 1994.

[75] B. BUZAN, *New Patterns of Global Security …op.cit.*

[76] Art. 8 della CEDU sulla protezione dei dati di carattere personale «1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente». Sui profili interpretativi del disposto si rinvia alla *Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence*, pubblicata dalla Corte europea dei diritti dell'uomo, di cui al link:<https://www.echr.coe.int/documents/d/echr/guide_art_8_eng>.

per i diritti dell'uomo e le libertà fondamentali (art. 10)[77], nel Patto internazionale sui diritti civili e politici (art. 19)[78] e nei Trattati europei (*infra* 4).

Relativamente all'ordinamento italiano, diversamente dai concetti di "sicurezza e ordine pubblico" che hanno trovato puntuale definizione nelle fonti primarie come vedremo a breve (*infra* 3.2), la "sicurezza nazionale" è una nozione che resta giuridicamente nebulosa, nonostante sia stata progressivamente normativizzata[79]. Nel proseguo analizzeremo il dato letterale delle norme, nonché le pronunce della giurisprudenza sul punto al fine di individuare appigli interpretativi di tale nozione evanescente.

Innanzitutto la sicurezza nazionale trova espressa menzione nel testo Costituzionale nella sola lettera dell'art. 126, ove è attribuito al Presidente della Repubblica il potere di sciogliere i Consigli regionali e rimuovere il Presidente della Giunta per ragioni, tra le altre, anche di sicurezza

---

[77] Art. 10 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, sulla libertà di espressione «1 Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive. 2 L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».

[78] Art. 14, Patto internazionale sui diritti civili e politici, «1. Tutti sono eguali dinanzi ai tribunali e alle corti di giustizia. Ogni individuo ha diritto ad un'equa e pubblica udienza dinanzi a un tribunale competente, indipendente e imparziale, stabilito dalla legge, allorché si tratta di determinare la fondatezza di un'accusa penale che gli venga rivolta, ovvero di accertare i suoi diritti ed obblighi mediante un giudizio civile. Il processo può svolgersi totalmente o parzialmente a porte chiuse, sia per motivi di moralità, di ordine pubblico o di sicurezza nazionale in una società democratica, sia quando lo esiga l'interesse della vita privata delle parti in causa, sia, nella misura ritenuta strettamente necessaria dal tribunale, quando per circostanze particolari la pubblicità nocerebbe agli interessi della giustizia; tuttavia, qualsiasi sentenza pronunciata in un giudizio penale o civile dovrà essere resa pubblica, salvo che l'interesse di minori esiga il contrario, ovvero che il processo verta su controversie matrimoniali o sulla tutela dei figli. 2. Ogni individuo accusato di un reato ha il diritto di essere presunto innocente sino a che la sua colpevolezza non sia stata provata legalmente. 3. Ogni individuo accusato di un reato ha diritto, in posizione di piena eguaglianza, come minimo, alle seguenti garanzie: a) ad essere informato sollecitamente e in modo circostanziato, in una lingua a lui comprensibile, della natura e dei motivi dell'accusa a lui rivolta; b) a disporre del tempo e dei mezzi necessari alla preparazione della difesa ed a comunicare con un difensore di sua scelta; c) ad essere giudicato senza ingiustificato ritardo; d) ad essere presente al processo ed a difendersi personalmente o mediante un difensore di sua scelta; nel caso sia sprovvisto di un difensore, ad essere informato del suo diritto ad averne e, ogni qualvolta l'interesse della giustizia lo esiga, a vedersi assegnato un difensore d'ufficio, a titolo gratuito se egli non dispone di mezzi sufficienti per compensarlo; e) a interrogare o far interrogare i testimoni a carico e ad ottenere la citazione e l'interrogatorio dei testimoni a discarico nelle stesse condizioni dei testimoni a carico; f) a farsi assistere gratuitamente da un interprete, nel caso egli non comprenda o non parli la lingua usata in udienza; g) a non essere costretto a deporre contro se stesso o a confessarsi colpevole. 4. La procedura applicabile ai minorenni dovrà tener conto della loro età e dell'interesse a promuovere la loro riabilitazione. 5. Ogni individuo condannato per un reato ha diritto a che l'accertamento della sua colpevolezza e la condanna siano riesaminati da un tribunale di seconda istanza in conformità della legge. 6. Quando un individuo è stato condannato con sentenza definitiva e successivamente tale condanna viene annullata, ovvero viene accordata la grazia, in quanto un fatto nuovo o scoperto dopo la condanna dimostra che era stato commesso un errore giudiziario, l'individuo che ha scontato una pena in virtù di detta condanna deve essere indennizzato, in conformità della legge, a meno che non venga provato che la mancata scoperta in tempo utile del fatto ignoto è a lui imputabile in tutto o in parte. 7. Nessuno può essere sottoposto a nuovo giudizio o a nuova pena, per un reato per il quale sia stato già assolto o condannato con sentenza definitiva in conformità al diritto e alla procedura penale di ciascun paese».

[79] A. MONTI, *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, in *Quaderno speciale CASD n. 1 - Scenari globali e interessi nazionali: pandemia, continuità, cambiamento*, 2020, reperibile al link:<https://www.casd.it/course/view.php?id=441&lang=en>.

nazionale[80]. Mentre, nella formulazione dell'art. 117, co. 2, Cost., tra le materie di esclusiva competenza legislativa dello Stato, è fatto riferimento alla "difesa e Forze armate; sicurezza dello Stato; armi, munizioni ed esplosivi" (lett. d).

Nella normazione primaria il concetto è stato invece ricondotto all'organizzazione del Sistema di informazione per la sicurezza della Repubblica (SISR) nell'ambito degli artt. 6 e 7 della legge del 3 agosto 2007, n. 124, recanti rispettivamente disciplina delle Agenzie informazioni e sicurezza esterna (AISE) e interna (AISI), ove viene fatto riferimento alle nozioni di «difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica» (art. 6) nonché alla «sicurezza interna della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica» (art. 7), ove precisiamo che le richiamate nozioni di "sicurezza della Repubblica" e "sicurezza dello Stato" sono sinonimi di "sicurezza nazionale". In particolare, la prima è stata oggetto di discussione in sede parlamentare in occasione della riforma del sistema di *intelligence* avvenuta con la richiamata L. 124/2007, ove l'espressione sicurezza della Repubblica è stata preferita ad altre definizioni in quanto «concetto [...] più ampio rispetto a quello di "Stato", utilizzato dalla L. 801/1977, che regolava in precedenza la materia»[81].

Tuttavia, l'assimilazione del compito di tutela della sicurezza nazionale (*rectius* sicurezza della Repubblica) agli apparati di *intelligence* non deve far pensare che tale funzione sia esclusivamente rimessa a tali Organismi. Come osserva Autorevole dottrina, tale visione porterebbe ad una "semplificazione culturale" che non tiene conto del fatto che la tutela della sicurezza nazionale interseca diverse competenze che portano l'*intelligence* a collaborare con altri attori istituzionali i quali, in una «funzione non monopolista, ma pluralista», sono rappresentati dalle forze di polizia, le forze armate, la diplomazia, fino ad estendersi, di fatto, a tutta la pubblica amministrazione[82].

Altro contributo è stato quello apportato dalla giurisprudenza della Corte Costituzionale a partire dalle due note sentenze del 1976 e 1977. Intervenendo in materia di segreto di Stato, con la prima pronuncia, il cui oggetto di discussione era «il diverso trattamento del segreto militare rispetto al segreto d'ufficio e professionale», la Corte ha qualificato le «notizie concernenti la forza, la preparazione o la difesa militare dello Stato» su cui trova applicazione la disciplina sul segreto militare, di cui all'art. 86 cod.pen.mil. Pace, come beni che involgono «il supremo interesse della sicurezza dello Stato nella sua personalità internazionale, e cioè l'interesse dello Stato-comunità alla

---

[80] L'art. 2 del decreto Legislativo n. 149/2011, prevede che lo scioglimento e la rimozione avvengano per responsabilità politica nel caso in cui venga accertata dalla Corte di Conti la sussistenza di un grave dissesto finanziario, con riferimento al disavanzo sanitario. In particolare la fattispecie che costituisce ipotesi di grave violazione di legge e che riguarda le Regioni assoggettate al piano di rientro, si configura al verificarsi di specifiche condizioni: a) il Presidente della Giunta regionale, nominato commissario ad acta non abbia adempiuto, in tutto o in parte, all'obbligo di redazione del piano di rientro o agli obblighi operativi, anche temporali, derivanti dallo stesso; b) si riscontri, in sede di verifica annuale, il mancato raggiungimento degli obiettivi imposti dal piano di rientro, con conseguente perdurare del disavanzo sanitario oltre la misura consentita dal piano medesimo o suo aggravamento. Tali ipotesi sono rincondotte alla diretta responsabilità, con dolo o colpa grave, del Presidente della Giunta regionale. Il Presidente rimosso è incandidabile alle cariche elettive e di governo a livello locale, regionale, nazionale ed europeo per dieci anni.

[81] Sul punto si rinvia al Dossier del Servizio studi della Camera sulla riforma dei servizi, n. 115, del 18 dicembre 2007, di cui al link:<https://documenti.camera.it/leg15/dossier/Testi/AC0349.htm>.

[82] M. VALENTINI, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Napoli, Editoriale scientifica, 2017, pp. 56 ss. Secondo Alcuni, l'estensione del concetto alla pubblica amministrazione può essere dedotta dall'interpretazione del dovere di difesa della Patria di cui all'art. 52 Cost., quale dovere di solidarietà politica che «non si riduce alla sola difesa in armi, [come difesa dal nemico esterno] essendo ben suscettibile di adempimenti attraverso la prestazione di adeguati comportamenti di impegno sociale non armato» (R. URSI, *op. cit*., p. 56).

propria integrità territoriale, indipendenza e - al limite - alla stessa sua sopravvivenza». Interesse che il giudice costituzionale ha inoltre ritenuto «presente e preminente su ogni altro in tutti gli ordinamenti statali, quale ne sia il regime politico che trova espressione, nel nostro testo costituzionale, nella formula solenne dell'art. 52, che proclama la difesa della Patria "sacro dovere del cittadino"» (Corte Cost., sent. del 14 aprile 1976, n. 82).

Con la seconda sentenza, questa volta avente ad oggetto una questione di legittimità costituzionale sugli artt. 342 e 352 c.p.p. nella parte in cui si riferiscono al «segreto politico o militare» (art. 342) ovvero a «segreti politici o militari dello Stato o altre notizie che possono nuocere alla sicurezza dello Stato o all'interesse politico, interno o internazionale, dello Stato» (art. 352), la Corte è intervenuta al fine di fornire una interpretazione costituzionalmente orientata di tali nozioni. Richiamando e sviluppando il precedente del '76, il giudice costituzionale ha ricondotto la sicurezza nazionale (*rectius* «supremo interesse della sicurezza dello Stato»), proprio al concetto di difesa della Patria, assimilando così i due concetti. In particolare, nella stessa pronuncia, la Corte, oltre al dovere di cui all'art. 52 Cost., ha individuato anche altri «elementi e momenti imprescindibili» dello Stato, meritevoli di protezione, quali l'indipendenza nazionale, i principi di unità e indivisibilità dello Stato (di cui all'art. 5 Cost.) nonché la formula «Repubblica democratica» che riassume i caratteri essenziali dello Stato (di cui all'art. 1 Cost.).

Sulla scorta di ciò la Corte concludeva che «si può, allora, parlare della sicurezza esterna ed interna dello Stato, della necessità di protezione da ogni azione violenta o comunque non conforme allo spirito democratico che ispira il nostro assetto costituzionale dei supremi interessi che valgono per qualsiasi collettività organizzata a Stato e che, come si è detto, possono coinvolgere la esistenza stessa dello Stato» (Corte Cost., sent. del 24 maggio 1977, n. 86).

Indirizzo interpretativo che è stato a fondamento anche delle successive pronunce n. 106/2009, n. 40/2012 e n. 24/2014[83].

La coincidenza della sicurezza nazionale con la difesa dello Stato, ci porta a dover approfondire quest'ultima funzione per meglio comprendere il primo concetto. Come è stato osservato, la difesa militare è un'attività che si è evoluta nel corso del tempo, tale da non poter più essere identificata con la tipica sicurezza dei profili esterni dello Stato, ma si è progressivamente spostata verso due direzioni, quella sovranazionale e quella interna[84].

Rispetto alla prima, il ripudio della guerra come strumento di offesa e l'adesione alle organizzazioni che assicurano la pace e la giustizia fra le Nazioni, come l'Organizzazione delle Nazioni Unite (ONU), quali principi dettati all'art. 11 Cost., ha incrementato la partecipazione italiana nelle missioni militari all'estero in operazioni di *peace keeping*, *peace enforcement* e *post-conflict peace building*[85]. Evoluzione questa che deve inoltre essere interpretata anche alla luce dell'esperienza europea, che inevitabilmente ha portato ad uno spostamento delle politiche di difesa oltre i confini nazionali.

Relativamente al profilo interno, la torsione dei compiti di difesa in quelli di sicurezza pubblica ha fatto seguito alla crescente esposizione dell'Italia alle minacce internazionali di tipo ibrido, ossia

[83] La giurisprudenza costituzionale in tema di sicurezza nazionale e segreto di Stato può essere consultata anche dal sito del Sistema di informazione per la sicurezza della Repubblica al link:<https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/giurisprudenza-di-riferimento.html>.

[84] R. URSI, *op. cit.*, pp. 55 ss.

[85] Sulle forze ONU v. E. CANNIZZARO, *Diritto internazionale*, ed. II, Torino, Giappichelli, 2014.

conflitti asimmetrici ove sono utilizzati mezzi e metodi non convenzionali[86], tali da aver richiesto l'impiego delle forze militari all'interno dello Stato. È il caso delle iniziative promosse per far fronte alla minaccia terroristica che, sebbene sul piano delle fonti ordinarie abbiano confermato la ricordata prassi della "normalizzazione dell'emergenza", sul piano amministrativo hanno portato alla convergenza funzionale di due ambiti prima di allora distinti quali quello delle forze di polizia e quello militare quando ricorrano ragioni di gravità e urgenza[87].

In conclusione, la difesa è quell'azione dello Stato che ha innanzitutto per oggetto l'integrità territoriale e la popolazione, quali presupposti oggettivi, e dimensioni spaziali e personali entro cui si muove il potere organizzato[88]. Pertanto, la nozione deve essere intesa in prima istanza come il complesso di attività poste a difesa delle forze politiche dominanti, rappresentate negli organi costituzionali e la loro organizzazione, nonché anche dell'intera collettività nazionale e relativa organizzazione, quali sintesi della difesa dello Stato nelle due accezioni di Stato-apparato e Stato-comunità[89].

Abbiamo inoltre evidenziato l'evoluzione di questo concetto che lo ha portato ad acquisire significati diversi dalla mera difesa militare. Si faccia riferimento alla ricordata L. 124/2007 la quale prevede che le attività dell'AISE e dell'AISI si svolgono a protezione oltre degli interessi politici e militari, anche di interessi «[...] economici, scientifici e industriali dell'Italia»[90].

Altra evoluzione del concetto è rappresentata dall'attività di difesa oltre i confini dello Stato in ragione della partecipazione dell'Italia alle organizzazioni internazionali e alla difesa europea, per finalità di realizzazione della pace e della sicurezza, conformemente alle regole del diritto internazionale[91].

Cambiamenti che rendono quindi necessario riflettere sul concetto di sicurezza nazionale in relazione alle attuali esigenze e ad un quadro disciplinare su più livelli che eleva il bene sicurezza a interesse non solo nazionale, ma anche europeo e internazionale.

Difatti, tornando al dilemma definitorio inziale, è stato osservato come in un simile contesto, «[i]l concetto di sicurezza non si presta ad essere definito in sede meramente statale [ove] percezioni umane e condizionali sociali peculiari [...] potrebbero rappresentare un terreno di rafforzamento del "sovranismo" nazionale degli Stati membri», ma deve necessariamente essere definito alla luce dei

---

[86] Sui concetti di guerra asimmetrica ibrida si rinvia a M. BRESSAN, G. CUZZELLI, *Da Clausewitz a Putin: la guerra nel XXI secolo*, Milano, Ledizioni, 2022; C. JEAN, Guerre asimmetriche, infowar e nuova geopolitica, in Aspenia

[87] E. CHITI, *Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia e di difesa*, in L. FORNI, T. VETTOR, *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017, pp. 63 ss. v. anche F. PASTORE, *Il coordinamento delle forze di polizia e di sicurezza italiane nella lotta al terrorismo*, in *Dirittifondamentali.it*, fasc. 2, 2021, reperibile al link:<https://dirittifondamentali.it/wp-content/uploads/2021/05/Pastore-Il-coordinamento-delle-forze -di-polizia-e-di-sic urezza-italiane.pdf>.

[88] Cfr. G. DE VERGOTTINI, *Difesa*, in N. BOBBIO, N. MATTEUCCI, G. PASQUINO (diretto da), *Dizionario di politica*, Torino, Utet, 1990, pp. 299 ss.

[89] *Ibidem*.

[90] Cfr. art. 6, co. 2, e art. 7, co. 2, L. 124/2007. Sul punto vedi anche C. JEAN, P. SAVONA, *Intelligence economica. Il ciclo dell'informazione nell'era della globalizzazione*, Catanzaro, Rubettino, 2011.

[91] Sul punto si rinvia al codice dell'ordinamento militare, il d.Lgs. 15 marzo 2010, n. 66 (brevemente c.o.m.), ove all'art. 89, co. 4 c.o.m, relativo ai compiti delle Forze armate è previsto che «[i]n caso di conflitti armati e nel corso delle operazioni di mantenimento e ristabilimento della pace e della sicurezza internazionale i comandanti delle Forze armate vigilano, in concorso, se previsto, con gli organismi internazionali competenti, sull'osservanza delle norme di diritto internazionale umanitario».

principi e dei valori non solo della Costituzione italiana, ma anche dell'impianto costituzionale europeo e delle carte internazionali di cui l'Italia è firmataria[92].

3.2. Ordine e sicurezza pubblica

L'ordine pubblico e la sicurezza pubblica sono concetti che trovano definizione all'interno dell'art. 159 del decreto Legislativo 31 marzo 1998, n. 112, recante disciplina sul conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59. In particolare al comma 2 del disposto si apprende che

> Le funzioni ed i compiti amministrativi relativi all'ordine pubblico e sicurezza pubblica di cui all'articolo 1, comma 3, lettera l), della legge 15 marzo 1997, n. 59, [ossia ordine pubblico e sicurezza pubblica] concernono le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, inteso come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle istituzioni, dei cittadini e dei loro beni.

Si tratta tuttavia di una formulazione che tiene conto degli sviluppi della giurisprudenza costituzionale sul punto, la quale nel tempo è andata anche a dettagliare i contorni della nozione che non è stata esente di critiche. Proponiamo pertanto una lettura evolutiva del concetto alla luce di alcune pronunce del Giudice delle leggi ritenute rilevanti in materia e delle relative problematiche che l'interpretazione del concetto ancora solleva.

La prima riguarda innanzitutto l'endiadi "sicurezza pubblica" e "ordine pubblico". Con la sentenza n. 2 del 14 giugno 1956, la Corte costituzionale avocata in un giudizio di legittimità in via incidentale sulla compatibilità con l'art. 16 Cost. delle limitazioni alla libertà di circolazione e soggiorno per motivi di «ordine, sicurezza pubblica e pubblica moralità» previsti nel R.D. 18 giugno 1931, n. 773 (Testo unico delle leggi di pubblica sicurezza - TULPS) riteneva che

> [e]sclusa l'interpretazione, inammissibilmente angusta, che la "sicurezza" riguardi solo l'incolumità fisica, sembra razionale e conforme allo spirito della Costituzione dare alla parola "sicurezza" il significato di situazione nella quale sia assicurato ai cittadini, per quanto è possibile, il pacifico esercizio di quei diritti di libertà che la Costituzione garantisce con tanta forza. Sicurezza si ha quando il cittadino può svolgere la propria lecita attività senza essere minacciato da offese alla propria personalità fisica e morale; è l'"ordinato vivere civile", che è indubbiamente la meta di uno Stato di diritto, libero e democratico.

Nella stessa sede, a proposito del riferimento alle «persone pericolose per l'ordine e la sicurezza pubblica o per la pubblica moralità» (art. 157, co. 2, TULPS), precisava che

> la pericolosità in riguardo all'ordine pubblico non può consistere in semplici manifestazioni di natura sociale o politica, le quali trovano disciplina in altre norme di legge, bensì in manifestazioni esteriori di insofferenza o di ribellione ai precetti legislativi ed ai legittimi ordini della pubblica Autorità, manifestazioni che possono facilmente dar luogo a stati di allarme e a violenze, indubbiamente minacciose per la "sicurezza" della generalità dei cittadini, i quali finirebbero col vedere, essi, limitata la propria libertà di circolazione.

Con questa prima pronuncia la Corte andava quindi a ricondurre integralmente il concetto di "ordine pubblico" con quello di "sicurezza pubblica" sulla base di un'argomentazione logica

[92] Cfr. A. STERPA, *La sicurezza, la legalità e la certezza del diritto*, in A. STERPA, A. COIANTE, *Sicurezza legalità ed economia*, Napoli, Editoriale scientifica, 2020, p. 16.

riconducibile al fatto che senza sicurezza non c'è ordine, e senza ordine non c'è sicurezza[93]. Successivamente, in un caso afferente ai limiti alla libertà di espressione di cui all'art. 21 Cost., la Corte con la sentenza 8 marzo 1962, n. 19, affermava che

> L'esigenza dell'ordine pubblico, per quanto altrimenti ispirata rispetto agli ordinamenti autoritari, non è affatto estranea agli ordinamenti democratici e legalitari, né è incompatibile con essi. In particolare, al regime democratico e legalitario, consacrato nella Costituzione vigente, e basato sull'appartenenza della sovranità al popolo (art. 1), sull'eguaglianza dei cittadini (art. 3) e sull'impero della legge (artt. 54, 76-79, 97-98, 101, ecc.), è connaturale un sistema giuridico, in cui gli obiettivi consentiti ai consociati e alle formazioni sociali non possono essere realizzati se non con gli strumenti e attraverso i procedimenti previsti dalle leggi, e non è dato per contro pretendere di introdurvi modificazioni o deroghe attraverso forme di coazione o addirittura di violenza. Tale sistema rappresenta l'ordine istituzionale del regime vigente; e appunto in esso va identificato l'ordine pubblico del regime stesso. Non potendo dubitarsi che, così inteso, l'ordine pubblico è un bene inerente al vigente sistema costituzionale, non può del pari dubitarsi che il mantenimento di esso - nel senso di preservazione delle strutture giuridiche della convivenza sociale, instaurate mediante le leggi, da ogni attentato a modificarle o a renderle inoperanti mediante l'uso o la minaccia illegale della forza - sia finalità immanente del sistema costituzionale. Se per turbamento dell'ordine pubblico bisogna intendere l'insorgere di un concreto ed effettivo stato di minaccia per l'ordine legale mediante mezzi illegali idonei a scuoterlo - ed è da escludere che possa intendersi altro -, è perciò chiaro che non possono esser considerate in contrasto con la Costituzione le disposizioni legislative che effettivamente, e in modo proporzionato, siano volte a prevenire e reprimere siffatti turbamenti. Né può costituire impedimento all'emanazione di disposizioni del genere l'esistenza di diritti costituzionalmente garantiti. Infatti, la tutela costituzionale dei diritti ha sempre un limite insuperabile nella esigenza che attraverso l'esercizio di essi non vengano sacrificati beni, ugualmente garantiti dalla Costituzione. Il che tanto più vale, quando si tratta di beni che - come l'ordine pubblico - sono patrimonio dell'intera collettività.

In questa occasione la Corte superava la precedente accezione, avviata con la pronuncia del '31, di ordine pubblico ideale, ossia identificato con l'ordinamento in quanto sistema normativo o istituzionale dello Stato in un determinato momento storico, addivenendo all'accezione di ordine pubblico materiale, quale «bene inerente al vigente sistema costituzionale [e] finalità immanente del sistema costituzionale» connesso agli interessi dei consociati e ai fatti che ne ledono i beni, la cui tutela consente la compressione dell'esercizio di diritti costituzionalmente garantiti[94]. Cosicché la restrizione delle libertà non avviene quando queste presentino contenuti dissonanti rispetto ai valori costituzionali (ordine pubblico ideale), ma solo quando il comportamento si traduca in un turbamento per l'ordine pubblico materiale[95].

Come sarà poi sintetizzato dalla stessa Corte nelle successive pronunce, l'accezione di ordine pubblico argomentata nel '62 vede tale concetto come limite implicito alle libertà in quanto «ordine legale sul quale poggia la civile convivenza» (Corte cost., 29 dicembre 1972, n. 199; 3 agosto 1976, n. 210; 9 maggio 1985, n. 138)[96].

Altra questione è quella che ha interessato la distinzione tra le c.d. funzioni di polizia amministrativa e polizia di sicurezza. Con sentenza del 25 febbraio 1988, n. 218, la Corte costituzionale, in un giudizio per conflitto di attribuzione tra enti, riepilogava dell'ordine pubblico

---

[93] R. URSI, *op. cit.*, p. 62.

[94] Cfr. R. URSI, *op. cit.*, pp. 63-64.

[95] M. MAZZAMUTO, *Poteri di polizia e ordine pubblico*, in *Dir. Amm.*, nn. 3-4, 1998, p. 548.

[96] Come evidenziato da Alcuni, il riferimento all'ordine legale da parte della Corte intende richiamare la tradizione giuridica francese interpretando quindi l'ordine pubblico come ordine giuridico formato dall'insieme delle regole che disciplinano le azioni dei cittadini. In questi termini l'ordine pubblico si idenfica quindi con la legalità, e la sicurezza nel rispetto delle leggi.

quale concetto il cui contenuto è costituito «da quei beni giuridici fondamentali o da quegli interessi pubblici primari sui quali, in base alla Costituzionale e alle leggi ordinarie, si regge l'ordinata e civile convivenza dei consociati nella comunità nazionale» e a tal proposito indicava alcuni di tali interessi «fra i quali rientrano l'integrità fisica e psichica delle persone, la sicurezza dei possessi e il rispetto o la garanzia di ogni altro bene giuridico di fondamentale importanza per l'esistenza e lo svolgimento dell'ordinamento» i quali rappresentano il nucleo delle funzioni di polizia di pubblica sicurezza. Nella stessa sede la Corte puntualizza che i compiti di polizia di sicurezza «riguardano le misure preventive e repressive dirette al mantenimento dell'ordine pubblico e, pertanto, si riferiscono alle attività tradizionalmente ricomprese nei concetti di polizia giudiziaria e di quella di pubblica sicurezza (in senso stretto)», quelle di polizia amministrativa concerne invece «le attività di prevenzione o di repressione dirette a evitare danni o pregiudizi che possono essere arrecati alle persone o alle cose nello svolgimento di attività ricomprese nelle materie sulle quali si esercitano le competenze regionali (sanità, turismo, cave e torbiere, etc.), senza che ne risultino lesi o messi in pericolo i beni o gli interessi tutelati in nome dell'ordine pubblico».

Nel 2001 la Corte, nuovamente chiamata a pronunciarsi sulla differenza tra compiti di polizia amministrativa e quelli di polizia di sicurezza, andava a precisare il contenuto di questi ambiti, chiarendo che la definizione di ordine pubblico e sicurezza «nulla aggiunge alla tradizionale nozione [...]», che «riserva allo Stato [...] le funzioni primariamente dirette a tutelare beni fondamentali, quali l'integrità fisica o psichica delle persone, la sicurezza dei possessi ed ogni altro bene che assume primaria importanza per l'esistenza stessa dell'ordinamento». Non qualsiasi interesse pubblico alla cui cura siano preposte le pubbliche amministrazioni, dunque, «ma soltanto quegli interessi essenziali al mantenimento di una ordinata convivenza civile». Siffatta precisazione «è necessaria ad impedire che una smisurata dilatazione della nozione di sicurezza e ordine pubblico si converta in una preminente competenza statale in relazione a tutte le attività che vanificherebbe ogni ripartizione di compiti tra autorità statali di polizia e autonomie locali».

Come noto, nel 2001 veniva inoltre riformato il Titolo V della Costituzione, da cui veniva espunto qualsiasi riferimento all'«interesse nazionale»[97], e nell'elenco delle materie riservato alla competenza esclusiva dello Stato di cui all'art. 117, co. 2, lett. h), venivano collocati l'«ordine pubblico e sicurezza, ad esclusione della polizia amministrativa locale».

Il nuovo dettato sembra pertanto seguire l'orientamento interpretativo della Corte argomentato nello stesso anno, distinguendo espressamente i compiti di polizia di sicurezza da quelli di polizia amministrativa, e riservando i primi alla esclusiva competenza statale.

Tuttavia che nel corso degli anni la stessa Corte, ricorrendo al criterio della prevalenza, ha ricondotto nella materia dell'ordine pubblico e sicurezza, ambiti materiali diversi tra loro e caratterizzati da funzioni non coercitive come: la sicurezza stradale (Corte cost., 26 luglio 2002, n. 407); la disciplina dei giochi d'azzardo (Corte cost., 22 giugno 2006, n. 237); la sicurezza aeroportuale (Corte cost., 7 marzo 2008, n. 51); la regolamentazione dei beni sequestrati o confiscati alla criminalità organizzata (Corte cost., 2 dicembre 2011, n. 325; 23 febbraio 2012, n. 34); la

[97] R. BIN, *L'interesse nazionale dopo la riforma: continuità dei problemi, discontinuità della giurisprudenza costituzionale*, in *Le Regioni, Bimestrale di analisi giuridica e istituzionale*, n. 6, 2001, p. 1213, reperibile al link:<https://www.rivisteweb.it/doi/10.1443/5612>, nonché sul punto si rinvia anche a B. CARAVITA, *In tema di "interesse nazionale" e riforme istituzionali*, in *federalismi.it*, n. 6, 2003, reperibile al link:<https://www.federalismi.it/nv14/editoriale.cfm?eid=10&content=In%2Btema%2Bdi%2B%27%27interesse%2Bnazionale%27%27%2Be%2Briforme%2Bistituzionali&content_auth=Beniamino%2BCaravita%2Bdi%2BToritto>.

disciplina dell'assegnazione delle bande orarie negli aeroporti (Corte cost., 30 gennaio 2009, n. 18); la tracciabilità dei flussi finanziari (Corte cost., 12 marzo 2015, n. 33)[98].

Tale opera interpretativa ha portato ad una estensione del concetto di sicurezza che si interseca con la ripartizione delle ricordate funzioni di polizia tra Stato centrale e governo del territorio, evidenziando due livelli di sicurezza.

A tal proposito, nella sentenza del 23 dicembre 2019, n. 285, la Corte costituzionale, riprendendo la distinzione operata nel 2001 tra la «polizia locale urbana e rurale», di competenza concorrente, e le altre funzioni rientranti nella nozione di polizia amministrativa, trasferite alle Regioni come funzioni accessorie rispetto agli ambiti materiali loro attribuiti, da un lato, e le attribuzioni «attinenti alla sicurezza pubblica, riservate in via esclusiva allo Stato, ha ricordato che per costante orientamento della Corte, l'endiadi «ordine pubblico e sicurezza», di cui all'art. 117, comma e, let. h), Cost., allude a una materia in senso proprio, e cioè a una materia oggettivamente delimitata che di per sé non esclude l'intervento regionale in settori ad essa liminari. Il Giudice costituzionale individuava così che

> accanto al nucleo duro della sicurezza di esclusiva competenza statale, [l'ordinamento conosce] discipline regionali in settori prossimi ancorché con essa non coincidenti. La sicurezza può ben assumere una possibile declinazione pluralista, coerente con la valorizzazione del principio autonomistico di cui all'art. 5 della Costituzione: ad una sicurezza in «senso stretto» (o sicurezza primaria) può essere affiancata, infatti, una sicurezza «in senso lato» (o sicurezza secondaria), capace di ricomprendere un fascio di funzioni intrecciate, corrispondenti a plurime e diversificate competenze di spettanza anche regionale. Alle Regioni è così consentito realizzare una serie di azioni volte a migliorare le condizioni di vivibilità dei rispettivi territori, nell'ambito di competenze ad esse assegnate in via residuale o concorrente, come, ad esempio, le politiche (e i servizi) sociali, la polizia locale, l'assistenza sanitaria, il governo del territorio.

4. La sicurezza nell'ordinamento europeo

La dottrina ha individuato almeno tre questioni di sicurezza che possono rilevare nel diritto dell'Unione europea: quando uno Stato membro deroga (o domanda di derogare) al complesso di principi e norme europee per ragioni di sicurezza interna, quali ordine pubblico o sicurezza nazionale; quando l'Unione europea intende prendere decisioni per garantire la sicurezza dell'Unione stessa; ovvero quando uno Stato membro agisca nell'esercizio di potersi delegati dall'Unione europea, come ad esempio nel caso dell'applicazione di misure restrittive PESC o del terrorismo internazionale, o con riferimento all'entrata o espulsione di un individuo per motivi di sicurezza[99].

Se ci poniamo dal punto di vista degli ordinamenti, i tre casi sintetizzano bene la sicurezza nella dimensione europea. Il processo di integrazione, che come noto non è mai culminato in un'Unione

---

[98] Cfr. R. URSI, *op. cit.*, p. 70.

[99] Cfr. S. PEERS, *National Security and European Law*, in *Yearbook of European Law*, vol 16, Issue 1, 1996, p. 363 reperibile al link:<https://academic.oup.com/yel/article/16/1/363/1718740>, v. anche A. ALÌ, *Il diritto dell'Unione Europea e la tutela della sicurezza nazionale degli Stati membri. Osservazioni a margine di alcuni casi esaminati dalla Corte di giustizia dell'Unione Europe*, in U. GORI, L. MARTINO, *Intelligence e interesse nazionale*, Aracne, 2015, pp. 593-604.

federale[100], ci porta infatti a dover considerare la sicurezza europea su due piani: quello degli Stati membri che, come ricordato, possono derogare agli obblighi funzionali alla garanzie delle libertà poste a fondamento del mercato comune; e quello dell'Unione in sè, ove devono ulteriormente distinguersi la tutela della sicurezza interna europea, afferente allo Spazio di libertà, sicurezza e giustizia (SLSG), dalla sicurezza dei profili esterni dell'Unione, ossia la Politica di sicurezza e difesa comune (PSDC).

La sicurezza nel contesto europeo si atteggia pertanto a fattore limitante delle libertà del mercato unico quando invocata dagli Stati membri, a obiettivo comune quando l'Unione agisce a protezione della sicurezza dei cittadini europei. In quest'ultimo caso riteniamo che l'azione dell'Unione vada oltre lo SLSG e la PSDC, stante la presenza nel TFUE di riferimenti settoriali alla sicurezza (come la sicurezza degli approvvigionamenti nel settore agricolo all'art. 39, lett. d)[101], la sicurezza dei trasporti all'art. 91, lett. c)[102], la sicurezza dei consumatori all'art. 169[103], la sicurezza dell'approvvigionamento energetico dell'Unione all'art. 194, lett. b)[104]), nonché il riferimento al *right to social security* (sicurezza e protezione sociale nel testo italiano) quale diritto equivalente alle forme di assistenza e previdenza sociale che conosciamo nel nostro ordinamento (vedi agli artt. 21, 48 e 153, par. 1, lett. c e par. 4).

Inoltre, l'art. 114, par. 3 del TFUE prevede che la Commissione possa adottare proposte legislative «in materia di sanità, sicurezza, protezione dell'ambiente e protezione dei consumatori» basandosi su un livello di protezione elevato, tenuto anche conto degli sviluppi fondati su riscontri scientifici.

---

[100] Sul punto v. R. DUCCI, B. OLIVI, *L'europa incompiuta*, Padova, Cedam, 1970; R. H. RAINERO (a cura di), *Storia dell'integrazione europea*, Milano, Marzorati, 1997; L. LEVI, *Unificazione europea*, in in N. BOBBIO, N. MATTEUCCI, G. PASQUINO, *Dizionario di politica*, Torino, 1990, pp. 1198 ss.

[101] Cfr. art. 39, par. 1, lett. d), TFUE il quale prevede che «Le finalità di politica agricola comune sono: [...] d) garantire la sicurezza degli approvvigionamenti». Si tratta di un obiettivo caratterizzante ogni politica agricola, la cui realizzazione può essere affidata tanto a misure che assicurino l'autosufficienza dell'Unione - quali l'ammasso pubblico, sussidi alla produzione o politiche di sostegno dei prezzi - quanto alla conclusione di accordi commerciali preferenziali con Paesi terzi (C. CATTABRIGA, L. VISAGGIO, *Commento all'art. 39 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014, p. 627).

[102] Cfr. art. 91, par. 1, lett. c), ove dispone che «[a]i fini dell'applicazione dell'art. 90 e tenuto conto degli aspetti peculiari dei trasporti, il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale e del Comitato delle regioni, stabiliscono: [...] c) le misure atte a migliorare la sicurezza dei trasporti». Il disposto è stato introdotto dal Trattato di Maastricht ed ha valore ricognitivo della giurisprudenza della Corte di giustizia sul punto (L. SCHIANO DI PEPE, *Commento all'art. 91 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014, pp. 966 ss.).

[103] Cfr. art. 169, par. 1, TFUE, che prevede «[a]l fine di promuovere gli interessi dei consumatori ed assicurare un livello elevato di protezione dei consumatori, l'Unione contribuisce a tutelare la salute, la sicurezza e gli interessi economici dei consumatori nonché a promuovere il loro diritto all'informazione, all'educazione e all'organizzazione per la salvaguardia dei propri interessi». Anche in questo caso il disposto intende fissare un insieme di obiettivi, tra cui anche quello della sicurezza, che avevano già trovato applicazione per mezzo di diversi atti di diritto derivato, come la Direttiva 88/378/CEE sulla sicurezza dei giocattoli, poi sostituita dalla Direttiva 2009/48/CE, e della giurisprudenza della Corte di giustizia in tali ambiti (P. MENGOZZI, *Commento all'art. 169 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014, pp. 966 ss.).

[104] Cfr. art. 194, par. 1, lett. b), di cui «[n]el quadro dell'instaurazione o del funzionamento del mercato interno e tenendo conto dell'esigenza di preservare e migliorare l'ambiente, la politica dell'Unione nel settore dell'energia è intesa, in uno spirito di solidarietà tra Stati membri, a: [...] b) garantire la sicurezza dell'approvvigionamento energetico nell'Unione». La sicurezza dell'approvvigionamento energetico con il Trattato di Lisbona è stata integralmente ricondotta nel campo applicativo dei Trattati, superando così la diffidenza degli Stati ad affidare all'Unione un'azione così complessa (M. MARLETTA, *Commento art. 194 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014, pp. 1656 ss.).

4.1. I concetti di ordine pubblico e sicurezza nazionale per l'ordinamento europeo

Nonostante il processo di integrazione abbia interessato molti ambiti prima di competenza nazionale, la tutela della sicurezza è restata una prerogativa sovrana degli Stati che non hanno mai interamente ceduto all'Unione. La questione apre al rilevante tema della delimitazione delle competenze tra Stati membri e Unione europea rispetto alla tutela dell'ordine pubblico e della sicurezza nazionale[105]. Innanzitutto, l'art. 5, par. 2, TUE stabilisce che «[i]n virtù del principio di attribuzione, l'Unione agisce esclusivamente nei limiti delle competenze che le sono attribuite dagli Stati membri nei trattati per realizzare gli obiettivi da questi stabiliti. Qualsiasi competenza non attribuita all'Unione nei trattati appartiene agli Stati membri».

Conformemente a ciò, il par. 2, dell'art. 4, TUE specifica che:

> L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali. Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro [enfasi aggiunta][106].

Tale elencazione, non esaustiva, è frutto dell'accordo raggiunto nel Consiglio europeo di Bruxelles del 21-22 giugno 2007, ove, su richiesta del Regno unito[107], venne introdotta la tutela della sicurezza nazionale, individuata come competenza statale permanente[108], senza tuttavia fornire elementi utili per la sua interpretazione. Fatta una breve panoramica delle clausole limitative delle competenze ci si deve infatti chiedere che significato abbiano tali espressioni, che afferiscono ad ambiti di discrezionalità statale per l'ordinamento europeo.

---

[105] A. ALÌ, *Il diritto dell'Unione europea e la tutela della sicurezza nazionale degli Stati membri. Osservazioni a margine di alcuni casi esaminati dalla Corte di giustizia dell'Unione europea*, in U. GORI, L. MARTINO, *Intelligence e interesse nazionale*, Roma, Aracne, 2015, pp. 593 ss. Per uno studio comparato dal punto di vista delle scienze politiche sul concetto di sicurezza nazionale negli ordinamenti europei si rinvia a A. KATTLER, F. ETTENSPERGER, *National internal security policies across Europe – a comparative analysis applying big data clustering techniques*, in *Political Research Exchange*, vol. 2, 2020, repribile al link:<https://www.tandfonline.com/doi/full/10.1080/2474736X.2020.1787796? scroll=top&needAccess=true>.

[106] Dalla prospettiva del diritto internazionale, secondo una certa dottrina la clausola deve essere intesa come ricognitiva del principio di diritto internazionale generale relativo alla sovrana uguaglianza degli Stati ove lo Stato agisce in autotutela a preservare l'integrità territoriale (C.C. GIALDINO (diretto da), *Codice dell'Unione Europea operativo: TUE e TFUE commentati articolo per articolo, con la carta dei diritti fondamentali dell'Unione Europea*, Napoli, Simone, 2012, pp. 77 ss.). Il primo comma del disposto, il quale richiamando l'art. 5 TUE dispone che «qualsiasi competenza non attribuita all'Unione nei trattati appartiene agli Stati membri» è collegato al secondo, poiché tra le prerogative dello fondamentali dello Stato non rientra solo la sua organizzazione in senso stretto, ma anche il sistema delle competenze non attribuite all'Unione tra cui anche quella della sicurezza nazionale (M.C. BARUFFI, *Commento art. 4 TUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, Cedam, 2014, pp. 14 ss.). Sul punto v. anche M. CARTABIA, *Commento art. 4, par. 2, TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014, pp. 23 ss.

[107] J.C. PIRIS, *Il Trattato di Lisbona*, Milano, Giuffrè, 2013, p. 224.

[108] G. GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, Roma-Bari, Laterza, 2020, p. 12. Tale clausola di competenza statale permanente, aggiunta su esplicita richiesta del Regno Unito, deve essere inoltre letta in combinato disposto con l'art. 276 del TFUE, che esclude il controllo da parte della Corte di Giustizia sulla «validità o la proporzionalità di operazioni condotte dalla polizia o da altri servizi incaricati dell'applicazione della legge di uno Stato membro o l'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna».

Relativamente al concetto di sicurezza nazionale, la questione non è di secondario rilievo poiché in un'altra disposizione dei Trattati, l'art. 346 del TFUE[109], viene fatto riferimento agli «interessi essenziali della propria sicurezza» quale limite alla divulgazione di informazioni da parte dello Stato membro alle istituzioni europee (v. art. 4, par. 3, TUE), e alla Commissione di richiederle (art. 337 TFUE); e quale presupposto legittimante il mercato delle armi, munizioni e materiale bellico[110].

Come ha precisato la Corte di giustizia, il riferimento agli "interessi essenziali della propria sicurezza" non può riguardare aspetti economici[111], dovendo piuttosto essere ricondotta al rispetto della sovranità nazionale, integrità territoriale e politica di difesa degli Stati membri[112]. Orientamento che ha trovato conferme anche nella dottrina che ha ritenuto tale nozione più ristretta rispetto a quella di sicurezza nazionale di cui all'art. 4, par. 2 TUE[113].

Tuttavia, stante la riserva di sovranità permanente di cui al citato art. 4 TUE, non è possibile individuare una definizione chiara del concetto di sicurezza nazionale al di là di quanto ritenuto dalla Corte di giustizia secondo cui «la sicurezza nazionale [...] costituisce attività dello Stato o delle autorità statali non correlate ai campi di attività degli individui»[114].

Sulle nozioni di "ordine pubblico", "pubblica sicurezza" e "salute pubblica", negli anni '70 l'Avvocato generale Warner, nella causa 30/77, *Regina c. Pierre Buchererau,* osservò che «gli autori del trattato intendessero con esse contraddistinguere tre nozioni diverse anche se, forse,

---

[109] Il testo dell'art. 346 TFUE (ex articolo 296 del TCE) prevede che «1. Le disposizioni dei trattati non ostano alle norme seguenti: a) nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza; b) ogni Stato membro può adottare le misure che ritenga necessarie alla tutela degli interessi essenziali della propria sicurezza e che si riferiscano alla produzione o al commercio di armi, munizioni e materiale bellico; tali misure non devono alterare le condizioni di concorrenza nel mercato interno per quanto riguarda i prodotti che non siano destinati a fini specificamente militari. 2. Il Consiglio, deliberando all'unanimità su proposta della Commissione, può apportare modificazioni all'elenco, stabilito il 15 aprile 1958, dei prodotti cui si applicano le disposizioni del paragrafo 1, lettera b)».

[110] Il disposto introduce due eccezioni alla libera circolazione delle informazioni e del materiale bellico mediante l'introduzione di una clausola di salvaguardia. Tali ipotesi devono considerarsi tassative e non costituiscono una clausola generale di esclusione del diritto dell'Ue. Difatti lo Stato membro è tenuto a provare che le misure derogatorie siano necessarie a tutelare gli «interessi essenziali della propria sicurezza», anche se le autorità nazionali godono di una certa discrezionalità sul punto (v. causa T-26/01, Fiocchi munizioni). Inoltre, relativamente all'ipotesi b), le misure adottate dallo Stato «non devono alterare le condizioni di concorrenza del mercato interno», a ciò la Commissione di concerto con lo Stato interessato, esamina le condizioni per rendere tali misure conformi ai Trattati e tal fine, in deroga all'art. 258 TFUE, la Commissione o qualsiasi Stato membro possono ricorrere direttamente alla Corte di giustizia se ritengono che un altro Stato membro faccia un uso abusivo dei poteri di cui all'art. 346 TFUE (I. PALANDRI, *Commento art. 346 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, Cedam, 2014, pp. 1546). Si precisa inoltre, relativamente all'ipotesi a), che il rifiuto di fornire informazioni è legittimo solo da parte degli Stati, alle condizioni di cui sopra, ma non anche alle imprese (v. F. SCIAUDONE, *Commento art. 346 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014, p. 2517).

[111] *Ex multis*, Corte di Giust., sent. 14 marzo 2000, causa C-54/99, pt. 17, relativa al regime francese di *golden share*, ove il giudice europeo ha ritenuto che «se è pur vero che gli Stati membri restano sostanzialmente liberi di determinare, conformemente alle loro necessità nazionali, le esigenze dell'ordine pubblico e della pubblica sicurezza, resta il fatto che tali motivi, nel contesto comunitario, particolarmente in quanto autorizzano una deroga al principio fondamentale della libera circolazione dei capitali, devono essere intesi in senso restrittivo, di guisa che la loro portata non può essere determinata unilateralmente da ciascuno Stato membro senza il controllo delle istituzioni comunitarie [...]. L'ordine pubblico e la pubblica sicurezza possono essere quindi invocati solamente in caso di minaccia effettiva ed abbastanza grave ad uno degli interessi fondamentali della collettività [...]. Tali motivi non possono essere inoltre distolti dalla loro propria funzione per essere utilizzati, in realtà, a fini puramente economici».

[112] I. PALANDRI, *Commento all'art. 346 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, 2014, p. 1546.

[113] A. ALÌ, *Il diritto dell'Unione europea e la tutela della sicurezza nazionale degli Stati membri. …op. cit.*, p. 597.

[114] CGUE, sentenza del 28 gennaio 2008, *Productores de Música de España (Promusicae) v Telefónica de España SAU*.

sovrapponendosi l'una all'altra [...] per il resto, gli autori del trattato sembrano aver voluto lasciare al diritto comunitario derivato ed alla giurisprudenza di questa Corte il compito di definire ed elaborare la nozione di "ordine pubblico"»[115]. In quella sede la Corte di giustizia ebbe infatti modo di indicare il contenuto dell'espressione "ordine pubblico" tenendo tuttavia conto del fatto che un'interpretazione troppo ristretta avrebbe escluso qualsiasi valutazione unilaterale da parte degli Stati membri, dall'altro, riconoscendo il carattere relativo della nozione che può variare in base alle epoche e agli ordinamenti, riteneva di dover lasciare alle competenti autorità nazionali un certo grado di discrezionalità entro i limiti posti dai trattati. Così la Corte concluse che la nozione non comprende solo la perturbazione dell'ordine sociale insita in qualsiasi infrazione di legge, ma presuppone anche un elemento in più, ossia «l'esistenza di una minaccia effettiva ed abbastanza grave agli interessi fondamentali della collettività» (pt. 35 motivi).

Formulazione che è stata poi recepita anche a livello normativo. Si faccia riferimento al considerando 41 della Direttiva 2006/123, relativa ai servizi nel mercato interno, ove il legislatore europeo, aderendo all'indirizzo della Corte di giustizia ha definito l'ordine pubblico come concetto comprensivo «la protezione contro una minaccia effettiva e sufficientemente grave per uno degli interessi fondamentali della collettività e può includere, in particolare, questioni legate alla dignità umana, alla tutela dei minori e degli adulti vulnerabili ed al benessere degli animali» e precisando che analogamente, «la nozione di pubblica sicurezza comprende le questioni di incolumità pubblica».

Si consideri inoltre, escluso il concetto di sicurezza nazionale che, come intuibile, ha una accezione prevalentemente nazionale essendo una prerogativa sovrana riservata alla competenza dei soli Stati ex art. 4, par. 2 TUE, l'ordine pubblico è invece un concetto che può essere colto sotto diverse dimensioni, sia degli ordinamenti interni, sia degli ordinamenti sovranazionali. Nel particolare caso dell'ordinamento europeo tali piani sono stati ritenuti fortemente connessi arrivando a maturare un significato autonomo nell'ordinamento europeo, il c.d. ordine pubblico europeo, distinto dall'ordine pubblico nazionale[116].

---

[115] Conclusioni dell'Avvocato generale Jean-Pierre Warner del 28 settembre 1977, causa C-30/77 (*Regina c. Boucherau*).

[116] Si tratta di un concetto che fino al Trattato di Maastricht coincideva con l'ordine pubblico economico, e che acquisterà valore anche politico dopo la firma del Trattato, sul punto v. conclusioni Avvocato generale Mayras, sentenza 4 dicembre 1974, causa 41/74, *van Duyn*. In letteratura v. D. RINOLDI, *L'ordine pubblico europeo*, Napoli, Editoriale scientifica, 2005; ID, *Ordine pubblico europeo e spazio giuridico continentale*, in U. DRAETTA, N. PARISI, D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia dell'Unione europea: principi fondamentali e tutela dei diritti*, Napoli, Editoriale Scientifica, 2007; F. ANGELINI, *Ordine pubblico e integrazione costituzionale europea. I principi fondamentali nelle relazioni tra interordinamentali*, Padova, Cedam, 2007, ove l'A. individua una nozione di ordine pubblico comunitario sia dall'azione interpretativa della Corte di giustizia nella sentenza *Eco Swiss c. Benetton*, causa 126/97, ove la Corte «fa valere l'eccezione per motivi di ordine pubblico nella funzione tipica del diritto internazionale privato, assimilabile alla nozione consacrata dall'art. 27, co. 1, della Convenzione di Bruxelles, finalizzata ad evitare la produzione di effetti dei giudizi contrari ai principi contrari all'ordine pubblico», nonché nei Trattati dell'Unione ed infine nella costituzione dello Spazio di libertà, sicurezza e giustizia (pp. 196 ss). V. anche G. CALESINI, *Diritto europeo di polizia*, Roma, Laurus Robuffo, 2007, pp. 211 ss. ove l'A. ritiene che nel sistema giuridico europeo, l'espressione ordine pubblico europeo è relativa, potendosi intendere come il comune denominatore degli ordini pubblici nazionali, come la concezione europea dell'ordine pubblico nazionale o come ordine pubblico delle istituzioni europee. Alla luce di ciò, l'A. ritiene che una concezione europea di ordine pubblico ideale "inteso come insieme dei principi fondamentali costitutivi dell'equilibrio dell'ordinamento sia rinvenibile nella Carta di Nizza. O. FERACI, *L'ordine pubblico nel Diritto dell'Unione europea*, Milano, Giuffrè, 2012, pp. 323 ss.

4.2. La sicurezza come interesse collettivo europeo. SLSG e PSDC tra integrazione economica e politica

Per molto tempo il tema della sicurezza, così come anche quello della difesa ad essa collegato, sono rimasti fuori dal processo di integrazione europea. Il motivo può facilmente essere ricondotto al fatto che vi è un legame indissolubile tra la sicurezza e la sovranità degli Stati, ragione delle diverse ritrosie e battute di arresto al processo "comunitarizzazione" di questi due ambiti.

I successivi sviluppi del cammino di integrazione europea, in particolare dal Trattato di Maastricht in poi, hanno tuttavia portato i settori della sicurezza e della difesa ad evolversi in maniera distinta. Per comprendere ciò, dobbiamo necessariamente contestualizzare l'esperienza europea alla luce dei due modelli di integrazione funzionalista e federalista che possiamo definire, il primo come quell'approccio che «assegna un primato temporale e logico all'integrazione economica, accompagnata da una robusta componente giuridica», ove il secondo, invece, «ritiene prioritaria la dimensione politica, compresa quella fondamentale della politica estera, in quanto tocca al potere politico decidere l'integrazione, darle impulso e assumere la direzione della sua concreta realizzazione, assicurandone al contempo il carattere democratico»[117].

Nella dichiarazione di Schuman del 1950, con il quale è stato dato avvio all'integrazione europea, erano state gettate le fondamenta per la realizzazione della federazione degli Stati del continente europeo, «un'Europa unita» il cui obiettivo essenziale sarebbe stato quello di «servire la pace»[118].

Nonostante sia stata proprio un'esigenza di sicurezza a dare avvio al processo di integrazione, considerato che tale lungimirante progetto presupponeva «l'eliminazione del contrasto secolare tra la Francia e la Germania»[119], nei primi Trattati delle allora Comunità europee non v'è traccia di riferimenti né alla sicurezza, né alla difesa comune. Il progetto europeo si sarebbe dovuto realizzare gradualmente, seguendo un approccio di ispirazione funzionalista che avrebbe portato prima di tutto all'unificazione economica degli Stati.

L'integrazione "funzionale" interessò infatti da subito i soli settori economici e tecnici, non coinvolgendo il settore militare. L'istituzione delle prime Comunità europee del carbone e dell'acciaio (CECA) del 1951 e per l'energia atomica (EURATOM) del 1957, ne sono una prova. Tuttavia, non sono mancate occasioni per applicare il metodo funzionalista anche al settore della difesa e la relativa costituzione di un esercito europeo, tuttavia il fallimento del Trattato istitutivo della Comunità europea della difesa (CED) dato dalla mancata ratifica da parte della Francia nel 1954, ha segnato lo sviluppo di questo settore determinandone la sua estraneità dal processo di comunitarizzazione, che lo caratterizza ancora oggi[120].

Diverso sviluppo è stato quello della sicurezza interna che, sulla scorta degli Accordi di Schengen, ha trovato particolare valorizzazione nel Trattato di Maastricht del 1992, andando a

---

[117] E. GREPPI, *Politica estera e difesa europea*, in M. VELLANO, A. MIGLIO, *Sicurezza e difesa comune dell'Unione europea*, Milano, Wolters Kluwer, 2023, pp. 7 ss. Per una teoria generale sul funzionalismo e federalismo v. D. MITRANY, *The progress of international government*, Londra, 1993; ID, *A working peace system*, Londra, 1943; E. HAAS, *The uniting of Europe: Political, Social and Economic Forces*, Londra, 1958: ID, *Beyond the Nation State*, Stanford, 1964.

[118] Il testo della dichiarazione di Schuman del 9 maggio 1950 è reperibile presso il sito dell'Unione europea, al link:<https://european-union.europa.eu/principles-countries-history/history-eu/1945-59/schuman-declaration-may-1950_it>.

[119] *Ibidem*.

[120] Sul punto si rinvia a B. CARAVITA, *Difesa europea, quali prospettive*, in *federalismi.it*, n. 1, 2019; M. FRAU, *I nodi irrisolti della difesa comune europea. Una prospettiva federalista*, in *federalismi.it*, n. 6, 2022.

costituire il c.d. terzo pilastro dell'Unione relativo alla cooperazione nei settori della giustizia e degli affari interni (GAI).

I due epiloghi caratterizzano l'attuale disciplina della sicurezza interna e della difesa a seguito del Trattato di Lisbona.

Relativamente alla sicurezza interna europea, il Trattato ha infatti sancito la conclusione del processo di comunitarizzazione riconducendo il complesso di materie che compongono lo Spazio di libertà, sicurezza e giustizia (SLSG) in un un'unica disciplina, il Titolo V del TFUE (artt. 67-89), ove sono articolate nei tre filoni: libertà (visti, immigrazione e asilo, controlli alle frontiere esterne dell'Unione), sicurezza (quale la cooperazione giuridica e giudiziaria in materia penale, cooperazione di polizia), e giustizia (accesso alla giustizia e cooperazione giuridica e giudiziaria in materia civile). La sicurezza interna europea è stata quindi completamente attratta dalle regole comuni dei Trattati, cosicché diversamente dal passato, gli atti delle istituzioni e la loro procedura di adozione sono ricondotte alla disciplina comune dei Trattati e al controllo giurisdizionale della Corte di giustizia.

Sul punto, di rilievo è la precisazione fornita all'art. 67, par. 1, TFUE ove è previsto che lo SLSG deve realizzarsi nel «rispetto dei diritti fondamentali nonché dei diversi ordinamenti giuridici e delle diverse tradizioni giuridiche degli Stati membri». Tale clausola, certamente ripetitiva di quanto già delineato nell'art. 4 TUE, richiama tuttavia alla necessità di «tener conto delle specificità nazionali allorché l'Unione si propone di interferire in settori nei quali gli Stati hanno sempre gelosamente difeso la propria sovranità»[121]. Caratteristica che ha portato la materia ad essere ricondotta nell'ambito della competenza concorrente tra Unione e Stati membri (art. 4, par. 2, lett. j, TFUE).

Il settore della difesa è invece rimasto ancorato al metodo intergovernativo, secondo cui le decisioni sono adottate all'unanimità degli Stati membri che si impegnano a dare vita ad una politica comune ma conservando il controllo delle loro rispettive politiche nazionali[122].

I Trattati prevedono infatti che l'Unione sia competente in materia di politica estera di sicurezza comune relativamente a tutte le questioni relative alla politica estera e alla sicurezza dell'Unione, «compresa la definizione progressiva di una politica di difesa comune che può condurre a una difesa comune» (art. 24, par. 1 TUE). Come è stato osservato, i riferimenti "può produrre" o "definizione progressiva" sono indici di una politica incentrata su processi decisionali di stampo intergovernativo, affidati a decisioni prese all'unanimità dagli Stati all'interno del Consiglio dell'Unione europea[123]. Tale politica è rappresentata dalla Politica di sicurezza e difesa comune (PSDC) che è parte integrante della politica estera e di sicurezza comune dell'UE (PESC). La PSDC costituisce il principale quadro politico mediante il quale gli Stati membri possono sviluppare una cultura strategica europea della sicurezza e della difesa, affrontare insieme i conflitti e le crisi, proteggere l'Unione e i suoi cittadini e rafforzare la pace e la sicurezza internazionali. Osserviamo tuttavia che, come già registrato anche livello nazionale (*infra* 3.1), la progressiva rilevanza della dimensione esterna di sicurezza dell'Unione, soprattutto per fini di protezione da minacce di tipo transfrontaliero spesso condotte in modalità ibrida[124], ha portato ad una sempre più stretta

---

[121] R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione europea*, Torino, Giappichelli, 2020, p. 536.

[122] E. GREPPI, *Politica estera e difesa europea*, in M. VELLANO, A. MIGLIO, *Sicurezza e difesa comune dell'Unione europea*, Milano, Wolters Kluwer, 2023, pp. 10 ss.

[123] *Ibidem.*

[124] Esistono molteplici definizioni di "minacce ibride", ma il concetto indica la combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali (cioè diplomatici, militari, economici e tecnologici), che

connessione delle politiche di SLSG con quelle di difesa europea, sia nelle missioni civili, sia in quelle militari[125].

Nonostante i diversi sviluppi, tratti comuni possono essere colti a livello organizzativo e di potere. La resistenza all'integrazione da parte degli Stati nei due settori ha portato sia la sicurezza interna, sia la difesa, ad essere organizzate a livello europeo sul principio del coordinamento, (diverso da quello della gerarchia che caratterizza gli ordinamenti nazionali), e alla istituzione di competenti amministrazioni comuni che tuttavia non detengono poteri finali, ossia l'esercizio dei poteri autoritativi di sicurezza, ma solo poteri strumentali, perlopiù relativi alla raccolta e gestione di informazioni, assistenza, promozione di raccordi e collegamenti con amministrazioni nazionali[126].

4.3. L'esigenza di sicurezza degli Stati membri come limite alle libertà dell'Unione europea

Si è già argomentato sull'ordine pubblico e la sicurezza nazionale nel diritto europeo relativamente alla questione delle delimitazioni delle competenze dell'Unione di cui agli artt. 4 e 5 del TUE.

Da una ricognizione del TFUE possiamo individuare un corpo di disposizioni ove viene fatto riferimento ai concetti di "ordine pubblico", "pubblica sicurezza" e "sanità pubblica". Si tratta di ipotesi in cui tali concetti operano come limiti alle fondamentali libertà funzionali alla realizzazione del mercato unico: ossia alla deroga al divieto di restrizioni quantitative o misure ad effetto equivalente alla esportazione/importazione di merci (art. 36)[127], alla circolazione dei lavoratori (art.

possono essere usati in modo coordinato da soggetti statali o non statali per raggiungere determinati obiettivi (pur rimanendo sempre al di sotto della soglia di una guerra ufficialmente dichiarata). Cfr. JOIN(2016) 18 final.

[125] S. SALUZZO, *I rapporti tra la politica di sicurezza e difesa comune e le altre politiche esterne dell'Unione europea*, in M. VELLANO, A. MIGLIO, *Sicurezza e difesa comune dell'Unione europea*, Milano, Wolters Kluwer, 2023, pp. 131 ove l'A. fa riferimento alle operazioni EUNAVFOR, ATALANTA ed EUNAVFOR MED SOPHIA. Nello stesso senso v. anche la Security Union Strategy 2020-2025, COM(2020) 605 final, del 24 luglio 2020, ove è fatto riferimento alle diverse minacce globali. Sul piano amministrativo si rinvia a E. CHITI, *Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia e di difesa*, in L. FORNI, T. VETTOR, *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017, pp. 63 ss.

[126] Cfr. E. CHITI, B.G. MATTARELLA, *La sicurezza europea*, in *Rivista trimestrale di diritto pubblico*, vol. 58, fasc. 2, 2008, pp. 316 e 329.

[127] Cfr. art. 36 TFUE prevede che «[l]e disposizioni degli articoli 34 e 35 lasciano impregiudicati i divieti o restrizioni all'importazione, all'esportazione e al transito giustificati da motivi di moralità pubblica, di ordine pubblico, di pubblica sicurezza, di tutela della salute e della vita delle persone e degli animali o di preservazione dei vegetali, di protezione del patrimonio artistico, storico o archeologico nazionale, o di tutela della proprietà industriale e commerciale. Tuttavia, tali divieti o restrizioni non devono costituire un mezzo di discriminazione arbitraria, né una restrizione dissimulata al commercio tra gli Stati membri».

45, par. 3)[128], al diritto di stabilimento (art. 52, par. 1)[129] ed infine alla circolazione di capitali (art. 65, par. 1, lett. b)[130].

Altro corpo di disposizioni interessano lo SLSG, come l'art. 72 che consente agli Stati membri di mantenere uno certo spazio di discrezionalità nell'applicazione di misure che questi ritengono necessarie per il mantenimento dell'ordine pubblico e della sicurezza interna, potendo in questo caso derogare all'applicazione delle norme europee (es. quelle relative allo SLSG)[131], l'art. 276 che limita la competenza della Corte di giustizia a sindacare della validità o proporzionalità delle operazioni effettuate dall'applicazione delle leggi di uno Stato membro o l'esercizio delle responsabilità incombenti sugli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna[132]. Infine, l'art. 347, posto a salvaguardia del funzionamento del mercato interno, prevede che gli Stati membri si consultano al fine di prendere una decisione comune sulle disposizioni da adottare per evitare che il funzionamento del mercato interno risenta delle misure che uno Stato membro è stato indotto ad adottare unilateralmente in caso di agitazioni interne che turbino l'ordine pubblico, gravi tensioni internazionali o guerra[133].

---

[128] Cfr. art. 45 TFUE prevede la libertà di circolazione dei lavoratori all'interno dell'Unione, tuttavia al par. 3 prevede che «3. Fatte salve le limitazioni giustificate da motivi di ordine pubblico, pubblica sicurezza e sanità pubblica, essa importa il diritto: a) di rispondere a offerte di lavoro effettive; b) di spostarsi liberamente a tal fine nel territorio degli Stati membri; c) di prendere dimora in uno degli Stati membri al fine di svolgere un'attività di lavoro, conformemente alle disposizioni legislative, regolamentari e amministrative che disciplinano l'occupazione dei lavoratori nazionali; d) di rimanere, a condizioni che costituiranno l'oggetto di regolamenti stabiliti dalla Commissione, sul territorio di uno Stato membro, dopo aver occupato un impiego».

[129] Cfr. art. 52, par. 1 TFUE prevede che «1. Le prescrizioni del presente capo e le misure adottate in virtù di queste ultime lasciano impregiudicata l'applicabilità delle disposizioni legislative, regolamentari e amministrative che prevedano un regime particolare per i cittadini stranieri e che siano giustificate da motivi di ordine pubblico, di pubblica sicurezza e di sanità pubblica».

[130] Cfr. art. 65, par.1, lett. b) TFUE dispone che «1. Le disposizioni dell'articolo 63 non pregiudicano il diritto degli Stati membri: [...] b) di prendere tutte le misure necessarie per impedire le violazioni della legislazione e delle regolamentazioni nazionali, in particolare nel settore fiscale e in quello della vigilanza prudenziale sulle istituzioni finanziarie, o di stabilire procedure per la dichiarazione dei movimenti di capitali a scopo di informazione amministrativa o statistica, o di adottare misure giustificate da motivi di ordine pubblico o di pubblica sicurezza».

[131] Cfr. art. 72 TFUE, «Il presente titolo non osta all'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna». L'articolo non prevede quindi un settore riservato alla competenza esclusiva degli Stati membri, ma chiarisce che questi possono adottare (o mantenere) disposizioni ulteriori rispetto a quelle comuni. La deroga alle disposizioni del diritto europeo è consentita solo quando vi sia l'esigenza di garantire il mantenimento dell'ordine pubblico e della sicurezza interna anche in considerazione di valutazioni di politica estera (A. ADINOLFI, *Commento art. 72 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, 2014, p. 468).

[132] Cfr. art. 276 TFUE, «Nell'esercizio delle attribuzioni relative alle disposizioni dei capi 4 e 5 della parte terza, titolo V concernenti lo spazio di libertà, sicurezza e giustizia, la Corte di giustizia dell'Unione europea non è competente a esaminare la validità o la proporzionalità di operazioni condotte dalla polizia o da altri servizi incaricati dell'applicazione della legge di uno Stato membro o l'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna». Tuttavia la riserva di competenza a favore degli Stati non esclude in controllo da parte della Corte di giustizia sul loro operato rispetto alle normative nazionali in un procedimento di infrazione o in sede interpretativa in via pregiudiziale (R. CAFARI PANICO, *Commento art. 276 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, 2014, p. 1368)

[133] Cfr. art. 347 TFUE, «Gli Stati membri si consultano al fine di prendere di comune accordo le disposizioni necessarie ad evitare che il funzionamento del mercato interno abbia a risentire delle misure che uno Stato membro può essere indotto a prendere nell'eventualità di gravi agitazioni interne che turbino l'ordine pubblico, in caso di guerra o di grave tensione internazionale che costituisca una minaccia di guerra ovvero per far fronte agli impegni da esso assunti ai fini del mantenimento della pace e della sicurezza internazionale». Relativamente al riferimento all'ordine pubblico, è stato rilevato come questa disposizioni sia analoga a quella dell'art. 36 TFUE, tuttavia mentre quest'ultima consente deroghe ad un solo aspetto del mercato interno (esportazioni/importazioni di merci), l'art. 347 TFUE riguarda le disposizioni del mercato interno in generale, pertanto la deroga ha una accezione più ampia della prima. La Corte di giustizia è potenzialmente competente a verificare l'esistenza di tali condizioni, ma non esistono criteri per determinare se si è in

Meno numerosi sono i richiami al concetto di sicurezza nazionale, previsto all'art. 73 TFUE ove viene riconosciuta la più ampia discrezionalità agli Stati membri circa l'organizzazione e responsabilità di forme di cooperazione e di coordinamento tra i dipartimenti competenti delle rispettive amministrazioni responsabili per la salvaguardia della sicurezza nazionale[134], e al punto 20 delle Dichiarazioni allegate all'atto finale della conferenza intergovernativa che ha adottato il Trattato di Lisbona, ove è previsto, relativamente all'art. 16 TFUE, che la ogniqualvolta le norme in materia di protezione dei dati personali possano avere implicazioni dirette per la sicurezza nazionale, si dovrà tener conto delle caratteristiche specifiche della questione, tenendo conto della legislazione di riferimento. Ulteriore riferimento è inoltre nel già menzionato art. 346 TFUE, ove sebbene non sia espressamente richiamata la sicurezza nazionale, la formula «interessi essenziali della propria sicurezza» è stata tuttavia ricondotta dalla dottrina al rispetto della sovranità nazionale, integrità territoriale e politica di difesa degli Stati membri[135].

L'ordine pubblico e la sicurezza nazionale si pongono quindi come limiti al rispetto degli obblighi di diritto derivato appena accennati in quanto espressione di prerogative sovrane degli Stati. Tuttavia, il ricorso a tali clausole è a sua volta limitato, sia dal rispetto di determinate condizioni, sia dal fatto di essere oggetto di sindacato da parte della Corte di giustizia circa la necessità e proporzionalità della misura adottata dallo Stato membro[136]. Elementi questi che quindi negano la possibilità di un ricorso arbitrario da parte degli Stati a tali clausole.

Entrando nello specifico, è proprio sulla scorta delle pronunce del Giudice europeo che, dovendo valutare di volta in volta le circostanze specifiche che hanno indotto lo Stato a ricorrere a provvedimenti limitativi delle libertà per motivi di sicurezza, sono stati enucleati una serie di parametri[137] che andiamo ad analizzare nel prosieguo.

a) La minaccia diretta all'interesse fondamentale della collettività

Nella ricordata causa 30/77, *Regina c. Pierre Buchererau*, la Corte di giustizia, con una sentenza dal tenore ricognitivo rispetto a quanto già affermato nelle pronunce precedenti, ha chiarito che il richiamo all'ordine pubblico da parte degli Stati membri presuppone «oltre alla perturbazione

presenza di una grave tensione internazionale o se questa costituisce una grave minaccia di guerra (I. PALANDRI, *Commento art. 347 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, 2014, p. 1548).

134 Cfr. art. 73 TFUE, prevede che «Gli Stati membri hanno la facoltà di organizzare tra di loro e sotto la loro responsabilità forme di cooperazione e di coordinamento nel modo che ritengono appropriato tra i dipartimenti competenti delle rispettive amministrazioni responsabili per la salvaguardia della sicurezza nazionale». Si precisa che l'esclusione della competenza europea rispetto al settore della sicurezza interna ha ad oggetto l'esecuzione delle misure coercitive e non la materia relativa all'uso della forza in sé, essendo ammesso l'intervento della legislazione europea nel disciplinare la cooperazione in materia di sicurezza interna (V. BOLICI, *Commento art. 73 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, 2014, p. 469).

135 GORI, *Commento art. 223 CEE*, in R. QUADRI, R. MONACO, A. TRABUCCHI, *Trattato istitutivo della comunità economica europea*, vol. III, Milano, Giuffrè, 1965, pp. 1626 ss.

136 Si ricorda che anche nei casi in cui sono previste limitazioni all'azione della Corte di giustizia (art. 276 TFUE), o nel caso in cui l'ammissibilità del ricorso alla clausola di ordine pubblico sia totalmente rimessa alla decisione degli Stati membri (art. 347 TFUE), la Corte conserva comunque il potere di valutare l'operato degli Stati (al riguardo si rinvia alle note 131 e 132 rispettivamente relative ai due menzionati articoli).

137 Cfr. D. RINOLDI, *L'ordine pubblico europeo*, Napoli, Editoriale scientifica, 2005, pp. 287 ss., ove l'A., individua tra le condizioni alle quali è subordinato l'utilizzo del limite di ordine pubblico nella: interpretazione restrittiva degli eventi suscettibili di determinare il ricorso a tale limite; la minaccia diretta ad un interesse per la società nazionale; l'irrilevanza della diversità di tutela predisposta nei singoli Stati membri per l'interesse che si vuole proteggere; Le garanzie processuali a tutela dell'individuo destinatario di misure di ordine pubblico.

dell'ordine sociale insita in qualsiasi infrazione della legge, l'esistenza di una minaccia effettiva ed abbastanza grave per uno degli interessi fondamentali della collettività» (pt. 35 motivi).

In questi termini si comprende che l'ordine pubblico per l'ordinamento europeo assolve la funzione di salvaguardia degli interessi degli Stati, ma non nella loro totalità. Nella medesima sede il Giudice europeo ha infatti escluso che esigenze di carattere economico possano rappresentare eventi così gravi tali da giustificare l'adozione di tali clausole restrittive. La successiva giurisprudenza è tuttavia arrivata ad un contemperamento di questo principio secondo cui i motivi economici possono rientrare tra i presupposti legittimanti l'evocazione della clausola restrittiva purché «superati e assorbiti in esigenze di più ampia portata»[138].

b) Il rispetto del principio di proporzionalità

Nella causa 222/84, *Johnston c. Chief Constable of the Royal Ulster Constabulary*, del 15 maggio 1986, la Corte, adita in via pregiudiziale, ricordava che nel determinare la portata di qualsiasi limitazione di un diritto individuale, occorre rispettare il principio di proporzionalità «che fa parte dei principi giuridici generali sui quali è basato l'ordinamento giuridico comunitario [ed] esige che siffatte limitazioni non eccedano quanto è adeguato e necessario per raggiungere lo scopo perseguito [...]» (pt. 38 motivi)[139].

c) Il doppio sindacato giurisdizionale in sede nazionale ed europea

La pronuncia dell'84 non precisava tuttavia chi avesse il compito di effettuare tale valutazione e secondo quali parametri. Come sarà precisato nella successiva causa 367/89, *Richardt e Les Accessoires Scientifiques SNC*, venne innanzitutto ritenuto di competenza del «giudice nazionale [...] valutare se il regime instaurato rispetti il principio di proporzionalità, tenendo conto di tutti gli elementi di ogni fattispecie [...]». Nel caso specifico, tali elementi vennero individuati ne «l'attitudine della merce a pregiudicare la sicurezza dello Stato, le circostanze in cui l'infrazione è stata commessa e la buona o mala fede dell'operatore che intendeva effettuare il transito e disponeva all'uopo dei documenti rilasciati da un altro Stato membro» (pt. 25 motivi).

Nella sentenza del 17 ottobre 1995, causa 83/94, *Leifer*, la Corte confermava tale sindacato del giudice nazionale e qualificava il principio di proporzionalità come parametro di accertamento, nelle specifiche circostanze, che i provvedimenti adottati perseguano effettivamente lo scopo di salvaguardare la pubblica sicurezza e quindi accertare se tali misure siano «necessarie e adeguate per raggiungere gli obiettivi perseguiti e se non fosse stato possibile raggiungere detti obiettivi mediante misure meno restrittive» (pt. 34 sulla terza questione)[140].

Tale limite deve tuttavia essere inteso non solo a livello interno, relativamente all'impatto sui diritti e libertà costituzionali degli Stati membri, ma anche nei suoi effetti esterni, dovendo la misura restrittiva essere giustificata e delimitata in maniera uniforme, tenendo conto anche dei principi

[138] Cfr. CGUE, sentenza 10 luglio 1984, causa 72/83, *Campus Oil*, ove al punto 35 è stato ritenuto che «tenuto conto della gravità delle conseguenze che l'interruzione delle forniture di prodotti petroliferi può avere per l'esistenza di uno Stato, si deve ritenere che lo scopo di garantire una fornitura minima costante di prodotti petroliferi trascenda le considerazioni di carattere puramente economico e possa quindi rientrare nella nozione di pubblica sicurezza».

[139] Cfr. CGUE, *Johnston contro Chief Constable of the Royal Ulster Constabulary*, sentenza 15 maggio 1986, causa 222/84. ,Medesimo principio sarà poi richiamato anche nella sentenza 26 aprile 1988, causa 352/1985, *Bond van Adverteerders*; sentenza 4 ottobre 1991, causa 367/89, *Aimé Richardt e Les Accessoires Scientifiques SNC*; sentenza 13 luglio 2000, causa 423/98, *Alfredo Albore*;

[140] CGUE, sentenza del 17 ottobre 1995, causa 83/94, *Leifer*.

generali relativi ai diritti e le libertà dell'Unione europea. È in questo caso che interviene la Corte di giustizia dovendo verificare che la misura adottata a livello nazionale, nell'esercizio del potere discrezionale riconosciuto, non si dimostri essere in realtà una restrizione (economica) mascherata.

Alla luce di quanto fin qui affrontato, emerge che la sicurezza e l'ordine pubblico sono considerate dall'ordinamento europeo come due ambiti decisionali di competenza nazionale per i quali gli Stati membri godono di una certa discrezionalità, sebbene limitata solo ad ipotesi eccezionali contemplate dagli stessi Trattati[141]. Nel caso *Sirdar*, causa 273/97, la Corte ha infatti escluso la possibilità di concepire «una riserva generale, inerente al Trattato, che escluda dall'ambito d'applicazione del diritto comunitario qualsiasi provvedimento adottato per motivi di pubblica sicurezza» (pt. 16 motivi)[142]. Nella stessa sede veniva inoltre rilevato che talune delle deroghe previste dal Trattato riguardano solo le norme relative alla libera circolazione delle merci, delle persone e dei servizi, e non le disposizioni in materia sociale del Trattato (pt. 18 motivi).

Pare quindi sussistere un sottile equilibrio tra le esigenze di sicurezza avvertite a livello nazionale e le libertà europee, quali libertà dirette a garantire il buon funzionamento del mercato unico. Da una parte, gli atti di diritto derivato possono arrivare a coinvolgere questioni e situazioni che possono riferirsi alla sicurezza interna, come ad esempio il settore della difesa (vedi l'appena citato caso *Sirdar*), dall'altra gli Stati membri possono derogare alle libertà fondamentali funzionali all'economia europea, ma non possono adottare misure per fini di sicurezza che siano oltremodo sproporzionate. Come è stato osservato «[o]ltre quella soglia l'ordinamento europeo pare reputare irrilevante la protezione dei diritti costituzionali interni realizzata attraverso prerogative di pubblica sicurezza, o per lo meno un valore contendibile da parte di quelli connessi alla concorrenza ed alla libera circolazione soprattutto di servizi e di persone»[143].

Riepilogando, così come a livello nazionale sono stati individuati i presupposti legittimanti misure restrittive delle libertà per motivi di sicurezza[144], allo stesso modo riteniamo di poter trarre i medesimi parametri anche per l'ordinamento europeo relativamente ai casi in cui gli Stati membri intendano ricorrere a tali misure.

Le condizioni alle quali è subordinato l'utilizzo di misure restrittive delle libertà per fini di sicurezza da parte degli Stati membri possono infatti essere individuate innanzitutto nel fatto che tali clausole possono essere attivate solo nelle eccezionali ipotesi previste dai Trattati. L'esigenza di sicurezza avvertita deve avere ad oggetto una minaccia reale e concreta ad un interesse della società nazionale, la misura deve essere necessaria e proporzionata nel limitare i diritti individuali per lo scopo da perseguire. Infine, il ricorso a tali misure è oggetto di sindacato sia dei giudici nazionali, sia della Corte di giustizia.

---

[141] Si rinvia alle diverse disposizioni contenenti le calusole sicuraterie prima trattate in nota 131 e 132.

[142] CGUE, sentenza 26 ottobre 1999, causa C-273/97, *Sirdar*.

[143] C. BUZZACCHI, *Sicurezza e* securitization *tra Stato, Unione europea e mercato*, in F. PIZZOLATO, P. COSTA (a cura di), *Sicurezza, Stato e mercato*, Milano, Giuffrè, 2015, p. 114.

[144] G. DE VERGOTTINI, *Sicurezza e diritti fondamentali … op. cit.*, p. 22.

CAPITOLO II

CYBERSICUREZZA E CYBERRESILIENZA TRA ORDINAMENTO EUROPEO E ITALIANO

SOMMARIO: 1. Il quadro delle politiche e delle amministrazioni nel cyberspazio europeo tra sovranità tecnologica e sicurezza - 1.1 Il rafforzamento delle infrastrutture informatiche: tra soggetti critici e infrastrutture di Internet - i) La sicurezza delle risorse informatiche infrastrutturali: la disciplina *Network and Information Security* (NIS) - ii) La resilienza operativa digitale per il settore finanziario - iii) Dalle infrastrutture ai beni: il rafforzamento delle catene di approvvigionamento dei beni ICT - iv) La prospettiva europea sulla sicurezza delle connessioni e dell'Internet globale - 1.2 La (cyber)consapevolezza situazionale europea e le relative amministrazioni - 1.3. La vulnerabilità umana e il rafforzamento delle competenze informatiche - 2. Il d.L. 82/2021. L'architettura italiana di cybersicurezza - 2.1 Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) - 2.2 *Segue*. Oltre il segreto di Stato. Il controllo sul *procurement* informatico per fini di sicurezza e interesse nazionale - 2.3. *Segue*. L'estensione della sicurezza nazionale "statica" sui beni ICT: il caso delle TELCO e del 5G - 3. La definizione di cybersicurezza tra norma tecnica e giuridica - 3.1. Il concetto giuridico di cybersicurezza europea: tra sicurezza del mercato unico e sicurezza dell'umano - 3.2. La cybersicurezza nazionale italiana - 4. Il concetto di resilienza - 5. Introduzione alla cyberresilienza - 5.1. La cyberresilienza europea - 5.2. La cyberresilienza nazionale - 6. La terminologia del rischio informatico e le dimensioni della cybersicurezza europea - 7. La privatizzazione della sicurezza - 7.1 *Segue*. Il ruolo dei privati nella normazione tecnica di sicurezza: il caso della cybersicurezza - 7.2 *Segue*. I partenariati pubblico-privati europei di cybersicurezza per lo scambio di informazioni - 8. Gli interessi di rilevanza giuspubblicistica sottesi alla cybersicurezza: una relazione mediata tra sicurezza e tecnologie informatiche - 9. Considerazioni conclusive sulla (cyber)sicurezza tra normativo e politico

1. Il quadro delle politiche e delle amministrazioni nel cyberspazio europeo tra sovranità tecnologica e sicurezza

Dal 2020 in poi la strategia di cybersicurezza europea ha visto un importante riformulazione dei suoi obiettivi in prospettiva del mutato contesto internazionale. Ne sono prova le parole della Presidente della Commissione europea Ursula von der Leyen nel discorso sullo stato dell'Unione del settembre dello stesso anno, ove è stato fatto riferimento al concetto di "sovranità tecnologica" quale «capacità che l'Europa deve avere di fare le proprie scelte, sulla base dei propri valori, rispettando le proprie regole» in relazione alla tecnologia presente nonché anche quella del prossimo futuro[1].

Il riferimento al concetto di sovranità, particolarmente significativo sia per le scienze giuridiche, sia per altre scienze sociali, ha suscitato inevitabili critiche e dibattiti da parte della dottrina che si è interrogata sul significato del più ampio concetto di sovranità europea[2], in certi casi tentando anche

[1] U. VON DER LEYEN, *A Union that strives for more. My agenda for Europe. Political Guidelines for the next European Commission 2019-2024*, reperibile al link:<https://commission.europa.eu/ system/files/2020-04/ political -guidelines-next-commission_en_0.pdf>.

[2] Sul punto v. T.E. VERELLEN, *European Sovereignty Now? A Reflection on What It Means to Speak of "European Sovereignty"*. in E*uropean Papers*, n. 5, 2020, 307-318 reperibile link:<https:// www.europeanpapers.eu/fr/ e-journal/european-sovereignty-now-reflection-on-what-it-means- european - sovereignty>.

di distinguere la sovranità tecnologica[3] da altri concetti affini, come quelli di "sovranità digitale"[4] e di "autonomia strategica"[5], anch'essi diffusamente utilizzati nei documenti dell'Unione. Dal punto di vista giuridico, l'utilizzo di un simile concetto da parte delle istituzioni europee ha portato Alcuni ad indagare il rapporto tra la sovranità degli Stati membri e quella europea alla luce delle disposizioni - e soprattutto dei limiti - dei Trattati dell'Unione, prospettando «un mutamento della natura giuridica dell'UE»[6].

Secondo Altri, il concetto in questione sarebbe «un'affermazione politica e non giuridica [che] indica un obiettivo che si vorrebbe raggiungere e non descrive uno stato di fatto»[7].

In entrambe le ipotesi sembra percepibile un tratto di inconsistenza giuridica di tale nozione sia in riferimento all'oggetto di riferimento della sovranità, per l'appunto la "tecnologia" (quale?, quali?), o piuttosto il "digitale", sia sul piano giuridico alla luce dei limiti posti dai Trattati dell'Unione sul punto.

Per quel che interessa la presente trattazione, riteniamo utile far riferimento allo studio condotto da alcuni Studiosi che hanno proposto una concettualizzazione della nozione di sovranità tecnologica europea sulla base dei documenti politici dell'Unione[8]. Partendo dalla definizione generale di sovranità digitale come «"a form of legitimate, controlling authority" over—in the digital context—data, software, standards, services, and other digital infrastructure, amongst other things»[9], lo studio ha individuato cinque ambiti ove si è fatto ricorso più volte a questo concetto, quali: «data governance, constraining platform power, digital infrastructures, emerging technologies e cybersecurity»[10].

È proprio all'interno di questi settori che possiamo infatti incasellare le recenti iniziative legislative europee in tema. Vedi gli interventi legislativi sulla protezione dei dati personali, come il Regolamento generale 2016/679 (c.d. GDPR) e la Direttiva 2016/680 anche nota come direttiva di polizia, nonché da ultimo il Regolamento 2022/868 (c.d. *Data Governance Act*), ma anche le iniziative sulla regolazione delle piattaforme come il *Digital Markets Act* (DMA), e il *Digital Services Act* (DSA).

---

[3] S. COUTURE, S. TOUPIN, *What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?*, in *GigaNet: Global Internet Governance Academic Network*, Annual Symposium 2017, 2018, reperibile al link:<https://ssrn.com/abstract=3107272 or http://dx.doi.org/ 10.2139/ssrn.3107272>.

[4] L. FLORIDI, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy & Technology*, 2020; M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, n. 1, 2022.

[5] Si faccia riferimento alla definizione di autonomia strategica adottata dal Consiglio Affari Esteri dell'UE nel 2016 come la «capacità di agire autonomamente quando e dove necessario e con i partner quando possibile». v. Consiglio dell'Unione Europea, *Council conclusions on implementing the EU Global Strategy in the area of Security and Defence*, 14 November 2016, reperibile al link:<https://www.consilium.europa.eu/media/ 22459/eugs-conclusions- st14149en16.pdf>.

[6] S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in in: *I Post di AISDUE, III, 2021, Sezione Atti Convegni AISDUE*, n. 5, 20 dicembre 2021, p. 70, ove l'A. in riferimento alla "sovranità digitale" osserva che il ricorso a tale concetto «implica la volontà di trasformare l'Unione in un soggetto statuale capace di gestire in modo autonomo la tecnologia. Si tratta dunque, in linea di principio, di un progetto integrazionista molto ambizioso, attraverso il quale si realizza un trasferimento di sovranità dagli Stati membri all'organizzazione e come tale, va oltre l'obiettivo che consiste nel potenziare l'"autonomia strategica" dell'Unione, in quanto presuppone un mutamento della natura giuridica dell'UE».

[7] G. FINOCCHIARO, *La sovranità digitale?*, in *Dir. pubbl.*, fasc. n. 3, settembre-dicembre 2022, p. 811.

[8] H. ROBERTS, J. COWLS, F. CASOLARI, J. MORLEY, M. TADDEO, L. FLORIDI, *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, in *Internet Policy Review*, 2021, reperibile al link:<https://ssrn.com/abstract=3937345 or http://dx.doi.org/10.2139/ ssrn.3937345>.

[9] ID., *op. cit.*, p. 6.

[10] *Ivi*, p. 9.

Rilevanti sono anche le iniziative relative alle infrastrutture digitali, come il progetto GAIA-X[11], e il Regolamento 2023/1781 che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il Regolamento 2021/694 (c.d. *Chips Act*)[12].

Relativamente al primo, il progetto GAIA-X è un'iniziativa della Commissione europea, della Germania, della Francia, attraverso la costituzione di un'organizzazione non-profit, introdotta per risolvere il problema della dipendenza da infrastrutture *cloud* straniere. Si tratta di un ecosistema volto a costituire un'infrastruttura affidabile, ispirata ai principi di apertura, trasparenza, interoperabilità, autenticazione e fiducia, volta a consentire la condivisione delle informazioni in maniera sicura attraverso un sistema di certificazione dei nodi e degli attori che forniscono servizi al suo interno (*federated system*)[13]. Nello specifico il progetto si basa su una componente infrastrutturale che include le componenti per memorizzare, trasferire ed elaborare i dati, ove gli *stakeholder* coinvolti in questo ecosistema sono fornitori di servizi *cloud*, di connessioni e servizi *cloud edge*, e una componente costituita dai dati e la costruzione di servizi intelligenti a seconda dei diversi settori industriali.

Con il *Chips Act* l'Unione europea ha inteso promuovere lo sviluppo di capacità per consentire la progettazione e la produzione di tecnologie dei semiconduttori di prossima generazione e l'integrazione di sistemi in tali tecnologie, nonché anche approfondire la collaborazione tra i principali operatori in tutta l'Unione, consolidare le catene di approvvigionamento e il valore dei semiconduttori nel territorio europeo, rispondere alle esigenze dei settori industriali chiave e creare nuovi mercati, attraverso la costituzione di un meccanismo di *governance*[14].

Relativamente alla cybersicurezza, deve innanzitutto precisare che il raggiungimento di adeguati livelli di sicurezza e resilienza delle infrastrutture e delle trasmissioni informatiche è un elemento chiave per diverse politiche dell'Unione come la *Shaping Europe's Digital Future*[15], il *Recovery Plan* proposto dalla Commissione europea[16], nonché il successivo dispositivo di ripresa e resilienza (*Next Generation Ue*), la *Global Strategy for the EU's Foreign and Security Policy,*[17] e la *European Council*

---

[11] Si rinvia al sito ufficiale dell'iniziativa di cui al link:<https://gaia-x.eu/>.

[12] Regolamento 2023/1781, del 13 settembre 2023 che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il regolamento (UE) 2021/694 (regolamento sui chip), reperibile al link:<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/? uri=CELEX:32023R1781>.

[13] GAIA-X, *Technical architecture*, Federal Ministry for Economic Affairs and Energy (BMWi), 2020, reperibile al link:<https://www.bmwk.de/Redaktion/EN/Publikationen/gaia-x-technical- architecture.pdf?__blob=publicationFile&v=1>. In particolare sul concetto di "*federed system*" il documento precisa che «GAIA-X specifies federated systems of autonomous Providers, tied together by a specified set of standards, frameworks, and legal rules. The federation supports decentralization and distribution» (p. 4).

[14] Cfr. considerando 4 e 7 del Reg. (UE) 2023/1781. Nello specifico, relativamente al meccanismo di *governance* nel settore dei semiconduttori, il considerando 7 prevede che «[a] livello dell'Unione, il regolamento dovrebbe istituire un consiglio europeo dei semiconduttori, composto da rappresentanti degli Stati membri e presieduto dalla Commissione, al fine di favorire un'attuazione agevole, efficace e armonizzata del presente regolamento, la cooperazione e lo scambio di informazioni. Il consiglio europeo dei semiconduttori dovrebbe fornire consulenza e assistenza alla Commissione su questioni specifiche, compresa l'attuazione coerente del presente regolamento, agevolando la cooperazione tra gli Stati membri e scambiando informazioni sulle questioni relative al presente regolamento. Il consiglio europeo dei semiconduttori dovrebbe inoltre fornire consulenza alla Commissione in materia di cooperazione internazionale relativa ai semiconduttori. Il consiglio europeo dei semiconduttori dovrebbe tenere riunioni distinte per i diversi compiti attribuitigli a norma dei vari capi del presente regolamento. Le riunioni possono svolgersi in diverse composizioni dei rappresentanti di alto livello e la Commissione può istituire sottogruppi».

[15] Shaping Europe's Digital Future, COM(2020) 67 final.

[16] Europe's moment: Repair and Prepare for the Next Generation, COM (2020) 98 final.

[17] https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Strategic Agenda 2019-2024[18]. Tra queste merita attenzione il piano di politiche europee sulla sicurezza in generale, la *Security Union Strategy 2020-2025*, ove, secondo nostra interpretazione, si apre ad un inedito processo integrativo in questo settore per mezzo del potenziamento dei sistemi di scambio informativo.

Ciò può essere dedotto da quanto indicato nella stessa Strategia ove viene evidenziato che:

> [a]nche se la responsabilità primaria della sicurezza incombe ai singoli Stati membri, negli ultimi anni è emerso chiaramente che la sicurezza di uno Stato membro è la sicurezza di tutti. L'UE può apportare una risposta multidisciplinare e integrata, fornendo agli operatori della sicurezza negli Stati membri gli strumenti e le informazioni di cui hanno bisogno[19].

Come già argomentato, il sistema di sicurezza europeo si è sviluppato nel tempo sulla logica della cooperazione intergovernativa, non trovando mai una piena comunitarizzazione. L'esclusiva competenza degli Stati membri in materia di sicurezza, vedi la presenza nei Trattati delle clausole di tutela della "sicurezza nazionale" o dell'"ordine pubblico e della sicurezza" quali condizioni legittimanti il regime eccezionale statale rispetto all'applicazione del diritto europeo, è uno dei tratti caratterizzanti la politica europea in questo ambito[20].

Tuttavia, nonostante tali prerogative che accentrano il ruolo degli Stati, tale indirizzo non ha precluso la successiva elaborazione di politiche e la creazione di istituzioni comuni che hanno inevitabilmente richiesto l'impegno coordinato e cooperativo sia tra gli Stati membri, sia tra questi e le competenti autorità europee, al fine di garantire l'esigenza di sicurezza in tutto lo spazio europeo. Osservando l'evoluzione storica della cooperazione tra gli Stati europei nel settore di polizia, ci si accorge che è proprio nella raccolta, archiviazione, trattamento e scambio di informazioni che trova concreta realizzazione il processo integrativo in questo settore[21].

La citata Strategia intende pertanto riaffermare il ruolo sempre più rilevante dello *sharing* informativo tra i diversi attori coinvolti, e dall'altro potenziare le competenti amministrazioni europee

---

[18] https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/

[19] The EU Security Union Strategy 2020-2025, COM (2020) 605 final, del 24 luglio 2020, reperibile al link:<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC 0605>.

[20] Vale la pena richiamare il contenuto dell'art. 4, co. 2, del Trattato sull'Unione europea (TUE) ove è previsto che «L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali. Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro». Tale clausola di competenza statale permanente, aggiunta su esplicita richiesta del Regno Unito, deve essere inoltre letta in combinato disposto con l'art. 276 del Trattato sul funzionamento dell'Unione europea (TFUE), che esclude il controllo da parte della Corte di Giustizia sulla «validità o la proporzionalità di operazioni condotte dalla polizia o da altri servizi incaricati dell'applicazione della legge di uno Stato membro o l'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna».

[21] Nella elencazione dei principali atti legislativi sulla cooperazione di polizia disponibile presso il sito del Parlamento europeo (di cui al link:<https://www.europarl.europa.eu/factsheets/en/sheet/156/cooperazione-di-polizia> consultato il 26 novembre 2023) risulta che gran parte di questi siano volti a istituire meccanismi di comunicazione per favorire lo scambio di informazioni tra i Paesi membri, v. la Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi; il Regolamento (UE) 2018/1862 sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale; il Regolamento (UE) 2019/818 che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione; la Direttiva (UE) 2019/1153 che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati; il Regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici online, applicabile dal 7 giugno 2022.

in questo settore, con l'auspicio di creare un ambiente affidabile e sicuro per favorire l'esercizio di tale pratica tra tutti gli attori coinvolti all'interno dello spazio dell'Unione.

Esigenza di condivisione maggiormente avvertita nel contesto della cybersicurezza ove tale pratica rappresenta sin dalle origini, a livello internazionale, un valido strumento proattivo in caso di incidenti di sicurezza a vasto impatto[22]. Sulla scorta di ciò, l'articolazione amministrativa europea di cybersicurezza, similmente a quella di sicurezza in senso tradizionale, si è sviluppata nel tempo attraverso l'istituzione di diversi organismi di coordinamento decentrati, organizzati perlopiù sul modello delle agenzie dotate di personalità giuridica[23], che trovano nello scambio informativo tra di esse, nonché con le competenti autorità degli Stati membri, l'elemento essenziale per lo svolgimento delle loro funzioni.

Dal 2004 è presente l'Agenzia Europea per la Cybersicurezza (ENISA), istituita 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» ed inoltre «[p]oiché le reti elettroniche sono in larga misura private, l'Agenzia dovrebbe avvalersi delle informazioni del settore privato e cooperare con esso» (cons. 11). L'Agenzia venne inizialmente dotata di un mandato temporaneo, via via esteso con i Regolamenti (UE) n. 1007/2008, e n. 580/2011. Tuttavia, solo con il Regolamento 2019/881, il c.d. *Cybersecurity Act*, è stato conferito all'ENISA un mandato permanente, rafforzandone il ruolo, i compiti, le responsabilità, e predisponendo maggiori risorse al fine di contribuire al supporto degli Stati membri nel prevenire e rispondere efficacemente agli attacchi informatici.

In particolare, l'Agenzia ricopre la funzione di segretariato della rete composta dai gruppi di intervento nazionali (c.d. rete CSIRT), nonché sostiene la cooperazione operativa tra questi e il gruppo di intervento dell'Unione, il CERT-UE, che ha la funzione di rispondere in modo efficiente alle minacce informatiche dirette contro le reti e i sistemi istituzionali dell'Unione europea.

I CSIRT, *Computer Security Incident Response Teams* sono unità di intervento decentrate, istituite presso i singoli Stati membri (eventualmente anche all'interno di autorità competenti[24]), con l'incarico di svolgere attività reattive, come l'intervento in caso di incidente informatico, ed anche proattive, come il monitoraggio degli incidenti a livello nazionale, l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti e la relativa analisi di tali rischi e incidenti. In entrambi i casi, questi soggetti rappresentano i nodi nevralgici dei processi di *cyber information sharing*. Difatti, da una parte ricevono le informazioni sulle minacce informatiche in quanto ricettori delle notifiche degli incidenti di cybersicurezza da parte dei soggetti verso cui trova applicazione la disciplina NIS; dall'altra, partecipano alla più ampia cooperazione informativa a livello europeo per mezzo della rete che riunisce i rappresentanti dei gruppi di

---

[22] Si faccia riferimento *Linee guida sulla sicurezza dei sistemi di informazione* diffuse dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) nel 2002, reperibile al link:<https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm>, ove sono stati elaborati nove principi tra cui anche quelli di «3) Risposta: Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza […]»; «8) Gestione della sicurezza: Le parti interessate devono adottare un approccio globale della gestione della sicurezza […]»; «9) Rivalutazione: Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti di informazione e introdurre adeguate modifiche nello loro politiche, pratiche, azioni e le procedure di sicurezza […]».

[23] Sulle agenzie amministrative europee v. E. CHITI, *Le agenzie europee. Unità e decentramento nelle amministrazioni europee*, Padova, Cedam, 2002.

[24] È ad esempio il caso del CSIRT Italia trasferito presso l'Agenzia Nazionale per la Cybersicurezza (ACN) con il decreto-legge n. 82 del 2021. Sul punto sia concesso rinviare a F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in f*ederalismi.it,* n. 12, 2022.

intervento di tutti gli Stati membri e la squadra CERT-UE, sotto il segretariato dell'ENISA (c.d. rete di CSIRT)[25].

Tale attività trova inoltre il supporto del "Gruppo di cooperazione", organismo composto dai rappresentanti degli Stati membri, dalla Commissione e dall'ENISA, la cui funzione è quella di agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri fornendo orientamenti e consulenza alle istituzioni europee nonché effettuando valutazioni coordinate dei rischi di cybersicurezza ed elaborando relazioni utili ai fini del riesame della disciplina NIS da parte della Commissione[26].

Nonostante gli sforzi diretti a istituire un quadro amministrativo e regolamentare in materia di scambio informativo, nella "Strategia dell'UE in materia di cybersicurezza per il decennio digitale" presentata nel dicembre 2020[27], si apprende che «[l]'Unione europea è priva di consapevolezza situazionale collettiva [c.d. *cyber situational awareness*] in materia di minacce informatiche» (vedi infra 1.2). Secondo la Commissione il problema è dovuto, da una parte allo scarso coinvolgimento del settore privato nella cooperazione informativa, dall'altra alla resistenza degli Stati membri a condividere le informazioni in maniera sistematica e completa, rendendo così estremamente difficoltoso il funzionamento dei meccanismi di *cyber information sharing* tra gli Stati membri e le istituzioni dell'UE in caso di crisi o incidenti informatici transfrontalieri su larga scala[28].

La stessa Presidente della Commissione Ursula von der Leyen, nel citato Discorso sull'Unione, ha ribadito la necessità di «gettare le basi per un processo decisionale collettivo» basato la scambio di «conoscenze provenienti da tutti i servizi e da tutte le fonti, dallo spazio ai formatori del personale di polizia, dall'*open source* alle agenzie di sviluppo».

---

[25] In particolare, l'art. 15 Dir. (UE) 2022/2555, prevede che la rete svolge i seguenti compiti: «a) scambiare informazioni per quanto riguarda le capacità dei CSIRT; b) agevolare la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT; c) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità; d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di cibersicurezza; e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni; f) su richiesta di un membro della rete di CSIRT potenzialmente interessato da un incidente, scambiare e discutere informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati; g) su richiesta di un membro della rete di CSIRT, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro; h) fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva; i) cooperare e scambiare migliori pratiche con i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro; j) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a: i) categorie di minacce informatiche e incidenti; ii) preallarmi; iii) assistenza reciproca; iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri; v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4, su richiesta di uno Stato membro; k) informare il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera j) e, se necessario, chiedere orientamenti in merito; l) fare il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA; m) su richiesta di un singolo CSIRT, discutere le capacità e lo stato di preparazione di tale CSIRT; n) cooperare e scambiare informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche in tutta l'Unione; o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9; p) fornire orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa».

[26] Cfr. art. 14 Dir. (UE) 2022/2555.

[27] JOIN(2020) 18 final, *Comunicazione congiunta al parlamento europeo e al consiglio. La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, reperibile al link:<https:// eur-lex.europa.eu/ legal-content/ IT/ TXT/ PDF/ ?uri= CELEX:52020JC0018&from=IT>.

[28] *Ibidem.*

È sulla scorta di tali considerazioni che la disciplina di cybersicurezza europea è stata recentemente aggiornata e potenziata anche in questi aspetti che interessano la cooperazione informativa.

Dalla lettura della strategia osserviamo tuttavia che l'impegno dell'Unione in questo settore è più ampio e comprende il potenziamento di attività che interessano sia il profilo infrastrutturale fisico (sicurezza "del" cyberspazio), sia in quello immateriale (sicurezza "nel" cyberspazio), affidata alle diverse strategie di contrasto della criminalità informatica, di difesa nonché anche alle attività di prevenzione, disincentivo, dissuasione e risposta a comportamenti dolosi nel cyberspazio.

Per quel che interessa la presente trattazione, ci concentreremo sul primo di questi, quello infrastrutturale, contenuto nel capitolo sulla "Resilienza, sovranità tecnologica e leadership" della Strategia, le cui politiche sono perlopiù riconducibili a tre obiettivi: i) il rafforzamento delle infrastrutture informatiche presso soggetti rilevanti o essenziali (vedi la disciplina NIS), delle catene di approvvigionamento di beni ICT, delle connessioni comprese le reti mobili a banda larga, i dispositivi IoT, fino all'Internet globale; ii) il rafforzamento delle politiche preventive e reattive attraverso il potenziamento dello scambio di informazioni di cybersicurezza all'interno dell'Unione (vedi lo *European Cybersecurity Shield*), iii) ed infine, lo sviluppo di competenze informatiche a livello europeo.

1.1 Il rafforzamento delle infrastrutture informatiche: dai soggetti critici alle infrastrutture di Internet

L'interdipendenza di settori chiave alle reti e alle infrastrutture informatiche è alla base dell'esigenza di porre in sicurezza tali sistemi. Prima ancora di sviluppare politiche di sicurezza "diffusa" aventi ad oggetto le catene di approvvigionamento ICT e l'Internet globale, gli interventi dell'Unione europea sul punto si sono concentrati sulla sicurezza informatica dei soggetti operanti in settori chiave (o critici) per il fine di garatire la sicurezza del mercato unico interno.

i) La sicurezza delle risorse informatiche infrastrutturali: la disciplina Network and Information Security (NIS)

La direttiva (UE) 2016/1148 (Direttiva NIS I) è il primo strumento con il quale l'Unione ha inteso innalzare i livelli di sicurezza delle reti e dei sistemi informativi al fine di evitare che le attività economiche e sociali europee, nonché il funzionamento del mercato interno possano essere impattati dagli effetti negativi degli attacchi informatici.

Si tratta di una disciplina di armonizzazione minima volto a istituire un omogeneo livello di protezione attraverso l'imposizione di una serie di obblighi diretti sia verso gli Stati membri, sia verso le infrastrutture critiche pubbliche e private individuate. Tali oneri possono essere brevemente sintetizzati ne: 1) l'obbligo per tutti gli Stati membri di predisporre strategie nazionali di cybersicurezza; 2) l'istituzione di una cooperazione interstatale in ambito strategico; 3) la realizzazione di una rete operativa di intervento in caso di incidente informatico; 4) la declinazione di una serie di obblighi per gli operatori di determinati settori individuati; 5) ed infine, l'obbligo per tutti gli Stati di istituire autorità competenti a livello nazionale, punti di contatto unici e gruppi di intervento[29].

[29] Cfr. A. ROTONDO, *Cyber security e protezione delle infrastrutture critiche: l'efficacia del modello europeo*, in S. MARCHISIO, U. MONTUORO, *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, Giappichelli, 2019, p. 132.

A partire dal gennaio 2023 è entrata in vigore la Direttiva (UE) 2022/2555 (Direttiva NIS II)[30], che ha abrogato la Direttiva NIS I. Rispetto alla previgente disciplina, con il recente intervento il legislatore europeo è andato ad estendere la platea di soggetti rientranti nel campo applicativo della Direttiva introducendo strumenti di armonizzante più incisivi.

Ai sensi della Direttiva (UE) 2016/1148, gli Stati membri erano responsabili di identificare i soggetti che soddisfacevano i criteri per essere considerati operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD), così come era conferito agli Stati membri un ampio potere discrezionale per quanto riguarda l'attuazione degli obblighi in materia di sicurezza e segnalazione degli incidenti che pertanto sono stati attuati in modi significativamente diversi a livello nazionale.

Al fine di eliminare tali ampie divergenze tra gli Stati membri, la disciplina NIS II ha ovviato alle carenze dovute alla differenziazione tra gli OSE ed FSD, rivelata obsoleta in quanto non rifletteva l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno, introducendo un criterio uniforme per la determinazione dei soggetti rientrano nell'ambito di applicazione della disciplina. I soggetti così determinati sono classificati dalla Direttiva NIS II in due categorie, "essenziali" e "importanti", in funzione della loro rilevanza per il settore o il tipo di servizio che forniscono, nonché delle loro dimensioni[31].

Ed inoltre, data l'intensificazione e la crescente sofisticazione delle minacce informatiche, la Direttiva prevede che gli Stati membri dovrebbero adoperarsi per garantire che i soggetti esclusi dall'ambito di applicazione della stessa raggiungano un livello elevato di cybersicurezza e sostengono l'attuazione di misure equivalenti di gestione dei rischi di cybersicurezza, che riflettono la natura sensibile di tali soggetti.

ii) La resilienza operativa digitale per il settore finanziario

Peculiare è il recente intervento del legislatore europeo il quale ha dettato una apposita disciplina per il settore finanziario. Il motivo è dovuto al fatto che una relazione del 2020, il Comitato europeo per il rischio sistemico (CERS), considerato l'elevato livello di interconnessione tra entità finanziarie, mercati finanziari e infrastrutture del mercato finanziario, ha evidenziato che tale settore soffre di una potenziale «vulnerabilità sistemica» dal momento che incidenti informatici localizzati potrebbero rapidamente diffondersi da una qualunque delle entità finanziarie dell'Unione all'intero sistema finanziario, senza trovare alcun ostacolo nelle frontiere geografiche[32].

Così, con il Regolamento (UE) 2022/2554, il legislatore europeo ha introdotto una disciplina relativa alla «resilienza operativa digitale per il settore finanziario» (DORA), pubblicata in Gazzetta ufficiale lo stesso giorno di un altro atto: la Direttiva (UE) 2022/2557, relativo alla resilienza dei soggetti critici (Direttiva CER). Sul riferimento alla "resilienza" nei due atti si avrà modo di argomentare più avanti (*infra* 4), per il momento ci soffermeremo su alcuni aspetti generali della disciplina DORA.

In particolare sul rapporto tra questo Regolamento e la Direttiva NIS II, dal momento che il DORA accresce il livello di armonizzazione delle varie componenti della resilienza digitale, introducendo

[30] Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva 2016/1148 (d'ora in poi Dir. NIS II), reperibile al link:<https:// eur-lex.europa.eu/ legal-content/ IT/ TXT/ PDF/ ?uri= CELEX: 32022L2555 &from=EN>.

[31] Cfr. art. 3 Dir. NIS II.

[32] CERS, *Systemic cyber risk*, febbraio 2020, reperibile al link:<https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf?fdefe8436b08c6881d492960ffc7f3a9>.

requisiti in materia di gestione dei rischi informatici e segnalazione di incidenti più rigorosi rispetto a quelli previsti dalla disciplina NIS II, il Regolamento prevede che il DORA sia da considerarsi «una *lex specialis* rispetto alla direttiva (UE) 2022/2555», ma allo stesso tempo stesso, è essenziale mantenere un saldo rapporto tra il settore finanziario e il quadro orizzontale di cibersicurezza dell'Unione dettato dalla disciplina MIS , per garantire la coerenza con le strategie di cibersicurezza adottate dagli Stati membri e permettere alle autorità di vigilanza finanziaria di venire a conoscenza degli incidenti informatici che colpiscono altri settori contemplati da tale direttiva.

Ciò è soprattutto vero nel particolare ambito dello scambio di informazioni di cybersicurezza. Per consentire l'apprendimento intersettoriale e attingere efficacemente alle esperienze di altri settori nella lotta alle minacce informatiche, le entità finanziarie disciplinate dalla NIS II dovrebbero continuare a far parte dell'«ecosistema» di quella direttiva.

Inoltre, Le autorità nazionali competenti dovrebbero poter partecipare alle discussioni strategiche delle politiche e ai lavori tecnici del gruppo di cooperazione ai sensi della Direttiva, nonché scambiare informazioni e cooperare maggiormente con i punti di contatto unici. Le autorità competenti previste dal presente regolamento dovrebbero anche consultare i CSIRT e collaborare con loro. Le autorità competenti dovrebbero inoltre poter chiedere il parere tecnico delle autorità competenti designate o istituite in conformità della Direttiva (UE) 2022/2555 e concludere accordi di cooperazione volti a garantire meccanismi di coordinamento efficaci e di risposta rapida.

iii) Dalle infrastrutture ai beni: il rafforzamento delle catene di approvvigionamento dei beni ICT

Nel "*consultation paper*" elaborato dall'ENISA nel 2019 avente ad oggetto il tema delle politiche industriali dei prodotti ICT nell'Unione, l'Agenzia europea ha ricondotto nella nozione di "sovranità digitale", tre diverse categorie concettuali, quali: la sovranità sui dati personali dei cittadini europei; la sovranità digitale dell'industria europea guidata dai dati; la sovranità digitale dell'Unione e degli Stati membri che la compongono[33]. Il rafforzamento della catena di approvvigionamento digitale (comprendente dati e cloud, tecnologie dei processori di nuova generazione, connettività ultra sicura e reti 6G), attiene certamente alla seconda categoria, quella attinente all'aspetto industriale, il cui fine è quello di garantire una posizione di autonomia strategica dell'Unione europea, ossia «la capacità dell'Europa di procurarsi prodotti e servizi che soddisfano i suoi bisogni e valori, senza indebite influenze dal mondo esterno» nell'acquisto e implementazione di prodotti e servizi ICT[34].

Il tema investe diverse questioni, prima fra tutte quella relativa alla catena di approvvigionamento di tali prodotti e servizi, la c.d. *supply chain*, ossia quell'insieme di processi che interessano la distribuzione di *hardware* e *software*, *storage* in *cloud* o locale, a cui deve essere garantito un certo livello di affidabilità in termini di sicurezza informatica[35].

---

[33] Cfr. ENISA, *Consultation paper – EU ICT industrial policy: Breaking the cycle of failure*, 2019, p. 10, reperibile al link:<https://www.enisa.europa.eu/publications/enisa-position-papers-and- opinions /eu-ict-industry -consultation-paper >.

[34] ENISA, *Cybersecurity research directions for the Eu's digital strategic autonomy*, 2019, p. 5, reperibile al link:<https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy>.

[35] In particolare, le vulnerabilità che affliggono i prodotti e servizi ICT nelle catene di approvvigionamento possono essere sfruttate dai criminali informatici per veicolare *supply chain attacks*, ossia azioni volte ad infettare componenti *software* o *hardware* a monte, ossia in fase di produzione, distribuzione o manutenzione e aggiornamento. In tal modo, compromesso il fornitore di tali prodotti e servizi, gli effetti dell'attacco potranno facilmente estendersi anche a valle, verso gli acquirenti e utilizzatori finali. Sul punto si consiglia la lettura del documento dell'ENISA, *Threat Landscape for*

Se osservata dal punto di vista delle politiche di sicurezza, tale disciplina ci sembra essere un passo in avanti dell'Unione europea che ha colto che l'esigenza non è più solo quella di proteggere settori chiave (o critici), ma di innalzare la sicurezza in ambiti più estesi non ponendo più l'accento sul soggetto ma sui beni ICT.

L'altra questione interessa l'*indipendenza* dell'Unione europea dalla catena di approvvigionamento di prodotti e servizi ICT provenienti da Paesi extra-Ue, ossia la c.d. autonomia strategica, già ricordata. Allo stato attuale, l'Unione non dispone ancora di sufficienti capacità, né di mezzi tecnologici e industriali, per garantire autonomamente la sicurezza della propria economia e delle proprie infrastrutture critiche[36].

A tal proposito con il Regolamento (UE) 2021/887[37], sono stati istituiti lo *European Cybersecurity Competence Centre* (ECCC) e la *Network of National Coordination Centres* (NCCs)[38], quali Centri aventi il compito, il primo di assumere incarichi specifici nell'ambito industriale, tecnologico e della ricerca in materia di cybersicurezza, gestendo contemporaneamente i finanziamenti legati a tale settore provenienti da diversi programmi, in particolare da Orizzonte Europa e dal programma Europa digitale e, se possibile, anche da altri programmi dell'Unione; i secondi, hanno il compito di declinare i programmi industriali assunti dall'ECCC a livello nazionale gestendo i fondi al fine di assolvere la missione e conseguire gli obiettivi di cui al citato Regolamento[39].

iv) La prospettiva europea sulla sicurezza delle connessioni e dell'Internet globale

Tra i punti della Strategia sono inserite anche le politiche volte a rafforzare la sicurezza delle connessioni in particolari settori quali le comunicazioni satellitari governative dell'Unione europea, le trasmissioni di informazioni riservate da parte delle autorità pubbliche, sia nazionali, sia europee, utilizzando tecnologia quantistica e forme di crittografia basate su tecnologia europea, la sicurezza delle reti 5G e quelle di futura generazione.

In considerazione di quanto già affrontato in precedenza (Parte I), di particolare interesse è l'obiettivo di garantire l'Internet, globale e aperto a fronte di «scenari estremi che compromettono l'integrità e la disponibilità del sistema root DNS globale»[40]. Nello specifico, con questa politica l'Unione intende sviluppare una rete di enti "risolutori" del sistema DNS al'interno del territorio europeo, incoraggiando i portatori di interessi, tra cui le imprese dell'UE, i fornitori di servizi Internet e i fornitori di *browser*, ad adottare una strategia di diversificazione della risoluzione.

Inoltre, dal documento si apprende che la Commissione intende contribuire a rendere sicura la connettività Internet sostenendo lo sviluppo di un servizio pubblico europeo di risoluzione DNS – l'iniziativa "DNS4EU" - che offrirà un servizio "alternativo" ed europeo per accedere all'Internet globale.

Supply Chain Attacks, 2021, reperibile al link:<https://www.enisa.europa.eu/ publications/threat-landscape- for-supply-chain-attacks>.

[36] Cfr. considerando 12, del Reg. (UE) 2021/887, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

[37] Regolamento (UE) 2021/887, del 20 maggio 2021 che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

[38] Si rinvia al sito ufficiale ECCC, di cui al link:<https://cybersecurity-centre.europa.eu/index_en>.

[39] Cfr. considerando 23 e 26, Reg. (UE) 2021/887.

[40] JOIN(2020) 18 final, *Comunicazione congiunta al parlamento europeo e al consiglio. La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, p. 11.

1.2 La (cyber)consapevolezza situazionale europea e le relative amministrazioni

La consapevolezza situazione o (*situational awareness* - SA) è strettamente legata alla cognizione umana e al modo in cui l'uomo percepisce l'ambiente. Per questo motivo, questo processo è stato studiato da diverse prospettive disciplinari, rendendo difficile la sua sistematizzazione a livello scientifico.

La definizione a cui si fa generalmente riferimento è quella fornita da Mica R. Endsley, Chief Scientist dell'Aeronautica Militare degli Stati Uniti, secondo cui la consapevolezza situazionale può essere intesa come un processo in tre fasi, rispettivamente di «[p]ercezione degli elementi nell'ambiente all'interno di un volume di tempo e di spazio, la comprensione del loro significato e la proiezione del loro stato nel prossimo futuro»[41]. In prima istanza, possiamo quindi intendere questo concetto come uno strumento che consente al decisore di valutare la scelta migliore da fare in base al contesto generale e alle variabili associate di rischio, pericolo e danno futuro di un evento di minaccia.

La *Cyber Situational Awareness* (CSA) è un ramo della tradizionale consapevolezza situazionale appena descritta che - appunto - trova applicazione nel contesto del cyberspazio, per proteggere gli asset informatici, prendere migliori decisioni di sicurezza informatica e migliorare le funzioni e l'organizzazione della sicurezza[42].

Nello specifico, il processo CSA è alimentato da un *pool* di informazioni costituito da dati provenienti da sensori informatici (sistemi di rilevamento delle intrusioni, ecc.), nonché da informazioni provenienti da processi di analisi da altre prospettive (ad esempio, analisi di intelligence sulle minacce, considerazioni geopolitiche degli analisti, ecc.)

Come è stato notato[43], l'attenzione della dottrina verso questo tema è ancora scarsa e frammentaria, e vorremmo aggiungere che i pochi studi che sono stati condotti riguardano per lo più il processo di *cyber situational awareness* dal punto di vista delle singole organizzazioni[44].

Questo chiarimento è necessario perché, nella Strategia citata e nel ricordato Discorso del Presidente della Commissione, l'Unione Europea ha fatto riferimento a un piano di "Cyber Situational Awareness collettiva" (CCSA). Si tratta di un indirizzo strategico, con relative ricadute sia giuridiche che organizzative-amministrative, che sembra andare verso una progressiva "europeizzazione" delle amministrazioni e degli strumenti (anche tecnici) responsabili del funzionamento dei processi di cybersecurity preventiva negli Stati membri.

Un esempio è dato dal *Cyber Solidarity Act,* disciplina che si pone a cavallo tra le politiche di resilienza e quelle di prevenzione, dissuasione e risposta. Nello specifico, si tratta di una iniziativa avanzata il 18 aprile 2023, dalla Commissione europea con una proposta di Regolamento che

---

[41] M.R. ENDSLEY, *Design and evaluation for situation awareness enhancement*, in *Proceedings of the Human Factors Society annual meeting*, vol. 32, 1988, 97, disponibil al link:<https://journals.sagepub.com/doi/10.1177/154193128803200221>. Si veda anche la definizione fornita dal Glossario del *National Institute of Standards and Technology* (NIST), che definisce la SA come segue:«all'interno di un volume di tempo e spazio, la percezione della postura di sicurezza di un'azienda e del suo ambiente di minaccia; la comprensione/significato di entrambi presi insieme (rischio); e la proiezione del loro stato nel prossimo futuro», disponibile all'indirizzo: <https://csrc.nist.gov/glossary/term/situational_awareness>.

[42] Sulle diverse definizioni del concetto di *Cyber Situational Awareness*, v. S. JAJODIA, P. LIU, V. SWARUP, C. WANG, *Cyber situational awareness*, in *Springer Science & Business*, 2009, disponibile al link:<https://link.springer.com/book/10.1007/978-1-4419-0140-8>.

[43] U. FRANKE, J. BRYNIELSSON, *Cyber situational awareness – A systematic review of the literature*, in *Computer & Security*, vol. 46, 2014, pp. 18-31, disponibile<https://www.sciencedirect.com/science/article/pii/S0167404814001011>.

[44] A. HORNEMAN, *Situational Awareness for Cybersecurity: An Introduction*, in *Carnegie Mellon University, Software Engineering Institute's Insights (blog)*, 2019, disponibile al link:<https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/>

stabilisce una serie di misure volte a rafforzare la solidarietà e le capacità di individuare, preparare e rispondere alle minacce e agli incidenti di sicurezza informatica nel contesto europeo[45].

Con questo strumento l'Unione intende incrementare la consapevolezza situazionale, la condivisione delle informazioni, nonché migliorare la preparazione e la risposta agli incidenti informatici a livello comune attraverso l'istituzione di tre nuovi meccanismi di raccordo: lo *European Cybersecurity Shield*, il *Cyber Emergency Mechanism* e il *Cybersecurity Incident Review Mechanism.*

Lo *European Cybersecurity Shield* è lo strumento di resilienza che avrà il compito di migliorare il rilevamento, l'analisi e la risposta alle minacce informatiche su larga scala attraverso l'istituzione di una nuova rete di piattaforme di *Security Operation Centres* SOC multinazionali. La prima fase del progetto è stata già avviata nel novembre 2022, e sono stati selezionati tre consorzi di centri operativi di sicurezza (SOC) transfrontalieri, che riuniscono enti pubblici di 17 Stati membri e dell'Islanda, nell'ambito del programma Europa digitale.

Il *Cyber Emergency Mechanism* avrà il compito di migliorare la preparazione e la risposta agli incidenti di cybersicurezza attraverso: la valutazione dei meccanismi di risposta implementati presso i settori particolarmente critici selezionati al termine di una generale valutazione del rischio a livello europeo; la creazione dell'*EU Cybersecurity Reserve*, ossia servizi di risposta agli incidenti erogati da fornitori di servizi privati («trusted providers»), attivati su richiesta degli Stati membri o di istituzioni dell'Unione, per aiutarli ad affrontare problemi significativi o incidenti di sicurezza informatica su larga scala: ed infine, attraverso la promozione dell'assistenza reciproca tra gli Stati membri ove uno di questi sia stato interessato da un incidente di cybersicurezza[46].

Relativamente al profilo operativo, tra le diverse modifiche, la nuova disciplina NIS ha istituito la "Rete europea delle organizzazioni di collegamento per le crisi informatiche" (*EU Cyber Crisis Liaison Organisation Network* - CyCLONe) con lo scopo di garantire una più stretta collaborazione e azione coordinata nei casi di incidenti di cyberisucrezza su larga scala. A tal fine la Rete sostiene la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala e garantisce il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione[47].

Da giugno 2023 è inoltre operativo il *Joint Cyber Unit*, cuore della nuova cooperazione operativa europea in materia di cybersicurezza. Si tratta di una piattaforma di raccordo ove i partecipanti, provenienti dalla comunità civile, diplomatica, dalle forze dell'ordine e dalla difesa, possono

---

[45] COM(2023) 209 final, reperibile al link:<https://digital-strategy.ec.europa.eu/en/ library/proposed -regulation -cyber-solidarity-act>.

[46] Sul concetto di "assistenza reciproca", l'art. 10, lett. c) dell'*EU Cyber Solidarity Act* si limita a fare rinvio alla medesima nozione disposta nella Direttiva NIS II. Considerati i contrasti interpretativi della dottrina sulla qualificazione dell'attacco informatico come attacco armato (v. E. CORSI, *La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale*, in *Research Analysis del Center for Cyber Security and International Relations Studies*, 2018), nonché lo stato dell'arte circa la definizione di una politica di sicurezza e difesa europea (v. M. FRAU, *I nodi irrisolti della difesa comune europea. Una prospettiva federalista*, in *federalismi.it*, n. 6, 2022), non è da escludersi che questo principio possa essere ricondotto all'omonimo principio di reciproca assistenza di cui all'art. 42 del TUE, ove è previsto che nel rispetto della politica e di sicurezza e di difesa «di taluni Stati membri» l'assistenza allo Stato aggredito sia subordinata al previo coinvolgimento della NATO, sul punto cfr. F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, Cedam, 2014, p. 42.

[47] Cfr. art. 16 Dir. (UE) 2022/2555.

avvalersi del supporto e delle competenze reciproche, soprattutto nel caso in cui le varie comunità debbano lavorare a stretto contatto, in occasione di incidenti su larga scala o crisi[48].

L'Unità non costituisce un organismo supplementare indipendente, ma è frutto della messa a disposizione di uno spazio comune fisico, situato a Bruxelles, e uno spazio virtuale composto da strumenti utili per una condivisione sicura e rapida delle informazioni.

Tra le amministrazioni europee che vi partecipano troviamo: relativamente alle politiche di polizia, lo *European Cybercrime Centre* (EC3), unità specializzata già istituita presso l'EUROPOL con funzioni di raccordo con le forze di polizia degli Stati europei[49]; sul piano diplomatico, lo *European External Action Service* (EEAS)[50] e il forum *Horizontal Working Party on Cyber Issues*[51]; infine, per quanto riguarda il settore difesa, il *framework Permanent Structured Cooperation* (PESCO)[52] e la *European Defence Agency* (EDA)[53].

1.3. La vulnerabilità umana e il rafforzamento delle competenze informatiche

Altro punto della strategia interessa l'esigenza di «migliorare le competenze della forza lavoro, per attrarre e trattenere i migliori talenti in materia di cybersicurezza», connessa alla promozione degli studi nelle scenze dure, c.d. STEMs, in particolare sostenendo «la partecipazione femminile nell'ambito dell'istruzione in campo scientifico, tecnologico, ingegneristico e matematico».

L'obiettivo è pertanto quello di sviluppare una maggiore consapeolezza (*awareness*) verso i temi della sicurezza informatica e delle informazioni (c.d. igiene informatica); e dall'altro, potenziare l'occupazione nei settori tecnologici, nonché la ricerca e sviluppo.

Relativamente al primo punto, il tema ci porta a dover riflettere su un aspetto di primaria rilevanza che riguarda la c.d. vulnerabilità umana.

Diversamente dal concetto di sicurezza tradizione, la cybersicurezza pone particolare rilevanza non solo verso il profilo esterno, ma anche verso quello della gestione del rischio endogeno che, nel caso specifico, ricomprende gli incidenti di sicurezza dovuti a condotte dolose di soggetti interni ad

---

[48] C(2021) 4520 *fina*l, *Sulla creazione di un'unità cibernetica congiunta*, 2021, reperibile al link:<file:/// C:/ Users/ Utente/ Downloads/ Recommendation_ jEPD6a3IejR8P3CCtEsbpHbUbI_ 77514.pdf>. A ben vedere il *Joint Cyber Unit* prende avvio dal precedente progetto "*Blueprint*" del 2017 istituito con la Raccomandazione (EU) 2017/1584 sulla risposta coordinata a incidenti e crisi di cybersicurezza su larga scala.

[49] Il Centro europeo per la criminalità informatica (*European Cybercrime Centre* - EC3) è un organismo istituito da Europol nel 2013, con sede all'Aia. La sua attività è quella di coordinare le attività transfrontaliere di contrasto alla criminalità informatica e funge da centro di competenza tecnica in materia. Per ulteriori si rinvia al sito ufficiale di cui al link: <https://www.europol. europa.eu/about-europol/european-cybercrime-centre-ec3>.

[50] Lo *European External Action Service* (EEAS), o anche Servizio europeo per l'azione esterna (SEAE), è il servizio diplomatico dell'UE, istituito per rendere più coerente ed efficace la politica estera dell'UE e rafforzare così l'influenza dell'Europa sulla scena mondiale. Per ulteriori si rinvia al sito ufficiale di cui al link: <https://www.eeas.europa.eu/_it>.

[51] Il forum *Horizontal Working Party on Cyber Issues* è stato istituito nel 2016 ed è responsabile del coordinamento dei lavori del Consiglio sulle questioni informatiche, principalmente la politica informatica e le attività legislative. Il Gruppo collabora strettamente con la Commissione europea ed altre istituzioni quali il Servizio europeo per l'azione esterna, l'Europol, l'Eurojust, l'Agenzia europea dei diritti fondamentali (FRA), l'Agenzia europea per la difesa (EDA) ed infine l'Agenzia dell'Unione europea per la cybersicurezza (ENISA).

[52] Il *Permanent Structured Cooperation* (PESCO) nel settore della politica di sicurezza e di difesa è stato istituito l'11 dicembre 2017 con decisione 2017/2315 del Consiglio. Tale strumento offre un quadro giuridico per pianificare, sviluppare e investire congiuntamente in progetti di capacità condivisi e migliorare la prontezza operativa e il contributo delle forze armate.

[53] L'Agenzia europea per la difesa è stata istituita con un'azione comune del Consiglio dei ministri del 12 luglio 2004, «per sostenere gli Stati membri e il Consiglio nel loro sforzo di migliorare le capacità di difesa europee nel campo della gestione delle crisi e per sostenere la politica europea di sicurezza e di difesa nella sua forma attuale e in quella futura».

amministrazioni, organi dello Stato o dipendenti di organizzazioni private, perpetrate con o senza l'ausilio di strumenti informatici (cc.dd. *insder threats*)[54]; e gli eventi riconducibili al c.d. fattore umano, ossia incidenti dovuti alla mera *inconsapevolezza* degli utenti circa il rispetto di buone pratiche di sicurezza informatica (*best practices*) o sulle tecniche di prevenzione da attacchi di ingegneria sociale[55]. In entrambi i casi, le minacce perpetrate, sebbene spesso circoscritte al solo livello locale, possono facilmente scalare di intensità, al punto da acquisire gradi di compromissione di interesse per la sicurezza nazionale in base alle funzioni, servizi o informazioni colpite. Motivo per cui, oltre al profilo della sicurezza esterna dalle minacce informatiche esogene, acquista prioritario rilievo anche il profilo della sicurezza interna.

2. Il d.L. 82/2021. L'architettura italiana di cybersicurezza

A pochi giorni da un attacco informatico contro il Centro Elaborazione Dati della Regione Lazio, il 3 agosto 2021 la Camera dei deputati e il Senato hanno convertito con modificazioni il decreto-legge n. 82 del 14 giugno 2021, in legge n. 109 del 4 agosto 2021.

Con tale intervento, dettato dalla condizione di «straordinaria necessità e urgenza» avvertita a livello nazionale in ossequio al crescente impatto degli attacchi informatici, nonché dalla priorità di garantire una sicura attuazione dei piani di trasformazione digitale delineati nel Piano Nazionale di Ripresa e Resilienza (PNRR)[56], l'Italia ha inteso aggiornare la c.d. architettura nazionale di cybersicurezza, attraverso la creazione di un sistema istituzionale *ad hoc*.

A ben vedere l'Italia aveva già avviato il suo cammino nel settore della protezione delle reti e delle risorse informatiche nel marzo 2013, con l'emanazione del c.d. decreto Monti, il n. 66/2013, e successivamente il c.d. decreto Gentiloni, il n. 87 del 13 aprile 2017, entrambi recanti «indirizzi per la protezione cibernetica e la sicurezza informatica nazionale». Sempre nel 2017, veniva inoltre varata una nuova Strategia Nazionale di Cybersecurity (SNC) con l'adozione del nuovo Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica (PN), volto a sviluppare gli indirizzi individuati nel precedente Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico (QSN), emanato nel 2013.

Le linee operative contenute nei citati documenti strategici sviluppavano un'architettura decisionale distribuita su tre livelli, di cui se ne riassume una loro articolazione alla luce del d.P.C.M. n. 87/2017. Il primo, quello politico e di coordinamento strategico, vedeva il Presidente del Consiglio dei ministri posto al vertice del sistema, supportato dal Comitato Interministeriale per la sicurezza della Repubblica (CISR), quale organo istituito con legge 3 agosto 2007, n. 124 presso la Presidenza del Consiglio dei Ministri, e avente funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza[57]. Il secondo livello, di carattere

---

[54] G. DE VERGOTTINI, *op. cit*, p. 77. Si tratta dei c.d. *insider threat*, ossia soggetti che sfruttano la propria posizione lavorativa nelle organizzazioni per veicolare attacchi dall'interno. A tal proposito v. M. STRANO, F. BATTELLI, M. BOCCARDI, R. BRUZZONE, B. FIAMMELLA, M. MATTIUCCI, A. RIGONI, *Insiede attack. Manuale di ricerca e di intervento sul computer crime nelle organizzazioni*, Roma, 2005.

[55] Per ingegneria sociale (o *social engineering*) si intende «l'uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è oppure manovrandoli. Di conseguenza l'ingegnere sociale può usare la gente per strapparle informazioni con o senza l'ausilio di strumenti tecnologici» (K.D. MITNICK, *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, Milano, 2002).

[56] Il Piano Nazionale di Ripresa e Resilienza (PNRR) pone la "sicurezza cibernetica" a fondamento del processo di trasformazione digitale.

[57] Cfr. art. 4, d.P.C.M. n. 66 del 19 marzo 2013.

operativo e amministrativo, vedeva la partecipazione del Nucleo per la Sicurezza Cibernetica (NSC), istituito nell'ambito dell'Ufficio del Consigliere Militare presso la Presidenza del Consiglio dei Ministri, con la funzione di supportare il Presidente nella materia della sicurezza del "cyberspazio" per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento[58]. Infine, il terzo livello, composto dagli Organismi di informazione per la sicurezza, responsabili di condurre attività di ricerca informativa, nonché analisi, valutazioni e previsioni sulle minacce, ed alla trasmissione di informazioni rilevanti al NSC, e agli altri soggetti – sia pubblici che privati – interessati all'acquisizione di informazioni[59].

Si precisa tuttavia che il previgente sistema di cybersicurezza nazionale, istituito con il decreto Monti e poi modificato con il decreto Gentiloni, prevedeva anche altri organi deputati alla cybersicurezza nazionale. Questi erano rispettivamente: il NISP - Tavolo interministeriale di crisi cibernetica e l'osservatorio di sicurezza previsto dal d.P.C.M. Monti in seno al Ministero dello Sviluppo Economico, i quali non vennero poi riconfermati nel sistema delineato nel decreto Gentiloni teso ad alleggerire la gestione delle crisi e ad accentrare le responsabilità.

Il citato intervento legislativo apportato con il d.l. n. 82/2021 è intervenuto su tale Sistema riformandolo e specializzandone le competenze nel settore della cybersicurezza. Confermando in parte l'impostazione precedente, l'attuale architettura di nazionale di cybersicurezza, risulta infatti composta da:

i) il Presidente del Consiglio dei ministri – ovviamente confermandone la posizione di vertice del Sistema – con compiti più estesi ed elevati rispetto a quelli assegnati nella previgente architettura, richiamando la formulazione dell'art. 1 dell'appena citata l. n. 124 del 2007[60], «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della sicurezza nazionale nel cyberspazio». Le ulteriori competenze interessano l'adozione della strategia nazionale di cybersicurezza[61], sentito il Comitato Interministeriale per la Cybersicurezza (CIC), nonché la nomina e la revoca del direttore generale e del vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale (ACN), previa deliberazione del Consiglio dei ministri, e informando

[58] Cfr. artt. 8 e 9, d.P.C.M. n. 66 del 19 marzo 2013.

[59] Cfr. art. 7, d.P.C.M. n. 66 del 19 marzo 2013.

[60] Cfr. art. 1, co. 1, lett. a), legge 3 agosto 2007, n. 124, il quale prevede che al Presidente del Consiglio dei ministri sono attribuiti, in via esclusiva «l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento».

[61] Si tratta di un documento la cui stesura è contemplata all'art. 7 della direttiva NIS I, rubricato "Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi". Come precisato nell'Allegato 1 della Comunicazione della Commissione europea, "Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", COM (2017)476 final del 4 ottobre 2017, tale strategia «è equiparabile alla "strategia nazionale di cybersicurezza" (NCSS)» (p. 5) (documento consultabile sul sito della Commissione europea al link:<https:// ec.europa.eu/ transparency/ documents-register/ detail?ref=COM(2017)476&lang=it>). L'art. 6. co.1, del decreto legislativo 65/2018, con il quale l'Italia ha recepito la direttiva NIS I, fa infatti riferimento alla NCSS, prevedendo al comma 2 che «nell'ambito della strategia nazionale di cybersicurezza, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto: a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi; b) il quadro di governance per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; e) i piani di ricerca e sviluppo; f) un piano di valutazione dei rischi; g) l'elenco dei vari attori coinvolti nell'attuazione». Il co. 4 del decreto legislativo 65/2018, novellato a seguito dell'entrata in vigore del decreto-legge n. 82/2021, prevede inoltre che «l'Agenzia per la cybersicurezza trasmette la strategia nazionale in materia di cybersicurezza alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale».

preventivamente di tali nomine il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), e le Commissioni parlamentari competenti.

ii) l'Autorità delegata, a cui sono conferiti per la prima volta competenze in materia di cybersicurezza, aggiornando così il dettato dell'art. 3, co. 1-*bis*, della legge 3 agosto 2007, n. 124[62]. In particolare, la nuova normativa prevede che il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, potrà delegare le funzioni attribuitegli in via non esclusiva dalla stessa, ad un Ministro senza portafoglio o ad un Sottosegretario di Stato[63], che prenderà il nome di "Autorità delegata", tenuta ad informare costantemente il Presidente sulle modalità di esercizio delle funzioni delegate, il quale, «fermo restando il potere di direttiva», può in qualsiasi momento avocare a sé l'esercizio di tutte o di alcune di esse, ed inoltre, in relazione alle funzioni delegate, partecipa alle riunioni del Comitato interministeriale per la transizione digitale (CITD)[64].

I tratti innovativi della disciplina possono invece essere colti nella istituzione e introduzione nel nuovo assetto decisionale dei due già citati organi: il Comitato Interministeriale per la Cybersicurezza (iii) e l'Agenzia per la Cybersicurezza Nazionale (iv).

iii) il Comitato Interministeriale per la Cybersicurezza (CIC), sostitutivo delle funzioni del Comitato Interministeriale per la Sicurezza della Repubblica (CISR) in materia di cybersicurezza. Si tratta di un organo istituito presso la Presidenza del Consiglio dei ministri con funzioni di «consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello "spazio cibernetico»[65]. Si precisa, tuttavia che dal dettato dell'art. 10 emerge che, sebbene il CISR non sia espressamente contemplato tra gli attori della nuova architettura di cybersicurezza, l'Organo ne prenda parte ove convocato dal Presidente del Consiglio dei ministri nei casi di «crisi che coinvolgono aspetti di cybersicurezza»[66].
In particolare, le funzioni del CIC consistono: a) nel proporre al Presidente del Consiglio dei ministri degli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; b) l'esercizio dell'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; c) la promozione dell'adozione di iniziative necessarie a favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori

---

62 L'attribuzione al Presidente del Consiglio dell'«alta direzione e responsabilità generale delle politiche di cybersicurezza», e l'introduzione dell'Autorità delegata, sono i tratti che legano l'architettura nazionale di cybersicurezza alla medesima direzione operativa e strategica del Sistema di informazione per la sicurezza della Repubblica.

63 Cfr. art. 3 della l. 3 agosto 2007, n. 124. Nel caso specifico, la delega è stata affidata con il d.P.C.M. 8 marzo 2021, al Sottosegretario di Stato Franco Gabrielli.

64 Il CITD è organo istituito con il decreto-legge 1 marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55, con il compito di assicurare «il coordinamento e il monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti in via ordinaria». Sul punto, cfr. art. 8, co. 2, del decreto legge 1° marzo 2021, n. 22, convertito con modificazioni dalla legge 22 aprile 2021, n. 55, "*Disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri*".

65 Cfr. art. 4, co. 1, del d.l. n. 82/2021.

66 Cfr. art. 10 del d.l. n. 82/2021, ove al co. 1, prevede che «nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia», nonché, al co. 2, che «il Nucleo [per la Sicurezza Cibernetica] assicura il supporto al CISR e al Presidente del Consiglio dei ministri, nella materia della cybersicurezza, per gli aspetti relativi alla gestione di situazioni di crisi ai sensi del comma 1, nonché per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, ivi comprese le attività istruttorie e le procedure di attivazione necessarie, ai sensi dell'articolo 5 del decreto-legge perimetro».

privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in tal materia; d) esprimere pareri sul bilancio preventivo e sul bilancio consuntivo dell'ACN, nonché esprimere il suo parere, dietro richiesta del Presidente del Consiglio dei ministri, anche su «l'adozione della strategia nazionale di cybersicurezza» (art. 4)[67].

iv) l'Agenzia per la Cybersicurezza Nazionale (ACN), quale agenzia amministrativa[68] deputata alla «tutela degli interessi nazionali nel campo della cybersicurezza»[69], dotata di personalità giuridica di diritto pubblico e autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal d.l. n. 82/2021[70].
La normativa affida all'ACN una molteplicità di funzioni riconducibili a diversi ambiti di azione dell'Agenzia, la quale assicura il «coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore» (art. 7, lett. a).

---

[67] Competenza questa che può essere dedotta dall'art. 4 comma 6 del decreto in commento, ove è espressamente previsto che il CIC si sostituisca al CISR nelle funzioni a questo attribuite dal decreto istitutivo del PSNC, «fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge perimetro». Il comma 3 dispone che al Comitato prendano parte: il Presidente del Consiglio dei Ministri, che lo presiede; l'Autorità delegata, ove istituita; il Ministro degli affari esteri e della cooperazione internazionale; il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico; il Ministro della transizione ecologica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e della mobilità sostenibili e, infine, come previsto dal comma 4, il direttore generale dell'ACN, che svolge le funzioni di segretario del Comitato. Inoltre, ai sensi del comma 5, è previsto che il Presidente del Consiglio dei ministri possa chiamare a partecipare alle sedute del CIC, anche a seguito di loro richiesta, e senza diritto di voto, altri soggetti eventuali, quali gli altri Ministri oltre quelli componenti il Comitato, nonché le altre autorità civili e militari di cui, di volta in volta, si ritenga necessaria la presenza in relazione alle questioni da trattare.

[68] In generale sulle agenzie amministrative v. G. ARENA, *L'esperienza delle agenzie nel sistema amministrativo svedese*, in *Riv. trim. dir. pubbl.*, 1974, pp. 69 ss.; ID., *Agenzia amministrativa*, in *Enc. giur. Treccani*, Roma, 1999, pp. 1 ss.; N BASSI, *Agenzie nazionali ed europee*, in *Enc. dir., Annali*, II, t. 2, Milano, 2009, pp. 41 ss.; H. CAROLI CASAVOLA, *L'amministrazione centrale*, in L. FIORENTINO (a cura di), *Le amministrazioni pubbliche tra conservazione e riforme*, Milano, 2008, pp. 1 ss.; L. CASINI, *Le agenzie amministrative*, in *Riv. trim. dir. pubbl.*, 2003, pp. 393 ss.; C. CORSI, *Agenzia e agenzie: una nuova categoria amministrativa?*, Torino, 2005; L. CASINI, E. CHITI, *L'organizzazione*, in G. NAPOLITANO (a cura di), *Diritto amministrativo comparato*, Milano, 2007, pp. 61 ss.; M. CLARICH, B.G. MATTARELLA, *L'Agenzia italiana del farmaco*, in G. FIORENTINI (a cura di), *I servizi sanitari in Italia*, Bologna, 2004, pp. 263 ss.; M. D'ALBERTI, *Lezioni di diritto amministrativo*, Torino, 2013, pp. 80 ss; C. TOVO, *Le agenzie decentrate dell'Unione Europea*, Napoli, 2016; L. FIORENTINO, A. STANCANELLI, *Le agenzie fiscali (articoli 57, 61-74)*, in S. PAJNO, L. TORCHIA (a cura di), *La riforma del governo*, Bologna, 2000, pp. 401 ss.; C. FRANCHINI, *L'organizzazione*, in S. CASSESE (a cura di), *Trattato di diritto amministrativo*, I, II ed., Milano, 2003, I, pp. 297 ss.; F. MERLONI, *Le agenzie nel sistema amministrativo italiano*, in *Dir. pubbl.*, n. 3, 1999, pp. 717 ss.; F. MERLONI, *Le agenzie a cinque anni dal d.lgs. n. 300: l'abbandono del modello generale?*, in G. VESPERINI (a cura di), *La riforma dell'organizzazione centrale*, Milano, 2005, pp. 21 ss.; G. NAPOLITANO, *L'Agenzia per l'acqua*, in *Giorn. dir. amm.*, 2011, pp. 1077 ss.; G. PETRONI, *Nuovi profili organizzativi dell'evoluzione del sistema amministrativo pubblico*, Padova, 1988; G. SCIULLO, *Alla ricerca del centro*, Bologna, 2000; G. VESPERINI, *Le agenzie (articoli 8-10)*, in S. PAJNO, L. TORCHIA (a cura di), *La riforma del governo*, Bologna, 2000, pp. 145 ss; G. SORICELLI, *Le agenzie amministrative nel quadro dell'organizzazione dei pubblici poteri*, Napoli, 2002.

[69] art. 5, co. 1, del d.l. n. 82/2021.

[70] Per una disamina del provvedimento v. L. PARONA, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di Diritto amministrativo*, n. 6, 2021; Sia inoltre concesso rinviare a F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in f*ederalismi.it,* n. 12, 2022.

Merita evidenziare in questa sede che, in virtù di tali obiettivi, l'ACN non è solo Autorità nazionale per la cybersicurezza, ma anche Autorità nazionale di certificazione della cybersicurezza ai sensi del Reg. (UE) 2019/881, assumendo tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni (art. 7, co. 1, lett. e), nonché Centro nazionale di coordinamento ai sensi del Reg. (UE) 2021/887 che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (art. 7, co. 1, lett. aa).

v) il Nucleo per la cybersicurezza (NC), già istituito con il decreto Monti del 2013, ove era denominato "Nucleo per la sicurezza cibernetica" (NSC) e collocato presso il DIS. Il d.l. n. 82/2021, trasferisce invece, in via permanente, il Nucleo presso l'ACN, modificandone così la sua composizione presidenziale - non più affidata al vicedirettore, ma al direttore generale dell'Agenzia o, per sua delega, al vicedirettore generale - e conservando le funzioni precedentemente affidate. Il Nucleo è responsabile del coordinamento, nel rispetto delle proprie competenze, delle azioni dei diversi attori che compongono l'architettura istituzionale nelle attività di prevenzione, preparazione e gestione delle eventuali situazioni di "crisi cibernetica", nonché di attivazione delle procedure operative di allertamento.

2.1 Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Sebbene la direttiva NIS I abbia costituito un primo passo verso la messa in (cyber)sicurezza delle reti su tutto il territorio dell'Unione, l'applicazione del principio di sussidiarietà ha lasciato fuori dal campo applicativo della normativa diversi settori di indubbia rilevanza per l'interesse nazionale degli Stati membri.

Con il decreto-legge del 21 settembre 2019, n. 105, convertito con modificazioni in legge 18 novembre 2019 n. 133, l'Italia, istituendo il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), è intervenuta 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 [...]»[71].

L'art. 1 co.1, del decreto-legge 105/2019 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, è istituito il perimetro di sicurezza nazionale cibernetica».

[71] Cfr. S. MELE, *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*, Milano, 2020, p. 186. Nello specifico, confrontando le due citate discipline, il PSNC comprende anche quei soggetti attivi nei settori interno, difesa, spazio e aerospazio, telecomunicazioni, economia e finanza, servizi digitali, tecnologie critiche.

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[72].

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, affidando poi tale compito – come per la direttiva NIS – ad alcune amministrazioni centrali dello Stato. Si tratta di disposizioni che hanno l'obiettivo di definire 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[73].

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[74].

L'art. 3 del d.P.C.M. dispone che «in via prioritaria» e fatta salva l'estensione ad altri settori in sede di aggiornamento, sono inclusi nel Perimetro, «in applicazione del criterio di gradualità»:

- I soggetti pubblici operanti nel settore governativo, concernente, nell'ambito delle amministrazioni dello Stato, le attività delle amministrazioni CISR;
- I soggetti pubblici o privati operanti nei settori, ove non ricompresi in quello governativo, dell'interno, della difesa, dello spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro.

Al comma 2, sulla base della distinzione in settori, sono indicate le amministrazioni responsabili dell'individuazione dei soggetti afferenti al Perimetro[75].

---

[72] Per un quadro compleato sui diversi provverimento che compongono la materia si invita a consultare il sito della Camera dei deputati, all'apposita sezione "Aree tematiche" relativa alla "Sicurezza cibernetica" di cui al link:<https://temi.camera.it/leg18/temi/sicurezza_cybernetica.html> (ultima consultazione 23.11.23).

[73] art. 2, lett. a), d.P.C.M. 30 luglio 2020, n. 131.

[74] art. 2, lett. b), d.P.C.M. 30 luglio 2020, n. 131.

[75] Per il settore governativo provvedono le amministrazioni CISR (Affari esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico), mentre relativamente agli altri: per il settore interno, è competente il Ministero dell'interno; settore difesa, il Ministero della difesa; settore spazio e aerospazio, la Presidenza del Consiglio dei ministri; per il settore energia e telecomunicazioni, il Ministero dello sviluppo economico; per il settore economia e finanza, il Ministero dell'economia e delle finanze; per il settore trasporti, il Ministero delle infrastrutture e dei trasporti; per il settore servizi digitali, il Ministero dello sviluppo economico in accordo con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione; per il settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione, in accordo con il Ministero dell'Università e della ricerca; per il settore enti previdenziali/lavoro, il Ministero del lavoro e delle politiche sociali. Si precisa inoltre che, come per la normativa NIS, l'elencazione dei soggetti afferenti al Perimetro è contenuta

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 quale definito da uno Stato membro conformemente al diritto nazionale»[76].

Declinando ed estendendo gli obblighi di sicurezza contemplati dalla direttiva NIS, 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.

Relativamente ai primi, sulla scorta di successivi regolamenti attuativi, l'attuale disciplina impone agli attivi rientranti Perimetro i seguenti adempimenti:

- Notifica degli incidenti di sicurezza aventi impatto su beni ICT, sistemi informativi o servizi informatici al gruppo di intervento CSIRT italiano (ora stabilito presso l'ACN), secondo le tempistiche previste dal d.P.C.M. del 14 aprile 2021, n. 81: ossia, sei ore per gli incidenti «meno gravi», e un'ora per gli incidenti «più gravi» così come individuati nelle tabelle di tassonomia degli incidenti allegate al decreto (All. A);
  Tuttavia, come si apprende dal sito della Camera dei deputati nell'area tematica "Sicurezza cibernetica"[77], si prevede l'emanazione di un ulteriore regolamento relativo alla disciplina delle procedure di notifica degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui art. 1, comma 3, d.L. 105/2019.
  Si aggiunge inoltre che per effetto dell'art. 37-*quater*, co. 1, del decreto-legge 9 agosto 2022, n. 115, convertito con modificazioni dalla Legge 21 settembre 2022, n. 142, è stato introdotto il co. 3-*bis* all'art. 1 del d.L. 105/2019[78]. A tale disposizione a fatto seguito la determina del Direttore generale dell'ACN che il 3 gennaio 2023 ha previsto che i soggetti afferenti al Perimetro notifichino allo CSIRT Italia entro 72 ore anche quegli incidenti aventi un impatto

all'interno di un atto amministrativo a cui è stata apposta la classificazione di segretezza: l'atto non è pertanto pubblicato e non è accessibile. Sul diritto di accesso amministrativo e segretezza vedi M. CAPORALE, *Segreto di Stato, segreto amministrativo e sistema di classificazione delle informazioni*, Libreria Bonomo editrice, Bologna, 2013.

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

[77] Si rinvia al link:<https://temi.camera.it/leg18/temi/sicurezza_cybernetica.html>, consultazione ultima il 28 novembre 2023.

[78] Il testo della disposizione è il seguente «3-bis. Al di fuori dei casi di cui al comma 3, i soggetti di cui al comma 2-bis notificano gli incidenti di cui all'articolo 1, comma 1, lettera h), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza diversi da quelli di cui al comma 2, lettera b), del presente articolo, fatta eccezione per quelli aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici del Ministero della difesa, per i quali si applicano i principi e le modalità di cui all'articolo 528, comma 1, lettera d), del codice di cui al decreto legislativo 15 marzo 2010, n. 66. I medesimi soggetti effettuano la notifica entro il termine di settantadue ore. Si applicano, per la decorrenza del termine e per le modalità di notifica, in quanto compatibili, le disposizioni dell'articolo 3, comma 4, secondo e terzo periodo, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81. Si applicano, altresì, le disposizioni di cui all'articolo 4, commi 2 e 4, del medesimo regolamento. Con determinazioni tecniche del direttore generale, sentito il vice direttore generale, dell'Agenzia per la cybersicurezza nazionale, è indicata la tassonomia degli incidenti che debbono essere oggetto di notifica ai sensi del presente comma e possono essere dettate specifiche modalità di notifica».

sulle reti, sui sistemi informativi e sui servizi informatici di propria pertinenza "diversi" dai beni ICT[79].

- Adozione delle misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici così come elaborate dalla Presidenza del Consiglio dei ministri e dal Ministero dello sviluppo economico, «tenendo conto degli standard definiti a livello internazionale e dell'Unione europea». Tali misure sono state raccolte nei due allegati B e C del citato d.P.C.M. n. 81/2021, adottato su proposta del CISR, e con il previo parere delle Commissioni parlamentari competenti, rispettivamente attinenti: il primo, a «misure di livello più elevato», il secondo, si riferisce a «misure minime di sicurezza per la tutela delle informazioni».
  Si tratta pertanto di due provvedimenti che intendono promuovere un livello di sicurezza basilare omogeneo per tutti i soggetti afferenti al Perimetro (allegato C), declinando misure più incisive ed elevate a seconda della natura di tali soggetti così come individuato nella disciplina generale del regolamento (allegato B).

Altra peculiarità della disciplina, riguarda l'art. 5 del d.l. 105/2019, relativo alle determinazioni del Presidente del Consiglio dei ministri in caso di «crisi di natura cibernetica», ossia in presenza «di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici». Il disposto prevede che il Presidente del Consiglio, su deliberazione del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti, impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati, fornendone informazioni entro trenta giorni al COPASIR. Preme precisare che tale intervento è soggetto al criterio di proporzionalità atteso che la sua attivazione è possibile «per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione».

Infine, il d.l. 105/2019 dispone un'articolata disciplina sanzionatoria strutturata su sanzioni amministrative e illeciti penali[80]. Relativamente alle prime, queste intervengono nelle ipotesi di mancato adempimento degli obblighi di predisposizione e di aggiornamento degli elenchi e di notifica, di inosservanza delle misure di sicurezza, di mancata comunicazione al CVCN, dell'intenzione di procedere all'affidamento di forniture di beni, sistemi e servizi ICT, l'impiego di prodotti e servizi in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN, la mancata collaborazione per l'effettuazione delle attività di test, il mancato adempimento delle prescrizioni indicate in esito alle attività di ispezione e verifica, nonché il mancato rispetto delle prescrizioni di utilizzo dettate dal CVCN.

Sul piano penale, l'art. 1, co. 11, del d.l. 105/2019, introduce una nuova fattispecie penale, nello specifico di reato comune, che prevede: «Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento

[79] Art. 2, determina, 3 gennaio 2023, del Direttore generale ACN.

[80] T. E. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001*, in *Rivista 231*, n. 1, 2020, reperibile al link:<https://www.rivista231.it/Articoli/2020/1/1236/>;

delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni».

Si precisa inoltre che tale fattispecie, in virtù dell'art. 11-*bis* del decreto Perimetro, è entrata a far parte del catalogo dei reati presupposto, la cui commissione comporta la responsabilità amministrativa da reato dell'ente, di cui al decreto legislativo 8 giugno 2001, n. 231.

Il procedimento di accertamento delle violazioni e irrogazione delle sanzioni a carattere amministrativo è affidato all'ACN, e qualora l'Agenzia ravvisi ipotesi penalmente rilevanti, questa è tenuta ad informare la Procura della Repubblica per le indagini giudiziarie nell'ambito del procedimento penale che verrà instaurato, ai sensi e per gli effetti del Codice di Procedura Penale.

2.2 *Segue*. Oltre il segreto di Stato. Il controllo sul *procurement* informatico per fini di sicurezza e interesse nazionale

Lo strumento tipico per tutelare la sicurezza nazionale è il segreto[81]. Tuttavia sottoporre ad un regime di classificazione un'impresa, ossia circoscrivere la conoscenza di informazioni, documenti, atti o attività a determinati soggetti, può avere un impatto negativo sull'attività economica[82].

Oltre all'individuazione dei soggetti ritenuti rilevanti per la sicurezza e l'interesse nazionale, tale esigenza ha quindi portato allo sviluppo di sistemi che si incentrano sul controllo del *procurement* e sulla certificazione dei prodotti. Quest'ultimo tema sarà trattato ampiamente nel proseguo. In tal sede ci soffermeremo pertanto sull'esercizio dei poteri di controllo sui beni ICT quali accertamenti che vengono effettuati sia in sede di acquisto, sia una volta che le risorse informatiche siano state implementate all'interno delle organizzazioni afferenti al Perimetro.

Innanzitutto, 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)[83]. 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).

Con il Decreto del Presidente della Repubblica del 5 febbraio 2021, n. 54, emanato in attuazione dell'art. 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, è stata dettagliata la disciplina sul punto. Nello specifico, oltre al CVNC, sono stati introdotti anche i Centri di Valutazione (CV) presso il Ministero dell'interno[84] e del Ministero della difesa (Ce.Va.)[85], nonché i Laboratori accreditati in

---

[81] Sul punto si rinvia a N. BOBBIO, *Democrazia e segreto*, Torino, Einaudi, 2011; M. BRUTTI, Arcana imperii. *Sulla generalogia del segreto*, in L. FORNI, T. VETTOR, *Sicurezza e libertà …op.cit.,* pp. 193 ss. nonché G. SCANDONE, *Il segreto di Stato*, in C. MOSCA, G. SCANDONE, S. GAMBACURTA, M. VALENTINI, *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)*, Milano, Giuffrè, 2008, pp. 397 ss. Per una lettura aggiornata sul punto v. G. SCANDONE, *Il segreto di Stato e la difesa della Repubblica. L'insegnamento dei recenti eventi internazionali*, in M. VALENTINI, G. MELIS, Pro bono communi. *Scritti in onore di Carlo Mosca*, Napoli, Editoriale scientifica, 2023, pp. 269 ss.

[82] A. PANSA, *La sicurezza nazionale. Innovazione e nuovi limiti*, in *Gnosis*, n. 1, 2019, p. 28.

[83] Si rinvia al sito ufficiale per ulteriori al link:<https://www.acn.gov.it/agenzia/organizzazione/cvcn>.

[84] 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 decreto-legge 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.

[85] Si rinvia al sito ufficiale per ulteriori al link:<https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/ Pagine/default. aspx>.

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.

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[86]. 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»[87].

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]»[88].

---

[86] L. FIORENTINO, *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. DELLA CANANEA, L. FIORENTINO, *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editoriale scientifica, 2020, p. 57.

[87] art. 5, co. 9, d.P.R. 54/2021.

[88] art. 4, d.P.R. 54/2021.

Tra le altre ipotesi, le valutazioni possono infatti costituire un'importante fase preliminare anche per l'attivazione dei poteri speciali da parte del Governo (cc.dd. *golden powers*)[89] 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 decreto-legge 15 marzo 2012, n. 21, potenziando e ampliandone il loro campo applicativo[90].

Per completezza, aggiungiamo inoltre che altra categoria di controlli interessa invece l'invio all'ACN degli elenchi, da aggiornare almeno ogni anno, comprensivi dell'analisi dei rischi, nonché della descrizione dell'architettura e della componentistica in uso presso i soggetti afferenti al Perimetro.

Analizzata brevemente la disciplina dei controlli sui beni ICT oggetto di fornitura per i soggetti afferenti al PSNC, pare ora opportuno indagare sull'identificazione di tali beni.

2.3. *Segue*. L'estensione della sicurezza nazionale "statica" sui beni ICT: il caso delle TELCO e del 5G

Alla luce di quanto sin qui trattato pare che il concetto di sicurezza nazionale, indefinito nell'ordinamento italiano, abbia trovato specificazioni sul piano delle fonti primarie e nelle pronunce della Corte costituzionale (soprattutto le prime due degli anni '70), ove l'indipendenza nazionale, l'integrità territoriale, l'unità e l'indivisibilità della Repubblica, i caratteri essenziali dello Stato democratico e l'esistenza stessa dello Stato sono gli elementi che sono stati considerati di supremo interessi meritevole di protezione da «[...] da ogni azione violenta o comunque non conforme allo spirito democratico che ispira il nostro assetto costituzionale [...]».

Concezione che tralaltro trova riscontro anche nel parere della sezione consultiva per gli atti normativi del Consiglio di Stato in fase di adozione del Regolamento per l'individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale (d.P.C.M. 108/2014) attuativo dell'art. 1, co. 1, del decreto Legge del 15 marzo 2021 n. 21 ove la sicurezza nazionale viene considerata

> un interesse pubblico composito, che presenta due facce: quella della difesa nazionale, deputata a preservare l'integrità dello Stato da minacce esterne di natura bellica, militare o a esse assimilabili, incardinata nel Ministero della difesa, e quella dell'ordine e della sicurezza pubblica, incardinata nel Ministero dell'interno[91].

Tali ricostruzioni sono frutto di un processo di individuazione dei beni meritevoli di protezione secondo una concezione della sicurezza come presupposto, modellata sulle minacce (prevalentemente

---

[89] 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".

[90] S. MELE, *Il Perimetro di Sicurezza Nazionale …op. cit.,* pp. 204 ss.

[91] Cons. Stato, sez. consultiva atti normativi, 20 febbraio 2014, n. 975/2014, reperibil al link:<https:// portali.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=consul&nrg=201400313&nomeFile=201400975_27.html&subDir=Provvedimenti>.

politiche) ritenute rilevanti a seconda delle circostanze che, a nostro modo di vedere, può essere ricondotta alla teoria della securitizzazione che abbiamo già trattato (Cap. I, 2).

Non sono mancate sul piano giuridico le critiche di chi ha riscontrato in tale approccio «uno sbilanciamento dell'area della valutazione della minaccia e delle misure per fronteggiarla, nella sfera dell'Esecutivo», con relativi «rischi in termini di diritti costituzionali di una valutazione formulabile a posteriori, caso per caso»[92].

In particolare è stato osservato che, nonostante la giurisprudenza costituzionale abbia sin dall'inizio ricondotto tale bene nell'ambito dello Stato-comunità, coinvolgendo quindi la «comunità e [i] suoi interessi, non mediati dal fattore politico», nella prassi ha tuttavia prevalso l'approccio "tradizionale" fondato sulla protezione dello Stato-apparato[93].

Il riferimento è al contenuto della pronuncia del '77, ove la Corte costituzionale a proposito del complesso di beni giuridici riferibili alla sicurezza nazionale ha chiarito che questi «devono attenere allo Stato-comunità e, di conseguenza, rimangono nettamente distinti da quelli del Governo e dei partiti che lo sorreggono»[94].

L'Autorevole dottrina ha così prospettato un approccio costituzionalmente orientato teso a valorizzare la sicurezza dello Stato, questa volta inteso come "comunità", attraverso la positivizzazione del concetto di sicurezza nazionale per mezzo di uno sforzo di sintesi del legislatore che tenga conto della normativa primaria e del portato delle pronunce della Corte costituzionale in materia, ma che integri anche

> la funzione di protezione della sicurezza nazionale con i principi, anche etici, delle democrazie costituzionali in un'ottica di garanzia che rafforzi le politiche di sicurezza, superando la visione statica e difensiva, disegnata prevalentemente sulla base di possibili minacce, con un differente approccio, potenzialmente dinamico e innovativo, orientato in direzione della sicurezza collettiva (*collective securit*y) e con una filosofia che non trascuri di considerare l'unità e la coesione come fattori determinanti[95].

Come noto, allo stato attuale, non esistono definizioni del concetto di sicurezza nazionale tra le fonti del nostro ordinamento, sebbene non sia mancato un timido tentativo recente (Cap. I, 3.1). Anche la definizione fornita nel *Glossario di intelligence* elaborato dal DIS[96] consiste in una

---

[92] M. VALENTINI, *Sicurezza della Repubblica e democrazia costituzionale …op. cit.*, pp. 37-38.

[93] Cfr. M. VALENTINI, *Sicurezza della Repubblica e democrazia costituzionale …op. cit.* p. 26 e 45.

[94] Cfr. Corte Costituzionale, sentenza 24 maggio 1977, n. 86, reperibile al link:<https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:1977:86>.

[95] M. VALENTINI, *Sicurezza della Repubblica e democrazia costituzionale …op. cit.* pp. 50-51.

[96] Si rinvia al *Glossario di intelligence. Il linguaggio degli Organismi informativi*, ver. 2019, di cui al link:<https://www.sicurezzanazionale.gov.it/ sisr.nsf/ archivio-notizie/ nuova-edizione-del-glossario-intelligence.html>, ove il concetto è definito come «[c]ondizione in cui ad un paese risultino garantite piene possibilità di sviluppo pacifico attraverso la salvaguardia dell'intangibilità delle sue componenti costitutive, dei suoi valori e della sua capacità di perseguire i propri interessi sui due ambiti costituzionali della sicurezza relativi alla sicurezza nazionale, e all'ordine pubblico. Sebbene vi sia una stretta relazione tra di essi, i due concetti sottendono interessi differenti che rendendo pertanto necessaria una loro trattazione separata. fondamentali a cospetto di fenomeni, condotte ed eventi lesivi o potenzialmente tali. È un bene costituzionale che gode di tutela prioritaria. A tale dimensione "oggettiva" del concetto di sicurezza nazionale ne viene spesso affiancata una "soggettiva", che indica la percezione, da parte dei cittadini, della capacità dello Stato di tutelare se stesso, la propria popolazione ed i propri interessi impiegando gli strumenti del potere nazionale (politici, economici, diplomatici, militari, informativi, etc.). Comunque si intenda definirla, la nozione di sicurezza nazionale – e quella, connessa, di interesse nazionale – mantiene in ogni caso una forte caratterizzazione dinamica, risultando legata tanto al grado di maturità del paese cui si riferisce quanto al contesto storico: ne costituisce esempio la rilevanza strategica assunta dai concetti di sicurezza economico-finanziaria e di sicurezza ambientale. Un'elencazione meramente indicativa degli elementi che rientrano nell'ambito della sicurezza nazionale – e sono come tali, oggetto di tutela ad opera del Sistema di informazione per la sicurezza della Repubblica – deve senz'altro includere

formulazione riepilogativa volta a fornire in poche parole il complessivo quadro concettuale del termine, da diverse prospettive non solo giuridiche, ma che non tiene conto della direzione dottrinale appena accennata.

Nel perdurare della concezione di sicurezza, descritta come «statica e difensiva», pare allora utile cercare di individuare i contorni del concetto analizzando le sue ricadute applicative tra le fonti primarie e secondarie.

L'attenzione è caduta sulla appena citata disciplina introdotta con il d.L. 21/2012, convertito con modificazioni dalla L. 11 maggio 2012, n. 56, che regola i poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni (c.d. *golden powers*)[97].

Si tratta di una disciplina rientrante tra le azioni di intervento dello Stato in economia che trae origine dalla precedente *golden share*[98], l'istituto originato nell'Inghilterra thatcheriana per salvaguardare le società non più assoggettate a controllo pubblico a seguito del processo di privatizzazione, introdotta in Italia con il decreto Legge 13 maggio 1994, n. 332. Tale intervento ha così attribuito allo Stato la possibilità di esercitare poteri speciali[99] nelle società privatizzate operanti nei settori strategici nei settori della difesa, dei trasporti, delle telecomunicazioni, delle fonti di energia, e degli altri pubblici servizi individuate con decreto del Presidente del Consiglio dei Ministri[100]. Poteri che sono stati ritenuti, a più riprese, sproporzionati dalla Corte di giustizia e dalla Commissione europea cha hanno così svolto un ruolo determinante nella ricerca di un difficile contemperamento tra le esigenze di sicurezza nazionale e i principi della libera concorrenza[101]. In

---

l'indipendenza, l'integrità e la sovranità della Repubblica, la comunità di cui essa è espressione, le istituzioni democratiche poste dalla Costituzione a suo fondamento, la personalità internazionale dello Stato, le libertà fondamentali ed i diritti dei cittadini costituzionalmente garantiti nonché gli interessi politici, militari, economici, scientifici ed industriali dell'Italia».

[97] AA.VV., *Golden power*, pubblicato dal Dipartimento delle informazioni per la sicurezza (DIS), dicembre 2019, reperibile al link:<https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/ uploads/2020/01/GNOSIS-golden-power-intelligence.pdf>; M. D'ALBERTI, *Il* golden power *in Italia: norme ed equilibri*, in G. NAPOLITANO (a cura di), *Foreign Direct Investment Screening. Il controllo sugli investimenti esteri diretti*, Bologna, 2020; R. MICCÙ (a cura di), *Un nuovo diritto delle società pubbliche? Processi di razionalizzazione tra spinte all'efficienza e ambiti di specialità*, Napoli, 2019, pp. 343 ss; D. SICLARI, *Privatizzazioni e mercato in un sistema concorrenziale*, in M. PELLEGRINI (a cura di), *Elementi di diritto pubblico dell'economia*, Padova, 2017, pp. 459 ss.; A. SACCO GINEVRI, *I "golden powers" dello Stato nei settori strategici dell'economia*, in *federalismi.it*, n. 22, 2016; Sullo studio della disciplina dallo spettro del diritto comparato v., G. SCARCHILLO, *Privatizzazioni e settori strategici: l'equilibrio tra interessi statali e investimenti stranieri nel diritto comparato*, Giappichelli, 2018.

[98] Sull'evoluzione F. GASPARI, *Libertà di circolazione dei capitali, privatizzazioni e controlli pubblici: la nuova golden share tra diritto interno comunitario e comparato*, Torino, 2015; nonché F. GASPARI, *Poteri speciali e regolazione economica tra interesse nazionale e crisi socioeconomica e politica dell'Unione europea*, in *federalismi.it*, n. 16, 2020, reperibile al link:<https://www.federalismi.it/nv14/articolo-documento.cfm?artid=43534>; F. BASSAN, *Dalla golden share al golden power: il cambio di paradigma europeo nell'intervento dello Stato sull'economia*, in *Studi sull'integrazione eur.*, vol. 9, n. 1 del 2014; L. ARNAUDO, À l'économie comme à la guerre. *Nota su golden power, concorrenza e geo-economia*, in *Mer. conc. reg.*, 2017; G. SCARCHILLO, *Dalla* Golden Share *al* Golden Power: *la storia infinita di uno strumento societario. Profili di diritto europeo comparato*, in *Contratto e Impresa – Europa*, 2015.

[99] S. VALAGUZZA, *Giurisprudenza comunitaria in tema di goldensharee principio di legalità*, in *Foro amm./CdS*, 2003, pp. 2752 ss., ove l'A. precisa che le due espressioni non coincidono. Entrambe attribuiscono al potere esecutivo la possibilità di intervenire in diversi modi su talune società, ma, mentre nel sistema della *golden share* (tipico è il caso del Regno Unito) «loStato conserva la qualità di azionista, restando titolare di un'azione di valore pressoché nullo, ma significativa del mantenimento di un collegamento, seppure formale, con la società», nel sistema dei poteri speciali «l'intervento pubblico prescinde totalmente dalla titolarità di alcuna azione, non corrispondendo ad una quota di partecipazione societaria»:

[100] Cfr. art. 2, d.L. n. 332/1994.

[101] A tal proposito v., R. GAROFOLI, *Golden power e controllo degli investimenti esteri: natura dei poteri e adeguatezza delle strutture amministrative*, in *federalismi.it*, 18 settembre 2019, p. 7, reperibile al link:<https://www.federalismi.it/

ottemperanza alle censure della Corte, il legislatore italiano (prima nel 2003, poi nel 2012 e nel 2020) è intervenuto ridimensionando in maniera significativa l'estensione e i presupposti applicativi di tali poteri.

Da ultimo, rilevante è l'integrazione apportata con il (PSNC), il quale, percorrendo il solco tracciato dal d.L del 2012, ha completato la disciplina dei *golden powers* coordinandola con il Regolamento n. 2019/452 che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione. Allo stesso tempo il decreto ha anche esteso il potere speciale nell'ambito della sicurezza dei sistemi informativi prevedendo l'implementazione di un articolato sistema di misure e controlli preventivi che saranno meglio definiti attraverso regolamentazione secondaria.

Tali interventi hanno portato lo Stato ad assumere ruoli diversi individuati nella «veste di *azionista* (quando il sistema ruotava attorno alla *golden share*), *regolatore* (con il d.l. 15 marzo 2012, n. 21, e il passaggio al diverso sistema dei *golden powers*), fino ad atteggiarsi, a *stratega*, chiamato a perimetrare la nozione di sicurezza nazionale e a verificarne la compromissione sulla base di una pluralità di valutazioni di tipo geo-economico e geo-politico»[102].

Tenteremo di indagare tale evoluzione dell'azione pubblica in economia soffermandoci sui beni qualificati come di interesse per la sicurezza nazionale, analizzando il percorso attuativo del d.L. 21/2021.

Diversamente dalla previgente disciplina, l'esercizio dei *golden powers* da parte del Governo è possibile rispetto a tutte le società, pubbliche o private, che svolgono attività considerate di rilevanza strategica, e non più soltanto rispetto alle società privatizzate o in mano pubblica. Tuttavia, le modalità di esercizio di tali poteri varia a seconda dei settori, ove è particolarmente stringente nei settori della difesa e della sicurezza nazionale (di cui all'art. 1, d.L. 21/2012) e meno stringente, nei settori dell'energia, dei trasporti e delle comunicazioni (di cui all'art. 2, d.L. 21/2012).

Per i primi, il requisito giustificativo è dato dalla «minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale»[103]. In tali settori il Governo può imporre specifiche condizioni all'acquisto di partecipazioni in imprese strategiche; porre il veto all'adozione di delibere, atti o operazioni di particolare rilevanza; opporsi all'acquisto di partecipazioni, ove l'acquirente

---

nv14/articolo-documento.cfm?Artid=40258>, ove l'A. scrive che «[l]a Corte, [...], non ha mai condannato in radice la *golden share*, rimarcando piuttosto che l'esercizio dei connessi poteri è compatibile con la disciplina dell'Unione a condizione che i conseguenti limiti alla libertà di circolazione dei capitali rispondano ad autentiche esigenze di sicurezza e di ordine pubblico o reali motivi imperativi di interesse generale». Il TFUE garantisce infatti all'art. 65 comma 1 lett. b) un diritto degli Stati membri «di prendere tutte le misure necessarie per impedire le violazioni della legislazione e delle regolamentazioni nazionali [...], o di adottare misure giustificate da motivi di ordine pubblico o di pubblica sicurezza». Cfr. V. SQUARATTI, *I limiti imposti dal diritto dell'Unione europea all'intervento pubblico nell'economia: la neutralità delle modalità di perseguimento di obiettivi imperativi di interesse generale*, in *Dir. comm. internaz.*, 2014, 4, 1073 ss. Sulla giurisprudenza in tema di *golden share* v. anche S. DE VIDO, *La recente giurisprudenza comunitaria in materia di golden shares: violazione delle norme sulla libera circolazione dei capitali o sul diritto di stabilimento?*, in *Dir. comm. int.*, 2007; G. PATTI, *I diritti speciali dello Stato tra libera circolazione dei capitali, golden shares e regole di diritto societario*, in *Europa e dir. priv.*, fasc.2, 2011.

[102] R. GAROFOLI, *Golden power e controllo degli investimenti esteri ...op. cit.* p. 1; v. anche G. NAPOLITANO, *L'irresistibile ascesa del golden powere la rinascita dello Stato doganiere*, in *Giorn. dir. amm.*, n. 5 del 2019. Cfr. F. FORTUNA, *I poteri speciali esercitabili da parte dell'esecutivo*, in R. MICCÙ (a cura di), *Un nuovo diritto delle società pubbliche? ...opc.cit.* p. 345, «Il d.l. 21/2012 paleserebbe, pertanto, un sostanziale e rimarchevole cambiamento di approccio da parte del legislatore, che oggi rinunzia a utilizzare strumenti tipici del diritto societario (come, per l'appunto, la previsione di clausole statutarie attributive di poteri speciali) per porsi, al contrario, come regolatore che interviene *ab externo* in presenza di fenomeni di interesse generale o, per così dire, "extra-sociali". Ecco, dunque, che l'intervento dello Stato sembrerebbe spostarsi da un piano squisitamente soggettivo (interventi esercitabili solo nei confronti di determinate e specifiche società) a un piano chiaramente oggettivo (poteri speciali azionabili indifferentemente verso qualsiasi società che svolga una determinata attività)».

[103] Cfr. art. 1, co. 1, d.L. 21/2012.

diverso dallo Stato italiano arrivi a detenere un livello di partecipazione al capitale in grado di compromettere tali interessi.

Per i settori dell'energia, dei trasporti e delle comunicazioni la condizione giustificativa per l'esercizio dei poteri del Governo non è data solo dalla citata minaccia di grave pregiudizio, ma anche dalla relativa «situazione eccezionale, non disciplinata dalla normativa nazionale ed europea di settore»[104] da questa scaturente.

Ci concentreremo in particolare sulle vicende applicative dei settori di cui all'art. 1 considerata la forte connessione, già argomentata, tra sicurezza nazionale e difesa che può inoltre essere colta anche «nell'omogeneità degli interessi oggetto di tutela»[105] della disciplina stante i diversi riferimenti a «l'integrità del sistema di difesa e sicurezza nazionale, la sicurezza delle informazioni relative alla difesa militare, gli interessi internazionali dello Stato, la protezione del territorio nazionale, delle infrastrutture critiche e strategiche e delle frontiere» di cui al comma 2, nonché «alla regolare prosecuzione delle attività, al mantenimento del patrimonio tecnologico, anche con riferimento alle attività strategiche chiave, alla sicurezza e alla continuità degli approvvigionamenti, oltre che alla corretta e puntuale esecuzione degli obblighi contrattuali assunti nei confronti di pubbliche amministrazioni, direttamente o indirettamente, dalla società le cui partecipazioni sono oggetto di acquisizione, con specifico riguardo ai rapporti relativi alla difesa nazionale, all'ordine pubblico e alla sicurezza nazionale» di cui al comma 3.

Il tema centrale è tuttavia interessato dalla individuazione degli attivi di rilevanza strategica nei predetti settori attuata per via regolamentare con i decreti del Presidente del Consiglio dei ministri[106]. In un primo momento, con il d.P.C.M. 30 novembre 2012, n. 253, il Governo ha individuato le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, salvo poi tornare nuovamente su tale elencazione con il d.P.C.M. 2 ottobre 2013, n. 129 che ha inserito tra le attività strategiche di tali settori anche gli «attivi di rilevanza strategica nel settore delle comunicazioni le reti e gli impianti utilizzati per la fornitura dell'accesso agli utenti finali dei servizi rientranti negli obblighi del servizio universale e dei servizi a banda larga e ultralarga».

L'effetto è stato quello di estendere tra i beni di interesse per la difesa e la sicurezza nazionale, qualsiasi rete e sistema di telecomunicazione, indipendentemente dal suo utilizzo[107]. La Commissione è intervenuta sul punto il 25 novembre 2013, osservando in una nota diretta al Governo la potenzionalità lesiva del decreto per il mercato unico, stante la riconduzione di quasi tutti gli impianti di comunicazione negli attivi strategici e, in riferimento a ciò rappresentava inoltre, dato che i decreti attuativi per i settori dell'art. 2 del d.L. 21/2012 non erano ancora stati emanati, quale fosse «il collegamento tra le attività nel settore delle comunicazioni incluse nel nuovo decreto e gli interessi essenziali di sicurezza che potrebbero essere seriamente pregiudicati»[108].

---

[104] Cfr. art. 2, co. 3, d.L. 21/2012.

[105] B. VALENSISE, *I settori strategici dopo la Riforma*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editotoriale scientifica, 2020, p. 138.

[106] Cfr. art. 1, co. 1, d.L. 21/2012.

[107] B. VALENSISE, *I settori strategici dopo la Riforma*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" ...op. cit.,* p. 141.

[108] A. FORTE, *I poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale*, in *Nomos*, n. 3, 2014, p. 10 reperibile al link:<https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2015/01/NOMOS32014_NOTE _FORTE.pdf>.

Con il d.P.R. 6 giugno 2014, n. 108 è stato così adottato il Regolamento che abrogava i due precedenti, riunendo in un solo atto le norme che individuano gli attivi strategici per il sistema di difesa e sicurezza nazionale, includendo tuttavia anche le «attività strategiche chiave».

Peculiare intervento quest'ultimo poiché, sebbene il decreto abbia ricondotto il settore delle telecomunicazioni nel coerente ambito dell'art. 2 del d.L. 21/2012 e relativi regolamenti attuativi, l'introduzione delle "attività strategiche chiave" ha aperto alla possibilità che gli attivi in tale settore possano rientrare, a determinate condizioni, nella disciplina della tutela del sistema di difesa e sicurezza nazionale. Dopo prime difficoltà interpretative sul fatto se la nozione fosse o meno riconducibile a quella di "attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale"[109], la relazione illustrativa del d.P.C.M. ha dipanato ogni dubbio chiarendo che la nozione è mutuata dall'art. 7, par. 3, dell'Accordo quadro di Farnborough del 27 luglio 2000[110], ratificato dall'Italia con L. 17 giugno 2003, n. 148, secondo cui tali attività «vengono a coincidere con quelle particolarmente sensibili, la cui tutela è assolutamente essenziale per mantenere su standard elevati ed adeguati all'evoluzione del quadro delle minacce le azioni di tutela dell'ordine e della sicurezza pubblica e della difesa civile»[111] e pertanto i richiami a tale nozione «rispondono alla logica di identificare, fra quelle di diretto interesse, un nucleo di attività particolarmente sensibili ai fini della difesa e dalla sicurezza nazionale, allo scopo di alzare la soglia dell'attenzione nella fase istruttoria relativa all'applicazione dei "poteri speciali"»[112].

Come anticipato, la materia è stata modificata nel 2019 sulla scorta della attuazione della disciplina sul ricordato Perimetro di Sicurezza Nazionale Cibernetica (PSNC). Con il d.L. 24 aprile 2019, n. 22, è stato introdotto l'art. 1-*bis* nel d.L. 21/2012 il quale ha esteso i poteri speciali del Governo ai servizi di comunicazione elettronica a banda larga con tecnologia 5G, basati sulla tecnologia cloud e altri attivi, qualificati come attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale[113].

Come precisato nella scheda di lettura del d.L. 22/2019, la definizione e l'indicazione delle azioni da intraprendere, sia a livello nazionale sia europeo, al fine di consentire lo sviluppo di un approccio dell'Unione che assicuri la sicurezza delle reti 5G, sono riportate nella Raccomandazione, della Commissione europea del 26 marzo 2019 sulla cybersicurezza delle reti 5G, ove tale tecnologia è definita

> a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy network elements based on previous generations

---

[109] Dossier n. 353 del 2012 del Servizio studi del Senato sul "Disegno di legge A.S. n. 3255 - Conversione in legge, con modificazioni, del decreto-legge 15 marzo 2012, n. 21, recante norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni".

[110] Il testo dell'Accordo è reperibile dal sito del Governo inglese al link:<https://assets.publishing.service.gov.uk/media/5a80912ded915d74e33fb 28e/TS0033_2001.pdf>.

[111] B. VALENSISE, *I settori strategici dopo la Riforma*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" ...op. cit.,* p. 145.

[112] *Ivi*, p. 146.

[113] M. CLARICH, *La disciplina del golden power in Italia e l'estensione dei poteri speciali alle reti 5G*, in G. NAPOLITANO (a cura di), *Foreign Direct Investments Screening. Il controllo sugli investimenti esteri diretti*, Bologna, il Mulino, 2019, pp. 112 ss; M. MENSI, *Il 5G e il "nuovo" paradigma di sicurezza dell'Unione europea. Regole a tutela di autonomia tecnologica e sovranità*, Report, del 15.5.2020, reperibila al link:<https://www.annabonfrisco.eu/ wp-content/uploads/2020/12/Report-PE-5G-Cyber-M.-Mensi.pdf>.

of mobile and wireless communications technology such 4G or 3G. 5G networks should be understood to include all relevant parts of the network[114].

Tuttavia, con il d.L. 21 marzo 2022, n. 21, recante misure urgenti per contrastare gli effetti economici e umanitari della crisi Ucraina, si è previsto «che ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia cloud, possono essere individuati con uno o più decreti del Presidente del Consiglio dei ministri, [...] previo parere delle Commissioni parlamentari competenti, che è reso entro trenta giorni dalla data di trasmissione degli schemi di decreto, decorsi i quali i decreti sono adottati anche in mancanza di parere»[115].

Come è stato osservato[116], l'evoluzione della disciplina degli attivi nei settori della difesa e della sicurezza nazionale ha visto una prima battuta d'arresto nel 2014 da parte della Commissione europea a proposito dell'intenzione del Governo italiano di estendere i beni rientranti in tali attività. La successiva estensione, avvenuta dal 2019 in poi, è invece avvenuta proporio su impulto della stessa Commissione che, sulla scorta della ricordata Raccomandazione del 26 marzo 2019, invitava gli Stati membri di innalzare i livelli di cybersicurezza nazionale tenento conto dei rischi che possono derivare da diversi fattori tecnici, quali le caratteristiche tecniche specifiche delle reti 5G, e, altri fattori, come il quadro giuridico e politico cui possono essere soggetti i fornitori di apparecchiature per le tecnologie dell'informazione e della comunicazione in paesi terzi.

La disamina del caso ci permette di arrivare ad alcune conclusioni sul concetto di sicurezza nazionale. Innanzitutto la disciplina dei *golden powers* nel sistema della difesa e sicurezza intende tutelare interessi che sono stati ricondotti a quelli caratterizzanti la sicurezza nazionale. Difatti il legislatore ordinario si è mosso all'interno del perimetro di quanto elaborato dalla Corte costituzionale nelle ricordate pronunce[117].

Fermi tali interessi, l'attuazione della disciplina ordinaria per via regolamentare ha tuttavia confermato la capacità del decisore di selezionare le paure dal quale fornire protezione e sicurezza. In particolare, la vicenda che delle TELCO e della tecnologia 5G ha evidenziato due aspetti: la prima è l'estensione del concetto di sicurezza nazionale, data dalla riconduzione negli interessi alla sicurezza nazionale di tali beni[118]; la seconda è che tale concetto non è più radicato alle sole esigenze avvertite a livello locale da parte di un singolo Stato membro, ma sia sempre più influenzato anche dagli ordinamenti sovranazionali. Come in questo caso l'Unione europea che, in un primo momento ha ritenuto tale estensione lesiva alla libera circolazione dei beni, salvo poi tornare sul punto alla luce dei nuovi sviluppi geopolitici e geoeconomici della Cina nel 2019[119].

---

[114] C(2019) 2335, *Cybersecurity of 5G networks*, 26 marzo 2019, p. 5, reperibila al link:<https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks>.

[115] Cfr. art. 28, co. 1, d.L. 21/2022, che ha moficato l'art. 1-*bis*, co. 1, del d.L. 21/2012.

[116] B. VALENSISE, *I settori strategici dopo la Riforma*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" ...op. cit.,* p. 148.

[117] B. VALENSISE, *I settori strategici dopo la Riforma*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" ...op. cit.,* p. 138.

[118] Capacità espansiva evidenziata da Alcuni rispetto al quadro disciplinare in tema di contrasto al terrorismo, A. MONTI, *Sicurezza e/o democrazia? Le debolezze strutturali nelle norme italiane sulla cybersecurity*, in *La Repubblica*, 3 novembre 2023 reperibila al link:<https:// www.repubblica.it/ tecnologia/blog/strategikon/2023/11/03/news/il_castrum_normativo_della_cybersecurity_italiana_ha_una_debolezza_strutturale-419494431/> (ultima consultazione 7.1.24).

[119] Si rinvia alla Risoluzione del Parlamento europeo del 12 marzo 2019 sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce (2019/2575(RSP)), reperibile al link:<https://www.europarl.europa.eu/doceo/document/ TA-8-2019-0156_IT.pdf?redirect>.

3. La definizione di cybersicurezza tra norme tecniche e giuridiche

Analogamente a quanto già svolto per la sicurezza in senso tradizionale, riteniamo che il primo approccio utile all'analisi al concetto di cybersicurezza sia quello letterale che vede l'apposizione del lemma "cyber" a quello di sicurezza, quale implicito riferimento all'elemento del "cyberspazio", di cui si è già parlato nella Parte I.

Nella medesima sezione, abbiamo anche evidenziato come l'interesse degli Stati verso il cyberspazio sia arrivato "dopo", a seguito dell'intensificarsi degli attacchi informatici, nonché dei loro effetti dirompenti sulla società. Prima di allora la sicurezza delle reti e dei sistemi informatici era affidata agli esperti di settore e alle aziende ICT che con il tempo eleborarono norme tecniche a tal proposito.

Prendendo in considerazione il panorama delle norme tecniche prodotte fino ad oggi è possibile distinguere almeno tre tipologie[120]. Innanzitutto, le norme di primo tipo, con il quale sono stati regolati i processi produttivi al fine di garantire determinate caratteristiche nei prodotti. Le norme di secondo tipo hanno trovato spazio quando la normazione tecnica ha iniziato ad interessare la progettazione e le caratteristiche prestazionali dei prodotti. Infine, con l'introduzione della famiglia di norme ISO 9000, si sono aggiunte le normative di terzo tipo, volte a normare l'intero sistema di produzione attraverso la formulazione dei c.d. sistemi di gestione della qualità.

Proprio all'interno di quest'ultima categoria di norme, 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 sulla sicurezza delle informazioni (*information security*)[121]. A tal proposito si faccia riferimento ad alcune definizioni individuate nel bollettino dell'Agenzia statunitense competente nella gestione delle tecnologie, la *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.).

Da ciò è possibile dedurre che 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

---

[120] P. ANDREINI, *La normativa tecnica tra sfera pubblica e 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 industiali*, Bologna, Il Mulino, 1995, pp. 90 ss.

[121] C. GALLOTTI, *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Lulu press, 2022, p. 122.

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.

In un documento del 2013, elaborato dal gruppo di supporto degli enti di normazione europea CEN e CENELEC, il *Cyber Security Focus Group* (CSCG), sono state raccolte e confrontate le definizioni del concetto di cybersicurezza all'interno di diverse norme tecniche[122].

L'indagine è particolarmente utile poiché l'analisi comparata delle formulazioni è stata condotta secondo alcuni criteri che possiamo assumere come parametri di riferimento.

Oltre alle tre proprietà appena ricordate, dal report emergono anche altri riferimenti quali: se l'azione di sicurezza abbia ad oggetto qualsiasi rischio proveniente dal cyberspazio, o piuttosto questa si focalizzi su determinate componenti, logiche o fisiche, ad esso connesse; la motivazione, si distinguono infatti formulazioni che fanno riferimento alle sole minacce condotte intenzionalmente, a quelle che ricomprendono anche gli indicenti di sicurezza non intenzionali. Ed infine, il riferimento o meno agli asset oggetto delle minacce, dato che non tutte le definizioni si estendono anche a quelli fisici, ricomprendendo solo quelli logici.

Passando al piano giuridico, i recenti interventi legislativi a livello europeo e nazionale hanno provveduto ad introdurre nei rispettivi ordinamenti il concetto di cybersicurezza (ed in Italia anche quello di cyberresilienza come vedremo *infra* 5.2).

Per quanto riguarda l'Italia, con il decreto-legge 14 giugno n. 82 del 2021 si è introdotto il concetto giuridico di «cybersicurezza» (di cui si dirà *infra* 3.2), sebbene in sede referente vi siano state proposte volte a rimpiazzare il lemma «sicurezza cibernetica»[123], così come era stato previsto per il PSNC.

In realtà il concetto di "sicurezza cibernetica" non è estraneo all'ordinamento italiano. Questo infatti era già stato utilizzato nel d.P.C.M. 131/20, nel d.L. 105/19 e prima ancora il d.Lgs. 65/18 che ha recepito la Direttiva NIS I, nonché ancora prima nel d.P.C.M. 17 febbraio 2017.

Il matematico Norbert Wiener, nella sua opera *Cybernetics: Or Control and Communication in the Animal and the Machine*, pubblicata nel 1948, definì la cybernetica come «la teoria del controllo e comunicazione negli animali e nelle macchine»[124]. Il legame tra la cybernetica e le reti informazionali avvenne tuttavia successivamente, sulla scorta degli studi del matematico russo Andrej Nikolaevič Kolmogorov che, mutuando dalla definizione di Wiener enfatizzò l'aspetto delle informazioni nei sistemi cybernetici. Secondo lo studioso la cybernetica è infatti «la scienza dei metodi di elaborazione e utilizzo delle informazioni nelle macchine, negli organismi viventi e nella loro combinazione»[125].

Alla luce di ciò, nel corso della presente trattazione, anche in conformità con il recente intervento legislativo del 2021, si è scelto di far riferimento al concetto di "cybersicurezza" in quanto immediata traduzione del lemma "*cybersecurity*", che ci permette di cogliere un ulteriore sfaccettatura del

---

[122] CEN-CENELC CSCG, *Recommendation #2 – Definition of Cybersecurity*, ver. 01.08, 2013.

[123] Si rinvia alla sezione Emendamenti relativi all'"Atto Camera: 3161" del sito della Camera - di cui al link:<https://www.camera.it/leg18/126?tab=3&leg=18&idDocumento=3161&sede=&tipo=#referente> - ove, tra le otto proposte emendative all'art. 1 del d.L. n. 82/2021 rientra anche quella relativa alla sostituzione della parola "cyberiscurezza" con quella di "sicurezza cibernetica".

[124] Cfr. N. WIENER, *Cybernetics: Or Control and Communication in the Animal and the Machine*, MIT University Press, Cambridge, 1948.

[125] Sul punto si rinvia a A. G. KEFALAS, *Cybernetics*, in *Encyclopedia of Information Systems*, 2003, reperibile al link:<https://www.sciencedirect.com/topics/computer-science/cybernetics>.

concetto potendo distinguere la *cyber-security* dalla "cyber-*safety*". A tal proposito, sia concesso rinviare alla seguente distinzione, secondo cui:

> security as unimpaired integrity of an entity itself, e.g., of a technical device, communication, a society, or a state, et cetera, from external risks and dangers, and safety as the absence of harmfulness or possible adverseness of such an entity to persons, their health, or economic or environmental situation. […] In relation to safety, risk is sometimes considered to be the eventual occurrence of unintentional events, while in security contexts risks are deemed to involve intentional malicious events[126].

3.1. Il concetto giuridico di cybersicurezza europea: sicurezza del mercato unico e sicurezza dell'umano

La definizione di "cybersicurezza" a livello europeo è stata introdotta al culmine di un lungo processo che ha preso avvio con la disciplina sulla protezione delle infrastrutture critiche.

Ripercorrendo brevemente le tappe più significative di questo percorso[127], già nel 2001 la Commissione europea adottava una Comunicazione sulla criminalità "informativa" ove veniva data la definizione di «sicurezza dei sistemi informatici e di rete» facendo riferimento alla «capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema»[128].

Nel 2004, anno in cui veniva istituita l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), il Consiglio europeo lanciava lo *European Program for Criminal Infrastructure Protection* (EPCIP) con lo scopo di incrementare la prevenzione, la preparazione e la risposta europea agli atti di terrorismo informatico attraverso l'istituzione di una rete di *information sharing* per la protezione delle infrastrutture critiche (la *Critical Infrastructure Warining Information Network* - CIWIN), nonché per l'erogazione di finanziamenti per la realizzazione di progetti sulla protezione delle infrastrutture critiche e il varo di una normativa riguardante le infrastrutture critiche europee che avverrà poi nel 2008 con la Direttiva 2008/114/Ce relativa all'individuazione e designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la loro protezione[129].

Nella Comunicazione sulla protezione delle infrastrutture critiche informatizzate del 2011[130], la Commissione constatava l'insufficienza delle strategie nazionali di cybersicurezza e della resilienza

---

[126] A. VEDDER, *Safety, Security and Ethics*, in A. VEDDER, J. SCHROES, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, Cambridge, Antwerp, Chicago, 2020, pp. 12-13, reperibile al link:<https://www.cambridge.org/core/books/security- and-law/CA0979A1D9C70C48222BBA997812D41F>.

[127] Sul punto v. A. ROTONDO, *Cyber security e protezione delle infrastrutture critiche: l'efficacia del modello europeo*, in S. MARCHISIO, U. MONTUORO (a cura di), *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, Giappichelli, 2019, p. 125.

[128] Cfr. art. 2, co. 1. COM (2000)890 del 26 gennaio 2001, Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione mediante la lotta alla criminalità informativa.

[129] In particolare, all'art. 2, lett. e), Direttiva 2008/114/Ce viene fornita la definizione di «protezione» come «tutte le attività volte ad assicurare funzionalità, continuità e integrità delle infrastrutture critiche per evitare, mitigare e neutralizzare una minaccia, un rischio o una vulnerabilità».

[130] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla Protezione delle infrastrutture critiche informatizzate. Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale, Bruxelles, 31 gennaio 2011.

dei loro sistemi e invitava gli Stati ad adottare una serie di misure basate sulla cooperazione transfrontaliera portando così all'esigenza di adottare uno specifico intervento armonizzato relativamente alla protezione delle infrastrutture critiche informatizzate.

Nel 2016 viene adottata la prima normativa sullo specifico tema della «sicurezza delle reti e dei sistemi informativi» con la Direttiva 2016/1148, per l'appunto anche nota come direttiva *Network and Information Security*- NIS, oggi abrogata dalla Direttiva (UE) 2022/2555 (direttiva NIS II) entrata in vigore il 17 gennaio 2023.

Nonostante la rubricazione, dall'analisi dei testi emerge come il legislatore europeo abbia inteso coniugare ancora una volta la sicurezza informatica con la protezione delle infrastrutture critiche. Difatti, parte delle prescrizioni volte a «garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno» (art. 1), consistono perlopiù in una serie di obblighi gravanti sui soggetti individuati nella Direttiva come «soggetti essenziali» e «soggetti importanti», che dovranno adempierli a pena di ingenti sanzioni amministrative[131].

Solo con il successivo Regolamento (UE) 2019/881, relativo all'ENISA e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (c.d. *Cybersecurity Act*), l'Unione, ha introdotto - per la prima volta all'interno di un atto normativo giuridico - la nozione di "cybersicurezza", definendola all'art. 2, n. 1, 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».

Dal breve quadro tracciato emerge innanzitutto la distinzione fondamentale tra i due concetti di «cybersicurezza» e di «sicurezza dei sistemi informatici e di rete».

La nozione di cybersicurezza europea - che comprende anche la "sicurezza delle reti e dei sistemi informatici" - è quindi diretta alla più ampia «sicurezza degli individui nel cyberspazio»[132].

Questo rappresenta un ulteriore elemento significativo della formulazione fornita dal legislatore europeo che, oltre ad aver definito per la prima volta la cybersicurezza all'interno di un atto normativo vincolante, è andato al di là del mero significato tecnico della materia (ossia la tutela della riservatezza, integrità e disponibilità delle risorse informartiche e delle informazioni racchiuso nella «sicurezza dei sistemi informatici e di rete»), giungendo al concetto di sicurezza dell'umano, dato il riferimento «[a]gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»[133].

Pertanto nell'ordinamento europeo la cybersicurezza comprende sia la protezione dei sistemi e delle reti, sia la protezione delle persone fisiche intese non solo come utenti, ma anche come coloro che sebbene non utilizzino tali risorse possono comunque essere impattati dagli effetti negativi di un attacco informatico su di esse o dalla loro mera disfunzione.

---

[131] Sulla "delega" della sicurezza dal potere pubblico agli amministrati seppur nell'ottica della cybersicurezza nazionale italiana v. A. MONTI, *Internet e ordine pubblico*, in G. CASSANO, S. PREVITI (a cura di), *Il diritto di internet nell'era digitale*, Milano, Giuffrè, 2020, 79, ove l'A. scrive «[...] chi è responsabile del funzionamento dei servizi essenziali deve farsi carico in proprio della loro difesa, sopportando le conseguenze del mancato rispetto di complessi obblighi tecnici e organizzativi in termini di sanzioni amministrative particolarmente afflittive».

[132] G. CHRISTOU, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy,* Londra, Palgrave, 2019, p. 187.

[133] Cfr. Cfr. art. 6, co. 1, n. 2 della Direttiva NIS II.

Secondo Alcuni[134], tale approccio "*human-centric*" promosso dall'Unione è un richiamo al concetto di «sicurezza umana» elaborato in seno alle Nazioni Unite[135] con il fine di riconcepire la sicurezza come azione non più legata alla sola protezione dello Stato e quindi all'uso della forza (c.d. approccio realista v. infra Cap. I, 2), ma interessandosi anche degli effetti delle minacce alla sicurezza internazionale che comprende anche la sicurezza energetica, climatica e, da ultimo quella del cyberspazio[136].

Sebbene ciò non abbia comportato alcuna certezza circa l'applicazione del diritto internazionale umanitario (c.d. DIU) nelle questioni relative al cyberspazio[137].

Si tratta pertanto di un passo in avanti che distingue tale definizione (giuridica), da quella contemplata dalle diverse norme tecniche sul punto le quali, come già anticipato, si limitano perlopiù ad indirizzare le azioni di cybersicurezza verso le reti, i sistemi e gli *assets* informatici[138] al fine di garantire continuità e sicurezza degli affari dell'organizzazione e quindi non esplicitano la direzione di tali azioni verso l'umano, la sua sicurezza e tantomento verso la tutela dei diritti e delle libertà[139].

Diversamente, la formulazione della definizione di «sicurezza dei sistemi informatici e di rete» è invece più vicina a queste norme teniche. Lo conferma il rinvio ai principi fondamentali della *computer* e della *information security*, ove viene fatto riferimento ai concetti di "disponibilità", "autenticità", "integrità" e "riservatezza" dei stitemi informatici e delle informazioni in essi conservati, trasmessi o elaborati, da azioni dolose o imprevisti[140].

In particolare la definizione, ripresa anche nella disciplina NIS II all'art. 6, co. 1, n. 2[141], prevede che il fine sia quello di garantire la continuità del servizio erogato e la protezione delle informazioni trattate dal soggetto fornitore (tra cui possono rientrare anche i dati personali). Sul concetto di garanzia della continuità di un servizio vi torneremo a breve a proposito della "cyberesilienza" (*infra* 5 e 5.1 nonché Pt. III, Cap. II. 2).

Riteniamo inoltre che tali definizioni debbano essere interpretate anche alla luce del contesto normativo in cui sono inserite o richiamate. Oltre al già citato *Cybersecurity Act*, e alla disciplina NIS, troviamo richiami alla sicurezza dei sistemi informatici e di rete, e alla cybersicurezza anche in

---

[134] Così G. DE VERGOTTINI, *Sicurezza e diritti fondamentali*, in in L.E.R. VEGA, L. SCAFFARDI, I. SPIGNO, *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, Editoriale scientifica, 2021, p. 30.

[135] Sulla genesi ed evoluzione del concetto si rinvia a R. JOLLY, D.B. RAY, *The Human Security Framework and National Human Development Reports*, United Nations Development Programme, NHDR Occasional Paper 5, 2006, pp. 4 ss.

[136] Il riferimento è al documento ONU, *Human Development Report*, 1994, p. 24, reperibile al link:<https://hdr.undp.org/content/human-development-report-1994>, ove è fatto riferimento alle diverse "componenti" della sicurezza umana.

[137] D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità nel cyberspace*, Napoli, Editoriale scientifica, 2020, p. 103.

[138] V. ad esempio le definizioni contenute nelle norme ISO/IEC 27002:2009, ITU-T X.1205, NIST Special Publication 800-39.

[139] La norma tecnica ISO/IEC 27032 definisce la cybersecurity come «preservation of confidentiality, integrity and availability of information in the Cyberspace», e definisce il cyberspazio come «the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form [enfasi aggiunta]».

[140] Sulla coicidenza di detta definizione con quelle presenti nelle norme tecniche di settore si faccia riferimento al documento elaborato dal Centro studi CEN-CENELC CSCG, *Recommendation #2 – Definition of Cybersecurity*, ver. 01.08, 2013, ove è stata condotta un'analisi comparata delle formulazioni secondo alcuni criteri quali: il riferimento al RID delle informazioni o dei sistemi informatici, l'oggetto dell'azione di sicurezza (se il cyberspazio in generale o determinati asset), e l'origine della minaccia (dolosa o non dolosa).

[141] Cfr. art. 6, co. 1, n. 2 della Direttiva NIS II, «la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi».

altre norme di diritto derivato. In particolare, nel Regolamento 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario (c.d. Regolamento DORA)[142], è fatto riferimento alla sola sicurezza delle reti e delle informazioni, mentre nella Direttiva 2022/2557, relativa alla resilienza dei soggetti critici (c.d. Direttiva CER), è precisato all'art. 1, par. 8, che la disciplina non trova applicazione alle materie della NIS II ma «gli Stati membri assicurano che la presente direttiva e la direttiva (UE) 2022/2555 siano attuate in modo coordinato»[143].

Il fine che accomuna le citate discipline è quello di - per riprendere le parole della NIS - «migliorare il funzionamento del mercato interno»[144]. La base di legittimità su cui trovano fondamento è infatti l'art. 114 TFUE che, come noto, disciplina il ravvicinamento delle legislazioni nazionali che possono ostacolare il funzionamento del mercato interno, cui si aggiungono norme speciali in materie specifiche. Nello specifico il disposto prevede che il legislatore europeo possa ricorrere alla procedura ordinaria per armonizzare le «disposizioni legislative, regolamentari ed amministrative» degli Stati membri per il raggiungimento degli obiettivi delineati a livello europeo (ex art. 26 TFUE) per «l'instaurazione e il funzionamento del mercato interno»[145].

Al comma 3, è previsto che la Commissione possa proporre a tal fine interventi in alcune materie, tra cui anche la sicurezza, ma solo per il perseguimento di «un livello di protezione elevato, tenuto conto, in particolare, degli eventuali nuovi sviluppi fondati su riscontri scientifici»[146].

Il ricorso a tale base di legittimità in una materia particolarmente trasversale come quella della cybersicurezza ha sollevato critiche nella dottrina[147]. Sebbene il quadro disciplinare al riguardo intende escludere ogni invasione nella sfera di competenza degli Stati[148], e sebbene nel caso della disciplina NIS il fine sia proprio quello di innalzare il livello di cybersicurezza nell'Unione, è stato osservato che «il centro di gravità di questa misura [NIS I] non sembra essere costituito dal mercato interno ma dal desiderio di armonizzare, seppur in modo minimo, le norme in materia di sicurezza che gli operatori delle reti e dei sistemi informativi devono rispettare a livello nazionale» e quindi «il centro di gravità di queste misure è costituito dal rafforzamento della sicurezza» piuttosto che del mercato unico[149].

---

[142] Il riferimento è alla sola sicurezza delle reti e dei sistemi informatici di cui all'art. 3, n. 4, del Reg. (UE) 2022/2554.

[143] Cfr. art. 1, par. 8, Dir. (UE) 2022/2557.

[144] Cfr. art. 1, co. 1, della Direttiva NIS II.

[145] Art. 114 TFUE.

[146] *Ibidem*.

[147] R. WESSEL, *Towards EU Cybersecurity Law: Regulating a New Policy Field*, in N. TSAGOURIAS, R. BUCHAN (a cura di), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 403–405; M. VARJU, *5G networks, (cyber)security harmonisation and the internal market: the limits of Article 114 TFEU*, in *European Law Review*, 2020, pp. 471-486.

[148] Oltre a quanto già argomentato sul punto in 1.1 (i), si faccia riferimento alla lettera dell'art. 1, par. 6, della Dir. (UE) 2022/2555 che prevede «La [...] direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati»; o all'art. 1, par. 5 della Dir. (UE) 2022/2557 ove è previsto che «La [...] direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e la difesa e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico».

[149] S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE, III, 2021, Sezione Atti Convegni AISDUE*, n. 5, 20 dicembre 2021, p. 81.

3.2. La cybersicurezza nazionale italiana

Il decreto-Legge 14 giugno n. 82 del 2021, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale», ha introdotto per la prima volta nell'ordinamento italiano, la nozione di cybersicurezza (nazionale).

In precedenza (*infra* 3.1), a proposito della sicurezza nazionale abbiamo avuto modo di evidenziare come sebbene questo concetto - fondamentalmente politico - sia stato oggetto di un processo di normativizzazione. I riferimenti normativi rinvianti ad esso lo rendono tuttavia un concetto dalla portata estremamente generale, privo di autonomia giuridica, e tendenzialmente immune dal controllo giuridico[150].

In questa sede analizzeremo pertanto il concetto di cybersicurezza nazionale tentando di cogliere eventuali differenze o somiglianze rispetto alla sicurezza nazionale tradizionale.

Innanzitutto, l'art. 1, co. 1, lett. a), del decreto, coordinato con la Legge di conversione 4 agosto 2021, n. 109[151], definisce la nozione come

> l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Precisiamo che l'inciso relativo alla «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» è stato introdotto nel corso dell'esame in sede referente delle Commissioni I e IX della Camera[152], per poi essere trasposto in sede di conversione nel testo della legge del 4 agosto 2021[153].

Come per la formulazione della cybersicurezza europea, anche la definizione di cybersicurezza nazionale è frutto di un processo di composizione ove è possibile individuare due anime: quella derivante dai principi e concetti elaborati nelle normative tecniche sulla sicurezza informatica e delle informazioni, e quella di carattere giuridico-politico, relativa alla collocazione della materia (anche) tra le attività dirette alla tutela della sicurezza e dell'interesse nazionale. Motivo per cui la citata "aggiunta" in sede referente ha conferito particolare rilievo alla formulazione, ma ha anche aperto a problemi interpretativi.

---

[150] Così A. MONTI, *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, in *Quaderno speciale CASD n. 1 - Scenari globali e interessi nazionali: pandemia, continuità, cambiamento*, 2020, reperibile al link:<https://www.casd.it/course/view.php?id=441&lang=en>.

[151] Si rinvia al link della Gazzetta ufficiale:<https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-08-04&atto.codiceRedazionale=21A04841&elenco30giorni=true>.

[152] Il disegno di legge in questione è stato identificato con il progressivo "Atto Camera: 3161". Nello specifico si rinvia alla sezione Emendamenti del sito della Camera - di cui al link:<https://www.camera.it/leg18/126?tab=3&leg= 18&idDocumento=3161&sede=&tipo=#referente> - ove è possibile scorrere le diverse proposte in sede referente (relative all'art.1 vi sono state otto proposte) che hanno portato all'attuale formulazione della disposizione. Gli emendamenti apportati dal Senato in sede di conversione, Atto Senato n. 2336, hanno invece interessato dagli artt. 4 e successivi, come è possibile notare al relativo sito:<https://www.senato.it/leg/18/BGT/Schede/Ddliter/testi/54303_testi. htm>.

[153] Si invita alla lettura del decreto-legge 14 giugno 2021, n. 82 (in Gazzetta Ufficiale - Serie generale - n. 140 del 14 giugno 2021), coordinato con la legge di conversione 4 agosto 2021, n. 109 (in Gazzetta Ufficiale - alla pag. 1), recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale».

Il riferimento alla "sicurezza nazionale" nello "spazio cibernetico" costituisce infatti un rinvio a due concetti su cui insistono, a loro volta, ulteriori dubbi interpretativi.

Relativamente al primo, si è già detto della sua eccessiva ampiezza e carenza di autonomia giuridica (*infra* Cap. I, 3.1). Caratteristiche queste che paiono trovare conferma anche nella definizione avanzata in sede referente, sempre a proposito del citato d.L. n. 82/2021, all'interno di un eventuale art. 1, co. 1, lett. a-*bis* al decreto, ove la "sicurezza nazionale" è stata descritta come «il dovere del Governo di proteggere e realizzare gli interessi nazionali nel rispetto dei principi costituzionali e delle prerogative del Parlamento»[154]. La proposta non ha poi trovato approvazione in sede di conversione.

Per quanto riguarda lo "spazio cibernetico" invece, oltre quanto già abbiamo trattegiato in precedenza (Parte I), pare necessario osservare che questo concetto ha trovato definizione in alcuni documenti interni. Nel "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" del 2013 questo veniva definito come

> l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete[155].

Secondo Alcuni la cybersicurezza nazionale non è completamente coincidente con il concetto di sicurezza nazionale, ma certamente vi rientra seppur solo relativamente ai beni e servizi di natura informatica[156]. Tale interpretazione ci sembra percorribile. Il riferimento è difatti all'inciso «fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124 [...]» che quindi distingue l'azione perm fini di cybersicurezza da quello per la "sicurezza della Repubblica".

Tuttavia, l'orientamento delle azioni di mera sicurezza informatica e delle informazioni «anche» ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nel cyberspazio, ci permette di concludere che la cybersicurezza, diversa dalla sicurezza nazionale, ne è comunque ricompresa e si esprime attraverso una estensione dell'azione di governo in questo settore.

Abbiamo già avuto modo di argomentare sulla vicenda che ha interessato le tecnologie 5G e il settore delle Telco nel 2019 (*infra* 2.3). Dal punto di vista politico, si è dimostrato come i poteri del Governo nell'ambito della (cyber)sicurezza nazionale non si limitino più soltanto all'apposizione del Segreto di Stato ma comprendono anche poteri di intervento in ambito economico. Nel particolare caso delle reti pubbliche di comunicazione, abbiamo evidenziato la progressiva estensione di tali prerogative dell'Esecutivo anche su beni prima di allora non ricompresi nell'ambito della sicurezza nazionale e della difesa.

Tuttavia non riteniamo di poter concludere che la cybersicurezza nazionale costituisca una *species* nel contesto delle "sicurezze" nazionali, pittosto pare ragionevole sostenere, come già intuito in dottrina, che la cybersiucrezza nazionale sia una componente trasversale alla difesa dello Stato e

---

[154] Vedi la proposta emendativa 0.1.7.2., dell'ex deputato Giovanni Luca Aresta, nelle commissioni riunite I-IX in sede referente riferita al C. 3161 0.1.7.2., pubblicata nel Bollettino delle Giunte e Commissioni del 15/07/2021. Si rinvia al link:<https://documenti.camera.it/apps/emendamenti/getProposteEmendative.aspx?contenitorePortante=leg.18.eme.ac.3161&tipoSeduta=1&sedeEsame=referente&urnTestoRiferimento=urn:leg:18:3161:null:null:com:0109:referente&tipoListaEmendamenti=1>.

[155] Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, 2013, p. 10.

[156] Cfr. A. PANSA, *La sicurezza nazionale …op.cit.*, p. 34.

all'ordine e alla sicurezza pubblica, quale «articolazione tecnica avente natura ordinatoria e non gerarchica»[157].

Infine, il riferimento a «gli obblighi derivanti da trattati internazionali», ci porta nuovamente a concludere che, come per la sicurezza in generale, tale concetto non può essere definito in sede meramente nazionale, ma deve comuqnue tener conto del più ampio quadro dei diritti, doveri e libertà degli ordinamenti sovranazionali.

4. Il concetto di resilienza

La resilienza nasce dell'esigenza di far fronte ad imprevedibili e incerti eventi dannosi, ossia rischi e pericoli, tali da mettere in crisi il "sistema" e impedendo al modello di sicurezza tradizionale di funzionare.

Come si comprenderà, sicurezza e resilienza non sono concetti slegati ma la rilevanza assunta da quest'ultimo, soprattutto nel contesto informatizzato, ne impone una trattazione specifica. Prima di ciò, riteniamo tuttavia opportuno soffermarci brevemente sulle richiamate nozioni di rischio e pericolo. La distinzione è innanzitutto frutto di un certo filone delle scienze sociali, riconducibile a Niklas Luhmann, che ha definito il rischio quale danno «conseguenza della decisione», e il pericolo quale danno dovuto a fattori esterni[158], differenziando così le minacce derivanti da decisioni proprie dell'individuo, da quelle provenienti da altri uomi o dall'ambiente circostante[159]. Da qui la relazione tra chi decide e chi subisce gli effetti della decisione: i rischi assunti da un decisore divengono infatti pericoli per coloro che sono coinvolti dalla scelta del primo[160].

Secondo le scienze sociali l'indeterminatezza della minaccia che caratterizza i tempi moderni, dal processo di industrializzazione in poi, sarebbe riconducibile proprio al fatto che lo sviluppo della vita associata e il crescente grado di complessità dei sistemi sociali hanno reso sempre più difficile per gli attori valutare le conseguenze dei propri comportamenti[161], dando così vita a quella che Ulrick Back ha definito la "società del rischio".

Deve tuttavia osservarsi che in questo clima di incertezza, che renderebbe qualsiasi azione umana fonte di eventuali rischi/pericoli, la rispettiva azione di protezione da parte del potere pubblico potrebbe facilmente scivolare in una concezione di massima sicurezza e di difesa totale che andrebbe fortemente a limitare le libertà umane. La gestione del rischio diventa quindi un tema particolarmente importante e sensibile nelle democrazie costituzionali volte a tutelare le libertà umane, soprattutto in considerazione del fatto che il rischio non ha necessariamente una accezione negativa, di possibile futuro danno, ma anche positiva, quale fattore che stimola innovazione e progresso[162].

---

[157] A. MONTI, *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, in *Quaderno speciale CASD n. 1 - Scenari globali e interessi nazionali: pandemia, continuità, cambiamento*, 2020, p. 6, reperibile al link:<https://www.casd.it/course/view.php?id=441&lang=en>.

[158] N. LUHMANN, *Sociologia del rischio*, traduzione di Giancarlo Corsi, Milano, Mondadori, 1996, pp. 11 ss. Precisiamo che tale distinzione non è invece considerata in U. BECK, *La società del riscio …op. cit.*

[159] In altri termini la differenza è che mentre con il concetto di pericolo si è soliti indicare un danno sicuro derivante da una certa azione od omissione, il rischio indica invece un danno futuro possibile, probabile (o meglio stocastico).

[160] *Ivi*, pp. 118 ss.

[161] E. NOCIFORA, *Sociologia della sicurezza, rischio e legalità democratica*, in AA.VV., *Sicurezza e democrazia*, Scriptaweb, Napoli, 2010, pp. 104 ss.

[162] A. GIDDENS, Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita, Bologna, Il Mulino, 2000, p.38, ove l'A. scrive che «[...] una positiva assunzione di rischio sta alla base di quell'energia che crea la ricchezza in un'economia moderna».

Anche in questo caso pertanto torna in gioco il principio di proporzionalità. I sistemi di gestione del rischio si basano infatti su due processi che riguardano: il primo l'accettazione di un certo grado di rischio; il secondo, il trattamento del rischio, ossia il "come" farvi fronte. In entrambo le ipotesi fondamentale è il calcolo del rischio, quale operazione che permette di rendere l'incertezza del danno calcolabile e quindi anche quantificabile secondo un certo sistema di valori e misure in considerazione della concreta realizzazione della minaccia.

Il rischio (R) è infatti determinato dal prodotto di due variabili date dall'impatto della minaccia su un determinato bene, persona o valore (I) tenuto conto del grado della probabilità (stocastica) che tale evento si verifichi (P) entrambe calcolate secondo una prestabilita unità di misura, pertanto in formule R = I x P.

L'introduzione del concetto di rischio ha quindi permesso all'uomo di procedere ad una qualche misurazione del pericolo, venendo a creare un divario tra il «rischio tecnico», ossia il rischio che risponde a variabili oggettive ed è quindi calcolabile, dal «rischio percepito», che invece resta una percezione soggettiva[163].

Abbiamo deciso di argomentare sul concetto di resilienza a seguito di tale breve introduzione sul rischio poiché, diversamente dalla sicurezza tradizionale che risponde a logiche di protezione reattiva, ove la lesione del bene rappresenta un fallimento per le politiche di sicurezza, la resilienza si sviluppa invece come un modello che accetta possibili crisi, shock imprevisti e perdite, quindi una politica di accettazione del rischio che contempla strumenti volti a farvi fronte con l'obiettivo di preservare la continuità e il funzionamento di un determinato sistema[164].

La resilienza, si concentra infatti sulla prevenzione dalle minacce e sulla minimizzazione degli effetti derivanti dalla realizzazione della minaccia (danno) con un approccio di tipo proattivo[165].

Tuttavia anche in questo caso riscontriamo l'assenza di una definizione univoca del concetto, nonostante i diffusi richiami all'interno di documenti politici e giuridici negli ultimi tempi[166].

Si tratta innanzitutto di un concetto a cui fanno riferimento diversi campi del sapere che vanno dalle scienze dei materiali, alla psicologia fino all'ecologia e l'economia[167]. Quindi lo troviamo sia nelle scienze esatte (*hard science*) sia in quelle umanistiche. La distinzione ci è utile poiché migrando dalla scienza dei materiali, ove per resilienza si intende il grado di resistenza alla rottura o deformazione di un elemento (c.d. prova d'urto)[168], l'utilizzo di questo concetto in riferimento agli individui, alle comunità e alla società più in generale, ha assunto secondo Alcuni almeno tre significati: «*resilience as maintenance*», ove è enfatizzato l'utilizzo della capacità di adattamento per mantenere lo *status quo*; «*resilience as marginality*», mirando a mantenere i cambiamenti prodotti da una crisi o uno shock in modo marginale al fine di preservare contro cambiamenti alle strutture o alle

---

[163] E. NOCIFORA, *Sociologia della sicurezza, rischio e legalità democratica …op.cit.,* p. 107.

[164] Cfr. C. FJÄDER, *The nation-state, national security and resilience in the age of globalisation*, in *Resilience: International Policies, Practices, and Discourses*, vol. 2, n. 2, 2014, pp. 114-129,

[165] F. CASTALDO, *Dalla cyber defence alla cyber resilience dell'infrastruttura critica. Alcune implicazioni strategiche e organizzative*, in *Rivista di economia e politica dei trasporti*, n. 3, 2019, reperibile al link:<https://iris.uniroma1.it/retrieve/handle/11573/1474610/1642734/Castaldo_Cyber-defense_2019.pdf>.

[166] Sul punto v. M.V. D'ONGHIA, *Resilienza, una parola alla moda*, in *Treccani*, 16 ottobre 2020, reperibile al link:<https://www.treccani.it/magazine/lingua_italiana/articoli/parole/Resilienza.html>.

[167] Cfr. J. WALKER, M. COOPER, *Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation*, in *Security Dialogue*, vol. 42, no. 2, 2011, pp. 143–60, reperibile al link:<http://www.jstor.org/stable/26301757>; ove le AA., fanno riferimento al concetto di resilienza negli studi di Crawford Stanley Holling, nell'ambito dell'ecologia e Friedrich August von Hayek, nel campo economico.

[168] Cfr. "Resilienza" in Enciclopedia della Scienza e della Tecnica, Treccani, 2008.

politiche esistenti; e «*resilience as renewal*», con l'obiettivo di trasformare, potenzialmente rimodellare, la struttura e le politiche esistenti, facendo affidamento sulla diversificazione tra molteplici strutture e istituzioni come riserve[169].

In riferimento alle scienze sociali, e in prima approssimazione possiamo evidenziare che la nozione abbia acquistato il senso di capacità di un "sistema" di prepararsi, adattarsi e riprendersi da perturbazioni od eventi avversi tale da conservare una condizione di normalità.

Tuttavia a tale accezione positiva, si accompagna anche un "lato oscuro" del concetto di resilienza che possiamo invece intendere come forma di resistenza al cambiamento e quindi all'innovazione e al progresso, o come incapacità di adattamento[170].

Dal punto di vista dei *security studies* invece, ed in particolare dalla prospettiva della richiamata Scuola di Copenaghen, nel paradigma di resilienza il decisore politico è parzialmente sollevato dal difficile compito di scegliere quali minacce prioritizzare[171], dato che tale modello è perlopiù concetrato sulla minimizzazione degli effetti delle minacce con un approccio *all hazard*, ossia considerando tutte le forme di minacce umane, tecniche e naturali, che vanno dal terrorismo e sabotaggio ai fallimenti dei sistemi tecnici e alle catastrofi naturali.
Sulla scorta di ciò, Alcuni hanno tentato di estrapolare degli indicatori comuni al fine di mettere a fuoco il concetto di resilienza secondo la formula:

> dato uno stato X di un osservabile Y [organizzazione; sistema; ambiente urbano/naturale], l'osservabile Y sarà resiliente tanto più saprà i) adattarsi agli eventi avversi, pervenendo ad uno stato X migliorato però dall'esperinza (stato X +); e ii) realizzare i propri obiettivi durante e nonostante la perturbazione[172].

5. Introduzione alla cyberresilienza

Alla luce di quanto argomentato in precedenza, e tentando di cogliere alcune parole chiave, possiamo sintetizzare la resilienza, in via approssimativa, come un concetto che si riferisce alla capacità di di un "sistema" di "resistere", "adattarsi", "riprendersi" alle "perturbazioni", "schock" o "crisi" in maniera tale da preservare sua esistenza o la sua "continuità".

Applicato al contesto delle reti, un palese esempio è rappresentato proprio da ArpaNet, la rete primordiale creata negli Stati Uniti durante guerra fredda e sviluppata sui principi della ridondanza (delle connenttività) e della distribuzione dei nodi al fine di consentire la continuità delle comunicazioni a seguito della distruzione di uno dei suoi nodi per causa di un attacco[173]. Principi questi che sono ancora oggi alla base del servizio Internet, la rete che connette tutte le reti del mondo.

---

[169] P. BOURDEAU, *Resiliencism: premises and promises in securitisation research*, in *Resilience: International Policies, Practices, and Discourses*, vol. 1, n. 1, 2013, pp. 3-17, reperibile al link:<https://www.tandfonline.com/doi/epdf/10.1080/21693293.2013.765738?needAccess=true>.

[170] T.A. WILLIAMS, D.A. GRUBER, K.M. SUTCLIFFE, D.A. SHEPHERD, E.Y. ZHAO, *Organizational response to adversity: Fusing crisis management and resilience research streams*, in *The Academy of Management Annals*, vol. 11, n. 2, 2017, p. 756, reperibile al link:<https://journals.aom.org/doi/abs/10.5465/annals.2015.0134?journalCode=annals>.

[171] Cfr. M. DUNN CAVELTY, C. ERIKSEN, B. SCHARTE, *Making cyber security more resilient: adding social considerations to technological fixes*, in *Journal of Risk Research*, vol. 26, n. 7, 2023, reperibile al link:<https://www.tandfonline.com/doi/full/10.1080/13669877.2023.2208146>.

[172] P.G. CHIARA, R. BRIGHI, *La dimensione della "resilienza" nel diritto UE della cyberiscurezza*, in *Ragion pratica*, 2024, p. 7.

[173] Sul punto di si rinvia a P. BARAN, *On Distributed Communications Networks*, Santa Monica, RAND Corporation, 1962, reperibile al link:<https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf>.

Passando da ArpaNet al cyberspazio, riteniamo utile far riferimento ad un documento del *Focus group* di ITU del 2015 dal titolo "*Cybersecurity, data protection and cyber resilience in smart sustainable cities*" (FG-SSC), ove viene fornito un utile quadro definitorio del concetto secondo la normazione tecnica dell'Organizzazione[174]. Nel documento il Gruppo prende innanzitutto in considerazione la definizione elaborata dall'ITU-T *Study Group* 17 (SG17) ove la resilienza è definita come la capacità del sistema di riprendersi da compromissioni o attacchi alla sicurezza.

Altro riferimento è ad un documento del 2014, "*Resilient Pathways: the adaptation of the ICT sector to climate change*", ove la resilienza è definita «[l]a capacità di un sistema o di un settore di resistere, riprendersi, adattarsi e potenzialmente trasformarsi di fronte a fattori di stress come quelli causati dagli impatti del cambiamento climatico»[175].

Considerato ciò, il rapporto tecnico ITU del 2015 aggiunge che la resilienza dei sistemi ICT sia collegata a una serie di attributi (quali la robustezza, la ridondanza, la flessibilità/adattabilità) che possono essere collegati alla sicurezza nei seguenti modi:

Robustezza e capacità di mantenere le prestazioni e continuare a operare, anche in caso di attacco cibernetico o altri incidenti (ad esempio, disastri naturali).

Ridondanza dei componenti di sistema che consentono al sistema di riprendere le operazioni, entro un tempo definito, in caso di interruzione improvvisa, totale o parziale.

Flessibilità e adattabilità alle nuove circostanze, compresa la capacità dei sistemi di prepararsi alle minacce future mediante l'aggiustamento/rettifica dei problemi che hanno permesso l'insorgere dell'incidente o che sono occorsi durante un incidente.

Ed in fine il report conclude che il raggiungimento della resilienza e della cybersicurezza nel contesto delle smart cities, «garantirà la continuità del servizio ai suoi cittadini [enfasi aggiunta]»[176].

La continuità del sistema, o la sua preservazione, è quindi l'obiettivo a cui aspira la resilienza. Tale relazione continuità/resilienza trova conferma anche nello standard tecnico ISO 22301, relativo alla "*Business continuity*", ove al punto 1, viene specificato che «[l]a continuità aziendale contribuisce a una società più resiliente [enfasi aggiunta]»[177].

In via approssimativa, possiamo quindi ritenere che la cyberresilienza consista nella capacità delle diverse componenti del cyberspazio - fisico, logico e umano - di rispondere agli incidenti di cyberiscurezza garantendo la continuità dei servizi. Tuttavia, dal breve quadro tratteggiato emerge come la resilienza, e quindi la preservazione della continuità del sistema si riferisca perlopiù ad elementi non umani, e che i cittadini (nel caso del report ITU) o la società in generale (vedi la ISO appena richiamata) godano solo indirettamente di tale azione.

Il tema apre alla questione della (cyber)resilienza dell'umano quale recente campo di indagine dei *security studies* volti a far ricomprendere nella nozione di "sistema" non solo il dominio fisico e quello informazionale del cyberspazio, ma anche il dominio cognitivo e sociale[178], al fine di sviluppare modelli di cyberesilienza che tengano conto anche di elementi riconducibili all'uomo quali la capacità di comprendere e far fronte psicologicamente ad una crisi[179].

---

[174] ITU-T, *Cybersecurity, data protection and cyber resilience in smart sustainable cities*, n. 3, 2015, p. 10, reperibile al link:<https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>.

[175] ITU, *Resilient Pathways: the adaptation of the ICT sector to climate change*, 2014, p. 16, reperibile al link:<https://www.itu.int/en/ITU-T/climatechange/Documents/Publications/Resilient_Pathways-E.PDF>.

[176] *Ibidem.*

[177] ISO 22301, *Resilience by Design and Resilience Embedded. Achieving Proactive Cyber Defense*.

[178] A. KOTT, I. LINKOV, Cyber Resilience of Systems and Networks, Cham, Springer, 2019, p. 2.

[179] M. DUNN CAVELTY, C. ERIKSEN, B. SCHARTE, *Making cyber security more resilient ...op.cit.,* p. 5.

5.1. La cyberresilienza europea

Come già anticipato, diversi documenti politici e giuridici menzionano i concetti di resilienza e cyberesilienza senza tuttavia darne una definizione. Tra questi vi rientrano anche gli atti dell'Unione europea ove, sebbene il concetto figuri nella denominazione del testo o venga spesso richiamato all'interno dell'atto, non è possibile individuare una definizione sul punto.

Nonostante tale assenza, secondo Alcuni, è proprio alla luce del concetto di resilieza («security as resilience») piuttostoché della sicurezza di controllo («security of control») che è possibile comprendere il «perché e [il] come» delle politche dell'Unione in questo settore, soprattutto alla luce delle azioni e delle istituzioni coinvolte[180]. Aderendo a tele tesi proponiamo qui di seguito una breve disamina delle politiche e degli atti di diritto derivato dell'Unione europea, al fine di comprendere il concetto di cyberresilienza in questo ordinamento.

La Strategia europea per la cybersicurezza del 2013, intitolata "cyberspazio aperto e sicuro", ricomprende tra le diverse sfide il raggiungimento della cyberresilienza, la cui promozione è posta sulla cooperazione tra il settore pubblico e privato[181]. In quella sede, oltre ad essere ricordato il quadro di normative europee in ambito di protezione delle reti, veniva infatti ricordato che tali obblighi legali «non dovrebbero però sostituire, né impedire, la collaborazione volontaria e informale, anche tra settori pubblico e privato, destinata a rafforzare i livelli di sicurezza e gli scambi di informazioni e buone pratiche», facendo così riferimento al partenariato europeo pubblico-privato per la resilienza (EP3R) quale piattaforma promossa a livello europeo per rafforzarela resilienza del settore TELCO (*infra* 7.2). In questo senso la cyberresilienza veniva quindi strettamente correlata alla protezione di una infrastruttura critica, sia essa di natura pubblica o privata.

Nella Strategia del 2017, la resilienza viene declinata nelle politiche europee assieme all'obiettivo di raggiungere l'autonomia strategica, promuovendo capacità in termini di tecnologie e competenze e contribuendo a costruire un mercato unico solido[182]. Si promuoveva così l'introduzione di un sistema di certificazione europeo volto ad attestare la cybersicurezza dei beni ICT, si dava attuazione alla Direttiva NIS I, si incentivava la cooperazione tra gli Stati membri al fine di fonire una rapida risposta alle emergenze[183]. A tal proposito si distinguevano inoltre le funzioni di cyberdifesa dell'Agenzia europea per la difesa nel settore della cyber, da quelli di cyberresilienza, di cui è competente l'ENISA[184]. Infine, il documento concludeva:

> Ci serve un'Europa che sia resiliente, che possa proteggere la sua popolazione in modo efficace anticipando i possibili incidenti di cibersicurezza, costruendo una forte barriera protezione nelle sue strutture e nei suoi comportamenti, riprendendosi rapidamente dagli eventuali ciberattacchi e opponendo deterrenti a coloro che se ne rendono responsabili. La presente comunicazione propone misure mirate che rafforzeranno ulteriormente le strutture e le capacità di cibersicurezza dell'UE in modo coordinato, con la piena cooperazione degli Stati membri e delle diverse strutture dell'UE interessate e nel rispetto delle rispettive competenze e responsabilità. La sua attuazione darà una chiara dimostrazione del fatto che l'UE

[180] G. CHRISTOU, *Cybersecurity in the European Union: Resilience and Adaptability …op.cit.,* pp. 171-172.
[181] JOIN(2013) 1 final, p. 5.
[182] JOIN(2017) 450 final.
[183] *Ivi*, p. 5, 7, 8.
[184] *Ivi*, p. 11.

e gli Stati membri collaboreranno al fine di stabilire uno standard di cibersicurezza consono alle sfide sempre più acute cui l'Europa deve oggi far fronte [enfasi aggiunta].

In questa sede si inizia quindi a delineare i contorni del concetto di (cyber)resilieza per l'ordinamento europeo e il rapporto funzionale con la (cyber)sicurezza: la resilienza costituisce una sorta di argine preventivo minimo che ha la duplice funzione di anticipare le minacce ma soprattutto di farvi fronte nel caso in cui le misure di sicurezza falliscano.

I citati obiettivi hanno trovato ulteriore sviluppo nell'attuale Strategia di cybersicurezza "per il decennio digitale" presentata nel 2020[185] e di cui ne abbiamo già avuto modo di analizzarne il contenuto nei suoi tre aspetti principali (*infra* 1).

Passando al piano di normativo, le menzionate politiche hanno trovato attuazione per mezzo di un complesso quadro di atti di diritto derivato. Tuttavia, passando in rassegna i quattro principali atti che compongono la legislazione europea in tema di cybersicurezza, la Direttiva NIS II, La Direttiva DORA e le proposte di Regolamento *Cyber Resilience Act* e *Cyber Solidarity Act*, ci si rende condo che anche in questo caso, sebbene il concetto di resilienza sia compreso nella denominazione del documento o se ne faccia rinvio al suo interno, non troviamo una sua definizione[186].

L'art. 6, par. 1, n 2 della Direttiva (UE) 2022/2555 (Direttiva NIS II), definisce la «sicurezza dei sistemi informatici e di rete» come «la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi [enfasi aggiunta]».

Mentre nella Direttiva (UE) 2022/2554 (DORA), all'art. 3, n. 1, è definito il concetto di «resilienza operativa digitale» quale «capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni».

Lo stesso giorno in cui sono ste pubblicate in Gazzetta ufficiale europea le due menzionate fonti, veniva pubblicata anche la Direttiva (UE) 2022/2557, relativa alla resilienza dei soggetti critici (Direttiva CER). Sebbene questa non trovi applicazione alle materie di cui alla Direttiva NIS II, o più in generale alla materia della cybersicurezza, facciamo riferimento a tale atto poiché all'art. 2, n. 2 è definito il concetto di «resilienza» come «la capacità di un soggetto critico di prevenire, attenuare, assorbire un incidente, di proteggersi da esso, di rispondervi, di resistervi, di adattarvisi e di ripristinare le proprie capacità operative».

Concetti di resilienza apparentemente distanti ma in realtà estrememante vicini e comunque riconducibili al nostro assunto iniziale: ossia di concetto che si riferisce alla capacità di di un "sistema" di "resistere", "adattarsi", "riprendersi" alle "perturbazioni", "schock" o "crisi" in maniera tale da preservare sua esistenza o la sua "continuità".

Infine nelle due proposte discipline *Cyber Resilience Act* e *Cyber Solidarity Act* la resilienza è menzionata in poche occasioni e non è presente alcuna definizione, neppure latamente riconducibile ad essa.

---

[185] JOIN(2020) 18 final.

[186] Cfr. P.G. CHIARA, R. BRIGHI, *La dimensione della "resilienza" …op.cit.*

Tuttavia, sebbene non via sia un'univoca definizione di (cyber)resilienza valida per tutte le poltiche appena elencate, pare ora opportuno analizzare verso quale obiettivo sono orientate tali azioni di resilienza. Ponendo attenzione sulle basi di legittimità il riferimento è costantemente al richiamato art. 114 del TFUE, fatta eccezione per la proposta di Regolamento (UE) 2023/109, il *Cyber Solidarity Act,* ove il fondamento legale è stato individuato dal legislatore europeo dell'art. 173, par. 3, TFUE che prevede che l'Unione e gli Stati membri garantiscano che siano presenti le condizioni necessarie per la competitività dell'industria dell'Unione, e l'art. 322, par. 1, TFUE, al fine di conferire al Meccanismo di Emergenza per la Cibersicurezza di un certo grado di flessibilità in relazione alla gestione di bilancio.

In ogni caso è chiaro che tali misure sono tutte rivolte ad aumentare i livelli di sicurezza delle infrastrutture critiche, dei servizi finanziari, dei beni ICT nonché al più generale obiettivo di «rafforzare le capacità nell'Unione per individuare, prepararsi e rispondere alle minacce e agli incidenti di cybersicurezza»[187], per il solo fine di garantire il funzionamento, o meglio la continuità, del "sistema" mercato unico europeo.

5.2. La cyberresilienza nazionale

Nel processo di conversione del d.L. n. 82/2021 è stato introdotto in sede referente all'art. 1, co. 1, la lett. b), recante la definizione di «Resilienza nazionale nello spazio cibernetico» che si riferisce a «le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131», da intendersi quindi come insieme di attività volte ad evitare un «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale [enfasi aggiunta]»[188].

Ad una prima analisi letterale della disposizione notiamo come tornino i caratteri del concetto di resilienza quale azione volta ad evitare una "interruzione o compromissione" del sistema.

Il tratto caratterizzante la disciplina italiana è proprio in quest'ultimo punto. Diversamente dalla resilienza europea, che come abbiamo appurato è diretta a preservare la continuità e il funzionamento delle reti per garantire a sua volta il funzionamento del mercato unico, il legislatore italiano per cyberresilienza nazionale indende l'insieme di azioni volte a preservare il "continuo" funzionamento del "sistema" Stato facendo tuttavia riferimento alle funzioni o servizi essenziali rientranti nella disciplina sul Perimetro di Sicurezza Nazionale Cibernetica (PSNC). Attività queste, il cui pregiudizio acquista rilevanza ai fini della sicurezza nazionale.

Ancora una volta notiamo l'inevitabile connubio resilienza/sicurezza il quale in questo caso assume tuttavia rilevanza ai fini della cybersicurezza nazionale, che in questo caso coincide con l'indipendenza, l'integrità o la sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero gli interessi politici, militari, economici, scientifici e industriali italiani.

Sul piano amministrativo, la resilienza (a bene vedere il d.L. in questo caso non fa esplicita menzione alla "resilienza nazionale nello spazio cibernetico") rientra tra gli obiettivi dell'Agenzia

[187] Art. 1, proposta Regolamento (UE) 2023/109.

[188] Cfr. art. 1, co. 1, lett. f), del DPCM 30 luglio 2020, n. 131.

per la cybersicurezza nazionale (ACN), attraverso la promozione di azioni comuni dirette per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonchè per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore[189].

L'implicito richiamo è quindi alle citate politiche e atti di diritto derivato europei in tema di protezione delle infrastrutture critiche, di sicurezza delle connessioni nonché di cybersicurezza dei beni ICT.

Ulteriore riferimento, questa volta espresso, è quello relativo alle «esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese»[190], a cui partecipano l'ACN e il Nucleo per la cybersicurezza (NC), quest'ultimo, eventualmente, anche in qualità di promotore e coordinatore[191].

6. La terminologia del rischio informatico e le dimensioni della cybersicurezza europea

La progressiva intruduzione di modelli di regolazione di tipo *risk-based* nelle politiche digitali[192] ha avuto l'effetto di introdurre nuovi concetti nelle fonti del diritto, come quelli di rischio, pericolo e minaccia, già noti nelle scienze sociali[193], e su cui abbiamo avuto modo di argomentare in precedenza.

Difatti il diritto pubblico "classico" non conosce la nozione di "rischio" ma solo quella di "emergenza" (v. infra Cap. I, 3.1), che costituisce una forte limitazione delle libertà individuali spesso non giungendo al risultato atteso. Pertanto è nella gestione (amministrativa) del rischio, grazie all'introduzione di tali modelli regolatori che oggi lo Stato e l'amministrazione pubblica e non solo riescono a fronteggiare le c.d. minacce globali[194].

Nel caso della cybersicurezza, altri di questi concetti, come quelli di "incidente"[195], "vulnerabilità"[196], "gestione del rischio"[197], sono invece stati acquisiti dalle ricordate norme tecniche.

Riteniamo tuttavia meritevoli di attenzione i concetti di «quasi incidente», «incidente» ed «incidente di cybersicurezza su vasta scala», definizioniti all'art. 6 della Direttiva NIS II, nonché quello di «incidente significativo» di cui all'art. 23, par. 3[198] della stessa, i quali lasciano intendere le

---

[189] Art. 7, co. 1, lett. a) del d.L. 82/2021.

[190] Art. 7, co. 1, lett. o) del d.L. 82/2021.

[191] Art. 9, co. 1, lett. c) del d.L. 82/2021.

[192] G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, vol. 59, n. 2, 2022.

[193] Cfr. F. BATTISTELLI, M.G. GALANTINO, *Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk*, in *Current Sociology,* vol. 67, n. 1, 2019, pp. 64-78.

[194] M. SIMONCINI, *La regolazione del rischio e il sistema degli standard: elementi per una teoria dell'azione amministrativa attraverso i casi del terrorismo e dell'ambiente*, Napoli, Editoriale scientifica, 2010.

[195] Art. 6, n. 6, NIS II, definisce l'«incidente» come «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi».

[196] Art. 6, n. 15 NIS II, definisce la «vulnerabilità» come «un punto debole, una suscettibilità o un difetto di prodotti ICT o servizi ICT che può essere sfruttato da una minaccia informatica».

[197] Art. 6, n. 8, NIS II, «gestione degli incidenti» sono «le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e riprendersi da esso».

[198] Cfr. art. 6, nn. 5, 6, 7 della Direttiva NIS II ove per «quasi incidente» si intende «un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato»; per incidente, «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi»;

diverse dimensioni della cybersicurezza e i gradi di intervento nella gestione del rischio informatico. Disciplina questa che deve inoltre essere interpretata alla luce del ricordato *EU Cyber Solidarity Act*, quale strumento volto a potenziare la gestione unica degli incidenti ad impatto diffuso nello spazio europeo.

La prima distinzione è sul piano della realizzazione o meno dell'impatto. Il «quasi incidente», è definito infatti come «un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato [enfasi aggiunta]»; mentre l'«incidente» è un «evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi [enfasi aggiunta]».

Tuttavia, altra differenza è tra il mero incidente appena definito, e l'«incidente significativo», ossia l'incidente che «a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli».

Infine, sul piano dimensionale vi è l'«incidente di cybersicurezza su vasta scala» quale «incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri [enfasi aggiunta]».

7. La privatizzazione della sicurezza

L'intervento dei privati nelle funzioni di sicurezza, in molti casi ricondotto all'espressione "privatizzazzione della sicurezza"[199], è un tema poco studiato dalla dottrina e che solitamente ha suscitato l'interesse degli studiosi relativamente al tema delle compagnie militari private, cc.dd. *Private Military or Security Companies services* - PMSCs[200] o, in altri casi, nelle forme di sicurezza privata a livello interno, come i servizi di vigilanza e le guardie giurate, che è l'aspetto su cui avremo modo di soffermarci in questo paragrafo.

In entrambe le ipotesi la privatizzazione della sicurezza è un processo che trova origine nella crisi nel paradigma weberiano che vede nello Stato l'unico detentore del legittimo uso della forza. Secondo le scienze sociologiche, il processo di globalizzazione ha portato ad una ri-articolazione dello Stato che ha di fatto trasferito alcune sue funzioni ad attori privati[201], tra cui, col tempo, anche quella della

---

ed infine per «incidente di cybersicurezza su vasta scala» si intende «un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri». La nozione di «incidente significativo» è invece introdotta all'art. 23, par. 3 della Direttiva rubricato "Obblighi di segnalazione", il quale lo definisce come un incidente che «a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli».

199 *Ex multis*, R. MANDEL, *The Privatization of Security*, in *Armed Forces & Society*, 2001, pp. 129–151 reperibile al link:<https://www.jstor.org/stable/45346910>.

200 Sulle PMSCs v. In particolare sulle E. MARCHETTI, *Private Military and Security Companies: il caso italiano nel contesto internazionale*, Roma, Edizioni Nuova Cultura, 2013, reperibile al link:<https://www.iai.it/sites/default/files/iaiq_07.pdf>; V. CALDERAI, *The Privatization of Military and Security Services and the Limits of Contract Law*, in EUI MWP, 2010/31, reperibile al link:<https://papers.ssrn.com/sol3/papers.cfm?abstract_ id=1887688>; P. W. SINGER, *Corporate Warriors: The Rise of the Privatized Military Industry*, New York, 2008. A livello normativo vedi la Risoluzione del Parlamento europeo del 4 luglio 2017 sulle imprese di sicurezza private (2016/2238(INI)) 2018/C 334/08.

201 S. SASSEN, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton, 2008.

sicurezza[202]. Tuttavia, questo processo non ha portato ad una piena affermazione dei privati in questo settore, quanto piuttosto l'instaurazione di forme di *governance* ibrida, caratterizzate da una stretta collaborazione (*rectius* cooperazione) con il potere pubblico, il cui risultato ha portato alle cc.dd. *global security assemblages*, ossia la formazione di nuove strutture e pratiche di sicurezza che sono allo stesso tempo pubbliche e private, oltre che globali e locali[203].

Dal punto di vista giuridico ciò si è tradotto in una progressiva distinzione di ruoli e funzioni prima appartenenti alla sicurezza pubblica (o primaria), a forme di sicurezza privata (o secondaria o sussidiaria o complementare[204]), e quindi alla partecipazione dei privati ad attività tradizionalmente affidate al monopolio pubblico, ulteriormente avvalorata della nuova formulazione dell'art. 118, comma 4, della Costituzione a seguito della riforma del 2001.

Secondo Alcuni infatti, il disposto da una parte «rende dunque doveroso per i pubblici poteri la verifica della possibilità di affidare a soggetti privati legalmente abilitati e di provata affidabilità e competenza [...] lo svolgimento di limitati compiti di mantenimento dell'ordine pubblico e della sicurezza in alcuni ben circoscritti settori della vita sociale», dall'altra, «consente ai pubblici poteri di incentivare in ogni modo il sorgere di altre eventuali attività di utilità generale svolte da associazioni (prive di scopi politici anche se dotate di un'organizzazione quasi militare, ma semmai prive di lucro e finalizzate a scopi di solidarietà sociale), le quali si propongano di coadiuvare le forze di polizia nel mantenimento dell'ordine pubblico e della sicurezza in almeno due ben determinati ambiti locali sociali»[205].

L'adunanza plenaria del Consiglio di Stato ha avuto modo di esprimersi sul punto, in un primo momento riconoscendo che tali funzioni di sicurezza sussidiaria o privata possono essere affidate a soggetti privati con atto amministrativo (in tal caso del Governo), purché vi sia un «riconoscimento legislativo in quanto il principio di legalità esige che sia la legge ad identificare i casi nei quali funzioni di sicurezza sussidiaria possano essere svolti da soggetti diversi dagli appartenenti alle Forze di polizia o Locali»[206]; e in un secondo momento, ove il Giudice amministrativo ha invece tracciato una distinzione tra la sicurezza "complementare" che riguarda «un ruolo più marginale del servizio, di mero completamento o integrazione rispetto ai compiti affidati allo Stato [...]», rispetto alla sicurezza "sussidiaria" caratterizzata invece da «un ruolo più intenso del servizio [...]»[207]. Più nel dettaglio, la dottrina ha specificato che nella categoria della sicurezza complementare rientrano le attività imprenditoriali svolte dai privati in tale ambito, mentre la sicurezza sussidiaria ricomprende l'esercizio non professionale da parte di enti associativi di compiti (soprattutto di monitoraggio e osservazione del territorio) ausiliaria rispetto a quelli esercitati dall'amministrazione di pubblica e indirizzati a rafforzare l'efficacia preventiva[208].

In entrambe le ipotesi si tratta comunque di attività ausiliarie, integrative e aggiuntive rispetto alla sicurezza primaria che resta espressione dell'esercizio di potestà pubbliche e di poteri autoritativi e

---

[202] R. ABRAHAMSEN, A. LEANDER, *Handbook of private security studies*, Londra, 2016.

[203] R. ABRAHAMSEN, M. C. WILLIAMS, *Security Privatization and Global Security Assemblages*, in *The Brown Journal of World Affairs*, vol. 18, n. 1, 2011, p. 171, reperibile al link:<https://www.jstor.org/stable/24590788>.

[204] C. MOSCA, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova, Cedam, 2012, p. 26.

[205] P. BONETTI, *Allocazione delle funzioni amministrative e le forme di coordinamento per le materie dell'ordine pubblico, della sicurezza e dell'immigrazione nel nuovo art. 118, della Costituzione*, in *le Ragioni*, n. 5, 2002, pp. 1143-1144.

[206] *Ivi*, p. 127, a proposito della pronuncia del Consiglio di Stato, Sez. I, Ad. plen., 14 luglio 2004, n. 7556.

[207] *Ivi*, p. 129 sulla pronuncia del Consiglio di Stato, Sez. I, Ad. plen., 4 febbraio 2009, n. 4330.

[208] R. URSI, *La sicurezza pubblica*, Bologna, Il Mulino, 2022, pp. 205-205.

coercitivi che possono esclusivamente essere svolti da agenti e ufficiali delle autorità di pubblica sicurezza.

Del medesimo avviso è stata anche la Corte di giustizia europea, sebbene questa abbia avuto modo di occuparsi di dette forme di sicurezza privata dal punto di vista del processo di integrazione del mercato unico, in particolare relativamente alla sicurezza complementare quale servizio di rilevanza economica.

Il Giudice europeo, con una serie di pronunce a partire dagli anni 70 del secolo scorso, si è trovato a dover risolvere questioni sorte dal contrasto tra le condizioni a cui gli Stati sottopongono l'esercizio di funzioni di sicurezza privata - la cittadinanza, il possesso della licenza, prestazione del giuramento, la fissazione amministrativa di tariffe - quali forme di controllo e sorveglianza a cui tali attività sono sottoposte da parte del pubblico potere degli Stati, con il diritto di stabilimento dei lavoratori nello spazio europeo.

Tali questioni hanno permesso così di estendere l'integrazione europea in questo settore. Dal contenuto delle pronunce della Corte si evince infatti che questa ha sottratto le attività imprenditoriali impegnate nel settore della sicurezza dai richiamati vincoli imposti dagli Stati, attraverso un'azione interpretativa volta a negare che l'intervento dei privati nelle funzioni tradizionalmente di prerogativa statale debbano automaticamente qualificarsi come esercizio di un pubblico potere, sul quale non possono trovare efficacia le libertà del mercato[209].

A tal fine il Giudice europeo ha così avuto modo di pronunciarsi sul concetto di «esercizio dei pubblici poteri» secondo l'ordinamento europeo, soprattutto rispetto al contenuto dell'allora art. 55 TCE, il quale escludeva dall'applicazione della libertà di stabilimento le attività private, che in uno Stato membro partecipino «sia pure occasionalmente» a tali poteri. In tali occasioni la Corte ha inizialmente fornito delle argomentazioni generali sulla relatività di detto concetto, posto che «una determinata attività può [...], in uno Stato, ricadere sotto l'art. 55 come partecipante, secondo il diritto di tale Stato, all'esercizio dei pubblici poteri, mentre in un altro Stato membro fruisce della libertà di stabilimento», per poi passare alla sua definizione quale «[...] esercizio di prerogative che esorbitano dal diritto comune, di poteri cogenti nei confronti dei singoli e dei beni, di cui non dispongono i comuni cittadini, e che consentono a colui cui sono stati attribuiti d'agire prescindendo dal consenso o perfino contro la volontà altrui»[210].

In altre pronunce il Giudice europeo è andato a meglio qualificare l'esercizio di funzioni di sicurezza privata rispetto alla sicurezza pubblica, precisando che «il mero contributo al mantenimento della pubblica sicurezza, che chiunque può essere chiamato a offrire, non costituisce esercizio di pubblici poteri», dato che il personale di sicurezza privata (nello specifico si trattava di un servizio di sorveglianza), sebbene, in circostanze ben definite, siano chiamati ad assistere le Forze dell'ordine, «si tratta pur sempre di funzioni ausiliarie» e pertanto ne discende che «le imprese e il personale privato di sorveglianza non partecipano direttamente e specificamente all'esercizio di pubblici poteri e che l'eccezione di cui all'art. 55, primo comma, in combinato disposto, se del caso, con l'art. 66 del Trattato, non si applica alla fattispecie»[211].

L'orientamento giurisprudenziale della Corte ha così dato avvio ad un processo di "liberalizzazione" dei servizi di sicurezza privata nell'Unione europea le cui realetà imprenditoriali

---

[209] C. BUZZACCHI, *Sicurezza e securization tra Stato, Unione Europea e mercato: prerogative dei pubblici poteri o attività economica ?*, in F. PIZZOLATO, P. COSTA (a cura di), *op.cit.*, pp. 114 ss.

[210] CGUE, sentenza 21 giugno 1974, causa 2/74.

[211] CGUE, sentenza 29 ottobre 1998, causa 114/97.

impegnate in questo settore trovano oggi rappresentanza nella *Confederation of European Security Services* (CoESS)[212], unica organizzazione riconosciuta dalla Commissione europea e attiva in un costruttivo dialogo sociale settoriale con UNI Europa[213], l'organizzazione europea rappresentante i sindacati dei lavoratori nei settori dei servizi.

7.1 *Segue*. Il ruolo dei privati nella normazione tecnica di sicurezza: il caso della cybersicurezza

Tra le divese attività del CoESS vi è anche la partecipazione attiva nei processi decisionali degli organismi di normazione tecnica sia a livello europeo (presso il CEN[214]), sia internazionale (presso l'ISO[215]). In particolare, in quest'ultimo caso riteniamo opportuno evidenziare che il CoESS segue i lavori del Comitato Tecnico ISO/TC 292 "Sicurezza e resilienza"[216], in particolare all'interno del Gruppo di Lavoro (WG) 6 "Sicurezza", il quale ha prodotto diverse norme tecniche in questo settore[217], tra cui anche la ISO 22300:2018 "*Security and resilience — Vocabulary*" che definisce al punto 3.192 il concetto di resilienza come la «[c]apacità di assorbire e adattarsi in un ambiente in continua evoluzione»[218].

Nel paragrafo precedente si è accennato all'interesse della dottrina verso il fenomeno della "privatizzazione" della sicurezza, ove si è fatto riferimento all'esercizio di tale funzione da parte di soggetti privati qualificati a tal proposito. Altro tema di non secondario rilievo riguarda le organizzazioni private che non hanno nulla a che fare con la sicurezza in senso tradizionale, pur essendone oramai largamente coinvolte: è il caso delle ricordate infrastrutture critiche operative in diversi settori di primaria rilevanza, nonché anche degli organismi di normazione privata (Parte. III), che possiamo invece interpretare come espressione della "sicurezza privata".

A tal proposito l'analisi delle politiche di cybersicurezza europea può rappresentare un emblematico esempio di questo rapporto. Diversi documenti strategici, tra cui anche la strategia dell'Unione europea per la cybersicurezza del 2013[219], fanno riferimento alla collaborazione tra pubblico e soggetti privati operanti in diversi settori, senza tuttavia precisare come debba realizzarsi

---

[212] Per ulteriori si rinvia al sito ufficiale della Confederazione, di cui al link:<https://www.coess.org/>.

[213] Il sito ufficiale dell'UNI è reperibile al link:<https://www.uni-europa.org/>.

[214] Nel 2008 è stata pubblicata la prima norma CEN riguardante la sicurezza privata, la EN 15602 "Fornitori di servizi di sicurezza - Terminologia", nel 2011, il CEN ha pubblicato l'EN 16082 "Servizi di sicurezza aeroportuale e dell'aviazione" e nel 2015, ha pubblicato l'EN 16747 "Servizi di sicurezza marittima e portuale". Oltre a tali norme, la CoESS ha contribuito attivamente allo sviluppo delle norme tecniche anche promuovendo la creazione nel 2015 di un Comitato Tecnico (CT) CEN, per coprire tutte le norme esistenti e future nel campo della sicurezza privata, il CEN CT 439. Inoltre, il CoESS contribuisce attivamente anche ai lavori del CEN CT 447, che mira a creare regole di appalto, sia pubbliche che private, che obblighino gli appaltatori a implementare il principio del miglior rapporto qualità-prezzo nell'acquisto di servizi. Per ulteriori informazioni sulla partecipazione del CoESS presso il CEN si rinvia al link:<https://www.coess.org/projects-and-standards.php?page=european-standards--cen>.

[215] A livello ISO, il CoESS segue attentamente il lavoro svolto dal Comitato Tecnico ISO 292 "Sicurezza e resilienza", e in particolare all'interno del Gruppo di Lavoro (WG) 6, "Sicurezza". Per ulteriori informazioni sul punto si rinvia al link:<https://www.coess.org/projects-and-standards.php?page= nternational-standards--iso>.

[216] Per informazioni sul Comitato tecnico ISO/TC 292 si rinvia la link:<https://www.isotc292online.org/>.

[217] L'ISO/TC 292 è stato istituito il 1° gennaio 2015 e vede la partecipazione di oltre 50 paesi. Opera nella standardizzazione nel campo della sicurezza per migliorare la sicurezza e la resilienza della società. Si rinvia per ulteriori alla relativa pagina dell'ISO/TC 292 di cui al link:<https://www.isotc292online.org/published-standards/>.

[218] ISO 22300:2018(en) Security and resilience — Vocabulary, reperibile al link:<https://www.iso.org/obp/ui/#iso: std:iso:22300:ed-2:v1:en>.

[219] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, del 7 febbraio 2013.

questa cooperazione nella pratica. Come si comprenderà il tema è particolarmente complesso in quanto non investe solo profili pratici, ma anche giuridici e politici. La domanda di fondo a cui la dottrina tenta di dare risposta è quella di trovare soluzioni che possano colmare il divario tra due opposte posizioni: la massimizzazione del profitto, ricercata dal settore privato, e la massimizzazione della sicurezza quale priorità dei governi.

Sebbene a nostro modo di vedere la ricerca di tali soluzioni da parte dell'Unione europea sia ancora *in fieri*, per il momento pare utile soffermarsi sul ruolo oggi ricoperto dagli attori privati nel processo di cybersicurezza europeo.

Benjamin Farrand ed Helena Carrapico in un recente studio hanno analizzato la progressiva rilevanza assunta dagli attori privati attivi nei settori della disciplina NIS[220]. Dall'analisi delle politiche di cybersicurezza adottate a partire dagli anni 2000, i due Autori hanno individuato tre momenti fondamentali: una prima fase, dal 2001, in cui i soggetti privati sono considerati vittime delle azioni di *cybercrime*, e quindi ricoprono un «passive role as object of regulation»[221]; successivamente, a seguito dell'istituzione dell'ENISA nel 2004, il settore privato non viene considerato solo come obiettivo di potenziali attacchi informatici ma anche come «active stakeholder that sholud form part of the regulatory structure»[222]; ed infine, con la Strategia per una società dell'informazione sicura del 2006, la Commissione ha ritenuto che «private sector does not only act as an adopter of regulation, bur can also be actively involved in shaping policy responses and the resulting regulation»[223].

Proprio in quest'ultima ipotesi, lo studio dimostra quindi come il settore privato abbia assunto un ruolo sempre più influente all'interno dei processi di regolazione in questa particolare branca securitaria. Il riferimento è a un documento dell'ENISA del 2012 ove si dimostra che gli standard adottati nelle norme di cyberisucrezza europee per garantire la sicurezza e l'integrità delle informazioni sono fortemente basati su alcuni standard industriali utilizzati nel mercato europeo delle telecomunicazioni[224]. Pertanto, come osservano i due Autori attraverso l'identificazione di standard di buone pratiche, nonché la posizione percepita degli esperti nel campo delle telecomunicazioni, tali soggetti, hanno influenzato gli standard mediante i quali la legislazione viene applicata e interpretata[225].

7.2 *Segue*. I partenariati pubblico-privati europei di cybersicurezza per lo scambio di informazioni

Nel paragrafo precedente si è avuto modo di porre a confronto, seppur brevemente, il rapporto tra il fenomeno (e i relativi studi) della "privatizzazione della sicurezza" e il ruolo dei privati nel contesto della cybersicurezza. In particolare dallo studio citato[226], è emersa la progressiva rilevanza di questi

---

[220] B. FARRAND, H. CARRAPICO, *Blurring public and private: cybersecurity in the age of regulatory capitalism*, in O. BURES, H. CARRAPICO (a cura di), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham, 2018, pp. 197-217, reperibile al link:<https://link.springer.com/chapter/10.1007/978-3- 319-63010-6_9>.

[221] ID., *op. cit*., 202.

[222] *Ivi*, 205.

[223] *Ivi*, 207.

[224] ENISA, *Shortlisting network and information security standards and good practices*, 2012, reperibile al link:<https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards>.

[225] B. FARRAND, H. CARRAPICO, *op. cit.*, 209.

[226] *Ibidem.*

attori soprattutto nell'ambito della normazione privata di sicurezza, che secondo Alcuni sarebbe indice di una "delega" dell'esercizio della funzione di sicurezza ai privati.

Mentre quest'ultimo aspetto sarà approfondito in Parte III, in questa sede, per ragioni di completezza, riteniamo utile evidenziare un altro fenomeno ove gli attori privati si limitano a collaborare con gli attori pubblici per fini di (cyber)sicurezza[227]. Difatti, l'esigenza di sicurezza delle reti e dei sistemi informatici ha richiesto da subito la collaborazione tra il settore pubblico e privato trovando concreta attuazione attraverso l'istituzione di partenariati *ad hoc*, soprattutto al fine di favorire la creazione di ecosistemi informativi volti a prevnire le minacce informatiche.

Ne sono un esempio i citati ISACs, partenariati pubblico-privati *non profit* istituiti originariamente negli Stati Uniti per aiutare le infrastrutture critiche attravero la raccolta centralizzata, valutazione e diffusione delle informazioni di cybersicurezza fornite dai CERTs e SOCs[228].

Anche a livello europeo[229], il parteneriato pubblico-privato è risultato essere lo strumento più adadatto per garantire la sicurezza informatica dei settori qualificati come critici, soprattutto al fine sviluppare la prevenzione, la preparazione e la risposta europea agli atti di terrorismo informatico attraverso l'istituzione della rete di *information sharing* per la protezione delle infrastrutture critiche CIWIN (*Critical Infrastructure Warining Information Network*)[230].

La convenienza circa l'utilizzo di questo strumento nel particolare contesto della cybersicurezza, nonché della protezione delle infrastrutture critiche è stato individuata da Alcuni nei seguenti motivi: «(a) the private sector 'owns or controls' a large number of CIs [critical infrastructures]; (b) the implementation of security policies depends on the involvement of the private sector in the 'definition of strategic public policy objectives as well as operational priorities and measures'; (c) PPPs 'would bridge the gap between national policy-making and operational reality on the ground'»[231].

Preme precisare che queste prime esperienze cooperative sono sorte su impulso dei governi ma la loro effettiva realizzazione e partecipazione è avvenuta in virtù della sola volontà dei soggetti che vi aderivano (c.d. approccio "*bottom-up*"). Auto-organizzati settorialmente secondo gli ambiti di operatività delle infrastrutture critiche (troviamo infatti ISACs nel settore finanziario, energetico, ecc.), la diffusione delle informazioni e degli allarmi sulle minacce informatiche avveniva sulla base di accordi di natura privata.

La allora Comunità europea si è limitata in un primo momento a promuovere la creazione di detti Centri a livello nazionale (esigenza ancora attuale date le recenti sollecitazioni), riconoscendo «the importance of multi-stakeholder models such as Public Private Partnerships (PPPs), built on a long term, bottom-up model to mitigate identified risks where such an approach delivers added value in

---

[227] Sulle forme di partecipazione pubblico-privata nella sicurezza si faccia riferimento da ultimo a E. BLACKSTONE, S. HAKIM, B.J. MEEHAM, *Handbook on Public and Private Security*, Cham, Springer International Publishing, 2023.

[228] N. CHOUCRI, S. MADNICK, P. KOEPKE, *Institutions for cyber security: International responses and data sharing initiative*, Working Paper CISL# 2016–10, Cybersecurity Interdisciplinary Systems Laboratory, MIT, Cambridge, MA, 2016, reperibile al link:<https://web.mit.edu/smadnick/www/wp/2016-10.pdf>.

[229] O. BURES, *Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships*, in O. BURES, H. CARRAPICO (a cura di), *op. cit.*, 32.

[230] Si rinvia al sito della Commissione europea a proposito dello CIWIN.

[231] F. CAPPELLETTI, L. MARTINO, *Achieving Robust European Cybersecurity through Public–Private Partnerships: Approaches and Developments*, in *EU Policy Review,* vol. 1, 2021, 62, reperibile al link:<https://www.researchgate.net/publication/348437509_Achieving_robust_European_cybersecurity_through_public-private_partnerships_Approaches_and_developments>.

helping to ensure a high level of network resilience»[232]. Anche l'ENISA, sulla scorta dell'implementazione della disciplina NIS, ha prodotto documenti sui modelli cooperativi per la costituzione dei ISACs nazionali[233].

Tuttavia, considerata la sempre più avvertita necessità di coordinare le procedure di scambio delle informazioni e degli allarmi in modo uniforme, l'Unione si è anche attività per creare partenariati a livello europeo. È il caso dell'*European Information Sharing and Alerting System* (EISAS)[234], progetto avviato nel 2007 con il fine di «colmare la lacuna nella condivisione di informazioni [...]» attraverso lo studio di modelli di analisi e diffusione delle informazioni di cybersicurezza utili alla creazione di uno spazio di condivisione comune[235].

Come si apprende dal "*Deployment Feasibility Study*" del 2013, il programma EISAS si poneva l'obiettivo di creare un sistema di scambio informativo su larga scala rafforzando la cooperazione dei già esistenti ISACs settoriali degli Stati membri e semplificando il flusso informativo grazie alla consegna di «materiali pre-prodotti ai partecipanti»[236]. Tra le altre "migliori pratiche" si avvertiva infatti l'esigenza di processare le informazioni raccolte dai Centri nazionali, al fine di disseminare dati di alta qualità, oltreché evitare la duplicazione degli stessi.

Diversamente, l'*European Public-Private Partnership for Resilience* - EP3R, ha rappresentato il primo tentativo di istituire un partenariato comune a livello europeo per affrontare problemi di sicurezza e resilienza nel settore delle telecomunicazioni[237].

Il progetto, avviato nel 2009, è stato successivamente chiuso nel 2013, nonostante la sua mensione nella Strategia europea per la cybersicurezza di quell'anno. Alcuni studiosi hanno ricondotto i motivi che hanno portato al fallimento di questa esperienza alla scarsa partecipazione degli aderenti al progetto sotto diversi profili: la mancanza di impegno nella condivisione delle informazioni, la mancanza di trasparenza procedurale, nonché la scarsa partecipazione delle infrastrutture di piccola e media dimensione, diversamente da quelle maggiori coinvolte in prima persona dalla disciplina NIS[238].

La condivisione delle informazioni sulle minacce informatiche e gli allarmi attraverso l'istituzione di strutture cooperative come i partenariati resta tuttavia una priorità per le politiche europee di cybersicurezza. Nonostante il fallimento dell'EP3R, nella Strategia per la cybersicurezza europea del 2013 veniva ribadito che «il partenariato europeo pubblico-privato per la resilienza (EP3R) costituisce una valida piattaforma a livello dell'UE che dovrebbe essere ulteriormente sviluppata»[239]. A tal fine l'ENISA ha creato, all'interno del framework della piattaforma NIS, tre gruppi di lavoro, con un focus specifico sugli strumenti di co-regolamentazione e relative politiche pubbliche con

---

[232] Consiglio europeo, *Council Resolution on a collaborative European approach to network and information security*, 2009/C 321/01, 2009, sezione IV, 7.

[233] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 2018, reperibile al link:<https:// www.enisa.europa.eu/publications /information-sharing-and-analysis-center-isacs- cooperative-models>.

[234] ENISA, *EISAS – European Information Sharing and Alerting System*, 2007; nonchè il report, *EISAS (enhanced) report on implementation*, pubblicato nel 2011.

[235] Sui diversi settori critici coinvolti nel circuito EISAS si rinvia al sito ufficiale.

[236] ENISA, *EISAS – European Information Sharing and Alerting System. Deployment Feasibility Study*, 2013.

[237] ENISA, *EP3R 2009-2013 Future of NIS Public Private Cooperation*, 2015.

[238] Cfr. K. IRON, *The Governance of Network and Information Security In the European Union: The European Public-Private Partnership for Resilience (EP3R)*, in S. GAYCKEN, J. KRUEGER, B. NICKOLAY (a cura di), *The Secure Information Society: Ethical, Legal and Political Challenges*, Berlino, Springer Publ., 2021, 83-116.

[239] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza ...,* 2013, 7. Si rinvia inoltre alla COM(2009) 149 final

riferimento alla gestione del rischio, alla condivisione delle informazioni e al coordinamento in caso di incidenti tra pubblico e attori privati, che hanno sostituito l'EP3R.

Nello stesso anno la Commissione europea accoglieva l'esigenza di istituire l'unità specializzata EC3 (*European Cybercrime Centre*) per il contrasto alla criminalità informatica presso l'Europol[240]. Si tratta di un caso di partenariato pubblico-privato ove tra le parti vi sono autorità che svolgono compiti di polizia. Nello specifico, come si apprende dal sito, l'EC3 si avvale di due gruppi di consultazione che includono attori del settore privato al fine di creare un ambiente cooperativo capace di cooperare sulle sfide legate alla criminalità informatica, promuovendo la collaborazione sia a livello strategico sia operativo[241].

Sulla scorta di tali gruppi, l'EC3 ha siglato diversi *Memoranda of Understanding* (MoU) con gli attori privati operanti in settori critici, come quello finanziario[242], ma soprattutto quelli attivi nel settore dei servizi di sicurezza informatica[243]. Tali accordi, sebbene siano espressione di una libera contrattazione privata, hanno avuto l'effetto di dirigere le parti verso fini pubblici e modelli comuni di condivisione delle informazioni di cybersicurezza che, da una parte hanno aiutato il settore privato ad innalzare i livelli di sicurezza, dall'altra hanno permesso all'EC3 di essere sempre aggiornato sulle ultime minacce informatiche[244].

8. Gli interessi di rilevanza giuspubblicistica sottesi alla cybersicurezza: una relazione mediata tra sicurezza e tecnologie informatiche

Abbiamo introdotto la cybersicurezza a partire dallo studio delle parole che compongono questo concetto, ossia quale azione di "sicurezza" in relazione al "cyberspazio". Ci si deve tuttavia chiedere in quali termini e forme venga esercitata tale azione in questo contesto, ma soprattutto verso quali interessi questa è orientata. Come vedremo, le due questioni sono in realtà connesse in quanto accomunate da una condizione: la mediazione del cyberspazio nelle sue diverse componenti.

Iniziando dalla prima questione, riteniamo utile ricorrere ad una concettualizzazione formulata in dottrina relativa al rapporto tra sicurezza e tecnologia ove si è tentata una sistematizzazione formulata in questi termini:

> sicurezza *attraverso* la tecnica (le tecnologie securitarie); sicurezza *della* tecnica (la sicurezza dei prodotti tecnologici); sicurezza *dalla* tecnica (la sicurezza rispetto all'uso della tecnologia fatto da altri: ad esempio la sicurezza del web)[245].

Tralasciando la prima relazione che non è oggetto della presente ricerca, ci concentreremo sulle due successive, ossia la sicurezza "della" tecnica e la sicurezza "dalla" tecnica, ove tuttavia assumeremo come secondo termine del rapporto il cyberspazio.

---

[240] Conclusioni 10603/12 del Consiglio sull'istituzione di un centro europeo per la criminalità informatica, 2012.

[241] Si rinvia alla pagina *The EC3 Advisory Groups – Law Enforcement and Private Sector Meetings to Discuss Latest Cybercrime Threats and Challenges*, del sito EUROPOL.

[242] Si rinvia alla pagina *Europol and the European ATM Security Team reaffirm their partnership in combating payment crimes*, del sito EUROPOL.

[243] Si faccia riferimento agli accordi con Karspersky, McAfee, Mnemonic, Microsoft, FireEye la cui documentazione è reperibile sul sito EUROPOL.

[244] R. BOSSONG, B. WAGNER, *A typology of cybersecurity and Public-Private partnership in the context of the European union*, in O. BURES, H. CARRAPICO (a cura di), *op. cit.*, 236.

[245] P. COSTA, F. PIZZOLATO, *Introduzione*, in P. COSTA, F. PIZZOLATO (a cura di), *Sicurezza e tecnologia*, Giuffrè editore, Milano, 2017, p. IX.

Rispetto al primo paradigma, la sicurezza "del" cyberspazio è proprio l'argomento della trattazione, ed è una dimensione della cybersicurezza che si rivolge alle componenti logiche e fisiche, o più in generale ai beni ICT, di cui è composto il cyberspazio.

Nel Cap. I, oltre al riferimento alle tre dimensioni - logica, fisica e sociale - del cyberspazio, abbiamo proposto una reinterpretazione del concetto (solo relativamente alle sue componenti logica e fisica) come spazio composto da "merci", cyberspazio merceologico per l'appunto.

Il limite e la mancata *expertise* tecnica del potere pubblico nel fornire sicurezza a tali "cose", ha fatto sì che questa esigenza passi oggi per l'azione di alternativi centri di aggregazione di interessi quali organismi internazionali non governativi che operano nel mercato, nel caso del nostro studio, gli enti di normazione e certificazione che elaborano norme tecniche anche in materia di sicurezza di tali beni.

Il tema sarà oggetto di apposita trattazione nella successiva Parte III, tuttavia in questa sede riteniamo di doverci soffermare sulla stretta connessione tra la sicurezza "del" cyberspazio con il secondo paradigma, relativo alla sicurezza "dal" cyberspazio. L'azione di sicurezza difatti è sempre diretta alla tutela di un interesse, riconducibile allo Stato e agli individui, che rende difficile credere che tale azione possa esaurirsi nella mera protezione di una "cosa", sia essa materiale o immateriale, in sé[246]. Da ciò il superamento della mera sicurezza dell'informazione e del supporto che la custodisce, definita nelle norme tecniche di settore, grazie alla introduzione della nozione di (cyber)sicurezza negli ordinamenti (soprattutto quello europeo) conferendone valore giuridico e politico.

Più nello specifico, alla luce di quanto fin qui argomentato, notiamo che la cybersicurezza nel multilivello, così come la sicurezza tradizionale, si dirige a livello nazionale verso la protezione dello Stato, delle sue componenti e dei consociati (Stato apparato e Stato collettività)[247], mentre a livello europeo abbiamo notato che oltre alla tipica sicurezza diretta alla salvaguardia del mercato unico e quella tecnica dell'*information* e *computer security* è stata introdotta anche la cybersicurezza dell'uomo, utilizzatore o non utilizzatore delle risorse informatiche, nonché anche dell'essere umano come consumatore di beni ICT (Parte III, Cap. III, 4.2, c).

Proprio su quest'ultimo punto, nonostante la richiamata definizione fornita nel *Cybersecurity Act*, al momento, nelle legislazioni sul punto non rinveniamo una espressa positivizzazione di diritti alla cybersicurezza per le persone, ma perlopiù obblighi verso le imprese attive nel mercato delle ICT, o verso enti qualificabili come infrastrutture critiche che, adempiendoli, indirettamente assicurano il rispetto di tali diritti degli individui, nonché la sicurezza dello Stato o del mercato unico.

La sicurezza "dal" cyberspazio, intesa qui come azione di protezione dell'umano-Stato-mercato da qualsiasi tipo di minaccia possa pervenire da tale ambiente (sia essa dolosa o non dolosa), prima che per le azioni di contrasto attraverso la rete (si pensi alle attività di indagine delle forze di polizia nel cyberspazio), passa necessariamente per la sicurezza infrastrutturale "del" cyberspazio. Non è un caso se l'articolato quadro legislativo europeo e nazionale sul punto si sostanzia in obblighi volti a mettere in (cyber)sicurezza i beni ICT installati presso soggetti ritenuti avere un valore critico per lo

[246] Se il cyberspazio non avesse alcun legame con il mondo fisico, e da questo non derivasse alcuna utilità non vi sarebbe l'esigenza di porre in protezione gli elementi che lo compongono quale indiretta forma di protezione delle persone e degli Stati.

[247] Allo stato attuale l'unica definizione introdotta nell'ordinamento italiano è quella di cybersicurezza nazionale all'art. 1, co. 1, lett. a) del d.L. n. 82/2021, che come già argomentato si sovrappone in parte con quella di sicurezza nazionale. Tuttavia, secondo Alcuni, tale concetto trascenderebbe da quello di sicurezza nazionale approdando anche alla dimensione della sicurezza e dell'ordine pubblico (A. MONTI).

Stato e per il mercato unico, o che circolano nel mercato e che pertanto devono rispettare determinati livelli di sicurezza oggetto di normazione tecnica *ad hoc*.

La relazione securitaria tra persone fisiche-Stato-mercato unico e il cyberspazio è quindi una relazione mediata: i primi possono essere sia vittime, dirette o indirette, di azioni malevole o malfunzionamenti delle risorse informatiche, sia allo stesso tempo beneficiari, delle azioni di cybersicurezza e cyberresilienza, da parte di attori pubblici o privati, sempre per il mezzo del cyberspazio, inteso nelle sue dimensioni logica e fisica.

Appurato tale rapporto, pare ora ragionevole chiedersi quali interessi siano rilevanti ai fini delle politiche di cybersicurezza e cyberresilienza. Non essendovi una chiara positivizzazione di diritti nelle discipline europea e nazionale di cybersicurezza, ma avendo chiarito la relazione mediata di sicurezza, dobbiamo necessariamente orientare la nostra attenzione sulle componenti del cyberspazio.

Come anticipato, questo ambiente è costituito da elementi fisici (*hardware*), che a livello macroscopico hanno rilevanza infrastrutturale[248], ed elementi immateriali, logici (*software*) nonché anche le informazioni e i dati personali che attraversano il cyberspazio.

Alla luce di ciò proponiamo una scomposizione degli elementi del cyberspazio che hanno acquisito, o possono acquisire, rilevanza a livello giuspubblicistico.

Il primo elemento a cui si è soventi fare immediato riferimento sono le infrastrutture informatiche (o di comunicazione) e i beni ICT, oggetto delle apposite discipline sulla protezione delle infrastrutture critiche e di sicurezza del prodotto. Ma al pari di queste, i recenti sviluppi tecnologici, ci portano a dover attenzionare anche i dispositivi indossabili e quelli impiantabili (si pensi da ultimo alle neurotecnologie).

Altra grande classificazione interessa invece le informazioni, all'interno del quale dobbiamo tuttavia distinguere: i dati che si riferiscono, o possono riferirsi, alle persone fisiche (i dati personali), nonché anche i dati non personali, ossia le mere informazioni che invece possono ricomprendere: le informazioni aventi valore economico; le informazioni aventi valore per la sicurezza dello Stato; i dati non personali ma potenzialmente riconducibili alla persona (es. big data e i dati sintetici).

9. Considerazioni conclusive sulla (cyber)sicurezza tra normativo e politico

Tirando le somme di quanto sin qui argomentato, ci pare che il tentativo di ricondurre i concetti di cybersicurezza e cyberesilienza nell'alveo della sicurezza in senso tradizionale abbia reso evidente, a nostro modo di intendere, come le questioni che involgono la cybersicurezza e la cyberesilienza sono le stesse che interessano la sicurezza e la resilienza in senso tradizionale sia sul piano interno, sia nei rapporti tra Stati membri, nello specifico l'Italia, e l'Unione europea.

Proviamo allora a riassumere i termini principali della questione. Muovendo dalle considerazioni sui due ordinamenti, nell'ottica autorità-libertà, sul piano nazionale abbiamo visto come la sicurezza si caratterizza sia riconducibile alla sfera dell'Esecutivo, sotto il controllo Parlamentare, il quale ha il potere di emanare misure di sicurezza nei casi previsti dalla legge, dovendo tuttavia bilanciare tali decisioni con i diritti e le libertà alla luce dei principi di necessità e proporzionalità, decisione sul quale potrà essere esercitato il sindacato della Magistratura.

Diverso ci pare essere invece il caso della resilienza che, come sarà argomentato più avanti (Pt. III, Cap. II, 2), costituisce un'esigenza di sicurezza che non si caratterizza per azioni di intervento

[248] Si pensi alle recenti questioni che riguardano i cavi sottomarini.

diretto, ma in azioni preventive o soprattutto successive ai fallimenti della sicurezza tradizionale, che si sostanziano quindi in misure di sicurezza "diluita" - o "mediata" - nella garanzia di buon funzionamento, integrità e continuità dei tanti servizi, funzioni e beni che hanno rilevanza per la collettività e che possono essere erogati o forniti sia dalla pubblica amministrazione, ma anche dai privati.

Tuttavia tornando sulla sicurezza di primo tipo, quella tradizionale, parte della dottrina ha avverito come non sempre questa sia dettagliatamente prevista all'interno di una norma. È il caso della sicurezza nazionale che, diversamente dai concetti di "sicurezza e ordine pubblico", non ha trovato puntuale definizione nelle fonti primarie, e il cui contenuto è di volta in volta individuato dalla giurisprudenza della Corte costituzionale, la quale ne ha tuttavia rimarcatoin più occasioni il suo carattere politico. A bene vedere questa condizione è stata interpretata da Illustre dottrina come «un limbo ove politico e giuridico convivono»[249], conferendo scarsa chiarezza, e quindi certezza giuridica, su questo concetto. Stessa condizione peraltro avvertita da Alcuni anche relativamente al concetto di (cyber)resilienza a livello europeo[250], con il rischio che la sicurezza nazionale finisca per essere un «*umbrella word* riassuntivo di un coacervo di situazioni varie (dalla tutela della ricerca scientifica a quella dei mercati o delle infrastrutture critiche)», che gode di una certa immunità politica tale da sottrarre l'azione dell'Esecutivo per tal fine «alle regole dell'interpretazione giuridica, al controllo della magistratura e, più in generale, al sistema di *checks and balances* che caratterizza l'ordinamento repubblicano»[251].

La normativizzazione della sicurezza non è tuttavia scevra dal rischio di «tradurre in norma giuridica ogni pretesa di protezione che emerge dalla comunità di individui»[252] con l'effetto di privarli della libertà di compiere scelte proprie e quindi del loro arbitrio[253].

Come si comprenderà il tema vede diverse posizioni dottrinarie che si attestano o sul polo dell'interpretazione della sicurezza come concetto politico, quindi l'attuale situazione ove la definizione del concetto è rimessa all'Esecutivo che ne assume la responsabilità, o sul polo normativo, quindi proponendo di conferire maggiore rilevanza alla voce del Parlamento che ne andrebbe a cristallizzare il suo contenuto all'interno di un disposto di legge.

Si consideri tuttavia che, sebbene la sicurezza nazionale sia un concetto che rinvia alla sovranità degli Stati, la partecipazione dell'Italia ai diversi trattati internazionali, tra cui anche quelli europei, impongono il rispetto dei principi da essi derivanti, i quali incidono necessariamente anche sul modo di interpretare e attuare le politiche di sicurezza.

---

[249] M. VALENTINI, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Napoli, Editoriale scientifica, 2017, pp [--].

[250] A. BENDIEK, R. BOSSONG, M. SCHULZE, *The EU's Revised Cybersecurity Strategy*, in *SWP Comments*, n. 47, 2017, reperibile al link:<https://www.swp-berlin.org/publications /products/ comments/2017C47_bdk_etal.pdf>.

[251] A. MONTI, *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica …op.cit*., p. 5. In particolare il riferimento è al silenzio del COPASIR sul noto caso Abu Omar per il quale l'Italia è stata condannata dalla Corte Europea dei Diritti dell'Uomo. Sul punto v. G. PISANELLI, *La sentenza della Corte costituzionale n. 24 del 2014 in materia di segreto di Stato*, in *Federalismi.it*, 6, 2014; C. BONZANO, *La Consulta alza il 'sipario nero': alla ribalta la deprecabile confusione normativa tra prova e fatto*, in *Archivio penale*, 2014; T. F. GIUPPONI, *Il segreto di Stato ancora davanti alla Corte (ovvero del bilanciamento impossibile)*, in *Diritto penale contemporaneo e Forum di Quaderni Costituzionali*, 2014; A. PACE, *Le due Corti e il caso Abu Omar*, in *Consulta on line*, 2014; A. CAPRIO, *L'"ultimo atto" della vicenda Abu Omar: cala il sipario ma qualche dubbio resta sulla scena*, in *Forum di Quaderni Cosituzionali*, 2014.

[252] A. STERPA, *La sicurezza dal punto di vista della Costituzione*, in C. BASSU, G. PISTORIO, A. STERPA, *Diritto pubblico della sicurezza*, Napoli, Editoriale scientifica, 2023, pp. 14 ss.

[253] *Ibidem*.

A tal proposito abbiamo analizzato come sul piano europeo la sicurezza si atteggia da una parte a fattore limitante le libertà del mercato unico quando invocata dagli Stati membri (per motivi di sicurezza nazionale, ovvero ordine e sicurezza pubblica), mentre costituisce un obiettivo comune quando l'Unione agisce a protezione della sicurezza dei cittadini europei e delle sue stesse istituzioni (SLSG e PSDC).

Inoltre, l'art. 114, par. 3 del TFUE prevede che la Commissione, al fine di garantire il buon funzionamento del mercato interno, possa adottare proposte legislative «in materia di sanità, sicurezza, protezione dell'ambiente e protezione dei consumatori» basandosi su un livello di protezione elevato, tenuto anche conto degli sviluppi fondati su riscontri scientifici.

L'esigenza securitaria interna avvertita a livello nazionale e quella sicurezza diretta al funzionamento del mercato unico, paiono quindi essere i due volumi che si incastrano nelle relazioni tra Stati membri e l'Unione europea in tema di sicurezza.

Tale sommaria ricostruzione ci è particolarmente utile al fine di tentare di interpretare il concetto giuridico di cybersicurezza così come è stato definito dal legislatore europeo e quello italiano.

Come già anticipato si tratta innanzitutto di una novità, in quanto fino al 2019, la cybersicurezza era un termine che non trovava univoca definizione neppure tra le norme tecniche di settore e, soprattutto, non aveva una dignità giuridica.

Con il *Cybersecurity Act*, l'Unione europea ha così conferito significato giuridico a questo concetto riconoscendone sia il suo "storico" portato di garanzia di sicurezza della riservatezza, integrità e disponibilità (c.d. R.I.D.) dei sistemi informatici e delle informazioni, sia collegando questo aspetto, di natura meramente tecnica, a quello, di derivazione internazionale, di "sicurezza dell'umano".

Tratto innovativo che invece non riscontriamo nei concetti di cyberisicurezza e cyberresilienza nazionale italiana, ove, come osservato, l'azione del Governo risulta essere orientata «anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nel cyberspazio».

Quindi da una parte, a livello interno, la cybersiucrezza è un concetto che rientra (ma non si sovrappone totalmente) alla sicurezza nazionale, mentre a livello europeo tale azione viene elevata a protezione delle persone fisiche intese non solo come utenti, ma anche come coloro che sebbene non utilizzino tali risorse possono comunque essere impattati dagli effetti negativi di un attacco informatico su di esse o dalla loro mera disfunzione.

Rispetto allo schema relazionale Stato membro-Ue tratteggiato rispetto alla sicurezza in senso tradizionale, l'introduzione del concetto di sicurezza dell'umano pare conferire un tratto distintivo e ulteriore alle politiche dell'Unione europea in questo frangente, tale da far ritenere che l'Unione abbia interpretato la cybersicurezza come diritto fondamentale.

La questione è particolarmente complessa poiché rinvia al dibattito sull'interpretazione della sicurezza come un diritto e di rilevanza fondamentale. Anche su questo punto troviamo tesi contrapposte tra chi sostiene tale orientamento interpretativo, e chi invece ritiene che le tesi sul punto «o provano troppo, oppure troppo poco»[254].

A ben vedere, non escludiamo, sarà la giurisprudenza della Corte di giustizia o le stesse istituzioni europee a confermarlo, che il riferimento all'umano debba piuttosto essere inteso come più ampio impegno dell'Unione ad attuare politiche del digitale che pongano la persona fisica e non solo le

[254] R. URSI, *La sicurezza pubblica …op.cit*., p. 76.. Così anche T.F. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Bologna, Libreria Bonomo Editore, 2010, pp. 68 ss.

informazioni in sè o il mercato, al centro, considerando non solo le vulnerabilità tecniche delle reti e di sistemi informatici ma anche quelle umane.

Simile interpretazione può trovare conforto in parte nell'analizzata Strategia per il decennio digitale (v. *infra* 1.3). Orientamento sostenuto da tempo anche da una certa dottrina che, proprio al fine di rendere la cybersicurezza europea «più resiliente», ha proposto di riformulare le politiche di valutazione del rischio previste dalla disciplina europea tenendo in considerazione non solo il rischio per i sistemi informatici e le informazioni, ma anche per l'uomo[255].

Altra questione interessa invece le basi con le quali il legislatore europeo ha conferito legittimità rispetto ai Trattati fondamentali alla sua azione legislativa sul punto. Il fine che accomuna le citate discipline è quello di - per riprendere le parole della NIS - «migliorare il funzionamento del mercato interno»[256]. La base di legittimità su cui trovano fondamento è infatti l'art. 114 TFUE che, come noto, disciplina il ravvicinamento delle legislazioni nazionali che possono ostacolare il funzionamento del mercato interno, cui si aggiungono norme speciali in materie specifiche. Nello specifico il disposto prevede che il legislatore europeo possa ricorrere alla procedura ordinaria per armonizzare le «disposizioni legislative, regolamentari ed amministrative» degli Stati membri per il raggiungimento degli obiettivi delineati a livello europeo (ex art. 26 TFUE) per «l'instaurazione e il funzionamento del mercato interno»[257].

Al comma 3, è previsto che la Commissione possa proporre a tal fine interventi in alcune materie, tra cui anche la sicurezza, ma solo per il perseguimento di «un livello di protezione elevato, tenuto conto, in particolare, degli eventuali nuovi sviluppi fondati su riscontri scientifici»[258].

Il ricorso a tale base di legittimità in una materia particolarmente trasversale come quella della cybersicurezza ha sollevato critiche nella dottrina[259]. Sebbene il quadro disciplinare al riguardo intende escludere ogni invasione nella sfera di competenza degli Stati[260], e sebbene nel caso della disciplina NIS il fine sia proprio quello di innalzare il livello di cybersicurezza nell'Unione, è stato osservato che «il centro di gravità di questa misura [NIS I] non sembra essere costituito dal mercato interno ma dal desiderio di armonizzare, seppur in modo minimo, le norme in materia di sicurezza che gli operatori delle reti e dei sistemi informativi devono rispettare a livello nazionale» e quindi «il

---

[255] M. DUNN CAVELTY, C. ERIKSEN, B. SCAHARTE, *Making cyber security more resilient: adding social considerations to technological fixes*, in *Journal of Risk Research*, 2023, pp. 801-814, reperibile al link:<https://doi.org/10.1080/13669877.2023.2208146>. Sebbene la tesi ci pare di particolare interesse, resta il problema di come valutare simile rischio dato che ha natura prettamente soggettiva, divermante dal rischio tecnico che, grazie al ricorso a parametri misurabili, acquista natura oggettiva (Rischio=Impatto del datto x Probabilità che il danno si concretizzi).

[256] Cfr. art. 1, co. 1, della Direttiva NIS II.

[257] Art. 114 TFUE.

[258] *Ibidem.*

[259] R. WESSEL, *Towards EU Cybersecurity Law: Regulating a New Policy Field*, in N. TSAGOURIAS, R. BUCHAN (a cura di), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 403–405; M. VARJU, *5G networks, (cyber)security harmonisation and the internal market: the limits of Article 114 TFEU*, in *European Law Review*, 2020, pp. 471-486.

[260] Oltre a quanto già argomentato sul punto in 1.1 (i), si faccia riferimento alla lettera dell'art. 1, par. 6, della Dir. (UE) 2022/2555 che prevede «La [...] direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati»; o all'art. 1, par. 5 della Dir. (UE) 2022/2557 ove è previsto che «La [...] direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e la difesa e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico».

centro di gravità di queste misure è costituito dal rafforzamento della sicurezza» piuttosto che del mercato unico[261].

Come osservato in dottrina, tale processo di "mercificazione della sicurezza europea" per mezzo dell'art. 114 TFUE se da un lato avrebbe l'effetto di favorire il processo di integrazione europea nel settore della sicurezza (con relativa erosione della sovranità degli Stati membri), dall'altro esporrebbe la sicurezza alle possibili iniziative di alcuni Stati all'annullamento delle misure volte a potenziare la sovranità tecnologica europea[262].

Il tema della sicurezza è strettamente legato a quello della sovranità: solo un potere sovrano è in grado di garantire sicurezza, sia per se stesso, ma soprattutto per gli individui che si trovano sul suo territorio. Come noto, la sicurezza è una materia che non è stata oggetto di integrazione nel contesto europeo. Pertanto, secondo nostra interpretazione, considerato che l'art. 114 TFUE è una base di legittimità non sufficiente, perlomeno essa sola, a garantire simile fine, riteniamo che l'unica possibile soluzione sia quella di provvedere ad una modifica dei Trattati europei ove gli Stati conferiscano maggiore sovranità all'Unione sul punto[263].

Soluzione ipotizzabile ma di difficile attuazione in quanto, oltre a presupporre un clima di maggiore fiducia tra tutti gli Stati membri e univoca visione degli obiettivi di sicurezza, si porrebbe anche la difficile questione, a livello pratico - si pensi alla più volte discussa proposta d'integrazione degli organismi di *intelligence* nazionali - di determinare chi sarà il decisore politico legittimato ad adottare determinazioni in questo ambito? e con quali responsabilità?[264]

---

[261] S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE, III, 2021, Sezione Atti Convegni AISDUE*, n. 5, 20 dicembre 2021, p. 81.

[262] Cfr. S. POLI, E. FAHEY, *The strengthening of the European Technological Sovereignty and its legal bases in the Treaties*, in *Eurojus*, fasc. 2, 2022, pp. 159 ss., reperibile al link:<https://rivista.eurojus.it/wp-content/uploads/pdf/Qui-2.pdf>.

[263] Cfr. B. CARAVITA, *Difesa europea, quali prospettive*, in *federalismi.it*, n. 1, 2019; M. FRAU, *I nodi irrisolti della difesa comune europea. Una prospettiva federalista*, in *federalismi.it*, n. 6, 2022; nonché sulle criticità dell'attuale sistema di difesa europeo v. A. RUFFO, *La difesa europea (PSDC) e la Costituzione italiana alla prova della Bussola Strategica 2022*, in *federalismi.it*, n. 7, 2024.

[264] Si faccia riferimento all'intervista a cura di Francesco Grignetti all'Autorità delegata Franco Gabrielli che ha avuto modo di dichiarare che «ipotizzare un'intelligence europea significa che non si è capito che cosa è l'intelligence. Intelligence è presidio della sovranità nazionale. Faccio un esempio: è normale attività che l'intelligence nella ricerca informatica svolga attività non convenzi0onali, anche commettendo reati, che vengono rigorosamente autorizzati e circoscritti dall'autorità politica. Questo prescrive la legge in Italia, come dappertutto. Ora, mi domando, questa futura intelligence comune a quale soggetto politico dovrebbe fare riferimento? Si dice di una regia europea. E chi dovrebbe fissare la priorità, se poi non c'è un singolo argomento su cui i ventisette governi siano d'accordo?», intervista pubblicata su F. GRIGNETTI, *Gabrielli: "Allarme terrorismo e clan criminali, l'intelligence europea è un controsenso"*, in *La Stampa*, del 23 settembre 2021, reperibile al link: https://www.lastampa.it/topnews/primo-piano/2021/09/23/news/gabrielli-allarme-terrorismo-e-clan-criminali-l-intelligence-europea-e-un-controsenso-1.40730795/. Nonché v. M. SAVINO, *Solo per i tuoi occhi? La riforma del sistema italiano di intelligence*, in *Giornale di diritto amministrativo*, dicembre 2007, reperibile al link:<https://www.irpa.eu/pubblicazione/solo-per-i -tuoi-occhi-la-riforma - del- sistema-italiano-di-intelligence-2/>.

PARTE III

LA CO-REGOLAMENTAZIONE DELLE CYBERSICUREZZE. LA NORMAZIONE TECNICA E LA CERTIFICAZIONE DI SICUREZZA DEI BENI, SERVIZI E PROCESSI ICT TRA ITALIA E UE

CAPITOLO I

NORMAZIONE E CERTIFICAZIONE TECNICA: ALCUNI ASPETTI GENERALI

SOMMARIO: 1. Introduzione - 2. La Normazione tecnica dalla prospettiva degli ordinamenti italiano ed europeo - 2.1. L'evoluzione storica della normazione tecnica tra pubblico e privato - 2.2. La norma tecnica nella teoria generale del diritto - 2.3. La norma tecnica tra ordinamento giuriudico e non giuridico - 2.4. Pubblico e privato nella produzione di norme tecniche - 2.5. Le norme tecniche volontarie pubblicizzate e l'incorporazione - 2.6. Le norme tecniche volontarie e il rinvio - 2.6.1. Gli organismi di normazione tecnica tra *munera publica* e natura privata - 2.6.2. Gli orginasmi di normazione nazionali - a) Il Comitato Elettrotecnico Italiano (CEI) - b) L'Ente Nazionale Italiano di Unificazione (UNI) - 2.6.3. Gli organismi di normazione internazionale - a) L'*International Telecommunication Union* (ITU) - b) L'*International Electrotechnical Commission* (IEC) - c) L'*International Organization for Standardization* (ISO) - 2.7 L'evoluzione delle norme (tecniche) armonizzate alla luce del diritto derivato - 2.7.1 *Segue*. Il Regolamento (UE) 1025/2012 sulla normazione europea - *a) I principi generali della normazione e il processo di formazione delle norme armonizzate - b) partecipazione delle rappresentanze sociali al processo di normazione - c) L'individuazione delle specificiche tecniche delle ICT nelle procedure di appalto - d) La disciplina dell'attività della Commissione e dei comitati nella normazione europea* - 2.7.2 *Segue*. La Direttiva (UE) 1535/2015 sulla procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione - 2.7.3 Segue. I recenti adattamenti e modifiche al Regolamento (UE) 1025/2012 - *a) Il Regolamento (UE) 2022/2480 - b) Il Regolamento (UE) 2023/988* - 2.7.4 Le norme (tecniche) armonizzate - 2.7.5 *Segue*. Il caso *James Elliot* sulle norme armonizzate - 2.7.6 *Segue.* Il caso *Stichting Rookpreventie* sull'accesso e opposizione alle norme volontarie (internazionali) - 2.7.7 *Segue*. Il caso *Public.Resource.Org Inc. et al.* sull'interesse pubblico all'accesso alle norme armonizzate - 2.7.8 Considerazioni sulla natura delle norme armonizzate alla luce degli approdi giurisprudenziali della Corte di giustizia - 2.8 Gli organismi europei di normazione tecnica - a) L'*European Committee for Standardization* (CEN) e l'*European Committee for Electrotechnical Standardization* (CENELEC) - b) Le rappresentanze sociali nelle *Partner Organizations* - c) L'European Telecommunications Standards Institute (ETSI) - 2.9 Le criticità dei sistemi di normazione tecnica e forme di controllo pubblico - 3. Il sistema di accreditamento - 3.1 Gli enti di accreditamento nel multilivello - 3.2 Il Regolamento CE 765/2008 - 3.3 La norma tecnica UNI CEI EN ISO/IEC 17011:2018 - 3.4 La natura giuridica dell'accreditamento e degli enti accreditatori: alcune considerazioni alla luce della dottrina italiana e su Accredia - 4. Il sistema di certificazione.

1. Introduzione

Il rapporto tra tecnica e diritto, per dirla con Stefano Rodotà, «incarna una relazione lunga e persino tempestosa, con amori e ripulse, e comunque con un continuo gioco di specchi e rimandi e

somiglianze, che possono essere apprezzati solo se si considerano i contesti culturali all'interno dei quali questa vicenda si è variamente sviluppata»[1].

Quando ci si approccia a questo tema si è soliti imbattersi in argomentazioni che vedono con diffidenza il progresso tecnologico alludendo a scenari di tipo tecno-deterministico[2] o tecnocratico[3], ove l'umanità è passivamente relegata a subire gli effetti negativi di tali sviluppi.

Con questo non intendiamo negare i pericoli che inevitabilmente possono derivare dalla tecnica ma, a nostro modo di vedere, riteniamo che simili orientamenti necessitino di essere interpretati e contestualizzati in considerazione del fatto che sebbene la tecnica si sia trasformata da mezzo a fine poiché «tutti gli scopi e i fini che gli uomini si propongono non si lasciano raggiungere se non attraverso la mediazione della tecnica»[4], la direzione del progresso tecnologico verso la «liberazione e [il] potenziamento delle energie morali dell'individuo», resta pur sempre una scelta dell'uomo[5]. Ricordava Schmitt, la tecnica «[...] può essere rivoluzionaria e reazionaria, può servire alla libertà e all'oppressione, alla centralizzazione e alla decentralizzazione»[6].

Indipendente dalle diverse interpretazioni del fenomeno, il tema è terreno di comuni riflessioni sul rapporto tra politica e tecnica[7], nonché tra diritto e tecnica[8], le quali approdano tutte a considerazioni conclusive sul falso mito della neutralità della tecnica. Le norme tecniche orami occupano uno spazio sempre maggiore in settori politici, come la sicurezza sul luogo di lavoro, la protezione dei

---

[1] S. RODOTÀ, *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, in G. COMANDÈ, G. PONZANELLI (a cura di), *Scienza e diritto nel prisma del diritto comparato. Atti del convegno tenutosi a Pisa il 22-24 maggio 2003*, Torino, 2004, p. 397.

[2] Il giusfilosofo Ugo Pagallo, in U. PAGALLO, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Torino, Giappichelli, 2014, spiega le tesi tecnodeterministe facendo cenno al noto paradosso di Zenone su Achille e la tartaruga, ove tuttavia in questo caso è la tartaruga, cioè il diritto, a non riuscire a raggiugere il piè veloce Achille, cioè la tecnologia. Difatti, le tesi tecno-deterministe assegnano al progresso tecnologico un assoluto potere incontrastabile al punto che «la corsa della tecnologia sarebbe troppo imperiosa e potente, per poter essere fermata da una semplice sentenza o editto» (p. 20), negando così la sussistenza di un rapporto dialettico tra diritto e tecnica. Esempio di tesi tecnodeterminista è la nota legge di Moore, la quale «a differenza delle leggi della fisica o della chimica, non è una vera e propria legge ma, piuttosto, è stata (ed è tuttora) una sorta di profezia che si auto-avvera; vale a dire una sfida, o un traguardo, che vede impegnati gli esperti nel ramo dei circuiti integrati e dei micro-processori in svariati laboratori del pianeta. [...] La morale che si deve trarre da queste riflessioni è che possiamo accogliere la legge di Moore come un elemento cruciale dell'odierna rivoluzione tecnologica e, tuttavia, respingere le tesi estreme del tecno-determinismo» (p. 23).

[3] Come distinto dalla magistrale dottrina di Natalino Irti, in N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, Laterza, 2009, pp. 122-123, «non è arduo distinguere il tecnico dal tecnocrate: il tecnico non sceglie i fini, ma sta al servizio di fini decisi dagli altri, egli ha soltanto il potere conoscitivo dei mezzi; il tecnocrate, poiché attinge ed applica le leggi naturali dell'economia, ha il potere conoscitivo dei fini. Egli sa dove bisogna andare, e perciò rifiuta o spegia la decisione politica dei fini, i quali non sono - così argomenta - materia di disputa e di voto ma di conoscenza oggettiva e neutrale», ove per "neutralità" deve intendersi «estraneità al conflitto; e il conflitto - anche si argomenta - appartiene alla politica, e non alle leggi dell'economia, le quali, appunto come oggettive e neutrali, sono certe e incontrovertibili». In questo senso si rinvia alle ricostruzioni di Claude-Henri de Rouvroy, conte di Saint-Simon.

[4] U. GALIMBERTI, *Psiche e techne*: l'uomo nell'età della tecnica, Milano, Feltrinelli, 2004, p. 37.

[5] V. FROSINI, *La democrazia nel XXI secolo*, Macerata, Liberilibri, 1997, p. 102 ove scrive che «[l]a civiltà tecnologica non ha annullato la funzione e il valore dell'individuo; essa, al contrario, ha potenziato il suo apporto alla vita civile, perché le masse non sono più eluse dal circuito dell'informazione che sostanzia il consenso pubblico, non sono più emarginate in una condizione di mera sopravvivenza fisica, non sono più chiuse dentro i confini di una casta sociale, come avveniva e avviene in certe esperienze storiche attuali. Il progresso tecnologico procede costantemente verso una liberazione e un potenziamento delle energie morali dell'individuo, ma questa direttiva di marcia potrà essere mantenuta *solo grazie all'impegno delle coscienze, perché essa è una scelta e non una fatalità*».

[6] C. SCHMITT, *Teologia politica* (1922), in *Le categorie del politico*, Bologna, Il Mulino, 2013 p. 179.

[7] G. GRASSO (a cura di), *Il governo tra tecnica e politica: atti del Seminario annuale dell'Associazione Gruppo di Pisa, Como, 20 novembre 2015*, Napoli, Editoriale scientifica, 2016.

[8] N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, Laterza, 2001.

consumatori e dell'ambiente, il trasferimento al mercato dei risultati della ricerca. Per dirla sempre con Schmitt, ciò porta a dover riflettere «su quale tipo di politica è abbastanza forte da impadronirsi della nuova tecnica e quali sono i reali raggruppamenti amico-nemico che crescono su questo terreno»[9].

Nel Capitolo I, abbiamo avuto modo di evidenziare uno dei tratti innovativi delle tesi di Reidenberg e Lessig, relativo all'aver indagato il "dietro le quinte" delle tecnologie informatiche e delle regole da queste dettate (*lex informatica* per il primo, *code* per il secondo), individuando nel «tecnologo sviluppatore e [nel] processo sociale attraverso il quale si evolvono le consuetudini»[10] le uniche fonti capaci di trovare applicazione nel cyberspazio.

Il dato attuale è che in realtà, oltre a tali soggetti, anche i poteri pubblici oggi partecipano a questo processo di regolazione, dimostrando «non solo di porter regolamentare ma anche "iper-regolare"»[11] il cyberspazio.

L'assunto derivato dalle tesi dei due studiosi ci è tuttavia utile per aver posto attenzione su coloro che dettano per primi le regole sulla tecnologia, consentendoci così di introdurre il tema dei poteri privati nel cyberspazio. In particolare ci concentreremo sul loro esercizio di potere attraverso la produzione di norme tecniche, quali atti che non hanno natura giuridica, in quanto non prodotti da un processo giuridico-politico, ma attraverso alternative forme di aggregazione di interessi all'interno di soggetti non statuali.

In particolare, oggetto del presente capitolo è la "co-regolazione delle cybersicurezze", quale forma di regolazione che implica una partecipazione pubblico-privata che ha reso innanzitutto necessario focalizzare l'attenzione sul rapporto tra la norma tecnica e la norma giuridica, nonché tra la norma tecnica e l'ordinamento giuridico in generale. Si tratta di temi mai sopiti nel dibattito che interessa tanto giuspubblicisti quanto giusprivatisti di cui, per quanto possibile, tenteremo di fornirne una ricostruzione che ci consentirà di contestualizzare il tema.

2. Normazione e certificazione tecnica dalla prospettiva degli ordinamenti italiano ed europeo

2.1. L'evoluzione storica della normazione tecnica

L'innovazione e lo sviluppo tecnologico sono da sempre legati alla normazione di tipo tecnico[12]. Tuttavia, se fino all'età moderna tale regolazione risultava essere condotta in modo frastagliato e non sistematico[13], con la rivoluzione industriale prende avvio l'attività di normazione nel senso moderno del termine[14], ossia quando si afferma l'avvertita necessità dell'"unificazione" della normazione tecnica[15].

---

[9] C. SCHMITT, *Teologia politica …op.cit*. p. 182.

[10] *Ivi*, p. 571.

[11] O. POLLICINO, *Potere digitale*, Estratto da I Tematici, V-2023, Potere e Costituzione, in *Enc. dir.,* 2023, p. 415.

[12] I. INKSTER, *History of technology,* vol. 28, London, Continuum, 2008.

[13] Si trattava di standard applicativi prodotti per ogni ambito dell'esistenza umana, dall'ingegneria edile alla produzione agricola e così via, ma senza avere un parametro di uniformazione su tali regole settoriali.

[14] P. ANDREINI, *La normativa tecnica tra sfera pubblica e 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 industiali*, Bologna, Il Mulino, 1995, p. 47.

[15] A tal proposito si consideri che «[i]l termine "normazione" deriva dal latino "norma" e significa 'regola". Fu poi tradotto con la parola "*standardization*" in inglese, "*normalisation*" in francese e "*Normung*" in tedesco, mentre il termine italiano "unificazione" fu coniato da Gabriele D'Annunzio, nel 1921, per indicare esattamente l'attività svolta dagli Enti

In particolare, tale attività ha interessato diversi aspetti che vanno dall'uniformazione delle unità di misura, all'unificazione terminologica fino a quella dimensionale dei prodotti e delle loro componenti[16].

Tuttavia, ciò che preme evidenziare in tale sede è l'evoluzione di tale normazione tra potere pubblico e privato, e tra piano nazionale e internazionale. Proponiamo pertanto una breve ricostruzione di alcune tappe che hanno segnato tale percorso a partire dalla rivoluzione industriale fino ad oggi.

La normazione tecnica nasce nel contesto industriale dapprima dall'esigenza delle singole aziende di definire le caratteristiche costruttive e dimensionali dei propri prodotti come specifiche interne «custodite gelosamente», generando di conseguenza effetti di c.d. *vendor lock-in* che obbligavano i clienti a rivolgersi sempre allo stesso fabbricante[17].

In questo primo periodo, il ricorso alle norme tecniche è quindi prevalentemente orientato verso obiettivi individuali delle singole imprese. Il passaggio dall'utilizzo di tali strumenti a fini di mercato, anziché seguendo una logica produttiva strettamente individuale, è un processo che si è sviluppato gradualmente nel tempo. Tale evoluzione ha consentito di passare dall'utilizzo della normazione tecnica come strumento per guadagnare posizioni di potere nel mercato, secondo logiche di monopolio, a un ruolo chiave nella realizzazione di un mercato aperto e competitivo attraverso l'uniformazione.

Una prima tappa, seppur embrionale in tal senso, può essere individuata nel momento in cui emerge la necessità di ampliare le specifiche tecniche aziendali anche ai fornitori di beni materiali e intermedi, con l'obiettivo di assicurare l'allineamento degli approvvigionamenti ai processi produttivi e agli standard qualitativi interni delle aziende. In particolare, i settori in cui si manifesta da subito l'esigenza di uniformazione delle norme tecniche di fabbricazione e di impiego dei beni industriali sono stati quello elettrotecnico, metallurgico e meccanico[18]. Inoltre, in quello stesso periodo, all'accresciuta complessità del panorama industriale consegue l'aumento dei soggetti interessati alle norme, rendendo essenziale stipulare intese collettive volte ad agevolare gli scambi commerciali e potenziare le condizioni di sicurezza durante la produzione e l'impiego dei prodotti[19].

È così che l'attività di normazione tecnica viene portata «fuori dagli ambiti aziendali (dove comunque permangono specifiche interne di qualità) e vengono convogliate in organismi indipendenti, a carattere settoriale o nazionale, di cui fanno parte, oltre ad esponenti delle industrie, rappresentanti delle pubbliche amministrazioni e delle università»[20]. Come è stato osservato, da questo momento «la pratica normativa si ufficializza [...], perdendo progressivamente quella forma di empirismo che ne aveva caratterizzato lo sviluppo iniziale» e di conseguenza «anche l'elaborazione delle norme diventa un processo istituzionalizzato»[21].

Fu così che prima su base nazionale e poi su base internazionale, prima per profili specifici e poi con vocazione universale, iniziarono a sorgere numerosi enti di normazione, dallo statuto giuridico

---

di Normazione che cominciavano a nascere in Europa agli inizi del XX secolo, ovvero stabilire regole ed, appunto, unificare secondo un ordine riconosciuto e, come tale, accettato» (UNI, *Le regole del gioco*, Milano, 2012, p. 19, reperibile al link:<https://www.cti2000.it/utils/downloadfile.php?table=news&id=35008>).

[16] P. ANDREINI, *La normativa tecnica tra sfera pubblica e privata …op.cit.* p. 47.

[17] *Ivi*, p. 48.

[18] *Ivi*, p. 47.

[19] *Ivi*, p. 48.

[20] *Ibidem.*

[21] UNI, *Le regole del gioco …op.cit.*, p. 25.

molteplice. Nel 1901, in Inghilterra nacque l'*Engineering Standards Committee*, in seguito *British Standard Institution* (BSI)[22]. In Germania e Francia, negli anni della Prima Guerra Mondiale, nacquero analoghi enti, rispettivamente il *Normen-Ausschuss der Deutschen Industrie* (NDI) nel 1917, poi rinominato *Deutsches Institut für Normung* (DIN), e l'*Association Française de Normalisation* (AFNOR) nel 1918. Negli Stati Uniti, sebbene con un ruolo prevalentemente volto al coordinamento e alla certificazione degli standard come *American national Standards*, nacque nel 1918 l'*American Engineering Standards Committee*, in seguito rinominata *American Standards Association* (ANSI)[23]. Quanto all'Italia, nel 1921 fu istituito l'UNIM (poi divenuto l'Ente Nazionale Italiano di Unificazione – UNI – nel 1930). Nato come associazione privata, l'UNI avrebbe acquisito la natura di ente pubblico nel 1931, per poi essere, nel 1959, riorganizzato come associazione privata senza scopo di lucro[24].

Nel complesso si trattta di enti istituzionalizzti le cui norme prodotte non sono obbligatorie. Eccezione per quei Paesi che hanno conosciuto forme di Stato totalitario a cavallo tra le due Guerre, come Germania e Italia, ove si registra «una tendenza a mutare le norme in regolamenti, intervenendo a trasformarne la natura da volontaria a cogente»[25]. Solo con la fine della guerra e con la stabilizzazione delle condizioni politico-economiche, gli Enti di Normazione ritrovano la loro natura volontaria[26].

Il nuovo ordine mondiale, istituito a seguito dei due grandi conflitti, e fondato sulla costituzione di un libero mercato globale richiese da subito una maggiore standardizzazione per facilitare lo sviluppo e il commercio a livello internazionale. In risposta a questa esigenza, nel 1947 venne fondata l'*International Organization for Standardization* (ISO), un organismo internazionale che si occupa di sviluppare e pubblicare norme tecniche a livello globale, il cui obiettivo principale è promuovere l'armonizzazione dei processi produttivi e dei criteri di qualità su scala internazionale.

Tuttavia altre organizzazioni a vocazione internazionale, erano già state istituite prima dell'ISO. Nel 1906 era stata fondata l'*International Electrotechnical Commission* (IEC), organismo competente nei settori dell'elettronica, elettrotecnica e delle tecnologie ad esse correlate, ma fu solo dopo la Seconda Guerra Mondiale che l'IEC acquisì maggiore rilevanza nel contesto della standardizzazione internazionale.

Altro attore fondamentale nel panorama delle organizzazioni internazionali è l'*International Telecommunication Union* (ITU), impegnato nella standardizzazione nel settore delle telecomunicazioni, e nella promozione dell'interoperabilità e dello sviluppo armonizzato delle tecnologie di comunicazione a livello globale, già istituito nel 1932.

In conclusione, come è stato osservato, per motivi storici, esistono due organizzazioni, «una per il settore elettrico e l'altra per tutti gli altri settori»[27]. Tali enti sono soggetti di natura privata ed operano nel più ampio multilivello globale, europeo e nazionale.

---

[22] Cfr. R. C. MCWILLIAM, *The First British Standards: Specifications and Tests Published by the Engineering Standards Committee, 1903–18*, in *Transactions of the Newcomen Society Journal*, vol. 75, Iss. 2, 2005, reperibile al link:<https://www.tandfonline.com/doi/pdf/10.1179/tns.2005.012>.

[23] H. SCHEPEL, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets*, Oxford, Hart, 2005, pp. 111-139; 145-148.

[24] A. BENEDETTI, *Certezza pubblica e "certezze" private, poteri pubblici e certificazioni di mercato*, Milano, Giuffrè, 2010, p. 92.

[25] UNI, *Le regole del gioco …op.cit.*, p. 26.

[26] *Ibidem.*

[27] G. ELIAS, *Le regole comunitarie per l'accesso al mercato unico: le misure per l'eliminazione delle barriere tecniche*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO (a cura di), *La normativa tecnica industriale …op.cit.,* p. 32.

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 invece l'*Ente Nazionale Italiano di Unificazione* (UNI) e il *Comitato Elettrotecnico Italiano* (CEI).

2.2. La norma tecnica nella teoria generale del diritto

L'attenzione della dottrina verso le regole formate dai privati e il loro relativo rapporto con l'ordinamento giuridico non rappresenta una novità. Il tema ha infatti sollecitato la speculazione di diversi Maestri del diritto da cui sono discese teorie interpretative e studi che hanno tentato di fare chiarezza su tale rapporto frutto di «complicazioni interessantissime»[28].

Quello tra diritto e normazione tecnica è infatti un rapporto di difficile categorizzazione sotto diversi profili. La dizione "norma tecnica" «è locuzione polisensa che ha un significato contenutistico e descrittivo, a sua volta impreciso e mutevole»[29]. Con tale espressione è infatti possibile fare riferimento alle norme giuridiche caratterizzate da un contenuto tecnico complesso, a norme tecniche prodotte da soggetti pubblici, nonché a norme tecniche elaborate da associazioni private.

Nel corso della presente trattazione avremo modo di affrontare questi aspetti, soprattutto gli ultimi due, ma per il momento riteniamo opportuno concentrarci sul profilo meramente concettuale tentando di tracciare i contorni della nozione di norma tecnica rispetto al concetto di norma giuridica.

Dalla dottrina della filosofia del diritto è stato osservato che «il concetto di regola tecnica è un concetto paradossale» poiché nelle regole tecniche non sussiste l'alternatività di cognitivo e normativo[30]. Difatti, come è stato definito (*rectius* ri-definito) da tale teoria, la «regola tecnica è una regola che prescrive un comportamento non in sè, ma in quanto condizione [...], di conseguimento d'un fine contingente [...]»[31].

La non alternatività tra cognitivo e normativo che caratterizza la regolazione tecnica porta quindi a doverci interrogare su tali due categorie, in modo da poter meglio comprendere la natura della norma tecnica. L'alternatività di cognitivo e normativo è infatti «una delle forme che assume la "grande divisione" [...], tra essere e dover essere, tra *Sein* e *Sollen*, tra *Is* e *Ought*»[32]. In altre parole la distinzione è tra quello che l'Autorevole dottrina di Hans Kelsen, tempo addietro, aveva già tracciato tra norma giuridica e legge naturale.

Mortati definiva la norma giuridica espressione della «volontà sociale» e ne individuava i caratteri strutturali nella fonte (cioè il potere) da cui essa deriva; dall'atto o il fatto in cui essa è incorporata; e

---

[28] L'espressione è di S. ROMANO in *L'ordinamento giuridico* [1918], Macerata, Quodlibet, 2018, p. 111.

[29] A. PREDIERI, *Le norme tecniche nello Stato pluralista e prefederativo*, in *Il diritto dell'economia*, 1996, pp. 251 ss.

[30] G.M. AZZONI, *Cognitivo e normativo: il paradosso delle regole tecniche*, in Milano, Francoangeli, 1991, p. 11. L'A. individua i diversi "contesti" della filosofia del diritto e del linguaggio giuridico in cui sono state studiate le regole tecniche, ossia gli studi sul fondamento ontologico delle norme, le teorie dell'ordinamento giuridico, le tipologie degli ordinamenti normativi, le teorie dell'atto giuridico, quelle della costitutività e infine nell'ambito degli studi sulla metadeontica. Concepite in questi termini, le regole tecniche sarebbero riconducibili alla categoria degli imperativi categorici di Kant (*La fondazione della metafisica dei costumi*, 1785), ossia quegli imperativi che, al contrario di quelli categorici (che prescrivono azioni buone in sé), prescriverebbero azioni buone al raggiungimento di un dato fine, il cui perseguimento è libero da parte dell'agente.

[31] *Ivi*, p. 13.

[32] *Ivi*, p. 11.

nel grado di efficacia che è ad essa attribuito[33]. Scriveva inoltre che, poiché la norma serve a rendere possibile un giudizio sulle azioni concrete, questa «deve per necessità concretizzarsi nella determinazione di ciò che si suol chiamare la "fattispecie legale", cioè l'ipotesi, presupposta astrattamente dalla legge, di un evento, determinato nei suoi elementi costitutivi, nonché degli effetti ad esso connessi»[34].

Le leggi naturali, come ad esempio le leggi della fisica, sono invece regole che descrivono delle realtà fenomeniche formulate in maniera tale da essere verificabili e quindi attestare se tale legge è vera o falsa.

Come è stato osservato, dal punto di vista della loro struttura, anche le norme giuridiche, al pari di quelle naturali, sono traducibili nei termini di un giudizio ipotetico: se accade il fatto A, allora consegue l'effetto B (ossia sussiste un rapporto di un fatto condizionante con una conseguenza condizionata)[35]. Per cogliere la differenza tra le due occorre allora muovere l'analisi da un diverso punto di vista.

Innanzitutto un primo tratto distintivo può essere colto in considerazione della loro natura costitutiva. Le norme giuridiche non descrivono una realtà materiale, ma creano una realtà astratta, quindi producono qualcosa che non esiste nella realtà e che prima di allora non era esistente a livello astratto. Esprimono quindi una relazione doverosa tra un fatto ed una conseguenza e «si impongono (od autoimpongono) per il conseguimento di determinate finalità [...]»[36]. Le leggi naturali si arrestano invece alla sola descrizione di fenomeni (natuali) che preesistono alla formulazione della regola formulata secondo i canoni del metodo scientifico sperimentale[37]. Ossia esprimono una correlazione «statisticamente probabile» di fenomeni, «stando ai più recenti indirizzi delle scienze naturali»[38].

Pertanto se quest'ultime regole sono verificabili, la norma giuridica invece «sfugge a un giudizio in termini di verità o falsità»[39].

Kelsen, interrogandosi sulla connessione tra causa (A) ed effetto (B) data dal giudizio ipotetico, distingueva che se nelle leggi della natura questa connessione assume la forma della causalità, del naturalisticamente necessitato, nelle norme giuridiche tale forma è data dall'imputazione, «il dover essere (*das Sollen*) con cui la dottrina pura del diritto rappresenta il diritto positivo»[40], cosicché:

---

[33] C. MORTATI, *Istituzioni di diritto pubblico*, Padova, Cedam, ed. VI, 1962, p. 25.

[34] *Ibidem*, pp. 25-26.

[35] H. KELSEN, *Reine Rechtslehre: Einleitung in Die Rechtswissenschaftliche Problematik* [1934], *Lineamenti di dottrina pura del diritto*, trad. it. R. TREVES, Torino, Einaudi, 2000, pp. 62 ss.

[36] V. CRISAFULLI, *Lezioni di diritto costituzionale*, vol. I, Milano, Cedam, 1970, p. 9.

[37] Cfr. M. TAMPONI, M. CONFORTINI, A. ZIMATORE, M. ZACCHEO, V. DI GRAVIO, A. PALMIERI, M. ORLANDI, S. MARTUCCELLI, S. RUPERTO, R. CARLEO, *Dieci lezioni introduttive a un corso di diritto privato*, Milano, Wolter Kluver, 2006, p. 3. Si tratta di un volumetto che raccoglie le trascrizioni delle lezioni di diritto privato (le prime dieci) di Natalino Irti, svolte da alcuni suoi allievi e destinate agli studenti che si avviano a frequentare un corso istituzionale di diritto.

[38] Cfr. V. CRISAFULLI, *Lezioni di diritto …op.cit.* p. 9.

[39] *Ibidem.*

[40] H. KELSEN, *Reine Rechtslehre …op.cit.* p. 63. In particolare l'A. scrive che «[i]l dovere (*Sollen*) giuridico, il quale è il verbo modale che, nella proposizione giuridica, collega la condizione con l'effetto abbraccia tutti e tre i significati: quello di prescrizione, quello di autorizzazione e quello di permissione positiva della conseguenza [...]. Questo dovere (*Sollen*) esprime soltanto il senso specifico in cui due fatti sono tra loro collegati da una norma giuridica» (p. 95). Per interpretazioni critiche alla teoria kelseniana si rinvia a N. BOBBIO, *Studi per una teoria generale del diritto*, Torino, Giappichelli, 1970, pp. 119 ss.

> La legge della natura dice: Se c'è A deve necessariamente (*muss*) esserci B; la legge giuridica dice: Se c'è A deve (*soll*) esserci B [...][41].

Se questa è la differenza tra la norma giuridica e quella naturale, tra mondo della realtà e mondo della doverosità, altra distinzione deve essere condotta proprio all'interno di quest'ultima dimensione tra la norma giuridica e le regole di condotta in generale. La dottrina è infatti solita ritenere che le regole giuridiche sono in rapporto di specie a genere con le regole di condotta, in quanto presentano tutte le caratteristiche delle seconde ma se ne differenziano per il tratto della giuridicità, ossia quando questa regola sia posta da una fonte del diritto[42].

Secondo tale interpretazione, tutte le regole che non derivino da atti o fatti ai quali una determinata collettività, in un dato momento storico, ha riconosciuto la forza di regole giuridiche, rientrano quindi nell'ampia categoria delle regole di condotta morali o religiose che sono indifferenti per il diritto[43].

Tratteggiata brevemente la distinzione tra norma giuridica e leggi naturali, e poi tra norma giuridica e quelle di condotta, pare ora possibile tornare al rapporto tra la norma giuridica e la norma tecnica.

Abbiamo introdotto tale concetto partendo dalla non alternatività tra cognitivo e normativo quale tratto caratterizzante la norma tecnica. Secondo un certo orientamento, data tale particolarità, la norma tecnica sarebbe una figura da tenere distinta rispetto alla norma giuridica (o alle «leggi della pratica»[44]).

In particolare, è stato osservato che in tali regole «[i]l passaggio dal cognitivo al normativo è descritto [...] nella relazione di presupposizione e condizionabilità logica del raggiungimento di un fine ad un comportamento che presuppone l'osservanza di regole scientifiche in una relazione di tipo quasi deduttivo»[45], ove «[l]a nozione di "presupposizione" richiama quella di "condizione", cioè di regola osservata in quanto necessaria non in sè ma per il perseguimento di un fine dell'agente»[46].

Pertanto anche in queste norme sussiste un nesso di necessità. È proprio su questo punto che riscontriamo una divisione nella dottrina italiana tra chi sostiene che tale nesso sia da considerarsi riconducibile al doveroso (*sollen*), inquadrando le norme tecniche fra le regole di condotta e quelle giuridiche, o al naturalisticamente necessitato (*mussen*), e quindi fra le leggi di natura.

Secondo Alcuni infatti sembra che «il nesso di necessarietà della norma tecnica debba considerarsi piuttosto doveroso che non naturalisticamente necessitato, proprio in quanto tendente ad un fine liberamente perseguibile»[47], tale che l'eventuale non corrispondenza della norma tecnica con la corrispondente legge natuale (la "smentita della norma tecnica") può essere assimilata «alla trasgressione della regola pratica»[48]. Teoria che poggia sulla qualificazione della norma giudica come una categoria di norma tecnica atteso che anche la regola pratica «è del resto essa stessa verificabile sperimentalmente e su questa possibilità riposa anzi l'individuazione delle costanti del comportamento umano»[49].

---

[41] *Ivi,* p. 64.

[42] A.A. V.V., *Dieci lezioni introduttive …op.cit.,* p. 5.

[43] *Ivi*, p. 10.

[44] V. CRISAFULLI, *Lezioni di diritto …op.cit.* p. 9.

[45] A. MOSCARINI, *Fonti dei privati e globalizzazione*, Roma, Luiss University Press, 2015, p. 93.

[46] *Ibidem.*

[47] F. MODUGNO, *Norma giuridica*, in *Enc. dir.*, vol. XXVIII, Giuffrè, 1978, pp. 329 ss.

[48] *Ibidem.*

[49] *Ibidem.* In particolare sulla assimilazione della norma giuridica alla norma tecnica si rinvia al il pensiero di A. RAVÀ, il quale in *Il diritto come norma tecnica*, Cagliari, 1911, a partire da un'accezione di norma tecnica quale norma comando

Diversamente, c'è chi ha ritenuto le norme tecniche avere un tratto di maggiore vicinanza con le regole della natura, dato che queste «non esprimono [...] alcuna volontà prescrittiva, ma soltanto enunciano l'esistenza, nell'ordine naturale, di un rapporto di causa a effetto tra un comportamento e l'evento ipotizzato»[50]. Secondo tale dottrina, sebbene alcune norme giuridiche appaiono simili a quelle tecniche, perché esigono l'osservanza di certe modalità, di una certa forma, il rispetto di certi termini, l'intervernto di certi organi o soggetti, affinché l'atto giuridico venga ad esistenza o sia valido, tuttavia tali norme «sono espressione di una volontà prescrittiva che vuole subordinare la produzione di certi effetti giuridici al rispetto delle modalità da essa stabilite»[51].

Altra dottrina ha infine qualificato le norme tecniche avere un ruolo strumentale, ossia avere un ruolo servente della norma giuridica fornendogli gli strumenti conoscitivi della tecnica[52]. Ed in particolare è stato ritenuto che tali norme «si distinguono dalle norme incondizionate per il fatto di contenere una condizione; si distinguono dalle norme condizionate per il fatto che la condizione [è] dipendente dalla [...] volontà [del destinatario] di raggiungere un certo fine»[53].

2.3. La norma tecnica tra ordinamento giuriudico e non giuridico

Fino ad ora abbiamo avuto modo di argomentare sul rapporto tra norma tecnica e norma giuridica da un punto di vista concettuale, e lo abbiamo volutamente fatto ripercorrendo le riflessioni della teoria normativa riconducibili alla teoria kelseniana[54]. Approcciamo questa volta il tema da una prospettiva dinamica. Tralasciando le diverse dottrine appena accennate, si è concordi nel ritenere che le norme tecniche (siano esse intese come ricondubili alle leggi naturali o a quelle di comportamento) sono comunque regole dissimili dalla norma giuridica. Nonostante le differenze, tra le norme tecniche di produzione privata e l'ordinamento giuridico, inteso come "diritto dello Stato", sussiste inevitabilmente una relazione[55].

Queste acquistano infatti rilevanza per l'ordinamento giuridico ogni qualvolta vengano "assunte" al suo interno[56]. Tipicamente ciò avviene attraverso gli istituti dell'incorporazione e del rinvio[57] (fisso e mobile).

---

strumentale al conseguimento di un fine, capovolge la prospettiva che vede le norme tecniche come parte del diritto, per sostenere, in estrema sintesi, che il diritto costituisca esso stesso una norma tecnica, in quanto norma condizionale da rispettare al fine del conseguimento dell'obiettivo della convivenza in società. Sul pensiero di A. Ravà si vedano G. AZZONI, *Cognitivo e normativo …op.cit*., pp. 64-78 e M.M. FRACANZANI, *Adolfo Ravà: fra tecnica del diritto ed etica dello Stato*, Napoli, Edizioni Scientifiche Italiane, 1998.

[50] M. MAZZIOTTI DI CELSO, *Norma giuridica*, in *Enc. giur.*, vol. XXII, 1990, pp. 3-4.

[51] *Ibidem*.

[52] Cfr. N. BOBBIO, *Norma giuridica*, in *Novissimo digesto italiano*, vol. XI, Torino, 1965, pp. 335-334, nonché anche P. BIONDINI, *Approcci definitori alla "norma tecnica"*, in N. GRECO, *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale*, Roma, Edises, 1999.

[53] N. BOBBIO, *Norma giuridica ..op.cit*. p. 334.

[54] H. KELSEN, *Reine Rechtslehre …op.cit*., pp. 207 ss.

[55] Come già astrattamente ipotizzato da Cesarini Sforza o «lo Stato fa proprio un altro ordinamento o parte di altro ordinamento, riproducendone le norme o rinviando espressamente ad esse, le quali quindi non si distinguono più da quelle emanate immediatamente dalla volontà statuale» o «lo Stato ignora gli altri ordinamenti, e quindi non ne riconosce l'efficacia giuridica [...]» W. CESARINI SFORZA, *Il diritto dei privati …op.cit*. p. 33.

[56] A. CAGLI, *Organizzazione e procedure dell'attività amministrativa tecnica nel settore 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 industiali*, Bologna, Il Mulino, 1995, p. 165.

[57] Per uno studio sui "rinvii" dal punto di vista della teoria generale del diritto si faccia riferimento a P. CAPPELO, *La fenomenologia del rinvio statico e del rinvio dinamico*, 2005, consultabile su <http://www.costituzionale

Torneremo su queste tecniche più avanti, per ora ci limitiamo ad un loro breve inquadramento. 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)[58].

La norma tecnica viene così acquisita all'interno della norma giuridica, e quindi entra a far parte dell'ordinamento giuridico, suscitando non pochi interrogativi sulla natura di tali fonti, soprautto una volta che la norma tecnica sia stata rinviata.

Per avere maggior chiarezza sul punto, la questione necessita di essere inquadrata nel più ampio dibattitto sul rapporto tra la norma tecnica (volontaria) e l'ordinamento giuridico, animato da orientamenti interpretativi vari originati da due quesiti di fondo: le norme tecniche sono parte dell'ordinamento giuridico? ovvero, se ne sono estranee, come si pongono allora rispetto a questo?

Come è stato osservato da Autorevole dottrina si frappongono due opposte teorie sul punto, quella monista (o statalista), secondo cui non è ammisibile altro diritto (inteso come complesso di norme) se non quello creato o realizzato dallo Stato con manifestazioni di sua volontà, e la teoria pluralista che, contrariamente alla prima, ammette che il diritto possa originarsi anche da esigenze o forze, di carattere individuale o sociale, indipendenti dall'esistenza dello Stato, anche se queste si concretizzano nello Stato e mediante manifestazioni della sua volontà[59].

Parte della dottrina, ravvisa da tempo la preminenza di fatto dello Stato nella vita giuridica. Superiorità che tuttavia non si esprime con la negazione delle altre possibili fonti del diritto, «ma

---

.unige.it/dottorato/Rinvio.htm>; F. SORRENTINO, *Le fonti del diritto*, Padova, 2015, p. 167 ss.; A. PAPA, *Alcune considerazioni sulla tecnica del rinvio nella produzione normativa*, in *Rassegna Parlamentare*, 1991, p. 286 ss. Per una valutazione complessiva sui problemi determinati dal rinvio statico e dinamico cfr. *Rinvio statico o dinamico?* Ricerca a cura dell'unità FIRB dell'Università di Genova (responsabile prof. P. Costanzo), aprile 2005, in <http://www.costituzionale.unige.it/dottorato/Rinvio.htm>; F. MODUGNO, *Pluralità degli ordinamenti*, cit., p. 16 ss.; M GIGANTE, *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in *Rivista italiana di diritto pubblico comunitario*, 1997, p. 313 ss; M. ATRIPALDI, *Il rinvio "intraistituzionale". Una tecnica per la produzione di norme giuridiche nella forma di Stato a tendenza sociocentrica*, in *Nomos*, n. 2, 2018, reperibila al link:<https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2018/05/Atripaldi.pdf>.

[58] N. GRECO, *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, pp. 37 ss.

[59] W. CESARINI SFORZA, *Ordinamenti giuridici (pluralità degli)*, in *Novissimo digesto italiano*, vol. XII, 1957, p. 1. Approfondendo le origini del contrasto, il Cesarini Sforza scrive «[s]e bene si osserva, l'affermazione che accanto all'ordinamento giuridico dello Stato possono coesistere altri ordinamenti ugualmente giuridici, ossia l'affermazione che più ordinamenti possono logicamente coesistenre, in tanto è possibile in quanto il concetto di "ordinamento" è perso nel senso logico-formale di sistema di rapporti, fra determinati oggetti, stabilito secondo un certo criterio. Variando questo criterio, cambia il sistema, onde gli stessi oggetti possono essere odinati in modi diversi, il che non toglie che tutti questi ordinamenti siano validi nello stesso modo. Se invece l'ordinamento è concepito non nel suo senso logico, ma come concreta manifestazione di una volontà ordinatrice, ossia come atto ordinatore in base un criterio scelto e applicato, allora non può più accadere che tutti i possibili ordinamenti siano validi allo stesso modo, bensì la validità di uno di essi esclude necessariamente quella degli altri. Il che come dire se si possono "pensare" molteplici ordinamenti per la medesima materia, viceversa non è possibile "ordinare" la medesima materia che in un unico modo alla volta [...]. Ora il contrasto fra le due teorie della pluralità e della statualità deriva essenzialmente dal duplice concetto di ordinamento [così esposto], e perciò, mentre la teoria pluralistica è inattaccabile entro l'ambito del concetto puramente logico o, come potrebbe dirsi, statico, invece gli argomenti che la sostengono non hanno nessun valore, se portati contro l'altra teoria che si basa sul concetto che potrebbe dirsi dinamico; ed è altrettanto vero il viceversa».

nell'essere lo Stato quell'ente che applica la parte più grande e più importante di questo diritto»[60]. Questo processo di «statalizzazione» secondo Alcuni troverebbe origine in teorie sul «carattere coattivo del diritto», che i giuristi moderni hanno ereditato dal giusnaturalismo di Samuel Puferndorf e Christian Thomasius, i quali ritenevano che «solo il diritto dello Stato è diritto, perché essendo diritto vero e perfetto solo quello coercibile, questa qualità può derivargli unicamente dallo Stato»[61].

La teoria pluaralista trova fondamento nella dottrina del Santi Romano, in particolare nella sua opera "L'ordinamento giuridico" del 1918, ove è stata teorizzata l'esistenza di «tanti ordinamenti giuridici quante istituzioni»[62] ove per "istituzione" è da riferirsi a «ogni ente o corpo sociale»[63]. Secondo la concezione istituzionalista, il diritto (obiettivo) «prima di essere norma, prima di concernere un semplice rapporto o una serie di rapporti sociali, è organizzazione, struttura, posizione della stessa società in cui si svolge e che esso costituisce come unità, come ente a sé stante»[64].

Pertanto per il Romano lo Stato, in quanto istituzione, è uno dei tanti ordianamenti operanti nella vita sociale, «una specie del genere "diritto"»[65], che vive insieme ad altri ordinamenti di non minore rilievo, come quello internazionale, quello della Chiesa, l'ordinamento delle associazioni non riconosciute dallo Stato (o da questo ritenute illecite, come la mafia ad esempio), l'ordinamento della famiglia, gli ordinamenti di enti privati con finalità di diversa natura, da quella economica, politica, culturale, sportiva e cosi via., talvolta fusi con quello statuale. Ma non per questo, secondo Romano, «il sistema statuale [è] l'unico sistema del mondo giuridico»[66].

La tesi porta pertnato alla disgiunzione del concetto di diritto dal concetto di Stato, secondo il quale se «il concetto di diritto si determina perfettamente senza quello dello Stato, al contrario non è possibile definire lo Stato senza ricorrere al concetto di diritto [...]»[67].

Sulla scorta di tali elaborazioni, Romano arrivava ad individuare di fronte all'ordinamento statale, un ordinamento generale dei privati, diverso da quello ad essi attribuito dallo Stato (ossia il diritto privato), e «perfettamente indifferente per lo Stato, che non ha occasione di occuparsene, nè per riconoscerlo nè per vietarlo»[68]. Ed in particolare, scriveva il Giurista, tale ordinamento trova origine nella incapacità dell'ordinamento statuale di adeguare e reggere la posizione dei privati «per la mancanza di norme più adatte alla vita moderna»[69].

Questo ordinamento priavato, parallelo a quello dello Stato, troverebbe quindi origine nell'esigenza di regolare fenomeni sociali evoluti, tra cui possiamo certamente includere anche l'innovazione tecnologica, con strumenti diversi da quelli della legge dello Stato.

---

[60] S. ROMANO, *Ordinamenti giuridici privati (appunti)*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, p. 1382. Analogamente, in relazione ai processi di produzione di norme speciali fuori dal codice civile cfr. N. IRTI, *L'età della decodificazione*, Milano, Giuffre, 1989, p. 36, ove scrive che «[l]a legge, scegliendo gli scopi e sollecitando attività, invade campo che l'ideologia liberale riserva alle decisioni dei privati [...]».

[61] W. CESARINI SFORZA, *Ordinamenti giuridici ...op.cit.*, p. 2 ove l'A. scrive che secondo questi teorici «solo il diritto dello Stato è diritto, perché essendo diritto vero e perfetto solo quello coercibile, questa qualità può derivargli unicamente dallo Stato».

[62] S. ROMANO, *L'ordinamento giuridico* [1918], Macerata, Quodlibet, 2018, p. 97. Ove con il concetto di "isitutizione" deve intendersi «il complesso di norme, di regole o precetti» che costituiscono diritto (obiettivo) (p. 117).

[63] *Ivi*, p. 44.

[64] *Ivi*, p. 38. Sulla distinzione tra diritto obiettivo - *norma agendi* - e diritto subiettivo - *facultas agendi* - si rinvia a S. ROMANO, *Ordinamenti giuridici privati ...op.cit.*, pp. 1374 ss.

[65] *Ivi*, p. 101.

[66] *Ivi*, p. 102.

[67] *Ivi,* p. 101.

[68] *Ivi*, p. 102.

[69] *Ivi*, p. 112.

Sul punto la normazione tecnica è un esempio emblematico. Essa è infatti interpretata come uno dei fenomeni che si pone fuori dalla legislazione e quindi in un "altrove" rispetto all'ordinamento giuridico[70]. Nello specifico, la norma tecnica è stata tipicamente ricondotta in quel particolare ambito dell'autonomia priavata già individuato dal Romano e che sarà poi definito da Cesarini Sforza come il «diritto dei privati», ossia un diritto parallelo a quello dello Stato che «i privati medesimi creano per regolare determinati rapporti di interesse collettivo in mancanza, o nell'insufficienza, della legge statuale»[71]. Un diritto che per l'appunto si distingue dal diritto privato, quale «complesso di *volontà statuali* miranti a regolare rapporti tra persone private»[72] *inter partes*, in quanto comprensivo delle regole non emanate dallo Stato e destinate ad essere osservate da soggetti ulteriori rispetto a quelli che le hanno redatte, tali da produrre effetti *erga omnes* per tutta la categoria (*rectius* corpi sociali compatti[73]) a cui queste si rivolgono[74].

Analogamente a quanto già osservato nel rapporto tra la produzione privata di regole e l'ordinamento giuridico, anche nel particolare caso delle normazione tecnica riscontriamo le due contrapposte posizioni tra chi, da una parte, vedendo nella normazione tecnica il pericolo di uno spostamento di potere in capo ai privati con conseguente elisione della potestà normativa pubblica[75], nonché la possibile deriva dell'«omologazione globale» dei sistemi di produzione che porterebbero

---

[70] Cfr. A. ZEI, *Tecnica e diritto. Tra pubblico e privato*, Milano, Giuffrè, 2008, pp. 5-6.

[71] W. CESARINI SFORZA, *Il diritto dei privati*, Milano, Giuffrè, 1963, p. 3.

[72] *Ivi*, p. 4. Sul rapporto tra diritto civile e potere pubblico dello Stato si rinvia alle magistrali parole di Filippo Vassalli secondo cui «Il diritto civile non è mai stato mancipio dello Stato come è avvenuto nella fase più recente. Non lo è stato per l'intriseca sua natura, nè pel suo processo di formazione. Il diritto civile [...] è disciplina di libere determinazioni. Vocazione delle norme che si dicono di diritto privato, perché concernenti codeste materie, è di realizzare certe esigenze di giustizia nei rapporti che si svolgono liberamente tra gli uomini: a tal fine non si richiede necessariamente l'intervento del potere pubblico. Il mirabile monumento del diritto romano è costituito prevalentemente per opera di giureconsulti, cioè di privati [...] e del pretore, cioè del magistrato che deve *ius dicere*, dichiarare ciò che è diritto nei singoli rapporti in contestazione, che ha dunque una funzione ben diversa dalla legislativa [...]. La legge, cioè il diritto dettato dai pubblici poteri, ha avuto uno sviluppo limitato, nell'orbita di codesti rapporti; originariamente segna e assicura i limiti nei quali l'autonomia privata si attua [...]» F. VASSALLI, *Extrastratualità del diritto civile*, in *Rivista italiana di scienze giuridiche,* 1951, pp. 482-483, il frammento è riportato in S. ROMANO, *Ordinamenti giuridici privati (appunti)*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, p. 1379.

[73] Sul punto si rinvia a V. CRISAFULLI, *Lezioni di diritto …op.cit.* p. 6, a proposito del concetto di "gruppo propriamente organizzato" ove il Crisafulli a proposito della teoria di Cesarini Sforza scrive che «uno tra gli elementi differenziali tra collettività "diffuse" e *i veri corpi sociali compatti* (gruppi-"enti") [è] nel carattere autoritario di questi ultimi».

[74] A tal proposito osservava S. ROMANO in *L'ordinamento giuridico …op.cit.*, p. 112, «[i]l diritto privato italiano non conosce alcun potre di supremazia, la cui figura non si rinviene se non nel campo del diritto pubblico. Esso quindi regola i rapporti che ricadono sotto le sue norme [...]. Senonché, ciò non corrisponde a realtà. Tutte le volte che si ha un organismo sociale, di qualche complessità, sia pure lieve, nel suo interno si instaura una disciplina, che contiene tutto un ordinamento di autorità, di poteri, di norme, di sanzioni». Come sintetizzato da Salvatore Romano, «[i]l diritto dei privati regola sì i rapporti tra persone private e talvolta quelli stessi che sono già regolati dal diritto privato e anche pubblico ma non emana dallo Stato nè immediatamente nè mediatamente»; e ancora «[...] formuliamo la domanda se un ordinamento statuale abbia dinnanzi a sè un ordinamento generale dei privati, distinto dalla pluralità degli ordinamenti particolari dei privati stessi. Cediamo debba darsi risposta affermativa a questo quesito [...]» (S. ROMANO, *Ordinamenti giuridici privati (appunti)*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, p. 1382 e 1393). Relativamente all'autonomia privata tracciata nel codice civile v. A.C. JEMOLO, *Lo "spirito di liberalità"*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, pp. 973 ss. Sulle due diverse accezioni di fonti dell'autonomia privata in studi recenti si rinvia anche a M. CERIONI, *Prime riflessioni sulle fonti dell'autonomia privata*, in *Annali della Facoltà giuridica dell'Università di Camerino – Nuova Serie*, n.1, 2012, reperibile al link:<https://afg.unicam.it/sites/afg.uni cam.it/files/ CERIONI_ prime_riflessioni_fonti.pdf>.

[75] M. GIGANTE, *Obblighi procedurali comunitari e attività normativa degli Stati membri*, in *Giur. it*., 2002, p. 910, ID, *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle norme armonizzate*, in *Riv. ital. dir. pubbl. comunit*., 1997, p. 323; R. BIN, *Il sistema delle fonti. Un'introduzione*, in AA.VV., *Studi in memoria di Giuseppe G. Florida*, Napoli, 2009, pp. 27 ss.

le economie più avanzate a dettare il poprio dominio sulle economie a scapito dei paesi più poveri[76], elabora ricostruzioni in chiave formalmente pubblica di tali strumenti interpretando quindi le norme tecniche come parte dell'ordinamento giuridico, e dall'altra chi, invece, riafferma la natura di tali norme quali espressione della ricordata autonomia privata, nello specifico di un "diritto dei privati", le cui caratteristiche sono nella non obbligatorietà e nel carattere privatistico, su cui l'ordinamento giuridico rinuncia ad intervenire direttamente.

Si comprenderà che il corretto inquadramento della questione necessita di un contemperamento dei due opposti interessi. Secondo Alcuni, le teorie del primo tipo correrebbero il rischio di non cogliere la complessità del sistema della normazione tecnica, la cui origine e sviluppo sono nelle dinamiche spontanee della produzione e innovazione dei privati[77]. Ma, allo stesso tempo, si ammette che la materia non può essere inquadrata in chiave esclusivamente privatistica[78].

Come già anticipato, il problema si pone in tutti quei casi in cui la norma tecnica entra in relazione con l'ordinamento giuridico[79]. Il che avviene seguendo gli schemi tipici dei criteri di collegamento fra gli ordinamenti, ossia attraverso la presupposizione, quando un ordinamento riconosce la qualificazione di alcuni fatti ad opera di altri ordinamenti, o il rinvio, mediante il quale le norme prodotte dall'ordinamento esterno sono richiamate dall'ordinamento giuridico facendole proprie (rinvio fisso o materiale o recettizio), oppure quando l'ordinamento giuridico «dichiara che certe materie o rapporti rimangano esclusi dalla sua sfera e abbandonati ad altro ordinamento»[80].

Una parte della recente dottrina[81], ha individuato una possibile chiave interpretativa del collegamento tra i due ordinamenti nelle tesi sviluppate da Salvatore Romano, il quale, riprendendo gli studi del padre, Santi Romano, sulla pluralità degli ordinamenti giuridici, ebbe modo di elaborare la teoria degli "ordinamenti giuridici privati".

Secondo questa dottrina,

> la sfera privata rimane, come istituzione originaria sulla base di un principio di separazione [...], coordinata o solo parzialmente subordinata, attraverso la funzione legislativa, all'organizzazione statuale stessa. Questa coordinazione e parziale subordinazione si concreta in "relazioni" con l'ordinamento statuale di vario genere e di varia configurazione[82].

Salvatore Romano, contrapponendosi alle dottrine giuspubblicistiche, ove registra una «netta tendenza ad accentuare la nota della subordinazione della sfera privata a quella pubblica», proponeva una teoria di «considerazione privatistica», senza tuttavia negare i temperamenti a tale elaborazione[83].

---

[76] B. HAZUCHA, *International Technical Standards and Essential Patents. From International Harmonization to Competition of Technologies*, in *Society of International Economic Law (SIEL)*, Second Biennial Global Conference, University of Barcelona, luglio 8-10, 2010, reperibile al link:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id =1632567>.

[77] Cfr. P. LAZZARA, *La normativa tecnica …op.cit.*

[78] *Ivi*, p. 431.

[79] Secondo la teoria di Santi Romano ciò presuppone una «rilevanza giuridica», ossia l'esistenza o il contenuto o l'efficacia di un ordinamento devono essere condizionate da un altro ordinamento in base ad un titolo giuridico, così S. ROMANO, *L'ordinamento giuridico …op.cit.*, p. 126.

[80] S. ROMANO, *L'ordinamento giuridico …op.cit.*, p. 135. Sul punto, il Romano, richiama le tesi di altra magistrale dottrina quale quella di Dionisio Anzillotti in D. ANZILOTTI, *Il diritto internazionale nei giudizi interni*, Bologna, Zanichelli, 1905, pp. 179 ss.

[81] P. LAZZARA, *La normativa tecnica …op.cit.*, nonché da ultimo, A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione,* Napoli, Editoriale scientifica, 2018.

[82] S. ROMANO, *Ordinamenti giuridici privati (appunti) …op.cit.*, p. 1415.

[83] *Ivi*, p. 1414. Nello specifico, precisa Salvatore Romano «[...] le due sfere si presentano ambedue necessarie. Vedremo anche se, come sfere, non si presentino anche come originarie, tenuto conto di quella dottrina che riconosce carattere

Secondo il Giurista infatti, quella che viene spesso interpretata come una "linea di demarcazione" tra ordinamenti pubblici e privati, costituisce allo stesso tempo una «linea di rapporto»[84]. A tal proposito, veniva preso in considerazione l'esempio della funzione legislativa ove da una parte, l'ordinamento privato, attraverso le persone fisiche, è operante nella funzione legislativa dello Stato (vedi ad esempio i partitici politici quale espressione del libero associazionismo dei cittadini), e l'ordinamento pubblico deve riconoscerlo a tutti gli effetti, ma dall'altro, la legge, rappresenta anche la «misura all'ingerenza del pubblico che l'ordinamento privato ammette nel suo campo»[85].

Il pregio di questa teoria è quindi quello di aver fornito ulteriori e più dettagliare argomentazioni sulla seprazione dei due ordinamenti, e di aver evidenziato che l'ordinamento privato acquista rilevanza per quello pubblico solo in determinate occasioni, ossia quando i due ordinamenti entrano in relazione. Tuttavia, stando a quanto descritto, resta il dubbio circa alcune questioni, prima fra tutte la qualificazione di tali espressioni dell'autonomia privata come ordinamenti (privati) dotati di giuridicità a tutti gli effetti.

A nostro modo di vedere, maggiori chiarimenti sul punto sono stati forniti da un recente orientamento dottrinario che, proprio a proposito delle regolezioni a contenuto tecnico scientifico, analizzate dalla prospettiva del diritto costituzionale, ha ritenuto che

> [l]'ordinamento tecnico resta [...] un ordinamento separato che non è in grado di acquistare il carattere della giuridicità, ma dei cui prodotti può avvalersi il legislatore per conferire loro specificamente ed occasionsionalmente forza normativa, in virtù della mediazione necessaria di una fonte imperativa [enfasi aggiunta][86].

Difatti secondo tale teoria le norme tecniche «non acquistano di per sè ed una volta per tutte il carattere della normatività, ma solo per il tramite della legge e per via della "scelta", mai irreversibile, effettuata di volta in volta dall'ordinamento giuridico»[87]. In altre parole, una determinata norma tecnica (volontaria) acquista il tratto della giuridicità, in via occasionale e nel solo caso specifico, per mezzo della «selezione volontaria» operata per il tramite della legge o altra fonte dell'ordinamento giuridico[88]. Pertanto, al dubbio se «quando una norma tecnica diventa il contenuto di una norma giuridica [o è da essa rinviata], non sarebbe la prima a giuridicizzarsi, ma la seconda a [...] tecnicizzarsi», tale teoria si pone a sostegno dell'ipotesi inversa, negando la tecnicizzazione della norma giuridica che la priverebbe di forza e riconoscendo il tratto della giuridicità alla norma tecnica tutte le volte che questa entra in relazione con l'ordinamento giurdico[89].

---

originario a quegli ordinamenti del c.d. diritto dei privati concepito fuori da ogni dipendenza dall'ordinamento statuale: questa asserzione potrebbe indurre a considerare sotto lo stesso profilo tutti, e non solo in parte, gli ordinamenti privati. Secondariamente c'è da terner presente un processo storico: da una comunità di privati si è distaccata l'organizzazione dei poteri pubblici [...]. Abbiamo però veduto come l'organizzazione a strato non tolga il carattere di ordinamento alla comunità dei privati, mentre deve ammettersi il riconoscimento della sopravvivenza delle consuetudini, almeno in una certa misura. Si aggiungano le note considerazioni secondo le quali la produzione delle norme è riservata, nell'autonomia, agli stessi privati, mentre l'efficacia è il principale compito dell'ordinamento centrale. Può quindi ripetersi quanto già osservato, e cioè che una società organizzata a Stato conserva tutte le sue caratteristiche di ordinamento giuridico privato».

[84] *Ivi,* p. 1415.

[85] *Ibidem.*

[86] A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione …op.cit*., p. 78.

[87] *Ivi*, p. 77.

[88] *Ivi*, p. 78.

[89] Cfr. F. SALMONI, *Le norme tecniche*, Milano, Giuffrè, 2001, pp. 165 ss. Tesi contrarie nella dottrina italiana hanno invece sostenuto, soprattutto nel caso dell'incorporazione che, «la norma giuridica non potrebbe mai avere un contenuto tecnico se non elementare, essendo in ogni altro caso il dato tecnico solamente un presupposto di fatto, da valutarsi dal giudice; di guisa che le norme di legge (o regolamento) che avessero invece tale contenuto non sarebbero norme aventi

L'ipotesi è quindi quella di applicare la tesi della separazione al particolare caso del rapporto fra il sistema giuridico e il sistema della normazione tecnica, nel solco della teoria della pluralità, ma senza assumere la pretesa di qualificare l'ordinamento a cui si rinvia come normativo o giuridico[90].

Simile interpretazione consentirebbe inoltre di spostare la riflessione sulla legittimità del potere privato nell'ambito della normazione e regolazione tecnica dalla applicazione delle norme tecniche e al loro rapporto con le norme giuridiche, al momento della loro produzione[91], e quindi sugli specifici procedimenti di formazione di tali norme, sulla qualifica dei soggetti che vi partecipano e con quale rilievo. Questioni che sono al centro dell'odierno dibattitto sul punto e che non escludono, ma anzi portano ancora una volta a dover concentrare la riflessione sulla legittimazione degli enti di normazione e sulla democraticità delle procedure di formazione delle norme tecniche[92].

2.4. Pubblico e privato nella produzione di norme tecniche

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 immettere sul mercato nonché, più recentemente, dei sistemi e processi industriali e dei servizi»[93].

A questa formulazione generale e sintentica sottendono tuttavia diverse tipologie di norme tecniche che possono essere raggruppate e inquadrate secondo molteplici criteri distintivi. Per quel che qui interessa, pare d'intresse considerare la tripartizione individuata da una certa dottrina in: norme originate da attori privati ma promulgate dai governi sovrani; norme originate e promulgate da attori privati in seguito a delega governativa; e norme adottate da attori privati senza l'approvazione o l'applicazione governativa[94].

Sebbene eleborata in considerazione delle tipologie di produzione delle norme tecniche negli Stati Uniti, riteniamo tale tripartizione utile anche nel nosto caso. In particolare, riadattando lo schema citato al contesto ordinamentale europeo-nazionale, riteniamo di poter andare oltre il parametro del coinvolgimento del governo, o meno, nella produzione di tali norne, facendo piuttosto riferimento ai criteri di collegamento tra ordinamenti già richiamati, e ponendo così attenzione sul momento di «selezione volontaria» della norma tecnica da parte dell'ordinamento giuridico per opera del legislatore (o anche del governo) mediante la legge o altra fonte dell'ordinamento[95].

Ponendo così in relazione le tipologie di norme tecniche disciplinate negli ordinamenti europeo e nazionale (pubbliche, volontarie ed armonizzate) con i criteri di collegamento tra ordinamenti (incormporazione, rinvio mobile e fisso, nonché da ultimo la "delega"), abbiamo ritenuto di

---

per destinatari la generalità dei soggetti dell'ordinamento e i giudici, ma i soli organi (tecnici) dell'amministrazione [...]». Così scriveva Vittorio Bachelet in V. BACHELET, *L'attività tecnica della pubblica amministrazione*, Milano, Giuffrè, 1967, p. 88, a proposito di Arnaldo De Valles, in A. DE VALLES, *Norme giuridiche e norme tecniche*, in A.C. JEMOLO (a cura di), *Diritto amministrativo, diritto costituzionale, diritto internazionale, diritto penale, procedura penale*, Milano, Giuffrè, 1963, pp. 175-188.

[90] *Ivi*, p. 77.

[91] Cfr. F. SALMONI, *Le norme tecniche*, Milano, Giuffrè, 2001, p. 31.

[92] M. ELIANTONIO, C. CAUFFMAN (a cura di), *The legitimacy of standardisation as a regulatory technique: a cross-disciplinary and multi-level analysis*, Cheltenham, Northampton, Edward Elgar, 2020.

[93] G. CAIA, F.A. ROVERSI-MONACO, *Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, Bologna, 1995, p. 13.

[94] S.L. SCHWARCZ, *Private Ordering*, in *Northwestern University Law Review*, 2002, p. 5, reperibile al link:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=298409>.

[95] Cfr. A. IANNUZZI, *Il diritto capovolto …op.cit.,* p. 78.

organizzare la trattazione che segue nel seguente modo: le norme tecniche volontarie pubblicizzate e l'incorporazione (2.5); le norme tecniche volontarie e il rinvio (2.6); ed infine, le norme tecniche armonizzate e la delega (2.7).

2.5. Le norme tecniche volontarie pubblicizzate e l'incorporazione

Diversamente dal passato, in particolare durante i periodi dello Stato di polizia ed anche dello Stato liberale[96], ove il potere pubblico era in grado di soddisfare gli interessi della collettività con propri atti normativi, anche in ambiti di tipo tecnico, il progresso scientifico tecnologico nonché la creazione di mercati sempre più globali, hanno portato all'esigenza di concentrare la normazione tecnica presso enti specializzati di natura privata (*infra* par. 2.1).

Questi enti sono responsabili della produzione delle norme tecniche volontarie, ossia di standard prodotti secondo propri processi di formazione e non aventi natura cogente.

Il soggetto, sia esso pubblico o privato, che intede conformarsi a detto standard lo fa in via volontaria e, se inoltre intederà certificare tale conformità, potrà farlo sulla scorta di un contratto (privato) con l'ente di certifciazione.

Tuttavia, può capitare che tali «norme originate da attori privati ma promulgate dai governi sovrani»[97], e che pertanto piuttosto che pubbliche potremmo qualificare come "pubblicizzate". In questo caso infatti la norma tecnica, adottata dagli enti di normazione privata, «è riprodotta, è trascritta, è materialmente recepita nel testo normativo di modo che, per tale via, essa viene incorporata nella norma giuridica e scompare in quest'ultima» con la conseguenza che «la norma tecnica incorporata nella norma giuridica, [...] assume la stessa vigenza formale "ed entra perciò a far parte, come norma imperativa, dell'ordinamento"»[98].

Vigenza formale che è quindi legata alla forma dell'atto fonte nel quale la norma tecnica è incorporata, di cui ne assorbe la stessa forza e le stesse caratteristiche[99], tra cui certamente anche il possibile esercizio di un controllo giurisdizionale[100]. Precisiamo tuttavia che aderendo alla tesi della "selezione volontaria" anziricordata, la norma tecnica resta comunque distinta da quella giuridica la quale la percepisce e fa propria nel suo contenuto.

Così, se da una parte questo criterio, fugato ogni dubbio sulla natura del contenuto della norma tecnica occasionalmente giuridicizzata mediante la sua trasposizione in una fonte giuridica, sembra essere la soluzione migliore sotto i profili della certezza del diritto e della tutela delle situazioni soggettive, dall'altra l'incorporazione avrebbe l'effetto di non traspondere nella fonte giuridica anche il carattere della adattabilità proprio della normazione tecnica.

---

[96] F. SALMONI, *Le norme tecniche …op.cit.*, pp. 147 ss.

[97] Cfr. S.L. SCHWARCZ, *Private Ordering …op.cit.*, p. 5.

[98] F. SALMONI, *Le norme tecniche …op.cit.*, p. 162. Sul punto v. inoltre V. BACHELET, *L'attività tecnica della pubblica amministrazione*, Milano, Giuffrè, 1966, p. 86; N. LUGARESI, *Profili comparatistici della norma tecnica: l'esperienza francese dell'AFNOR*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *La normativa tecnica industriale ...op.cit.,* p. 421, secondo cui con l'incorporazione «le norme tecniche assumono carattere imperativo per tutti i soggetti dell'ordinamento».

[99] F. SALMONI, *Le norme tecniche …op.cit.*, p. 162-163. Sul punto v. anche V. CRISAFULLI, *Lezioni di diritto costituzionale*, vol. II, Milano, Cedam, 1970, pp. 11 ss.

[100] V. BACHELET, *L'attività tecnica della pubblica amministrazione …op.cit.*, pp. 90 ss.; nonché M. GIGANTE, *Effetti giuridici nel rapporto tra tecnica e diritto ...op.cit.,* pp. 313 ss.

L'ineccepibilità di tale criterio sul piano delle fonti è superata dall'impraticabilità (*rectius* difficile applicazione) sul piano pratico, stante la necessità della noramzione tecnica di essere costantemente aggiornata in ragione dei nuovi risultati acquisiti nella scienza e nella tecni

2.6. Le norme tecniche volontarie e il rinvio

Come anticipato, la norma tecnica volontaria è la norma elaborata ed adottata dagli enti di normazione privati. Questa rappresenta pertanto l'espressione di quel diritto dei privati su cui abbiamo già argomentato e di cui siamo serviti per ragionare sul rapporto tra norma tecnica - per l'appunto - e ordinamento giuridico dalla prospettiva statica.

Nel paragrafo precedente si è fatto riferimento all'incorporazione quale metodo con il quale l'ordinamento giuridico, incorpora per l'appunto, ossia fa prorpio il contenuto della norma tecnica. Altro criterio di collegamento è quello del rinvio.

Si tratta di un istituto elaborato come criterio di collegamento di "ordinemanti giuridici originari" - per dirla con Santi Romano -, ossia ordinamenti statuali, che vede difatti ampia applicazione nel diritto internazionale privato[101].

Tuttavia, è proprio a partire dall'elaborazione romaniana che sono state avanzate ricostruzioni applicative di detto criterio non solo tra ordinamenti originari, ma più nel complesso tra «istituzioni». Il rinvio intraistituzionale[102], è infatti la tecnica che ha esteso l'applicazione del rinvio anche tra ordinamenti interni[103], rinnovando l'interesse degli studiosi su tale istituto[104].

I tipi di rinvio si distinguono in materiale (anche noto come "recettivio", "fisso" o "statico"), e rinvio formale ("non recettizio", "mobile", "dinamico" o nella dottrina risalente "presupposizione").

La differenza è che mentre nel primo caso, l'autore della norma rinviante «vuole il contenuto dell'atto [...] a cui si rinvia come contenuto del proprio atto normativo, ma anziché riprodurre materialmente nello strumento documentale il precetto contenuto nell'atto [...] richiamato [c.d. incorporazione], preferisce limitarsi a precisare il modo mediante il quale l'operatore giuridico può desumere aliunde il contenuto effettivo della propria volontà»[105] (relativamente alle norme tecniche il rinvio avviene richiamando gli estremi della norma); nel rinvio formale, o non recettizio, «il contenuto dell'atto [...] richiamato rimane estraneo alla volontà del rinviante [che] si limita a disporre che una determinata fattispecie trovi la propria regolamentazione in un precetto contenuto nell'atto

---

[101] L. PICCARDI, *La pluralità degli ordinamenti giuridici ed il concetto di rinvio*, in *Scritti giuridici in onore di Santi Romano*, vol. I, Padova, 1940; G. BALLADORE PALLIERI, *Il concetto di rinvio formale e il problema del diritto internazionale privato*, in *Rivista di diritto civile*, XXI, 1929, p. 412 ss. Nonché anche R. MONACO, *Rinvio nel diritto internazionale privato*, in *Enc. giuri*., vol. XXXI.

[102] F. BASSI, *La norma interna. Lineamenti di una teorica*, Milano, Giuffrè, 1963, pp. 159 ss.

[103] *Ibidem.*

[104] Per uno studio sul rinvio intraistituzionale nei tipi del rinvio fisso e mobile secondo la teoria generale del diritto si faccia riferimento a P. CAPPELO, *La fenomenologia del rinvio statico e del rinvio dinamico*, 2005, consultabile su <http://www.costituzionale .unige.it/dottorato/Rinvio.htm>; F. SORRENTINO, *Le fonti del diritto*, Padova, 2015, p. 167 ss.; A. PAPA, *Alcune considerazioni sulla tecnica del rinvio nella produzione normativa*, in *Rassegna Parlamentare*, 1991, p. 286 ss. Per una valutazione complessiva sui problemi determinati dal rinvio statico e dinamico cfr. *Rinvio statico o dinamico?* Ricerca a cura dell'unità FIRB dell'Università di Genova (responsabile prof. P. Costanzo), aprile 2005, in <https://www.tecnichenormative.it/contributi/rinvio.pdf>; F. MODUGNO, *Pluralità degli ordinamenti*, cit., p. 16 ss.; M GIGANTE, *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in *Rivista italiana di diritto pubblico comunitario*, 1997, p. 313 ss; M. ATRIPALDI, *Il rinvio "intraistituzionale". Una tecnica per la produzione di norme giuridiche nella forma di Stato a tendenza sociocentrica*, in *Nomos*, n. 2, 2018, reperibile al link:<https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2018/05/Atripaldi.pdf>.

[105] F. BASSI, *La norma interna … op.cit.,* pp. 160-161.

[...] richiamato»[106]. Ciò si verifica quanto l'autore della norma rinviante fa riferimento a clausole generali ove si prescrive una conformita allo "stato della scienza e della tecnica", allo "stato dell'arte" oppure alle "regole generalmente riconosciute dalla tecnica", "al meglio delle buone pratiche", e così via[107].

Date le sue caratteristiche, solitamente il rinvio materiale è considerato essere una particolare applicazione dell'incorporazione, ove i riferimenti agli estremi della norma tecnica interessata evitano la produzione di testi giuridici complessi e lunghi[108]. Tuttavia, parimenti al caso dell'incorporazione, sebbene in questo caso la dottrina non ha dubbi nel considerare la norma tecnica rinviata in via recettizia come «parte integrande dell'atto normativo rinviante con conseguente acquisto ad ogni effetto di diretta e piena efficacia nell'ambito dell'ordinamento che detto atto concorre a costituire»[109], dall'altro, il rinvio fisso comporta anch'esso un'inevitabile rigidità. Generando così un ulteriore dubbio, ossia «se le norme volontarie sono successive a quelle cogenti, quale delle due si applica? Quella cogente contenente una disciplina molto probabilmente obsoleta, ma giuridicamente vincolante, ovvero quella volontaria, contenente una disciplina sicuramente aggiornata alla migliore tecnologia disponibile in quel determinato momento storico, ma la cui inosservanza non ha alcuna conseguenza giuridica?», interrogativi questi che sono stati tuttavia chiariti dalla giurisprudenza di Cassazione in tema di violazione delle norme tecniche volontarie[110].

Diversamente, il ricorso al rinvio mobile, non recettizio, evita effetti di cristallizzazione della norma tecnica rinviata ma, secondo parte della dottrina, apre a problemi di legittimità della stessa riconducibili alla domanda: come può la norma tecnica, prodotta da un ente di normazione privato quindi sulla scorta di esigenze e obiettivi privati, essere giustificata nel regolamentare una materia, o parte di essa, eventualmente correlata a questioni di interesse pubblico?

A nostro modo di vedere, tale problema sussisterebbe solo in quelle ricostruzioni volte ad attribuire al sistema di normazione tecnica natura di ordinamento giuridico[111] e che, riscontrando difficoltà nel giustificare il sindacato di un giudice sulle norme tecniche, ricorrono al riconoscimento di un "*munus publicum*" attribuibile agli enti di normazione privati[112].

---

[106] *Ibidem.*

[107] Sul punto si rinvia ad A. ZEI, *Tecnica e diritto ...op.cit.,* pp. 18 ss.

[108]Cfr. V. BACHELET, *L'attività tecnica della pubblica amministrazione …op.cit.*, pp. 86-87, ove utilizza espressioni onnicomprensive che richiamano entrambi i metodi.

[109] F. BASSI, *La norma interna ... op.cit.,* p. 162.

[110] Sul punto si rinvia a F. SALMONI, *Le norme tecniche …op.cit*., p. 258.

[111] *Infra* par. 2.3. Inolte, cfr. F. BASSI, *La norma interna ... op.cit.,* p. 539; G. CADOCCI-PISANELLI, *L'invalidità come sanzione di norme non giuridiche*, Milano, Giuffrè, 1940, pp. 55 ss. i quali, al fine di ovviare al problema del riconoscimento del carattere giuridico delle norme tecniche, ricorrono alla figura della "presupposizione" (o anche "rinvio per presupposizione") che dovebbre riguardare tutti i casi in cui il richiamo al diritto di un altro ordinamento venga fatto al solo scopo di determinare un singolo elemento di una norma appartenente al "diritto interno", o in questo caso al sistema delle norme tecniche. In particolare, sul concetto di "rinvio per presupposizione" v. A. PIZZORUSSO, *Delle fonti del diritto*, Bologna, Zanichelli, 1977, p. 98. Pertanto, attraverso la presupposizione l'ordinamento giuridico attribuisce ad un comportamento, ad un fatto, ovvero ad un elemento di per se stesso oggetto di qualificazione da parte di altro ordinamento o sistema normativo, il ruolo di elemento costitutivo di una fattispecie a cui eventualmente è collegata – in caso di violazione – l'irrogazione di una sanzione (A. ZEI, *Tecnica e diritto ...op.cit.,* p. 203).

[112] A. PREDIERI, *Le norme tecniche nello stato pluralista e prefederativo*, in *Dir. pubbl. ec.*, 1996, pp. 291-295, il quale riprende le teorie di Massimo Severo Giannini sul punto in M.S. GIANNINI, *voce Organi (teoria generale)*, in *Enc. dir.*, XXXI, Milano, 1981. Così anche F. SALMONI, *Le norme tecniche …op.cit*., pp. 89 ss. proprio riprendendo le tesi del Predrieri, nonché pp. 374 ss. sulla tesi delle norme tecniche consensuali come il prodotto normativo di soggetti privati esercenti pubbliche funzioni.

Tali interpretazioni, di orientamento monistico, intendono qualsiasi aspetto della giuridicità in chiave esclusivamente statale[113]. Aderendo invece ad altre teorie, che accolgono la tesi del pluralismo degli ordinamenti a cui abbiamo già fatto riferimento (*infra* par. 2.3), riteniamo che il recupero delle garanzie pubbliche possa essere individuato nel momento della scelta della norma tecnica da recepire nell'atto giuridico per opera del legislatore, o del governo, quale azione che non esime l'autore del recepiemnto da responsabilità sul punto[114], e che farebbe acquistare il tratto della giuridicità, occasionalmente, ed alla specifica norma tecnica recepita, «senza assumere la pretesa di qualificare l'ordinamento a cui si fa rinvio come normativo o giuridico»[115].

Inoltre, la necessità di tali dottrine di attribuire "*munera publica*" agli enti di normazione privata, in quanto interpretati come produttori di norme (tecniche) che sono parte dell'ordinamento giuridico, non tiene conto del fatto che anche in questo caso il recupero delle garanzie è nella scelta, a monte, «dei pubblici poteri che potranno [...] accreditare un'organizzazione piuttosto che un'altra e che potranno in futuro confermare o revocare tale mandato»[116].

2.6.1. Gli organismi di normazione tecnica tra *munera publica* e natura privata

Nel precedente paragrafo si è accennato alle riscostruzioni dottrinarie volte ad attribuire "*munera publica*" agli enti di normazione privata. Si tratta di un orientamento interpretativo, riconducibile al più ampio contesto delle tesi moniste, che possiamo attribuire all'intuizione di Alberto Predieri, il quale lamentava «una generale tendenza di sottrazione di competenze normative allo stato o, quanto meno, di suoi apparati tradizionali», sotto un duplice aspetto, da una parte mediante la «fomazione di nuovi enti intermedi» sempre più attivi nelle procedure decisionali pubbliche (*rectius* codecisione)[117], e dall'altra da un avvertito decentramento dei centri di potere decisionali dato dal trasferimento del potere normativo dallo Stato ad altri soggetti non statali «i cui atti che pongono norme hanno effetti rilevanti e riconosciuti»[118].

La normazione tecnica, peraltro prodotta «in forza di norme comunitarie», è posta al centro delle riflessioni del Predieri a proposito di tale «erosione del potere normativo tecnico e correlativamente di sovranità statale»[119].

In particolare, il Giurista si interroga sulla complessa questione del sindacato del giudice su norme di «enti che hanno funzioni di interesse collettivo ma restano di diritto privato e producono norme che lo stato non ha fatto proprie recependole in suoi atti o approvandole»[120].

---

[113] P. LAZZARA, *La normativa tecnica ...op.cit,* pp. 420 ss.

[114] F. SALMONI, *Le norme tecniche …op.cit*., pp. 171 ss.

[115] A. IANNUZZI, *Il diritto capovolto ...op.cit.,* p. 77.

[116] *Ivi*, p. 78. Relativamente al sistema di accreditamento v. *infra* 3.

[117] A. PREDIERI, *Le norme tecniche nello stato pluralista e prefederativo* …op.cit., p. 278. In particolare, sulla partecipazione dei privati nelle decisioni pubbliche il Predrieri prosegue «[m]an mano gli enti rappresentantivi di interessi e i gruppi non agiscono più al di fuori dei procedimenti come gruppi di pressione, ma come soggetti che operano dentro i procedimenti, come portatori di domande, di proposte e di pareri che, in una seconda fase, vengono assunti nei procedimenti come elemento indispensabile e qualificante, in forza di *conventions* o per prassi che assicuri una consulatazione. In una terza fase, i gruppi appaiono come codecisori, con la ricerca di nuove forme di cooperazione per le decisioni, esprimendo scelte che possono condizionare quelle degli organi del potere pubblico, come veri o come elementi necessari alla decisione, quindi codecisivi».

[118] A. PREDIERI, *Le norme tecniche nello stato pluralista e prefederativo* …op.cit., pp. 278-279.

[119] *Ivi*, pp. 279 ss.

[120] *Ivi*, p. 293.

Così, con implicito richiamo alle tesi di Giannini[121], il Predieri interpreta tali enti come «ausiliari o portatori di un *munus* statale»[122], facendo leva sulla considerazione, corroborata dall'allora indirizzo giurisprudenziale della Suprema Corte, che gli enti di normazione sono organi della pubblica amministrazione seppur in mancanza di una concessione a tal proposito - e per questo qualificati «organi indiretti della pubblica amministrazione» - dato che l'investitura ad organo indiretto «[n]on è detto debba avvenire solo con un atto concessorio»[123]. Secondo Predieri infatti, la mera attribuzione di organismo nazionale di normalizzazione «costituisce un'investitura non meno valida, anche perché contenuta in atto comunitario dotato della primazia europea»[124].

Recente dottrina, in critica sulle posizioni del Predieri, ha osservato che la volontarietà delle norme tecniche, quale tratto comune a tutte (anche quelle armonizzate), indurrebbe ad escludere che il rapporto intercorrente tra le istituzioni europee e le ESOs possa tradursi in una delegazione di competenze normative[125]. La stessa Commissione europea in un documento del 2003, afferma che «più che di una delegazione di potere, si tratta del riconoscimento delle specifiche competenze di ciascun operatore»[126]. Pertanto gli enti di normalizzazione, mantengono lo status di soggetti di diritto

---

[121] M.S. GIANNINI, *Lezioni di diritto amministrativo*, vol. I, Milano, Giuffrè, 1950, p. 125, ove il Maestro provvede anche alla ricostruzione etimologica del vocabolo *munus* nei suoi tre significati di beneficio (*munus*-dono, *munificus*), difesa (*munio*, *munitio*) e servizio (*munificis milites*). Concetti che saranno poi ripresi e approfonditi nelle *Lezioni di diritto amministrativo anno 1959/1960*. In particolare, come osserva Francesco De Leonardis in F. DE LEONARDIS, *Soggettività privata e azione amministrativa. Cura dell'interesse generale e autonomia privata nei nuovi modelli di amministrazione*, Padova, Cedam, 2000, p. 83, nota 226, i munera sono diversamente inquadrati dal Giannini nelle due opere. Nelle lezioni del 1950 l'A. inquadra infatti i concessionari nella categoria dei «*munera* pubblici ad assunzione convenzionale» e afferma che le concessioni possono riugardare sia pubblici servizi che pubbliche funzioni, dato che i *munera* che si assumono in seguito a convenzione sono denominati concessioni. «Anzi si dice di solito concessioni di pubblici servizi, benché esse possano essere anche concessioni di pubbliche funzioni, e benché nell'esercitare servizi pubblici vi siano sempre dei momenti nei quali si svolgono in realtà funzioni pubbliche (così nell'applicare sanzioni amministrative, per es. pecuniarie, per le violazioni dei regolamenti dei servizi)» (*Lezioni di diritto amministrativo*, vol. I, Milano, Giuffrè, 1950, p. 183).

Nel *Corso di diritto amministrativo, Dispense anno accademico 1964/1965*, Giannini precisa che «la sistematica da noi proposta nelle *Lezioni* del 1950, in cui si suggeriva l'utilizzazione di *munus* va rivista, in base ai nuovi studi, così come esposta nel testo», e infatti «non regge la spiegazione in base al concetto di munus, dal momento che il titolare dell'ufficio dato in concessione fa parte della struttura dei pubblici poteri, ed è trattato come qualunque altro titolare d'ufficio a contratto: ha doveri, diritti, tra i quali patrimonialmente importante quello al corrispettivo» (*Corso di diritto amministrativo, Dispense anno accademico 1964/1965*, Milano, Giuffrè, 1965, p. 259).

Mentre nel 1959, Giannini afferma, parlando di atti amministrativi di soggetti privati che «la dottrina intende riferirsi agli atti di privati esercenti pubbliche funzioni o pubblici servizi, e quindi di soggetti privati per modo di dire, perché in realtà si tratta di componenti il plesso di pubblici poteri» (voce *Atto amministrativo*, in *Enc. dir.*, vol. IV, Milano, 1959, p. 58). Mentre nel manuale del 1970 ritiene che «non possono essere conferiti (o quantomeno non dovrebbero esserlo) gli uffici che sono titolari di potestà pubbliche a carattere autoritativo e che pertanto emettono provvedimenti amministrativi. Gli uffici non conferibili sono individuati come quelli che esercitano pubbliche funzioni. Per cui il criterio è che siano conferibili ad imprese solo quegli uffici che siano titolari di compiti che concretano servizi pubblici. Difatti nella pratica gli uffici conferiti ad impresa sono chiamati concessioni di pubblici servizi» (*Corso di diritto amministrativo …op.cit.,* p. 255). Così anche in *voce Organi (teoria generale)*, in *Enc. dir.*, XXXI, Milano, 1981, p. 53.

[122] *Ivi*, p. 279.

[123] *Ivi*, pp. 294-295.

[124] *Ibidem*.

[125] A. ZEI, *Tecnica e diritto …op.cit.,* pp. 361 ss.

[126] v. *Vademecum on European Standardisation*, pubblicato dalla Direzione generale per le imprese della Commissione europea, il 1 marzo 2004, pt. 2.1.2, reperibile al link:<https://law.resource.org/pub/eu/ vademecum/complete. vademecum.pdf>, ove la Commissione scrive che «Il concetto di mandato si basa sul principio della partnership, della cooperazione e della chiara suddivisione dei compiti tra le autorità pubbliche e gli enti di normazione europei debitamente riconosciuti. Attraverso un mandato, le autorità pubbliche chiedono agli enti di normazione europei di redigere specifiche tecniche di natura normativa che soddisfino "le loro" esigenze. Nella pratica, tali standard devono consentire ai produttori di progettare e realizzare prodotti conformi ai requisiti legali. Da un lato, spetta alle autorità pubbliche stabilire rigorosi requisiti per tutelare l'interesse pubblico. Dall'altro lato, è compito di coloro che preparano gli standard redigere norme

privato, perseguono i loro scopi e persistono nello svolgere un'attività fondamentalmente autoregolativa, posto che anche nel caso delle norme armonizzate, non hanno obbligo di adottarle potendo anche riufiutare la richiesta della Commissione[127].

Parimenti, anche l'interpretazione che vede gli enti di normazione esercitare attività di interesse pubblico, secondo una certa dottrina, non pare giustificare una loro "ulteriore" soggezione al potere di indirizzo e controllo dello Stato[128]. Anzitutto perché quello tra enti di normazione privati e Stato è una «parziale coincidenza di interessi» che rende possibile spiegare il rapporto tra questi «ricorrendo alla figura del rapporto di servizio, della concessione, dell'esercizio privato di pubbliche funzioni o di qualunque altra figura che implichi una forma di soggezione degli Enti di normazione ad un potere di indirizzo delle autorità»[129].

Negazione dell'"ulteriore"soggezione poiché tali enti sono già oggetto di una forma di controllo e indirizzo dell'autorità pubblica dato dai presupposti indicati dalla legge per il riconoscimento ufficiale dell'ente (c.d. accreditamento). Esercizio di controllo-limite che pare tuttavia essere duplice e non riguardare solo gli enti di normazione, ma anche il legislatore, o il governo, che nel momento della scelta della norma tecnica di cui avvelersi (per incorporazione o per rinvio), vedono la propria discrezionalità limitata alle sole norme prodotte da enti accreditati[130].

2.6.2. Gli orginasmi di normazione nazionali

Gli organismi di normazione sono stati introdotti già al paragrafo introduttivo (*infra* 2 e 2.1) ove stata svolta una breve ricostruzione storica. In questa sede ci soffermeremo sui singoli enti nei tre livelli globale, europeo e nazionale (italiano), avendo modo di ricostruire il loro ordinamento interno secondo quanto dettato dallo Statuto, nonché soffermandoci sulle procedure decisionali, e quindi sul voto dei partecipanti.

Per esigenze argomentativepartiremo dagli enti di normazione italiani, l'*Ente Nazionale Italiano di Unificazione* (UNI) e il *Comitato Elettrotecnico Italiano* (CEI), per poi passare alla trattazione di quelli presenti a livello internazionale, ed infine a al piano europeo.

a) Il Comitato Elettrotecnico Italiano (CEI)

Il Comitato Elettrotecnico Italiano (CEI), è tra i primi enti di normazione tecnica al mondo e il primo in Italia. Fondato nel 1907 dal consigli generale dell'Associone Elettrotecnica ed Elettronica Italiana (AEI, dal 2013 AEIT - Associazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica

adeguate che soddisfino tali requisiti e tengano conto dello "stato dell'arte". Pertanto, non si tratta di delegare poteri, ma di riconoscere le competenze specifiche di ciascun operatore. Sono i mandati che descrivono e giustificano, caso per caso, i compiti che le autorità pubbliche assegnano agli enti di normazione europei. Su questi mandati dipendono la chiarezza del ruolo di ciascuna parte, la complementarietà tra regolamenti e norme e la qualità della normazione europea [enfasi aggiunta]».

[127] Art. 20 Reg. 1025/2012, v. inoltre A. ZEI, *Tecnica e diritto …op.cit.,* p. 371.

[128] A. ZEI, *Tecnica e diritto …op.cit.,* p. 131. Si precisa che le formulazioni dell'A. sono svolte in considerazione degli enti di normazione in Austria. Riteniamo tuttavia che tali considerazioni possano estendersi in generale anche all'ordinamento italiano.

[129] *Ivi*, p. 132.

[130] Cfr. A. ZEI, *Tecnica e diritto …op.cit.,* p. 130. Il tema dell'acceditamento come forma di controllo pubblico sarà ripresa anche *infra* 3.

e Telecomunicazioni[131]), e costituitosi in forma autonoma nel 1909, fu rifondato nel 1946 dall'AEI, dall'Enel e dall'Associazione nazionale delle industrie elettrotecniche ed elettroniche (ANIE)[132].

La Legge n. 186 del 1º marzo 1968, ha stabilito che «[t]utti i materiali, le apparecchiature, i macchinari, le installazioni e gli impianti elettrici ed elettronici devono essere realizzati e costruiti a regola d'arte» e che gli stessi «realizzati secondo le norme del Comitato Elettrotecnico Italiano si considerano costruiti a regola d'arte»[133].

L'art. 1 dello Stato, prevede che «[i]l CEI è un'associazione culturale a carattere scientifico e tecnico, senza scopo di lucro» che, tra i diversi compiti, è impegnato nel «promuovere e favorire la rispondenza alla legge e alla regola dell'arte dando la massima diffusione alla propria attività attraverso tutti i sistemi considerati idonei [...]», nonché mantiene «i contatti necessari, a livello culturale e di ricerca, per seguire l'evoluzione tecnologica e [mantiene] aggiornati i propri studi nel campo normativo»[134].

Ai sensi dell'art. 3, lo Statuto contempla i soci del CEI, distinti in diverse categorie: soci promotori[135], soci di diritto[136], soci effettivi[137], soci onorari[138], soci benemeriti[139], soci aderenti[140].

---

[131] La Associazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telecomunicazioni è stata costituita il 1° gennaio 1897 con la denominazione originale di "Associazione Elettrotecnica Italiana". È stata eretta in Ente Morale con R.D. 3 febbraio 1910 n° 42, ed ha assunto la denominazione di "Associazione Elettrotecnica ed Elettronica Italiana – AEI" con DPR 1° luglio 1964, pubblicato nella Gazzetta Ufficiale n° 263 del 26 ottobre 1964. Successivamente ha assunto la denominazione di "Federazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telecomunicazioni" con approvazione della Prefettura di Milano in data 28 ottobre 2003 – Registro Persone Giuridiche n. 455 della pagina 710 – Volume 2°. Dal 1° novembre 2013, a seguito di referendum sociale, ha assunto l'attuale denominazione, nel seguito abbreviata in AEIT. Nella AEIT è confluita la AIIT – Associazione Italiana Ingegneri delle Telecomunicazioni, fondata nel 1962. Maggiori informazioni sono reperibili sul sito uggiciale al link:<https://www.aeit.it/aeit/r02/struttura/pagedin.php?cod=home>.

[132] F. SALMONI, *Le norme tecniche …op.cit.*, pp. 230 ss.

[133] Cfr. art. 1, L. 186/1968.

[134] Art. 1 Statuto del CEI (d'ora in poi Statuto CEI), Approvato con decreto del Presidente della Repubblica 9 settembre 1972, n. 837, con le modificazioni apportate con decreto ministeriale 23 marzo 1994 (pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 258 del 4 novembre 1994) con decreto del direttore generale per lo sviluppo produttivo e la competitività del Ministero dell'Industria, del Commercio e dell'Artigianato (pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 6 del 9 gennaio 2001) e con le modifiche iscritte in data 6 luglio 2006 nel Registro delle Persone Giuridiche della Prefettura di Milano, reperibile al link:<https://static.ceinorme.it/ ceinorme/statuto.pdf>.

[135] Art. 4 Statuto CEI, secondo cui sono soci promotori: la Federazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telecomunicazioni (AEIT), la Federazione Nazionale Imprese Elettrotecniche ed Elettroniche (ANIE), ed ENEL Spa.

[136] Art. 5 Statuto CEI, il quale prevede che sono soci di diritto: il Ministero dell'Interno; il Ministero dello Sviluppo Economico; il Ministero delle Infrastrutture e della Mobilità Sostenibili; il Ministero dell'Istruzione; il Ministero dell'Università e della Ricerca; il Ministero della Difesa; il Ministero del Lavoro e delle Politiche Sociali; il Ministero della Transizione Ecologica; il Ministero della Salute; il Ministero della Cultura; il Consiglio Nazionale delle Ricerche. Possono inoltre diventare soci di diritto altri Ministeri che, invitati dal Presidente Generale del CEI, diano la loro adesione. Il Presidente Generale del CEI è inoltre delegato ad aggiornare le denominazioni dei Ministeri sopra elencati alla loro denominazione ufficiale.

[137] Art. 6 Statuto CEI, per il quale sono soci effettivi gli Enti pubblici e privati, Società od altri organismi interessati alle attività del CEI che ne facciano domanda e siano ammessi dal Consiglio.

[138] Art. 7 Statuto CEI, prevede che sono soci onorari le persone che abbiano acquistato notorietà per aver svolto studi e lavori notevoli nel campo della normativa tecnica ed unificazione elettrica, cui venga riconosciuta tale qualifica dall'Assemblea, su proposta del Consiglio del CEI.

[139] Art. 8 Statuto CEI, dispone che sono soci benemeriti i Soci che abbiano contribuito in modo particolarmente rilevante all'attività del CEI. Ad essi verrà riconosciuta tale qualifica dall'Assemblea, su proposta del Consiglio. Il socio benemerito mantiene tutti i diritti spettantigli al momento della sua nomina a benemerito.

[140] Art. 9 Statuto CEI, il quale prevede che sono soci aderenti gli enti, le società e le persone fisiche che ne facciano domanda e vengano ammesse. I soci aderenti non partecipano all'Assemblea.

All'art. 16 sono invece determinati gli organi componenti il Comitato, ossia l'Assemblea, il Consiglio, il Comitato Esecutivo, il Presidente Generale, il Collegio dei Revisori dei Conti, il Collegio dei Probiviri, gli Organi Tecnici. In particolare, tra quest'ultimi Organi[141], composti da le Commissioni Centrali, i Comitati e Sottocomitati Tecnici, e i Gruppi Settoriali, Commissioni Miste e Speciali, guidate dalla Commissione Centrale Superiore Tecnica - CST[142], è ai Comitati e Sottocomitati Tecnici che è affidata l'attività normativa.

L'art. 35 dello Stato prevede infatti che

> I Comitati e i relativi Sottocomitati sono costituiti dal Comitato Esecutivo. I Comitati Tecnici sono organi a carattere nazionale con il compito di predisporre ed elaborare le norme nel settore di loro rispettiva competenza.
> La composizione dei Comitati deve garantire la presenza di tutte le categorie interessate di Soci e il loro funzionamento e tenere conto degli accordi internazionali. La costituzione, i compiti e le attribuzioni sono fissate dal Regolamento per gli Organi Tecnici [enfasi aggiunta][143].

Tuttavia per la loro disciplina, il Regolamento generale[144], all'art. 9[145], rinvia al Regolamento per Organi Tecnici[146]. Tra le disposizioni di quest'ultimo documento, pare utile richiamare il dettato dell'art. 4 recante disciplina dei "Principi della Normazione", secondo cui

> Il CEI opera in conformità alle regole ed ai principi stabiliti dal Regolamento 1025/2012/UE e s.m.i. ed ai principi riconosciuti dall'Organizzazione Mondiale del Commercio nel settore della normazione. Il CEI agisce, inoltre, nel rispetto dello statuto, del regolamento generale e delle Direttive ISO/IEC e dei Regolamenti CEN-CENELEC che regolano le attività normative in ambito internazionale ed europeo. L'attività normativa del CEI si ispira, in particolare, ai principi di: Partecipazione delle Parti Interessate; Ricerca del consenso; Trasparenza; Imparzialità [enfasi aggiunta][147].

Principi questi dettagliati nei successivi articoli di cui, la "partecipazione delle parti" all'art. 4.1, ove è previsto che

> Una parte interessata è un soggetto, anche plurale, il cui interesse è o può essere direttamente o indirettamente influenzato da una norma o da un progetto di norma.

mentre per quanto riguarda la "ricerca del consenso", l'art. 4.2 dispone che

---

[141] Art. 33 Statuto CEI.

[142] Art. 34 Statuto CEI, il quale prevede che La Commissione Centrale Superiore Tecnica è nominata dal Comitato Esecutivo. Ne fanno parte i Presidenti dei Gruppi Settoriali e ha il compito di coordinare le attività specifiche dei Comitati Tecnici e Sottocomitati Tecnici e di trovare soluzione ai problemi tecnici di carattere generale che non siano di competenza dei singoli Comitati Tecnici o Sottocomitati. La costituzione, i compiti e le attribuzioni sono fissate dal Regolamento per gli Organi Tecnici.

[143] Art. 35 Statuto CEI.

[144] Regolamento generale del CEI (d'ora in poi Reg. gen. CEI), reperibile al link:<https://static.ceinorme.it/ceinorme/regolamento-generale.pdf>.

[145] Art. 9 Reg. gen. CEI, prevede che Per la CST (Commissione Centrale Superiore Tecnica), i Gruppi Settoriali e le Commissioni Miste o Speciali, nonché per i Comitati Tecnici e Sottocomitati si rimanda al Regolamento per gli Organi Tecnici. Il Comitato Esecutivo nomina i Presidenti dei Comitati Tecnici e dei Sottocomitati tra i rappresentanti proposti dai Soci. Tutte le partecipazioni nell'ambito degli Organi Tecnici del CEI hanno durata triennale, scadono al termine del triennio nel corso del quale la carica ha avuto inizio e sono rinnovabili. La durata in carica del Presidente/Vicepresidente di Comitato non può superare i tre mandati consecutivi.

[146] Regolamento per gli Organi Tecnici (d'ora in poi Reg. org. tec.), reperibile al link:<https://static.ceinorme.it/ceinorme/regolamento-organi-tecnici.pdf>.

[147] Art. 4 Reg. org. tec.

> Il contenuto tecnico di una norma o di un qualsiasi altro documento normativo sottoposto al voto o a commenti secondo le procedure internazionali o nazionali, è approvato sulla base del "consenso".
> Il consenso deve essere inteso come un "accordo generale, caratterizzato da assenza di giustificate opposizioni, provenienti da parti rilevanti degli interessi coinvolti, e da un processo che implichi tentativi per tenere conto dei punti di vista di tutte le parti coinvolte e per conciliare tutti i pareri contrastanti", così come definito dalla ISO/IEC Guide 21 e dalla Norma CEI UNI EN 45020.
> La precondizione per il raggiungimento del consenso è che sia garantita la più ampia e bilanciata rappresentanza possibile delle parti interessate nella composizione degli Organi Tecnici. Va sottolineato che il consenso non implica necessariamente l'unanimità.
> Il consenso si intende raggiunto se il Presidente di CT o SC non riceve ferme e giustificate opposizioni avanzate o sostenute da rappresentanti di Organizzazioni che, in modo diretto o per il ruolo di rappresentanza collettiva, costituiscono una "parte rilevante degli interessi coinvolti". Le Parti rilevanti degli interessi coinvolti sono costituite dalle Organizzazioni che rappresentano, in larga misura, interessi generali rilevanti che sono o possono essere influenzati dal progetto di norma preso in esame. La valutazione di rilevanza è da effettuarsi in relazione allo specifico progetto di norma.
> Le opposizioni formali devono essere motivate da ragioni tecniche o oggettive e presentate con una comunicazione ufficiale scritta.
> Eventuali contrasti o pareri discordi tra rappresentanti di Soci facenti parte di Organizzazioni che costituiscono una "parte rilevante degli interessi coinvolti" devono essere ricomposti con una decisione della Organizzazione, presentata formalmente al Presidente della CT o SC.
> L'opposizione formale nel CT o SC di un rappresentante di un singolo Socio in contrasto con la posizione dell'Organizzazione a cui è associato non è riconosciuta. Le opposizioni formali dovranno essere discusse in seno al CT o al SC debitamente convocato per discuterle e trovare il modo di superarle, con il contributo fattivo del Technical Officer del CEI che deve assicurare che siano rispettate le dinamiche nella ricerca del consenso. In caso non si riesca a conciliare le opposizioni formali, il CT o il SC ricorre al Direttore Tecnico del CEI, per risolvere la controversia, secondo le procedure definite nell'Allegato 1 [enfasi aggiunta][148].

Infine all'art. 38 dello Statuto, è disciplinato il momento conclusivo del processo di normazione, ossia la pubblicazione della norma tecnica «sotto l'intestazione "Norma Italiana CEI" registrata in Tribunale»[149].

b) L'Ente Nazionale Italiano di Unificazione (UNI)

L'Ente Italiano di Normazione (UNI) è l'Organismo Nazionale di Normazione comunicato dallo Stato Italiano alla Commissione Europea ai sensi del Regolamento UE n.1025/2012, e attuato con il Decreto Legislativo n.223/2017. L'UNI svolge attività in tutti i settori esclusi quelli elettrotecnico ed elettronico dei quali si occuapa il CEI.

L'Ente è stato costituito nel 1921 con il nome di UNIM, quale associazione senza scopo di lucro competente nel settore della meccanica. Questa venne rinominata UNI e riconosciuta giuridicamente con regio decreto n. 1107, del 18 luglio 1930, quando la sua attività venne estesa a tutti i settori tecnici nei quali si rese necessario disporre di normative tecniche nazionali.

Nel 1955, l'UNI venne ristrutturata con un nuovo Statuto, riconosciuto con d.P.R. n. 1522 del 20 settembre 1955. Tuttavia, il riconoscimento ufficiale avvenne nel 1986 con Legge n. 317, del 21 giugno 1986 che ha dato attuazione alla Direttiva CEE 83/189.

Al momento in cui si scrive, l'ultima versione dello Statuto è quella del 2020 ove, tra le altre cose, è stata introdotta la regolamentazione della *governance* interna[150]. Inoltre, rispetto al CEI, la

[148] Art. 4.2 Reg. org. tec.

[149] Art. 38 Statuto CEI.

[150] Per ulteriori si rinvia alla comunicazione "*Nuovo Statuto: autorizzazione al decollo!*" disponibile sul sito ufficiale dell'UNI, al link:<https://www.uni.com/nuovo-statuto-autorizzazione-al-decollo/>.

documentazione che illustra l'organizzazione e la gestione dell'UNI è molto più numerosa ed estesa in diversi ambiti dell'Ente.

Iniziando la trattazione dal citato Statuto, all'art. 1 è espressamente contemplato che «UNI è una associazione senza scopo di lucro con sede in Milano. I principi cui si ispira sono di affermare la dignità della Persona e tutelare i Diritti Umani fondamentali [enfasi aggiunta]», il cui scopo è quello di «svolgere attività di normazione, ossia studiare, elaborare, approvare, pubblicare e diffondere documenti di applicazione volontaria – norme tecniche, specifiche tecniche, rapporti tecnici e prassi di riferimento – al fine di coordinare gli sforzi per migliorare e standardizzare prodotti, servizi, persone ed organizzazioni, con l'obiettivo di semplificare la progettazione, la produzione e la distribuzione, garantendo prestazioni di sicurezza e di qualità, rispetto per l'ambiente e tutela dei consumatori e dei lavoratori, in tutti i settori economici, produttivi e sociali»[151]. In particolare, tra le diverse attività prodromiche al raggiungimento di tali scopi, riteniamo d'interesse evidenziare quelle volte a «promuovere la cultura della normazione verso tutte le componenti della società civile e della Pubblica Amministrazione con particolare attenzione al mondo degli studenti e dei consumatori» (let. g), e a «promuovere attività a carattere scientifico e culturale riguardanti la normazione e la sua interazione con altre pratiche e discipline, con particolare attenzione al mondo accademico e a quello della ricerca» (let. h)[152].

I soci dell'UNI si distinguono in: soci fondatori (che al momento unico socio è la Confederazione Generale dell'Industria Italiana - Confindustria), soci di diritto[153] e soci ordinari[154].

Tra di soci di diritto, troviamo anche gli Enti Federati, quali soggetti che svolgono l'attività di normazione in senso proprio. L'art. 2 dello Stato li disciplina come organizzazioni che, sulla base di una Convenzione di Federazione con UNI, disciplinata da apposito Regolamento interno[155], svolgono attività di normazione, ciascuna per il settore di propria competenza, sul piano nazionale, europeo e internazionale, nel rispetto dello Statuto e dei principi contenuti nel Regolamento UE n.1025/2012 e del Decreto Legislativo n.223/2017.

A livello interno, l'organizzazione dell'Ente è costituita dagli Organi statutari, individuati nell'Assemblea dei soci, nel Comitato di Indirizzo Strategico, nel Consiglio Direttivo, nella Giunta Esecutiva, nel Presidente, nel Collegio dei Revisori Legali, nel Collegio dei Probiviri, nel Comitato di Coordinamento delle Pubbliche Amministrazioni[156].

---

[151] Art. 1, Statuto UNI, testo approvato mediante Referendum il 29 luglio 2020 e iscritto nel Registro delle Persone Giuridiche della Prefettura di Milano al numero d'ordine 281 della pagina 536 del volume 2 il 26 agosto 2020.

[152] Ibidem.

[153] Art. 4 Statuto UNI, sono soci di diritto i Ministeri presenti nel Comitato di Indirizzo Strategico, l'Ente Italiano di Accreditamento (ACCREDIA), il Consiglio Nazionale delle Ricerche (CNR) e gli Enti Federati. I soci di diritto sono esentati dal versamento delle quote. La partecipazione di esperti nominati dai soci di diritto nelle Commissioni Tecniche dell'UNI è stabilita in un apposito Regolamento approvato dal Consiglio Direttivo.

[154] Art. 5 Statuto UNI, il quale prevede che possono far parte dell'UNI in qualità di soci ordinari i soggetti interessati all'attività di normazione: a) gli enti pubblici; b) le associazioni, federazioni e confederazioni di qualsiasi natura; c) gli ordini e collegi territoriali, i consigli e le associazioni nazionali professionali; d) gli enti tecnici, scientifci e di ricerca e di istruzione, le università, i consorzi, gli enti professionali, economici, assicurativi e previdenziali; e) le imprese; f) i professionisti e le società di professionisti; g) le persone fsiche. I soggetti di cui alla lettera g) possono sottoscrivere solo 1 (una) quota ordinaria. Sono soci ordinari "di rappresentanza" i soggetti di cui alle lettere a), b), c) e d) che sottoscrivono almeno 20 (venti) quote ordinarie. Sono "grandi soci" i soci ordinari di rappresentanza che sottoscrivono almeno 200 (duecento) quote ordinarie.

[155] V. Regolamento UNI per la Convenzione di Federazione degli Enti Federati con UNI e del Comitato Consultivo degli Enti Federati, reperibile al link:<https://www.uni.com/chi-siamo/documenti/>.

[156] Art. 10 Statuto UNI.

Ai sensi dell'art. 22, lett. f), il Consiglio Direttivo è competente per la nomina degli esperti della Commissione Centrale Tecnica (CCT) sulla base delle segnalazioni dei rispettivi soggetti rappresentati. Si tratta di un organo particolarmente importante in quanto deputato a diverse funzioni di indirizzo e controllo a livello tecnico rilevanti ai fini del processo di normazione[157].

In particolare, l'apposito "Regolamento di convocazione, partecipazione e funzionamento della Commissione Centrale Tecnica"[158] (d'ora in poi Regolamento CCT), tra le diverse funzioni, dispone che la CCT, sovraintende e coordina i lavori delle CT (siano esse istituite presso l'UNI e presso gli Enti Federati) assicurando i corretti ambiti di competenza, anche in relazione alla gestione delle interdisciplinarietà (lett. d); indirizza alle competenti CT (siano esse istituite presso l'UNI o presso un Ente Federato) le richieste di progetti di norma pervenute all'UNI assicurando i corretti ambiti di competenza, anche in relazione alla gestione delle interdisciplinarietà (lett. e); delibera sui progetti di norma che vengono presentati dalle singole CT (siano esse istituite presso l'UNI o presso un Ente Federato) relativamente alla correttezza del processo di elaborazione (leet. f); ed infine, coordina a livello nazionale le attività normative svolte a livello europeo e internazionale, rispettivamente in sede CEN e ISO, avvalendosi delle competenti CT istituite presso l'UNI o presso gli Enti Federati, se esistenti, approvando gli interfacciamenti nazionali agli OT di CEN e ISO proposti dal Comitato di Presidenza CCT (lett. h)[159].

Pare inoltre di non secondario rilievo evidenziare che, ai sensi dell'art. 7 del Regolamento CCT, al fine di migliorare l'efficacia dell'attività di normazione, la CCT valuta, su proposta di una o più CT dell'UNI o di uno o più EEFF ovvero su iniziativa della Presidenza CCT, le proposte di costituzione di OT misti per lo studio di progetti di norma e/o per la gestione dell'attività normativa su argomenti caratterizzati da multi-competenza o da competenze comuni a più OT.

Le Commissioni Tecniche sono un organo comune sia presso l'UNI, sia presso gli Enti Federati e le loro funzioni, disciplinate da apposito Regolamento[160], consistono perlopiù nella predisposizione ed elaborazione di progetti di norma e nell'interfacciare le attività CEN e ISO nei settori di loro rispettiva competenza[161]. La composizione di ciascuna Commissione Tecnica garantisce una equilibrata rappresentanza delle parti economiche e sociali interessate.

Il Regolamento sulla politica associativa, entrato in vigore il 1 marzo 2022[162], prevede che le persone ("Esperti") che compongono gli organici delle Commissioni Tecniche, Sottocommissioni e Gruppi di Lavoro (nell'insieme "Organi Tecnici" – OT) UNI devono rappresentare soci ordinari o soci di diritto dell'UNI. Soggetti questi che possono essere inseriti nell'organico di un OT esclusivamente a fronte di una nomina formale di designazione a cura del socio UNI interessato. A meno degli specifici casi previsti per grandi soci e soci di rappresentanza, non è possibile designare nello stesso OT più rappresentanti dello stesso socio, «fatta salva la possibilità di inserire altre persone in qualità di osservatori»[163].

---

[157] Art. 31, lett. d) ed e), Statuto UNI.

[158] V. Regolamento di convocazione, partecipazione e funzionamento della Commissione Centrale Tecnica UNI (d'ora in poi Regolamento CCT), reperibile al link:<https://www.uni.com/chi-siamo/documenti/>.

[159] Art. 1 Regolamento CCT.

[160] V. Regolamento di funzionamento e coordinamento delle attività delle Commissioni Tecniche, reperibile al link:<https://www.uni.com/chi-siamo/documenti/>.

[161] Art. 34 Statuto UNI.

[162] Art. 3.2.1. de Il Regolamento di Politica Associativa UNI, reperibile al link:<https://www.uni.com/chi-siamo/documenti />.

[163] Art. 3.2.1 Regolamento di Politica Associativa UNI.

Il Regolamento contempla anche due "casi particolari" secondo cui, in aggiunta alla possibilità di designare rappresentanti esperti e osservatori, è possibile, per il corretto presidio delle attività europee (CEN) e internazionali (ISO) di competenza di ciascun OT, che il socio richieda a UNI di inserire in uno stesso OT già presidiato da una persona rappresentante il socio stesso, anche una o più persone che l'OT nomini quali proprie rappresentanti in sede CEN/ISO[164].

Inoltre, le persone giuridiche interessate esclusivamente a uno specifico progetto di norma tecnica nazionale, possono essere ammesse a partecipare al processo normativo, pur non essendo associati all'UNI, purché presentino una formale domanda che evidenzi la specifica competenza tecnica dell'organizzazione e della persona delegata a seguire i lavori e dichiarino la disponibilità al pagamento della quota forfettaria fissata dal Consiglio Direttivo UNI a copertura delle spese di servizio. Domanda su cui il Presidente della Commissione cui fa capo il progetto può esprimere motivati commenti. In assenza, l'UNI comunica l'ammissione che verrà formalizzata solo dopo il pagamento dell'importo forfettario per progetto[165].

Pertanto, oltre ai soggetti rappresentanti esperti e agli osservatori, il Regolamento in questione prevede anche la possibilità che altre categorie di soggetti prendano parte al processo di normazione. Deve tuttavia precisarsi che, stando a quanto stabilito dall'Allegato I al Regolamento relativo alle "Caratteristiche e diritti/servizi associativi dei Soci ordinari UNI", il peso partecipativo di ogni socio sia proporzionato alla categoria a cui questo appartiene (se singola persona fisica, soggetto rappresentante interessi diffusi, persona giuridica) e al contributo versato. L'art. 2 del Regolamento distingue infatti le titpologie di soci in: socio persona fisica (con contributo base o con contributo plus); socio con contributo agevolato; socio con contributo ordinario; socio con contributo speciale; socio di rappresentanza; grande socio, a cui l'Allegato fa corrispondere i relativi diritti/servizi associativi e numero di quote.

L'art. 35 disciplina la procedura di elaborazione dei progetti di norma tecnica e di pubblicazione in norme tecniche UNI, il quale prevede che i progetti di norma tecnica (o specifche tecniche o rapporti tecnici) sono elaborati dalle Commissioni Tecniche dell'UNI e degli Enti Federati fno al raggiungimento del consenso delle parti rappresentate sui contenuti.

Tali lavori di normazione nazionali possono inoltre essere preceduti da lavori di pre-normazione per l'elaborazione di "prassi di riferimento" (c.d. UNI/PdR) secondo le modalità stabilite dall'apposito Regolamento.

Come definite dal "Regolamento per le attività di sviluppo delle prassi di riferimento" (d'ora in poi Regolamento PdR), le UNI/PdR sono «documenti emanati da UNI che introducono prescrizioni tecniche o modelli applicativi settoriali di norme tecniche, elaborati sulla base di un rapido processo di condivisione in un tavolo ristretto, sotto la conduzione operativa di UNI» e precedono le attività di normazione nazionale[166].

Si tratta di «prodotti della normazione previsti dallo Statuto, differenti da norme tecniche, specifiche tecniche e rapporti tecnici», elaborati al fine di «gestire contenuti tecnici di *best practice*, talvolta già

[164] Art. 3.2.4.1 Regolamento di Politica Associativa UNI, ove in particolare è previsto che gli Osservatori CEN/ISO rappresentano UNI ai tavoli sovranazionali, ma nell'ambito dell'OT di competenza operano quali osservatori/osservatrici senza diritto di voto (essendo presente, nello stesso organico, altra persona con diritto di voto rappresentante lo stesso socio).

[165] Art. 3.2.4.2 Regolamento di Politica Associativa UNI.

[166] Art. 1 Regolamento per le attività di sviluppo delle prassi di riferimento (d'ora in poi Regolamento PdR), reperibile al link:<https://www.uni.com/chi-siamo/documenti/>.

consolidati in forma privata o consorziata, assicurando la funzione di tempestivo trasferimento di conoscenze e tecnologie che l'Unione Europea richiede alla normazione tecnica consensuale»[167].

La loro elaborazione avviene innanzitutto su proposta di soggetti interessati che rappresentano in maniera particolarmente significativa gli interessi di una collettività o di una filiera[168]. Tali soggetti, al fine di dare avvio all'attività UNI/PdR, devono inviare una richiesta in cui indicano finalità, benefici attesi, eventuale descrizione del contesto legislativo e normativo, descrizione sintetica del contenuto della proposta, potenziali soggetti destinatari/beneficiari della "prassi di riferimento"[169].

Lo sviluppo di una UNI/PdR avviene mediante la costituzione di un apposito Tavolo Tecnico, composto da esperti/e definiti/e in accordo con la parte proponente della UNI/PdR e gestito da una segreteria UNI o di un Ente Federato. La parte proponente della UNI/PdR deve assicurare che gli esperti e le esperte del Tavolo Tecnico da essa designati/e abbiano le competenze necessarie allo sviluppo del documento, coerentemente con i temi che saranno trattati[170].

Raggiunto il consenso degli esperti e delle esperte del Tavolo sul contenuto, il documento è sottoposto a consultazione pubblica, aperta a tutti, per raccogliere commenti e suggerimenti da parte del mercato, e di cui viene informata la CCT della consultazione[171]. La consultazione pubblica sulla UNI/PdR ha una durata di almeno trenta giorni (eventuali deroghe relative alla riduzione dei tempi della consultazione pubblica possono essere accordate dal Consiglio Direttivo laddove vi siano urgenze comprovate).

Infine, per favorire la loro massima diffusione, le UNI/PdR vengono messe a disposizione gratuitamente sul sito UNI, previa registrazione dell'utente, in formato elettronico sul catalogo dell'UNI[172], e restano in vigore per un periodo di tempo non superiore a 5 anni, entro il quale possono essere trasformate in una norma tecnica UNI o una specifica tecnica UNI/TS o in un rapporto tecnico UNI/TR, oppure essere ritirate[173].

Relativamente all'attività di normazione in senso proprio, oltre al dettato dell'art. 35 dello Statuto, la disciplina della procedura è dettagliata al "Regolamento di elaborazione e pubblicazione delle norme tecniche"[174], che distingue una procedura per lo sviluppo dei progetti di norma nazionale da parte delle CT (art. 2), e un altra per il contributo allo sviluppo delle norme europee (EN) e internazionali (ISO) (art. 3).

Relativamente alla prima, il Regolamento articola lo sviluppo dei progetti di nromazione nazionale in sei fasi essenziali: richiesta, proposta, inchiesta pubblica preliminare, affidamento e sviluppo del progetto di norma, inchiesta pubblica finale, approvazione finale e trasformazione del progetto in norma[175].

---

[167] Ibidem.

[168] Art. 2 Regolamento PdR.

[169] Art. 3 Regolamento PdR.

[170] Art. 5 Regolamento PdR, il quale prevede in particoalare che possono far parte del Tavolo anche esperti/e di Organi Tecnici dell'UNI e degli Enti Federati, in grado di apportare la propria competenza ed esperienza su tematiche/materie relative a quelle oggetto della UNI/PdR, per un numero massimo di un/a esperto/a per Organo Tecnico (sia esso istituito presso l'UNI o presso un Ente Federato). Eventuali deroghe sul numero dei partecipanti sono ammesse purché adeguatamente motivate.

[171] Art. 6 Regolamento PdR.

[172] Art. 7 Regolamento PdR.

[173] Art. 8 Regolamento PdR.

[174] V. Regolamento di elaborazione e pubblicazione delle norme tecniche UNI, reperibile al link:<https://www. uni.com/chi- siamo/documenti/>.

[175] Art. 2 Regolamento di elaborazione e pubblicazione delle norme tecniche UNI.

Innanzitutto, la proposta di un nuovo progetto di norma nazionale può essere presentata da uno o più componenti di una CT oppure dalla Segreteria della CCT a seguito di formale e motivata richiesta avanzata da qualsiasi soggetto interessato, pubblico o privato. Al fine di assicurare trasparenza al processo di normazione circa l'intenzione di avviare lavori di normazione in determinati settori o su specifici temi, la fase di avvio dei lavori per l'elaborazione di un progetto di norma è sempre preceduta da una Inchiesta Pubblica Preliminare (IPP), della durata di almeno quindici giorni. Le finalità dell'inchiesta sono molteplici e il Regolamento le individua nel: vagliare le esigenze del mercato; valutare se la futura norma risponde a una reale e diffusa esigenza degli operatori di settore; coinvolgere tutti i soggetti che rappresentano gli interessi in gioco; raccogliere elementi circa l'eventuale esistenza di norme, regolamenti e altra documentazione rilevante utile alla stesura del progetto o che trattano l'argomento.

Nel caso in cui in IPP vengano avanzate ferme opposizioni tecnicamente motivate da parte di soggetti rappresentativi, non risolte all'interno della CT o della CT mista competente[176], ovvero dall'intervento di Presidente o Coordinatore, interviene il Comitato di Presidenza CCT, che decide in merito nell'ambito dei compiti attribuitigli. La decisione è immediatamente operativa, solo se nessuna parte interessata presenta Appello nei 20 giorni successivi alla decisione. In caso di Appello, la decisione è di competenza della CCT, che si esprime nel più breve tempo possibile.

Superata positivamente la fase di IPP, la responsabilità della fase di sviluppo del progetto di norma è in carico alla CT competente e deve concludersi entro 18 mesi dalla data di inizio lavori. Lo sviluppo dei lavori prevede una programmazione delle attività con indicazione di compiti, responsabilità e tempi delle varie fasi (cronoprogramma) e un costante monitoraggio del corretto coinvolgimento delle parti interessate. Nel caso in cui non si raggiunga un accordo, la decisione è comunque di competenza del Comitato di Presidenza CCT, nell'ambito dei compiti attribuitigli, ed è immediatamente operativa, solo se nessuna parte interessata presenta Appello nei 20 giorni successivi alla decisione. In caso di Appello, la decisione è di competenza della CCT, che si esprime nel più breve tempo possibile.

I progetti di norma nazionale, approvati dalle CT, vengono avviati, nel rispetto delle procedure vigenti, alla fase di inchiesta pubblica finale (IPF), condotta tramite consultazione online nell'apposita sezione del sito UNI per una durata di 60 giorni, questa volta con la finalità di vagliare la posizione del mercato; raccogliere ulteriori contributi dagli operatori di settore; ottenere il consenso più allargato possibile sul progetto prima che diventi norma con particolare riferimento a chi non ha partecipato ai lavori di elaborazione del progetto.

Nel caso in cui in IPF vengano avanzate ferme opposizioni tecnicamente motivate da parte di soggetti rappresentativi, non risolte all'interno della CT o della CT mista competente, ovvero dall'intervento di Presidente o Coordinatore/Coordinatrice, interviene il Comitato di Presidenza CCT, che decide in merito nell'ambito dei compiti attribuitigli. La decisione è immediatamente operativa solo se nessuna parte interessata presenta Appello nei 20 giorni successivi alla decisione. In caso di Appello, la decisione è di competenza della CCT, che si esprime nel più breve tempo possibile. Si precisa che i commenti presentati da componenti della CT e non accolti dalla stessa nella fase di elaborazione della norma, qualora ripresentati in IPF non saranno tenuti in considerazione.

[176] *Ibidem*. In particolare, È in capo alla Presidenza della CT competente la responsabilità di rispettare i principi basilari della normazione tecnica, mentre il/la Funzionario Tecnico UNI o la Direzione dell'Ente Federato è "garante" del processo. In caso di contrasti gravi, non risolti all'interno della CT, la Presidenza della CT deve richiedere l'intervento del Comitato di Presidenza CCT, che decide in merito nell'ambito dei compiti attribuitigli dall'art. 5.5.g) del Regolamento CCT.

Il superamento con esito positivo della IPF è condizione per l'approvazione finale, da parte della CCT, del processo di trasformazione dei progetti in norma. I progetti di norma nazionale approvati dalla CCT sono sottoposti alla ratifica della Presidenza dell'UNI, che ne autorizza la pubblicazione mediante l'entrata a far parte del corpo normativo nazionale. La data di entrata in vigore della norma coincide con la data di entrata a far parte del corpo normativo nazionale ed è riportata nelle informazioni di copertina della norma.

Il contributo allo sviluppo delle norme europee (EN) e internazionali (ISO), è assegnato all'ambito degli OT di interfaccia nazionale individuati dalla CCT.

Tuttavia, la procedura diverge se relativa allo sviluppo di norme europee e o internazionali. Nel caso di norme EN, il recepimento è obbligatorio così come il ritiro di eventuali norme UNI nazionali in contrasto. Tale recepimento avviene mediante la pubblicazione della corrispondente UNI EN entro 6 mesi dall'emanazione della EN ovvero entro eventuali termini differenti stabiliti nella EN stessa. Tale pubblicazione non prevede l'approvazione della CT competente né della CCT.

Nel caso di norme ISO, l'adozione è facoltativa ed è deliberata dall'OT competente, che ne valuta la rispondenza, da un punto di vista tecnico, alle esigenze nazionali e che dispone il ritiro di eventuali norme UNI nazionali in contrasto. Nel valutare l'adozione di una norma ISO l'OT competente verificherà che la norma ISO non sia già stata recepita come EN ISO, l'assenza di una norma EN sullo stesso argomento (*stand-still*), l'assenza di una norma UNI nazionale ritenuta ancora valida, la compatibilità con disposizioni legislative/regolamentari, nazionali o europee. L'adozione di una norma ISO avviene mediante la pubblicazione della corrispondente UNI ISO. Tale pubblicazione prevede l'approvazione della CT competente e, previa IPP, della CCT.

2.6.3. Gli organismi di normazione internazionale

Nel presente paragrafo procederemo, in ordine alla loro fondazione nel tempo, all'analisi dei tre organismi di normazione internazionale, l'*International Telecommunication Union* (ITU), l'*International Electrotechnical Commission* (IEC) e l'*International Organization for Standardization* (ISO), avendo modo di soffermarci brevemente sulla loro storia e sugli aspetti organizzativi e di governance interna alla luce dei documenti ufficiali.

In questa sede, preme tuttavia fare una distinzione fondamentale. Mentre l'ISO e l'IEC sono organizzazioni internazionali a carattere non governativo, l'ITU è invece un'agenzia specializzata delle Nazioni Unite[177], ed è anche il più antico organismo di normazione internazionale[178].

a) L'*International Telecommunication Union* (ITU)

[177] Le agenzie specializzate sono organizzazioni internazionali autonome stabilite attraverso accordi intergovernativi e con ampie responsabilità internazionali, come definite nei loro strumenti fondamentali, nei settori economico, sociale, culturale, educativo, sanitario e correlati, che vengono messe in relazione con l'ONU attraverso accordi conclusi con il Consiglio Economico e Sociale (ECOSOC) di quest'ultima e approvati dall'Assemblea Generale delle Nazioni Unite.

[178] D. WESTPHAL, *International Telecommunication Union (ITU)*, in *Max Planck Encyclopedia of International Law*, 2014, reperibile al link:<https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690- e514 >.

L'*International Telecommunication Union* (ITU) è stata fondata nel 1865 come Unione Internazionale delle Telecomunicazioni per promuovere la cooperazione tra le reti internazionali di telegrafia[179]. Come anticipato ciò la rende una delle più antiche agenzie regolatorie livello globale.

Il 15 novembre 1947 venne siglato un accordo tra l'ITU e la appena creata Organizzazione delle Nazioni Unite che riconobbe l'ITU come "agenzia specializzata" per le telecomunicazioni globali[180]. L'accordo entrò in vigore il 1° gennaio 1949, inerendo ufficialmente l'ITU tra gli organi delle Nazioni Unite. Da questo momento ITU si è trasformata in una piattaforma unica per partenariati pubblico-privato su scala globale e accogliendo al suo interno il settore aziendale ed altre parti interessate[181].

La Convenzione internazionale del telegrafo (successivamente delle telecomunicazioni), oggi la Costituzione e la Convenzione dell'ITU, è il trattato fondamentale che ha stabilito la base legale dell'Unione e ne ha definito lo scopo e la struttura. Questa venne firmata nel 1865, stabilendo i principi fondamentali per la telegrafia internazionale. Successivamente nel 1906 venne sottoscritto un ulteriore Convenzione per il settore della radiotelegrafia[182].

Nel 1932, le due Convenzioni (quella del telegrafo e della radiotelegrafia) furono fuse in un unico documento, denominato Convenzione Internazionale delle Telecomunicazioni, che copriva i tre settori della telegrafia, telefonia e radio. La Convenzione Internazionale delle Telecomunicazioni fu regolarmente rivista fino al 1989, quando la Conferenza dei Plenipotenziari a Nizza decise di istituire una Costituzione e una Convenzione stabili. La Costituzione e la Convenzione del 1989 dell'Unione Internazionale delle Telecomunicazioni non ricevettero mai il numero richiesto di ratifiche e quindi non entrarono mai in vigore.

Una Costituzione e una Convenzione completamente riviste dell'Unione Internazionale delle Telecomunicazioni furono adottate alla Conferenza Plenipotenziaria Addizionale del 1992 tenutasi a Ginevra. Le successive conferenze plenipotenziarie hanno adottato solo strumenti emendativi ai documenti del 1992, tra cui anche le recenti versioni dei due documenti del 2023, adottate nell'ambito della Conferenza Plenipotenziaria 2022 e raccolte nel "*Collection of the basic texts of the International Telecommunication Union adopted by the Plenipotentiary Conference*"[183].

Dall'art. 1 della Costituzione si apprende che tra gli obiettivi dell'Unione vi è quello di «mantenere ed estendere la cooperazione internazionale tra tutti i suoi Stati membri per il miglioramento e l'uso razionale delle telecomunicazioni di ogni tipo; promuovere e potenziare la partecipazione di entità e organizzazioni alle attività dell'Unione e favorire una cooperazione fruttuosa e partenariati tra di esse e gli Stati membri per il raggiungimento degli obiettivi complessivi come definiti negli scopi

[179] L'Ente ha contribuito per oltre 150 anni alla connettività, interoperabilità e standardizzazione delle telecomunicazioni, dall'uso del codice Morse alle comunicazioni via satellite.

[180] H. VOLGER, *A concise encyclopedia of the United Nations*, Leiden, Boston, Martinus, Nijhoff, 2010, p. 458. V. anche ITU, *Overview of ITU's History*, reperibile dal sito ufficiale al link:<https://www.itu.int/en/history/Pages/ITUsHistory.aspx>; C. MALAMUD, *Exploring the Internet: A Technical Travelogue*, New Jersey, PIR Prentice Hall, 1993, p. 384. In tal senso si ponga attenzione alle risoluzioni adottate durante i Plenipotenziari a sostegno delle popolazioni nei processi di pace es. Risoluzione 32, *Technical assistance to the Palestinian Authority for the development of telecommunications* (Kyoto 1994), o Risoluzione 33, *Assistance and support to Bosnia and Herzegovina for rebuilding its telecommunication network* (Marrakesh, 2002).

[181] J. WOUTERS, *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 (a cura di), *The Evolution of Transnational Rule-Makers through Crises*, Cambridge, Cambridge University Press, 2023, pp. 66 ss.

[182] Dalla pagina "*Constitution and Convention Collection*", del sito ITU al link:<https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx>.

[183] ITU, *Collection of the basic texts of the International Telecommunication Union adopted by the Plenipotentiary Conference*, 2023, reperibile dal sito ufficiale nella sezione pubblicazioni della pagina del "Secretariato generale" al link:<https://www.itu.int/pub/S-CONF-PLEN-2022>.

dell'Unione»[184]. Ed in particolare, per quel che qui interessa, riteniamo utile evidenziare anche altri obiettivi richiamati nel disposto tra cui anche l'agevolare la standardizzazione mondiale delle telecomunicazioni, con una qualità di servizio soddisfacente[185]; coordinare gli sforzi per armonizzare lo sviluppo delle infrastrutture di telecomunicazione, in particolare quelle che utilizzano tecniche spaziali, al fine di sfruttare appieno le loro possibilità[186]; promuovere l'adozione di misure per garantire la sicurezza della vita mediante la collaborazione dei servizi di telecomunicazione[187].

L'ITU è composto da Stati membri (193[188]), e Membri settoriali (900[189]). Dal 1994, i Membri settoriali possono partecipare formalmente ai processi decisionali dell'ITU e dal 1998 sono riconosciuti come aventi diritti formali di partecipazione ai sensi della Costituzione dell'ITU. L'Unione è composta da tre settori: Radiocomunicazioni (ITU-R), Standardizzazione delle Telecomunicazioni (ITU-T) e Sviluppo delle Telecomunicazioni (ITU-D). Aziende e organizzazioni possono diventare membri di uno o più settori e aderire a questi come Membri settoriali o Associati.

A livello organizzativo, sono organi istituzionali dell'ITU, la Conferenza dei Plenipotenziari, che è l'organo supremo dell'Unione; il Consiglio, che agisce per conto della Conferenza dei Plenipotenziari; le Conferenze mondiali sulle telecomunicazioni internazionali; il Settore delle Radiocomunicazioni, che comprende conferenze mondiali e regionali sulle radiocomunicazioni, assemblee delle radiocomunicazioni e la Commissione del Regolamento Radio; il Settore della Standardizzazione delle Telecomunicazioni, che include assemblee mondiali sulla standardizzazione delle telecomunicazioni; il Settore dello Sviluppo delle Telecomunicazioni, che comprende conferenze mondiali e regionali sullo sviluppo delle telecomunicazioni; il Segretariato Generale[190].

Le diverse attività dell'Unione prendono avvio nei "Gruppi di Studio" (*Study Gorups*), che vengono rinnovati ogni quattro anni. Ciascun è responsabile di far progredire il lavoro dell'ITU in un campo specifico del mandato affidatogli dall'Unione. I mandati e i team di leadership di ciascun Gruppo di Studio del Settore sono decisi dagli organi direttivi rispettivi del Settore, cioè l'Assemblea di Radiocomunicazione (RA), l'Assemblea mondiale di standardizzazione delle telecomunicazioni (WTSA) e la Conferenza mondiale sullo sviluppo delle telecomunicazioni (WTDC). I Gruppi di Studio sono responsabili dello sviluppo della base tecnica per gli accordi dell'Unione e delle attività correlate. Questo del lavoro richiede la partecipazione di migliaia di esperti rappresentanti governi, industrie e accademie, che svolgono il loro lavoro all'interno di tali Gruppi.

Per quel che qui interessa ci concentreremo sul settore ITU-T che, ai sensi della Costituzione, è responsabile dello studio «di questioni tecniche, operative e tariffarie e adottando raccomandazioni su di esse al fine di standardizzare le telecomunicazioni su scala mondiale»[191]. Questo settore lavora con l'Assemblea mondiale di standardizzazione delle telecomunicazioni (WTSA), i Gruppi di Studio sulla standardizzazione delle telecomunicazioni; il Gruppo Consultivo per la Standardizzazione delle

[184] Art. 1 Constitution of International Telecommunication Union (d'ora in poi Cost. ITU).

[185] Art. 1, par. 2, lett. c) Cost. ITU.

[186] Art. 1, par. 2, lett. e) Cost. ITU.

[187] Art. 1, par. 2, lett. g) Cost. ITU.

[188] L'elenco degli Stati membri è disponibile sul sito ufficiale al link:<https://www .itu.int/online/mm/scripts/gensel8>.

[189] L'elenco dei Sector Members è disponibile sul sito ufficiale al link<https://www.itu.int/hub/membership/ our-members/directory/?myitu-industry= true&request= sector-members>.

[190] Art. 7 Cost. ITU.

[191] Art. 17 Cost. ITU.

Telecomunicazioni; il Bureau per la Standardizzazione delle Telecomunicazioni guidato dal Direttore eletto[192].

Nello specifico, l'ITU-T è costituito da membri di diritto, ossia le amministrazioni di tutti gli Stati membri, e da ogni entità o organizzazione che diventi Membro settoriale[193]. Relativamente alle procedure di voto, la Costituzione prevede che «ogni Stato Membro avrà un voto in tutte le conferenze plenipotenziarie, tutte le conferenze mondiali e tutte le assemblee del Settore e le riunioni dei gruppi di studio e, se è uno Stato Membro del Consiglio, in tutte le sessioni di tale Consiglio»[194], e nel caso di conferenze regionali, solo gli Stati Membri della regione interessata avranno il diritto di voto. Inoltre, gli Stati membri hanno il diritto di partecipare alle conferenze, all'elezione al Consiglio e hanno il diritto di nominare candidati per l'elezione come funzionari dell'Unione o come membri del *Radio Regulations Board*.

Per quanto riguarda i Membri settoriali, questi hanno il diritto di partecipare pienamente alle attività del Settore di cui sono membri, ed «avranno il diritto [...] di prendere parte all'adozione di Questioni e Raccomandazioni e alle decisioni relative ai metodi di lavoro e alle procedure del Settore interessato»[195].

La Convenzione disciplina, inoltre, l'eventuale dissenso in sede di votazione prevedendo innanzitutto che «[i]n linea di massima, ogni delegazione le cui opinioni non siano condivise dalle restanti delegazioni cercherà, per quanto possibile, di conformarsi all'opinione della maggioranza»[196].

Tuttavia, uno Stato membro che, durante una conferenza plenipotenziaria, si riserva il diritto di formulare riserve come specificato nella sua dichiarazione al momento della firma degli atti finali, può formulare riserve riguardanti un emendamento alla Costituzione o alla Convenzione fino a quando il suo strumento di ratifica, accettazione o approvazione dell'emendamento o l'adesione ad esso non sia stato depositato presso il Segretario Generale[197]. Se una decisione appare a una delegazione tale da impedire al suo governo di acconsentire a essere vincolato dalla revisione dei Regolamenti Amministrativi, tale delegazione può formulare riserve, definitive o provvisorie, riguardo a tale decisione, alla fine della conferenza che adotta tale revisione; tali riserve possono essere formulate da una delegazione a nome di uno Stato membro che non partecipa alla conferenza competente e che ha conferito a quella delegazione poteri di rappresentanza per firmare gli atti finali[198]. Una riserva formulata a seguito di una conferenza sarà valida solo se lo Stato membro che l'ha formulata la conferma formalmente al momento di notificare il suo consenso a essere vincolato dall'istrumento emendato o revisionato adottato dalla conferenza al termine della quale è stata formulata la riserva in questione[199].

b) L'*International Electrotechnical Commission* (IEC)

[192] *Ibidem*. Per la disciplina dell'ITU-T in ciascun consesso citato si rinvia alle relative disposizioni della Convenzione, di cui nello specifico artt. 13, 14, 14A, 15.
[193] *Ibidem*.
[194] Art. 3 Cost. ITU.
[195] *Ibidem*.
[196] Art. 32B Convention of International Telecommunication Union (d'ora in poi Conv. ITU).
[197] *Ibidem*.
[198] *Ibidem*.
[199] *Ibidem*.

L'*International Electrotechnical Commission* (IEC) venne fondata nel 1904 nell'ambito del Congresso Elettrico Internazionale di St. Louis, con la raccomandazione che «fossero intraprese misure per ottenere la collaborazione delle società tecniche del mondo mediante la nomina di una Commissione rappresentativa per esaminare la questione della standardizzazione della nomenclatura e delle specifiche degli apparecchi elettrici e delle macchine»[200].

Con tale iniziativa, le personalità che vi presero parte intendevano non solo favorire i commerci, ma anche mantenere le "influenze burocratiche" dei governi alla larga, istituendo così un'organizzazione non governativa[201]. Nello specifico, per riprendere le parole del preambolo dello Statuto, «[...] un'associazione senza scopo di lucro e non governativa con personalità giuridica in conformità agli articoli 60 e seguenti del Codice Civile Svizzero»[202].

Il primo Statuto venne redatto durante la riunione preliminare tenutasi a Londra nel 1906 e fu adottato nel 1908. Ulteriori versioni aggiornate vennero adottate per la prima volta nel 1949 e successivamente. Al momento in cui si scrive, è operativa la versione dello Statuto recentemente entrata in vigore nel 2022[203].

Dal preambolo si apprende che l'obiettivo dell'Ente è quello di promuovere la cooperazione internazionale in materia di standardizzazione e valutazione della conformità agli standard negli specifici settori dell'elettricità, dell'elettronica, delle tecnologie dell'informazione e tecnologie correlate, favorendo così la comprensione internazionale. Tuttavia, l'IEC è aperta anche a collaborazioni, dietro appositi accordi, con le altre due organizzazioni internazionali di normazione l'ISO e l'ITU, competenti in altri settori.

Alla luce del nuovo assetto di *governance*[204], i principali organi dell'Ente sono l'Assemblea generale (*General Assembly*), massimo organo decisionale dell'IEC, composto da rappresentanti delle organizzazioni nazionali membri (*National committee*), e si riunisce in sessioni annuali per discutere e decidere sulle questioni principali, inclusa l'approvazione di nuove norme o loro modifiche, votando a maggioranza semplice[205]; e l'*IEC Board*, organo esecutivo, composto dagli *IEC Officers*, ossia Presidente della Commissione, Vice Presidente, Vice Presidenti, Tesoriere, e Segretario Generale (tutti *ex officio*, senza diritto di voto), e quindici persone, elette dall'Assemblea Generale comprendenti uno da ciascun Membro del Gruppo A, e il resto da Membri non appartenenti al Gruppo A[206], il quale prende decisioni a maggioranza qualificata.

---

[200] R. WINCKLER, *Electrotechnical Standardization in Europe: A tool for the common market*, CENELEC, Brussels, 1994. La citazione è riportata sul sito ufficiale IEC, al link:<https://www.iec.ch/history/how-why-iec-was-started>.

[201] IEC, *Report of preliminary meeting*, Londra, 1906, p. 10, reperibile al link:<https://www.iec.ch/basecamp/ 1906-preliminary-meeting-report> ove risulta che « [...] Delegates and there had been no desire whatever to have bureaucratic influence imported into the Commission».

[202] Art. 1 Preambolo, *Statute and rules of procedures*, IEC (d'ora in poi Statuto IEC), Ginevra, 2021, reperibile al link:<https://www .iec.ch/basecamp/statutes- and-rules-procedure-2021-edition>.

[203] V. IEC, *Statute and rules of procedures*, Ginevra, 2021, reperibile al link:<https://www.iec.ch/basecamp/statutes-and-rules-procedure-2021-edition>.

[204] V. l'infografica illustrativa *IEC New Governance structure*, reperibile al link:<https://www.iec.ch/basecamp/ iec-new-governance-structure>.

[205] Art. 7 Statuto IEC.

[206] Art. 8 Statuto IEC.

Considerate le specifiche competenze, oltre a questi, riteniamo utile far mensione anche degli *Market Strategy Board* (MSB)[207], *Standardization Management Board* (SMB)[208] e del *Conformity Assessment Board* (CAB)[209].

Il modello di governo dell'IEC è basato sulla rappresentanza nazionale. Qualsiasi paese che intenda prendere parte alle attività della Commissione deve costituire o designare un Comitato Nazionale Elettrotecnico per il proprio paese, il quale, al momento dell'ammissione, prenderà il nome di Comitato Nazionale (*National committee*)[210]. Tale Comitato deve essere rappresentativo degli interessi degli *stakeholder* nazionali nei settori di attività dell'IEC, e non deve essere soggetto a influenze indebite da parte di un singolo *stakeholder*. Nello specifico, lo Statuto attribuisce ad ogni membro l'onere di garantire una serie di principi, tra cui quello dell'accesso aperto alla rappresentanza di tutti gli interessi privati e pubblici rilevanti nel suo Paese nei settori di attività della Commissione[211].

In base al livello di attività economica, valutato sulla base di criteri definiti nel Regolamento, un Comitato Nazionale può essere qualificato come Membro a pieno titolo (*Full member*) o come Membro associato (*Associate member*). La differenza è che, mentre un *Full member* ha il diritto di partecipare a tutte le attività tecniche della Commissione, ha diritto a un voto, e può nominare o proporre candidati per l'elezione al Consiglio di Amministrazione IEC, l'*Associate member*, ha il diritto di partecipare alle attività della Commissione ma non ha diritto di voto, tranne che in specifici comitati tecnici/questioni tecniche. Questi inoltre non ha il diritto di nominare o proporre candidati per l'elezione al Consiglio di amministrazione IEC.

c) L'*International Organization for Standardization* (ISO)

È stato già anticipato che la standardizzazione internazionale è iniziata nel settore elettrotecnico con la creazione dell'*International Electrotechnical Commission* (IEC) nel 1906. Successivamente nel 1926, venne istituita l'*International Federation of the National Standardizing Associations* (ISA) per creare standard nel campo dell'ingegneria meccanica. Nel 1930 l'ISA venne sciolta e nel 1946, su iniziativa del Comitato di Coordinamento degli Standard delle Nazioni Unite (UNSCC), sessantacinque delegazioni rappresentanti venticinque Paesi si riunirono alla Conferenza di Londra, ove decisero di creare una nuova organizzazione internazionale, l'ISO per facilitare il coordinamento internazionale e l'unificazione delle norme industriali[212]. La necessità era quella di formulare standard internazionali che potessero sostenere la ripresa economica dopo la Seconda Guerra Mondiale e facilitare la crescita industriale a livello globale.

In quell'occasione vennero anche redatti e adottati i primi Statuti e Regolamenti di procedura una volta ottenuta la ratifica da parte dei 15 organismi nazionali di standardizzazione presenti alla conferenza. Difatti, come è stato osservato, «contrariamente a quanto suggerisce il nome, ISO non è

---

[207] Art. 13 Statuto IEC.

[208] Art. 14 Statuto IEC.

[209] Art. 16 Statuto IEC.

[210] Art. 4 Statuto IEC.

[211] Ibidem.

[212] Come si apprende dal sito ufficiale «[p]oiché l'"*International Organization for Standardization*" avrebbe acronimi diversi nelle diverse lingue (IOS in inglese, OIN in francese per Organisation internationale de normalisation), i nostri fondatori decisero di utilizzare la forma abbreviata ISO. ISO deriva dal greco "*isos*", che significa uguale. Qualunque sia il paese, qualunque sia la lingua, siamo sempre ISO» (link:<https://www.iso.org/about-us.html#four>).

un'organizzazione internazionale tipica, ma piuttosto una rete transnazionale privata di comitati di standardizzazione»[213].

Come si apprende dall'art. 2 del suo Statuto, nella versione aggiornata al 2022[214], l'ISO è impegnata nello sviluppo della standardizzazione e delle attività correlate nel mondo, al fine di agevolare lo scambio internazionale di beni e servizi, migliorare la gestione dei processi aziendali, sostenere la diffusione delle migliori pratiche sociali ed ambientali e promuovere la cooperazione nei settori dell'attività intellettuale, scientifica, tecnologica ed economica. Rispetto alla sua antenata, l'ISA, col tempo la nuova organizzazione ha adottato standard che coprono un ampio spettro di tematiche che non riguardano solo la sfera economica, ma anche quella ambientale[215] e sociale[216]. La normazione ISO è mutata anche nell'oggetto con standard che vanno dalla definizione di termini e concetti, alle dimensioni e interoperabilità fisica dei beni, fino ai requisiti di qualità e sicurezza dei prodotti e servizi, agli standard di gestione, alle pratiche di valutazione della conformità, alla responsabilità sociale e al cambiamento climatico[217].

L'ISO è composta esclusivamente dagli enti di normazione nazionale, uno per ogni Stato che è parte dell'organizzazione. Nello specifico questi si distinguono in "*member bodies*", composti da gli organismi nazionali di standardizzazione più rappresentativi nei rispettivi paesi, dai "*correspondent and subscriber members*", ossia gli organismi nazionali di standardizzazione diversi dai primi e che possono partecipare ma senza diritto di voto[218]. Quindi anche lo sviluppo degli standard ISO si basa su un approccio basato sul consenso e i commenti di tutte le parti interessate sono presi in considerazione[219].

Relativamente alla struttura organizzativa, sono organi dell'ISO, la *General Assembly*, il *Council*, il *Technical Management Board*, le *Technical Committees*, e il *Central Secretariat*[220]. Tra questi, l'organo responsabile della normazione sono le Commissioni tecniche (*Technical Committees*), create, coordinate e supervisionate dal *Technical Management Board* che ha anche il potere di scioglierle.

In particolare, il *Board* sviluppa i termini di riferimento, da sottoporre all'approvazione del Consiglio, i quali verranno poi specificati nelle norme di procedura[221]. Qualsiasi *member body* può appellarsi al Consiglio su una decisione del *Technical Management Board* con una giustificazione appropriata[222]. Il Consiglio detiene infatti il potere di arbitrare gli appelli irrisolti e approvare eventuali revisioni delle procedure di appello proposte dal *Board*.

Come anticipato le *Technical Committees* sono gli organismi responsabili dello sviluppo delle norme tecniche internazionali ed anche di altri provvedimenti dell'ISO[223].

---

213 M. HEIRES, *The International Organization for Standardization (ISO)*, in *New Political Economy*, 2008, pp. 357-367, reperibile al link:<https://doi.org/10.1080/13563460802302693>.

214 V. ISO, *Statutes*, 2022, (d'ora in poi ISO Stat.) reperibile al link:<https://www.iso.org/structure.html>.

215 Il riferimento è alla norma ISO 14001, lo standard di gestione ambientale.

216 V. ad esempio la norma ISO 26000, lo standard per la responsabilità sociale.

217 S. BIJLMAKERS, *The International Organization for Standardization. A Seventy-Five-Year Journey toward Organizational Resilience*, in P. DELIMATSIS, S. BIJLMAKERS, M.K. BOROWICZ (a cura di), *...op.cit.*, pp. 261 ss.

218 Art. 3 ISO Stat.

219 Dal sito ufficiale dell'ISO al link:<https://www.iso.org/developing-standards.html>.

220 Art. 5 ISO Stat.

221 Art. 13 ISO Stat.

222 Art. 13 ISO Stat.

223 Art. 14 ISO Stat.

Uno o più *member bodies*, un Comitato tecnico o un Comitato di Sviluppo delle Politiche istituito dal Consiglio o da un'organizzazione esterna all'ISO, possono fare richiesta di avviare i lavori per lo sviluppo di standard in un determinato campo tecnico[224].

Ogni *member body* interessato a un argomento per il quale un Comitato tecnico è stato autorizzato avrà il diritto di essere rappresentato in quel comitato. I *correspondent and subscriber members* hanno il diritto di partecipare come osservatori. Tuttavia, il Consiglio può decidere di estendere i diritti di partecipazione a tali membri in via eccezionale[225]. Qualsiasi *member body* dell'Organizzazione può appellarsi su qualsiasi decisione di un Comitato tecnico con una giustificazione appropriata al *Board*[226].

2.7 L'evoluzione delle norme (tecniche) armonizzate alla luce del diritto derivato

L'esperienza dell'Unione europea nel settore nella normazione tecnica è di particolare interesse e rilievo ai fini della presente trattazione. In un primo momento l'Unione ha fatto ricorso allo strumento della standardizzazione per facilitare il processo di integrazione del mercato unico, e negli anni successivi è riuscita a coniugare tale azione con la tutela di garanzie sociali come la tutela dell'ambiente e la sicurezza individuale (come quella sul lavoro) e collettiva (es. quella dei prodotti)[227].

Come rilevato dalla dottrina un primo spartiacque può essere individato tra le politiche precedenti al 1973 e quelle successive[228]. Prima di tale data, infatti, l'obiettivo di abbattere le barriere tecniche tra gli Stati membri avveniva attraverso un programma di armonizzazione delle norme tecniche nazionali *ex post*, ossia per mezzo dell'adozione di Direttive tecniche dettagliate che si andavano a sovrapporre alle fonti nazionali. A tal proposito, al fine di raggiungere l'"armonizzazione totale" delle legislazioni nazionali, dal 1969 il Consiglio concluse una serie di accordi (*rectius gentlmen's agreements*)[229] che prevedevano una procedura di informazione in base al quale gli Stati si impegnavano a trasmettere alla Commissione i progetti che prevedevano l'introduzione di regole tecniche[230]. 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[231].

Nel 1973 venne infine introdotta la Direttiva 73/23/CEE concernente il ravvicinamento delle legislazioni degli Stati Membri relative al materiale elettrico destinato ad essere adoperato entro taluni limiti di tensione (meglio nota come Direttiva bassa tensione)[232]. Tale atto ha costituito una tappa fondamentale nell'evoluzione della normazione tecnica europea in quanto ha introdotto il concetto di

---

[224] Art. 14 ISO Stat.

[225] Art. 14 ISO Stat.

[226] Art. 14 ISO Stat.

[227] E. CHITI, *La normalizzazione*, in S. CASSESE (a cura di), *Trattato di diritto amministrativo*, vol. IV, 2003, p. 4027.

[228] F. SALMONI, *Le norme tecniche …op.cit.*, pp. 316 ss.

[229] V. *Accordo dei rappresentanti dei governi degli Stati membri riuniti in sede di Consiglio, del 28 maggio 1969 relativo allo status quo e all'informazione della Commissione* (Gazzetta ufficiale n. C 076 del 17/06/1969 pag. 0009 - 0010) ove viene precisato che tale accordo è da intendersi come "*gentlemen's agreement*" e quindi di un accordo non giuridicamente vincolante.

[230] A. ZEI, *Tecnica e diritto …op.cit.,* p. 279.

[231] P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, Bologna, 1995, p. 52.

[232] Direttiva 73/23/CEE successivamente modificata dalla Direttiva del Consiglio 93/68/CEE. Tale disciplina è stata abrogata dalla Direttiva 2014/35/UE attualmente in vigore.

"norma armonizzata" quale norma stabilita di comune accordo dagli organismi notificati dagli Stati membri e pubblicata secondo le procedure nazionali, e da aggiornare in funzione del progresso tecnologico e dell'evoluzione della "regola dell'arte" in materia di sicurezza[233].

In particolare, la Direttiva disciplinava direttamente gli obiettivi di sicurezza da raggiungere[234], rinviando per le specifiche tecniche alla normazione tecnica (volontaria) degli organismi di normazione. L'apposizione del marchio o il rilascio di attestati da parte dei competenti organismi, avrebbe così garantito una "presunzione di conformità" del materiale elettrico alla norma armonizzata, quindi agli obiettivi di sicurezza dettati dal Consiglio, e avrebbe sollevato il costruttore dall'onere di provare ciò.

Il progetto necessitava tuttavia di ulteriori dettagli circa alcuni aspetti applicativi, soprattutto la definizione dei requisiti essenziali, rimessi alla disciplina del legislatore europeo mediante le direttive, e le specifiche tecniche, formulate degli organismi di normazione. Sul punto è intervenuta la Direttiva 83/189/CEE del Consiglio del 28 marzo 1983 con il quale è stata novata la procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche al fine di evitare sovrapposizioni di norme tecniche, prevedendo così la formazione di ostacoli tecnici, ma soprattutto è l'atto con il quale si sono introdotte per la prima volta le definizioni di «specificazione tecnica», quale specificazione che figura in un documento e che definisce le caratteristiche richieste di un prodotto, quali i livelli di qualità o di proprietà di utilizzazione, la sicurezza, le dimensioni, comprese le prescrizioni applicabili ad un prodotto per quanto riguarda la terminologia, i simboli, le prove ed i metodi di prova, l'imballagio , la marchiatura e l'etichettatura[235]; «norma», quale specificazione tecnica approvata da un organismo riconosciuto a attività normativa per applicazione ripetuta o continua, la cui osservanza non è obbligatoria[236], e infine «regola tecnica», ossia specificazioni tecniche, comprese le disposizioni che ad esse si applicano, la cui osservanza è obbligatoria *de jure* o *de facto*, per la commercializzazione o l'utilizzazione in uno Stato membro o in una parte importante di esso, ad eccezione di quelle fissate dalle autorità locali[237].

La Direttiva ha inoltre istituzionalizzato gli organismi di normazione nazionali all'Elenco I dell'Allegato, ed ha indicato, nell'Elenco II, il CEN e il CENELEC come organismi di normalizzazione europei (anche noti come *European Standardisation Organisations* - ESOs).

Nonostante gli interventi normativi, il processo di integrazione del mercato unico si è tuttavia evoluto anche sulla scorta delle pronunce della Corte di giustizia, e dei Tribunali nazionali che, soprattutto tra gli anni '70 del secolo scorso e la metà degli anni '80, hanno contribuito ad abbattere gli ostacoli tecnici ed attenuare le politiche restrittive degli Stati membri.

Tra tutte merita menzione la sentenza *Cassis de Djon*[238], con il quale è stato introdotto il principio di mutuo riconoscimento, secondo cui «[o]gni prodotto importato da uno Stato membro dev'essere, in linea di massima, ammesso sul territorio del paese importatore se legalmente fabbricato, vale a dire se è conforme alla normativa od ai procedimenti di fabbricazione legittimi e tradizionali del paese

---

233 Cfr. art. 5 Direttiva 73/23/CEE.

234 Cfr. art. 1 Direttiva 73/23/CEE, ove è specificato che «[p]er materiale elettrico, ai sensi della presente direttiva, si intende ogni materiale elettrico destinato ad essere adoperato ad una tensione nominale compresa fra 50 e 1000 V in corrente alternata e fra 75 e 1500 V in corrente continua, fatta eccezione dei materiali e dei fenomeni di cui all'allegato II».

235 Art. 1, n. 1 Direttiva 73/23/CEE.

236 Art. 1, n. 2 Direttiva 73/23/CEE.

237 Art. 1, n. 5 Direttiva 73/23/CEE.

238 Sentenza della Corte del 20 febbraio 1979, Causa 120/78.

d'esportazione, e commercializzato sul territorio di quest'ultimo»[239]. Tuttavia, nella stessa sentenza, si ammetteva un temperamento nel caso in cui misure restrittive ad effetto equivalente da parte degli Stati membri siano necessarie per rispondere ad esigenze imperative attinenti, in particolare, all'efficacia dei controlli fiscali, alla protezione della salute pubblica, alla lealtà dei negozi commerciali e alla difesa dei consumatori[240].

Tuttavia, successivamente, nella causa *Gaetano Cremonini c. Maria Luise Vrankovich*, la Corte è andata a precisare che

> la direttiva 73/23, considerate le diverse concezioni della sicurezza cui si ispirano le disposizioni in vigore negli Stati membri, ha lo scopo di consentire la libera circolazione del materiale elettrico, fatto salvo però il rispetto di determinati requisiti di sicurezza stabiliti dalla direttiva. Questa, adottata in base all'art. 100 del Trattato, mira al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri per la parte in cui dette disposizioni possano opporre ostacoli tecnici agli scambi di tale materiale. Una direttiva del genere verrebbe privata del suo contenuto se le autorità nazionali competenti, nell'esercizio clei poteri loro riservati quanto alla forma ed ai mezzi per l'attuazione della direttiva, non rimanessero nei limiti di valutazione indicati da tale testo, poiché ogni superamento di quei limiti potrebbe far sorgere nuove disparità e quindi nuovi ostacoli agli scambi ed impedire conseguentemente la libera circolazione delle merci in un settore in cui il legislatore comunitario aveva preso disposizioni per assicurarla[241].

Altra tappa fondamentale è rappresentata dal "Nuovo approccio" in materia di armonizzazione tecnica e normazione[242] inaugurato nel 1985, quale strategia diretta a contribuire alla libera circolazione dei prodotti industriali e alla creazione di un contesto tecnico comune a tutte le imprese attraverso quattro principi, definiti nell'Allegato II, volti a imporre il metodo di formazione delle norme armonizzate già introdotto con la Direttiva bassa tensione, ad affidare la formazione delle specifiche tecniche agli organi di normalizzazione europei (CEN e CENELEC), specifiche che non hanno natura obbligatoria ma restano volontarie e, infine, il riconoscimento da parte degli Stati membri ai prodotti fabbricati secondo le norme armonizzate (o, a titolo provvisorio, le norme nazionali) la presunta conformità ai «requisiti essenziali» fissati dalla Direttiva, o nel caso in cui il produttore intenda fabbricare prodotti non conformi a tali norme, in che tal caso dovrà provare che i suoi prodotti rispondono ai requisiti essenziali fissati dalla Direttiva.

Secondo Alcuni, tale disciplina ha tratto ispirazione dal modello regolativo tedesco per la disciplina della tecnologia applicabile agli impianti e alla produzione industriale[243] sotto due aspetti, da una parte la tecnica normativa, consistente nell'enunciazione dei requisiti essenziali di sicurezza attraverso clausole e formulazioni di carattere generale e non determinato e sulla presunzione di conformità rispetto a norme tecniche volontarie; dall'altra, lo strumento giuridico prescelto per formalizzare il rapporto tra le istituzioni pubbliche e gli Enti di normalizzazione[244]..

---

[239] GUCE, n. C. 256/2, 3 ottobre 1980, Comunicazione della Commissione sulle conseguenze della sentenza emessa dalla Corte di giustizia delle Comunità europee il 20 febbraio 1979 nella causa 120/78 («Cassis de Dijon»), reperibile al link:<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:31980Y1003(01)&from=IT>.

[240] Sentenza della Corte del 20 febbraio 1979, Causa 120/78.

[241] Sentenza della Corte del 2 dicembre 1980, Causa 815/79, pt. 6 in diritto.

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

[243] A. ZEI, *Tecnica e diritto ...op.cit.,* pp. 290 ss. nonché A. PREDIERI, *Le norme tecniche nello stato pluralista e prefederativo* …op.cit., p. 283. Secondo Altri, già nella disciplina italiana, ed in particolare nella Legge 1° marzo 1968, n. 186, sulla regolazione dei prodotti elettrici, vi erano criteri informati al "Nuovo approccio" sul punto v. G. VESPERINI, *Il controllo della "sicurezza" e della "qualità" dei prodotti industriali: due modelli a confronto*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *op.cit.*, p. 126.

[244] *Ivi*, p. 291.

2.7.1 *Segue*. Il Regolamento (UE) 1025/2012 sulla normazione europea

Il 25 ottobre 2012 l'Unione ha adottato il Regolamento 1025/2012 sulla normazione europea[245]. Prima di tale data la normazione europea era disciplinata da un quadro normativo composto da tre atti legislativi diversi. La Direttiva 98/34/CE, che prevedeva una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, la Decisione n. 1673/2006/CE, relativa al finanziamento della normalizzazione europea e la Decisione 87/95/CEE, relativa alla normalizzazione nel settore delle tecnologie dell'informazione e delle telecomunicazioni. Alle soglie del 2010 tale complesso normativo si dimostrò non più al passo con gli sviluppi occorsi negli ultimi decenni, data l'avvertita esigenza di un'opera di semplificazione e adeguamento dello stesso.

In una risoluzione del Parlamento europeo del 21 ottobre 2010 sul futuro della normazione europea[246], e nella relazione del febbraio 2010 del Gruppo di esperti per la revisione del sistema europeo di normazione dal titolo «Normazione per un'Europa competitiva e innovativa: una visione per il 2020», furono infatti stabilite una serie di raccomandazioni strategiche volte a revisionare il sistema europeo di normazione.

Escluso il sistema di scambio informativo tra gli organismi nazionali di normazione, le organizzazioni europee di normazione e la Commissione in merito alle loro attività attuali e future di normazione, compreso il principio del mantenimento dello *status quo* applicabile agli organismi nazionali di normazione nel quadro delle organizzazioni europee di normazione, che prevede il ritiro delle norme nazionali dopo la pubblicazione di una nuova norma europea, i quali sono stati ritenuti necessari da mantenere, il Regolamento del 2012 ha sintetizzato le esigenze avvertite nel decennio precedente introducendo incisive e radicali innovazioni rispetto al previgente quadro regolatorio.

Tra questi troviamo innanzitutto l'estensione della disciplina sulla normazione europea non più solo ai prodotti[247] ma, per la prima volta, anche ai servizi, definiti come «qualsiasi attività economica non salariata, quale definita all'articolo 57 TFUE, fornita normalmente dietro retribuzione»[248]. Ciò è stato ritenuto necessario a fronte del fatto che «[n]ella prassi non è sempre possibile distinguere chiaramente le norme per i prodotti dalle norme per i servizi». Difatti molte norme per i prodotti hanno una componente servizi, mentre le norme per i servizi spesso riguardano in parte anche i

---

[245] 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.

[246] Risoluzione del Parlamento europeo del 21 ottobre 2010 sul futuro della normazione europea, 2012/C 70 E/05.

[247] Definiti all'art. 2, n. 6 Reg. (UE) 1025/2012 come «i prodotti di fabbricazione industriale e i prodotti agricoli, compresi i prodotti della pesca».

[248] Definiti all'art. 2, n. 7 Reg. (UE) 1025/2012. L'art. 57 TFUE recita «Ai sensi dei trattati, sono considerate come servizi le prestazioni fornite normalmente dietro retribuzione, in quanto non siano regolate dalle disposizioni relative alla libera circolazione delle merci, dei capitali e delle persone. I servizi comprendono in particolare: a) attività di carattere industriale; b) attività di carattere commerciale; c) attività artigiane; d) attività delle libere professioni. Senza pregiudizio delle disposizioni del capo relativo al diritto di stabilimento, il prestatore può, per l'esecuzione della sua prestazione, esercitare, a titolo temporaneo, la sua attività nello Stato membro ove la prestazione è fornita, alle stesse condizioni imposte da tale Stato ai propri cittadini». L'articolo definisce quindi il servizio sia in chiave positiva, ossia la prestazione normalmente fornita dietro retribuzione, con una elencazione meramente semplificativa, delle attività ricomprese, sia in chiave negativa, ove sancisce la residualità della disciplina rispetto alle altre libertà di circolazione contemplate dal TFUE (v. D. DIVERIO, *Art. 57 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, Cedam, 2014, pp. 428 ss.).

prodotti. Di conseguenza è stato ritenuto necessario adeguare il quadro giuridico a tali nuove circostanze ampliandone l'ambito di applicazione anche alle norme per i servizi[249].

L'indeterminatezza terminologica e gli sviluppi della disciplina sulla normazione hanno indotto il legislatore europeo a tornare ancora una volta sulle definizioni utili della materia andando a fornire maggiori dettagli e soprattutto distinguere alcuni concetti tra cui quelli di «specifica tecnica», «norma» e «prodotto della normazione europea».

Per «specifica tecnica» il Regolamento fa riferimento a un documento che prescrive i requisiti tecnici che un determinato prodotto, processo, servizio o sistema deve soddisfare[250]. Mentre per «norma» si intende una specifica tecnica, adottata da un organismo di normazione riconosciuto, per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi, distinta dalla nozione di «prodotto della normazione europea» con il quale si fa riferimento a qualsiasi altra specifica tecnica, diversa dalle norme europee, adottata da un'organizzazione europea di normazione per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi.

Nello specifico, nel concetto di norma il legislatore europeo ha ricondotto le categorie di «norma internazionale», ossia la norma adottata da un organismo di normazione internazionale, «norma nazionale», se adottata da un organismo di normazione nazionale ed ha poi distinto la norma europea dalla norma armonizzata, difatti:

> [...] b) «norma europea»: una norma adottata da un'organizzazione europea di normazione; c) «norma armonizzata»: una norma europea adottata sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione [...][251].

Particolare attenzione è stata inoltre posta dal legislatore europeo del 2012 su altri aspetti di rilievo che riteniamo poter individuare nei principi generali della normazione e nel processo di formazione delle norme armonizzate, tra cui rientra anche la disciplina del diritto di obiezione (a); nei profili della partecipazione delle rappresentanze nel processo di normazione (b); nel particolare caso della individuazione delle specifiche tecniche delle ICT nelle procedure di appalto (c); ed infine, nella disciplina dell'attività della Commissione e dei comitati nella normazione europea (d).

a) I principi generali della normazione e il processo di formazione delle norme armonizzate

Relativamente ai primi aspetti evidenziati, dobbiamo innanzitutto distinguere il processo di formazione delle norme europee da quello di formazione delle norme armonizzate. La normazione

---

[249] Cfr. cons. 10 Reg. (UE) 1025/2012.

[250] Art. 2, n. 4 Reg. (UE) 1025/2012, di cui nello specifico tale documento può stabilire uno o più degli elementi indicati nello stesso, ossia «a) le caratteristiche richieste di un prodotto, compresi i livelli di qualità, le prestazioni, l'interoperabilità, la protezione dell'ambiente, la salute, la sicurezza o le dimensioni, comprese le prescrizioni applicabili al prodotto per quanto riguarda la denominazione di vendita, la terminologia, i simboli, le prove e i metodi di prova, l'imballaggio, la marcatura e l'etichettatura, nonché le procedure di valutazione della conformità; b) i metodi e i processi di produzione relativi ai prodotti agricoli quali definiti all'articolo 38, paragrafo 1, TFUE, ai prodotti destinati all'alimentazione umana e animale, nonché ai medicinali, così come i metodi e i processi di produzione relativi agli altri prodotti, quando abbiano un'incidenza sulle caratteristiche di questi ultimi; c) le caratteristiche richieste di un servizio, compresi i livelli di qualità, le prestazioni, l'interoperabilità, la protezione dell'ambiente, la salute o la sicurezza, comprese le prescrizioni applicabili al fornitore per quanto riguarda le informazioni da fornire al ricevente, secondo quanto specificato dall'articolo 22, paragrafi da 1 a 3, della direttiva 2006/123/CE; d) i metodi e i criteri di valutazione della prestazione dei prodotti da costruzione, secondo la definizione dell'articolo 2, punto 1, del regolamento (UE) n. 305/2011 del Parlamento europeo e del Consiglio, del 9 marzo 2011, che fissa condizioni armonizzate per la commercializzazione dei prodotti da costruzione (37), in relazione alle loro caratteristiche essenziali».

[251] Art. 2, n 1, lett. b) e c) Reg. (UE) 1025/2012.

europea è infatti affidata agli organismi di normazione europei, ossia il CEN, il CENELEC ed ETSI, quali enti di natura privata e distinti dalle istituzioni europee, che producono norme tecniche conformemente alla propria disciplina interna (sul punto si rinvia *infra* 2.10).

Il considerando 2 del Regolamento si limita infatti a ricordare che «[l]a normazione europea è organizzata da e per i soggetti interessati sulla base della rappresentanza nazionale [enfasi aggiunta]», e che questa «si fonda sui 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 («principi fondatori»)». Pertanto, il legislatore europeo ha inteso ribadire che la normazione tecnica in generale è un'attività normativa diversa da quella giuridica, da cui non deriva la produzione di effetti giuridicamente vincolanti, essendo volontaria, e che non ha una vocazione *erga omnes* («da e per i soggetti interessati»). Tuttavia, allo stesso tempo, egli è consapevole che le norme possono avere un impatto sulla società, «in particolare sulla sicurezza e sul benessere dei cittadini, sull'efficienza delle reti, sull'ambiente, sulla sicurezza dei lavoratori e le condizioni di lavoro, sull'accessibilità e su altri settori di importanza pubblica [...]»[252], tema che sarà analizzato più avanti.

Sul punto evidenziamo che il considerando 9 precisa che, tenuto conto della ripartizione delle competenze tra l'Unione e gli Stati membri, «rimane di competenza esclusiva degli Stati membri stabilire i principi fondamentali in materia di sicurezza sociale, formazione professionale e sistemi sanitari nonché definire le condizioni quadro per la gestione, il finanziamento, l'organizzazione e la consegna dei servizi forniti nel quadro di tali sistemi, inclusa [...] la definizione dei requisiti e delle norme di qualità e sicurezza a essi applicabili [enfasi aggiunta]».

Per quanto riguarda le norme armonizzate, l'art. 10 del Regolamento si concentra sulle richieste di normazione alle organizzazioni europee, azione propositiva rimessa all'iniziativa della Commissione europea che può chiedere, entro i limiti delle competenze stabiliti nei Trattati, a una o più ESOs di elaborare una norma europea o un prodotto della normazione europea entro un determinato termine. Ed in particolare il disposto prevede che la Commissione «stabilisce i requisiti relativi al contenuto che il documento deve rispettare [...]».

Entro un mese dalla richiesta, l'organismo di normazione deve comunicare se accetta la proposta di normazione avanzata dalla Commissione[253].

In caso di esito positivo, l'organismo si impegna a formulare la norma o il prodotto della normazione europea conformemente ai requisiti di contenuto indicati da questa, nonché anche ai principi e disposti del Regolamento 1025/2012.

L'attività normativa dell'ente è pertanto vincolata al rispetto di queste prescrizioni che rappresentano anche il parametro di valutazione della Commissione per la successiva attività di controllo. In questa sede la Commissione valuta, infatti, insieme alle organizzazioni europee di normazione, la conformità dei documenti elaborati dall'organismo europeo a ciò delegato con la sua richiesta iniziale.

Se quanto prodotto soddisfa le prescrizioni fornite ed è conforme alla disciplina del Regolamento, la Commissione pubblica «senza indugio» il riferimento di tale norma sulla Gazzetta ufficiale dell'Unione europea.

---

[252] Cfr. cons. 22 Reg. (UE) 1025/2012.

[253] L'Organismo europeo può anche rifiutare la richiesta. Come si apprende dalla Relazione relativa all'attuazione del Regolamento (UE) n. 1025/2012 dal 2016 al 2020, COM(2022) 30 final, nel periodo 2015-2019 la Commissione ha presentato 35 richieste di normazione e altre nove nel 2020, per un totale di 44 richieste, di cui sei sono state rifiutate (13,6 %).

Ulteriore tratto innovativo della disciplina può essere colto nell'armonizzazione del diritto di obiezione formale alle norme armonizzate, dato che i diversi atti che componeva la previgente disciplina prevedevano procedure discordanti, e nell'estensione di tale diritto anche al Parlamento europeo[254]. L'art. 11 prevede infatti che, qualora uno Stato membro o il Parlamento europeo ritenga che una norma armonizzata non soddisfi le prescrizioni cui questa intende riferirsi, e che sono stabilite dalla pertinente legislazione dell'Unione in materia di armonizzazione, ne informa la Commissione fornendo una spiegazione dettagliata. La Commissione, previa consultazione del comitato in materia di armonizzazione (laddove esista), o previe altre forme di consultazione di esperti del settore, può decidere, se ancora non è avvenuto, di pubblicare, non pubblicare o di pubblicare con limitazioni i riferimenti alla norma armonizzata in questione sulla Gazzetta ufficiale dell'Unione. Ovvero, nel caso in questa sia stata pubblicata, di mantenere, mantenere con limitazioni o di ritirare i riferimenti alla norma armonizzata in questione in Gazzetta.

Pertanto, l'ultima parola resta pur sempre alla Commissione che, tenuto conto dell'obiezione, può anche non farne seguito.

b) La partecipazione delle rappresentanze sociali al processo di normazione

Come anticipato, il legislatore europeo è consapevole dell'impatto della normazione tecnica oltre gli "interessati" per il quale questa è stata organizzata, ossia per la società in generale[255], e pertanto promuove il potenziamento delle organizzazioni socialmente rappresentative. In particolare, il considerando 17 precisa che per rappresentanza di interessi della società e parti della società interessate alle attività di normazione europee si devono intendere le attività delle organizzazioni e delle parti che rappresentano «interessi di grande rilevanza sociale», quali interessi ambientali, dei consumatori o dei lavoratori dipendenti. Particolare riferimento è fatto poi alle attività delle organizzazioni e delle parti che rappresentano i diritti fondamentali dei dipendenti e dei lavoratori, ad esempio i sindacati[256].

Nello specifico gli interessi dei consumatori, dei lavoratori e dell'ambiente trovano concreta rappresentazione in tali sedi (ossia nei processi decisionali delle ESOs), rispettivamente per mezzo

[254] Cfr. cons. 29 Reg. (UE) 1025/2012.
[255] Cfr. cons. 22 Reg. (UE) 1025/2012.
[256] Cfr. cons. 17 Reg. (UE) 1025/2012.

delle associazioni europee ANEC[257], ETUC[258] ed ECOS[259], nonché gli interessi delle piccole imprese alla standardizzazione per mezzo dell'SBS[260] (quali associazioni finanziate dalla Commissione, come identificate all'Allegato III al Regolamento, proprio al fine di garantire il coinvolgimento di tali interessi nel processo di normazione europeo).

A tal proposito, l'art. 12 impone che la Commissione istituisca un «sistema di comunicazione per tutti i soggetti interessati», incluse le organizzazioni europee di normazione e le organizzazioni europee dei soggetti interessati che ricevono il finanziamento dell'Unione, affinché venga garantita un'idonea consultazione e l'adeguatezza al mercato prima di adottare il programma di lavoro annuale dell'Unione per la normazione europea; di approvare le richieste di normazione di cui all'articolo 10; di adottare una decisione in merito alle obiezioni formali a norme armonizzate; di adottare una decisione in merito all'identificazione delle specifiche tecniche delle ICT; e di adottare atti delegati[261].

Il legislatore favorisce pertanto la partecipazione delle rappresentanze, anche sociali, in diversi passaggi e attività chiave del processo di normazione europeo, incidendo indirettamente sugli Statuto degli enti di normazione europea che saranno obbligati a prevedere tali forme di partecipazione. Tuttavia, al considerando 23, è precisato che l'obbligo per le organizzazioni di normazione europee di incoraggiare e facilitare la rappresentanza e l'effettiva partecipazione di tutti i soggetti interessati

---

[257] Come si apprende dal sito ufficiale, ANEC è un'associazione internazionale senza scopo di lucro costituita in base alla legge belga, con un segretariato centrale a Bruxelles, in Belgio. L'Associazione è riconosciuta dalla Commissione Europea e dal Segretariato dell'EFTA, ed è membro effettivo del Gruppo Consultivo sulla Politica dei Consumatori della Commissione (CPAG) e osservatori nel Comitato sulle Norme (CoS). È anche membro di diversi comitati consultivi dell'Unione e di numerosi gruppi di esperti, tra cui il Forum di Alto Livello sulla Standardizzazione della Commissione (HLFS). ANEC ha sottoscritto il Registro europeo della trasparenza (n. 507800799-30) e si attiene al suo Codice di condotta. La rappresentanza dei consumatori nella standardizzazione europea è un'attività di interesse pubblico, e l'Associazione viene nominata solo dopo regolari inviti pubblici. È un'attività dipendente dai finanziamenti pubblici europei, in quanto è finanziata dall'Unione Europea (95%) e dall'EFTA (5%) come "Organizzazione dell'Allegato III" ai sensi del Regolamento (UE) 1025/2012. Per ulteriori si rinvia al link:<https://www.anec.eu/>.

[258] L'ETUC, la Confederazione Sindacale Europea, è la voce dei lavoratori europei nella standardizzazione. Con 45 milioni di membri appartenenti a 90 organizzazioni sindacali in 38 paesi europei, oltre a 10 Federazioni Sindacali Europee, l'ETUC promuove condizioni di lavoro di alta qualità nel processo di standardizzazione. L'ETUC ha lanciato il progetto ETUC STAND per rafforzare la voce dei lavoratori nella standardizzazione al fine di garantire che gli standard promuovano condizioni di lavoro di alta qualità. L'obiettivo è assicurare che l'UE non sia solo un mercato unico per beni e servizi, ma anche un'Europa Sociale, dove migliorare il benessere dei lavoratori e delle loro famiglie è una priorità altrettanto importante. Difendiamo valori sociali fondamentali come solidarietà, uguaglianza, democrazia, giustizia sociale e coesione. L'ETUC lavora su diverse aree di rilevanza per i lavoratori, tra cui il progresso industriale e gli standard dei servizi (ad esempio, manutenzione e facility management, servizi orizzontali, assistenza sanitaria). Il loro lavoro sugli standard è finanziato congiuntamente dalla Commissione Europea e dagli Stati membri dell'EFTA. Per ulteriori vedi il link:<https://www.etuc.org/en/organisation-and- people>.

[259] Fondata nel 2001, ECOS è l'unica organizzazione a livello mondiale che difende gli interessi ambientali nel processo di sviluppo degli standard a livello europeo e internazionale. La sua missione è influenzare lo sviluppo di strategie ambiziose per ridurre e controllare le fonti di inquinamento ambientale, e promuovere l'efficienza delle risorse e dell'energia, la salute ambientale e lo sviluppo sostenibile. ECOS è coinvolta in oltre 60 comitati tecnici in Europa e oltre e partecipa, principalmente attraverso esperti, ai lavori di sviluppo degli standard. Ai rinvia al link per ulteriori:<https://ecostandard.org/realifestandards/>.

[260] *Small Business Standards* (SBS) è un'associazione europea senza scopo di lucro finanziata congiuntamente dalla Commissione Europea e dagli Stati membri dell'EFTA. Il suo obiettivo è rappresentare e difendere gli interessi delle piccole e medie imprese (PMI) nel processo di standardizzazione a livello europeo e internazionale. Inoltre, mira a sensibilizzare le PMI sui benefici degli standard e a incoraggiarle a partecipare al processo di standardizzazione. SBS è stata fondata per rispondere all'aspirazione dell'Unione Europea di rendere il sistema di standardizzazione il più inclusivo, trasparente e aperto possibile, in linea con il Regolamento 1025/2012 sul Sistema Europeo di Normazione. Per ulteriori vedi il link:<http://www.sbs-sme.eu/>.

[261] Cfr. art. 12 Reg. (UE) 1025/2012.

«non comporta alcun diritto di voto per tali soggetti interessati, a meno che tale diritto di voto non sia previsto dal regolamento interno delle organizzazioni di normazione europee»[262].

Dalla mera partecipazione deve infatti essere distinto l'esercizio di voto che permette di dar "voce" a tali gruppi rappresentativi. Ma, come appena evidenziato, il legislatore ha preferito non imporre tale opzione agli enti di normazione europea, rispettando la loro capacità di autoregolamentarsi e lasciando quindi alla loro libera iniziativa la possibilità di conferire tale diritto alle rappresentanze civili.

Sul punto sono state sollevate critiche in dottrina, le quali, ancor prima del diritto di voto, si sono concentrante sul profilo della partecipazione. Sebbene le norme tecniche abbiano la capacità di produrre effetti sulla società diffusa, il sistema di partecipazione alle procedure di normazione, autoregolato dagli organismi di normazione, resta imperniato sul principio dell'interesse diretto concreto. Come è stato osservato, si tratta di un sistema a democraticità limitata dato che i soggetti che vi partecipano hanno un interesse concreto all'approvazione di quella determinata normativa tecnica, non già alla generalità dei consociati che, se non rappresentanti nelle sedi di formazione di tali norme tecniche, rimangono ad essi assoggettati pur non avendo concorso alla loro formazione[263].

Stesso principio opera in realtà anche per la partecipazione delle parti sociali, dato che il Regolamento le qualifica «interessate alle attività di normazione europee»[264]. D'altronde tentare di replicare la medesima rappresentanza dell'intera società dei Parlamenti in sede legislativa nei sistemi di normazione sarebbe impraticabile a livello fattuale, data la rilevanza globale di tali strumenti. La partecipazione di organizzazioni di rappresentanza sociale sembra pertanto la scelta più ovvia.

Alla luce di quanto fin qui analizzato riteniamo quindi che il difetto di democraticità che caratterizza la normazione tecnica può essere compensato solo dall'attività di promozione dell'Unione volta a rafforzare le organizzazioni rappresentative (il considerando 22 fa riferimento esplicito a quelle di consumatori, ambientali e sociali)[265], e al citato «sistema di comunicazione per tutti i soggetti interessati» il quale dovrebbe tenere in considerazione il maggior numero di organizzazioni rappresentative e soprattutto avere la capacità di prevedere su quali categorie di soggetti determinate norme tecniche possano produrre effetti sia direttamente, ma anche indirettamente[266].

Nell'Allegato III al Regolamento, il legislatore europeo ha fornito una elencazione di principi e criteri per l'identificazione delle «organizzazioni europee di soggetti interessati ammissibili al finanziamento dell'Unione» ove sono contemplate le organizzazioni europee che rappresentano le

[262] Cfr. cons. 23 Reg. (UE) 1025/2012.
[263] Cfr. F. SALMONI, *Le norme tecniche …op.cit*. p. 244.
[264] Cfr. art. 17 Reg. (UE) 1025/2012.
[265] Cfr. cons. 17 Reg. (UE) 1025/2012.
[266] Cfr. A. IANNUZZI, *Il diritto capovolto …op.cit.,* pp. 56 ss.

PMI[267], i consumatori[268], gli interessi ambientali[269] e quelle che rappresentano gli interessi sociali[270] nelle attività di normazione europea.

Tuttavia, parte della dottrina ritiene che nonostante ciò, tale «rappresentazione» dei singoli, privati, interessi dei gruppi che concorrono alla formazione delle norme tecniche (europee), difficilmente possa garantire parità tra le rappresentanze del mondo della produzione e dell'industria con quelle sociali dei consumatori o degli utenti in generale, trattandosi piuttosto di un rapporto di mediazione e mai di sacrificio a scapito degli interessi della produttività e redditività dei primi[271].

c) L'individuazione delle specifiche tecniche delle ICT nelle procedure di appalto

Con il Regolamento del 2012 il legislatore si è occupato delle specifiche tecniche che intervengono nelle procedure di approvvigionamento di *hardware*, *software* e servizi di tecnologia dell'informazione (d'ora in poi beni ICT) da parte delle pubbliche amministrazioni per mezzo delle procedure d'appalto.

Tali documenti aprono a due ordini di problemi: il primo è che spesso tali specifiche non rientrano in nessuna delle categorie di norme e omologazioni previste dalle discipline di appalto per la produzione o fornitura di servizi a livello europeo[272]; l'altro, è che spesso non sono neppure elaborate conformemente ai principi fondatori della normazione europea[273].

Il legislatore europeo del 2012 è così intervenuto sul punto stabilendo prescrizioni (disposte nell'Allegato II al Regolamento) relative all'identificazione delle specifiche tecniche dei beni ICT da utilizzare negli appalti, e stabilendo prescrizioni sotto forma di un elenco di criteri per dette specifiche tecniche e per i relativi processi di elaborazione, che garantiscano il rispetto degli obiettivi di interesse pubblico e le esigenze della società e basati sui principi fondatori[274].

---

[267] Un'organizzazione europea che rappresenta le PMI nelle attività di normazione europea che: a) è non governativa e senza scopo di lucro, b) ha quali suoi obiettivi e attività statutari rappresentare gli interessi delle PMI nel processo di normazione a livello europeo, nel sensibilizzare le PMI sulla normazione e nell'incoraggiarle a partecipare al processo di normazione; c) ha ricevuto un mandato dalle organizzazioni senza scopo di lucro che rappresentano le PMI in almeno due terzi degli Stati membri per rappresentare gli interessi delle PMI nel processo di normazione a livello europeo.

[268] Un'organizzazione europea che rappresenta i consumatori nelle attività di normazione europea che: a) è non governativa, senza scopo di lucro, esente da conflitti d'interesse di origine industriale, commerciale e professionale o da altri conflitti d'interesse; b) ha quali suoi obiettivi e attività statutari rappresentare gli interessi dei consumatori nel processo di normazione a livello europeo; c) ha ricevuto un mandato dalle organizzazioni nazionali senza scopo di lucro che rappresentano i consumatori in almeno due terzi degli Stati membri per rappresentare gli interessi dei consumatori nel processo di normazione a livello europeo.

[269] Si definisce organizzazione europea di soggetti interessati un'organizzazione europea che rappresenta gli interessi ambientali nelle attività di normazione europea e che: a) è non governativa, senza scopo di lucro, esente da conflitti d'interesse di origine industriale, commerciale e professionale o da altri conflitti d'interesse; b) ha quali suoi obiettivi e attività statutari rappresentare gli interessi ambientali nel processo di normazione a livello europeo; c) ha ricevuto un mandato dalle organizzazioni nazionali per l'ambiente senza scopo di lucro in almeno due terzi degli Stati membri per rappresentare gli interessi ambientali nel processo di normazione a livello europeo.

[270] Un'organizzazione europea che rappresenta gli interessi sociali nelle attività di normazione europea che: a) è non governativa, senza scopo di lucro, esente da conflitti d'interesse di origine industriale, commerciale e professionale o da altri conflitti d'interesse; b) ha quali suoi obiettivi e attività statutari rappresentare gli interessi sociali nel processo di normazione a livello europeo; c) ha ricevuto un mandato dalle organizzazioni nazionali senza scopo di lucro in ambito sociale in almeno due terzi degli Stati membri per rappresentare gli interessi sociali nel processo di normazione a livello europeo.

[271] F. SALMONI, *Le norme tecniche* …op.cit. p. 245.

[272] Cfr. cons. 30 Reg. (UE) 1025/2012.

[273] Cons. 31 Reg. (UE) 1025/2012.

[274] *Ibidem.*

Difatti, come era già stato osservato nel libro bianco sull'"Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE" del 2009[275], il contesto della normalizzazione delle ICT è radicalmente cambiato ed ha visto la sempre maggiore attività di forum e consorzi specializzati perlopiù globali, rispetto alle tradizionali organizzazioni preposte all'emanazione di norme, molti dei quali hanno assunto un ruolo di leader tra gli organismi di sviluppo di norme nel settore. Pertanto, in risposta al problema che l'Unione europea potesse non essere al passo con i tempi, e soprattutto al pericolo che l'attività di normazione di tali beni possa non incarnare i valori europei, si programmava di ammodernare la politica comunitaria di normalizzazione delle ICT e sfruttare appieno le potenzialità di emanazione di norme[276].

Così, l'art. 13 del Regolamento prevede 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 le prescrizioni dell'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 (MSP), 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[277].

Al momento la Commissione ha emanato una serie di decisioni con il quale 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)[278]

d) La disciplina dell'attività della Commissione e dei comitati nella normazione europea

Per garantire condizioni uniformi di esecuzione della disciplina, il Regolamento attribuisce alla Commissione competenze di esecuzione da esercitate conformemente al Regolamento (UE) n. 182/2011 che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione[279].

Nello specifico, l'art. 20 conferisce alla Commissione il potere di adottare atti delegati riguardo alle modifiche degli Allegati, al fine di aggiornare l'elenco delle organizzazioni europee di normazione di cui all'Allegato I per tenere conto dei cambiamenti di denominazione o di struttura degli stessi; e di adeguare i criteri per le organizzazioni europee dei soggetti interessati stabiliti nell'Allegato III a ulteriori sviluppi relativi alla loro natura di organizzazioni senza scopo di lucro e alla loro rappresentatività. Tuttavia, tale potere non può comportare la creazione di nuovi criteri né la soppressione di criteri esistenti o di categorie di organizzazioni.

---

[275] Libro bianco, *Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE - Prospettive*, 3 luglio 2009, COM(2009) 324 definitivo.

[276] *Ibidem*.

[277] Cfr. art. 13, par. 3, Reg. 1025/2012.

[278] O. KANEVSKAIA, *The law and practice of global ICT standardization*, Cambridge, Cambridge university press, 2023, pp. 83 ss.

[279] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione.

Si tratta di un potere che possiamo interpretare come una forma di controllo della Commissione sulle ESOs. Con la modifica degli Allegati, la Commissione può infatti rimuovere l'organismo di normazione europea che ritiene non avere più certi requisiti, o dall'altra può prevedere che nuove categorie di rappresentanze sociali possano partecipare al processo di normazione.

I considerando 49 e 50 specificano invece le procedure da adottare per le obiezioni alle norme armonizzare di cui all'art. 11, e per le richieste di normazione di cui all'art. 10, prevedendo che per le prime la Commissione adotti la procedura consultiva per adottare atti di esecuzione riguardanti le obiezioni a norme armonizzate e per le quali i riferimenti alla norma armonizzata in questione non sono ancora stati pubblicati nella Gazzetta ufficiale dell'Unione europea, dato che la norma in questione non ha ancora portato alla presunzione di conformità alle prescrizioni fondamentali della legislazione dell'Unione applicabile in tema di armonizzazione. Mentre per le seconde, è prevista la procedura d'esame seguita poi per ogni richiesta di normazione presentata presso le organizzazioni europee di normazione e per l'adozione di atti di esecuzione riguardanti le obiezioni a norme armonizzate per le quali i riferimenti alla norma armonizzata in questione sono già stati pubblicati nella Gazzetta ufficiale dell'Unione europea, dato che la norma in questione potrebbe avere conseguenze sulla presunzione di conformità alle prescrizioni fondamentali applicabili.

Tuttavia, l'atto delegato è adottato dalla Commissione solo se non vi sono state obiezioni nè del Parlamento, nè del Consiglio entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni.

Altra disciplina è quella che interessa il Comitato, composto da rappresentanti degli Stati membri, disciplinato dal Regolamento (UE) n. 182/2011[280], e istituito nel particolare ambito della normazione tecnica. La funzione del Comitato è quella di assistere la Commissione, sia nella procedura consultiva che in quella d'esame[281], nonché lavora in cooperazione con le organizzazioni europee di normazione e le organizzazioni europee dei soggetti interessati ammissibili al finanziamento dell'Unione in conformità con il presente regolamento[282].

In tali occasioni, il Comitato è tenuto ad esprimere un parere il quale, ai sensi della disciplina in questione sulla normazione, dovrebbe poter essere ottenuto mediante procedura scritta e il silenzio del membro del Comitato dovrebbe essere considerato come un tacito accordo, ed entro un certo termine, al fine di promuovere procedure decisionali rapide[283].

2.7.2 *Segue*. La Direttiva (UE) 1535/2015 sulla procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione

Il 9 settembre 2015, è stata adottata la Direttiva 1535/2015 sulla procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione[284]. Diversamente dal Regolamento del 2012, in questo caso il legislatore ha avvertito l'esigenza di dover

[280] Cfr. artt. 3, 6, 10 Reg. (UE) 182/2011.
[281] Art. 22 Reg. 1025/2012.
[282] Art. 23 Reg. 1025/2012.
[283] Cons. 52 Reg. 1025/2012.
[284] Direttiva (UE) 1535/2015 che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione).

intervenire in tale disciplina al fine di fornire maggiore chiarezza e razionalizzazione, provvedendo così alla sua codificazione[285].

Come abbiamo già evidenziato, la procedura d'informazione ha rappresentato uno strumento fondamentale per la realizzazione del mercato unico, quale requisito a garanzia della trasparenza dello stesso e quindi della competitività delle imprese che vi operano. In questo caso il fine è quello di evitare la sovrapposizione di diverse norme tecniche in uno stesso settore od obiettivo, tali da creare possibili incompatibilità. Non solo. Tale procedura acquista rilievo anche sul piano istituzionale europeo nell'attività della Commissione la quale, prima dell'adozione delle disposizioni tecniche, deve necessariamente disporre di informazioni.

Da ciò discende l'obbligo per gli Stati membri, che trova fondamento nell'art. 4 par. 3 del TUE, di agevolare tale funzione della Commissione, notificando i loro progetti di regolamentazione tecnica.

La disciplina del 2015 è diretta allo specifico settore della "società dell'informazione"[286], ove i ritmi del progresso tecnologico delle ICT ha imposto al legislatore di tornare sulla disciplina della procedura di informazione, dopo la Direttiva 98/34/CE, con interventi sulle definizioni, e interventi volti a migliorare il coordinamento della regolazione tecnica per mezzo di obblighi di notifica alla Commissione dei progetti di normazione nazionali, e il rinvio dell'adozione di tali progetti.

Così all'art. 1 lett. b, è stata fornita la definizione di «servizio», intendendo qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi[287].

È stata inoltre introdotta le nozione di «regola tecnica», intesa come 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 jure* 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 o in una parte importante di esso, nonché, le disposizioni legislative, regolamentari o amministrative degli Stati membri 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[288].

---

[285] Cons. 1 Dir. 1535/2015.

[286] Il termine è stato coniato nell'ambito degli organismi UE, in occasione della stesura del libro bianco della Commissione Europea del 1993, c.d. "rapporto Delors", nel quale venivano analizzate le conseguenze economico-sociali prodotte dallo sviluppo tecnologico nei diversi Stati membri.

[287] In particolare, il disposto precisa che ai fini della definizione si intende per: i) «a distanza»: un servizio fornito senza la presenza simultanea delle parti; ii) «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici; iii) «a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale.

[288] Art. 1, lett. f) Dir. 1535/2015. In particolare, come specificato dal disposto, costituiscono in particolare regole tecniche *de facto*: i) le disposizioni legislative, regolamentari o amministrative di uno Stato membro che fanno riferimento o a specificazioni tecniche o ad altri requisiti o a regole relative ai servizi, o a codici professionali o di buona prassi che si riferiscono a loro volta a specificazioni tecniche o ad altri requisiti ovvero a regole relative ai servizi e la cui osservanza conferisce una presunzione di conformità alle prescrizioni fissate dalle suddette disposizioni legislative, regolamentari o amministrative; ii) gli accordi facoltativi dei quali l'autorità pubblica è parte contraente e che, nell'interesse generale mirano al rispetto di specificazioni tecniche o di altri requisiti, o di regole relative ai servizi, ad eccezione del capitolato degli appalti pubblici; iii) le specificazioni tecniche o altri requisiti o le regole relative ai servizi connessi con misure di carattere fiscale o finanziario che influenzano il consumo di prodotti o di servizi promuovendo 'di tali specificazioni tecniche o altri requisiti o regole relative ai servizi; non sono contemplati le specificazioni tecniche, o altri requisiti o le regole relative ai servizi connessi con i regimi nazionali di sicurezza sociale.

Si tratta pertanto delle norme tecniche pubbliche di cui abbiamo già trattato (*infra* 2.5), e che con tale Direttiva hanno ricevuto riconoscimento nell'ordinamento europeo. In particolare, tali norme, stabilite dalle autorità designate dagli Stati membri, figurano in un elenco stabilito e aggiornato, all'occorrenza da parte della Commissione nell'ambito del comitato permanente[289], autoregolamentato e composto di rappresentanti designati dagli Stati membri che possono farsi assistere da esperti o consulenti e presieduto da un rappresentante della Commissione[290].

Per quanto riguarda il coordinamento della regolazione tecnica, il legislatore europeo ha imposto agli Stati membri due obblighi di comunicazione alla Commissione.

Il primo, ai sensi dell'art. 4, quando lo Stato membro ha presentato richieste agli organismi di normazione volte a elaborare specifiche tecniche[291]. L'altro, ai sensi dell'art. 5, quando gli Stati membri adottano un progetto di regola tecnica, salvo che si tratti del semplice recepimento integrale di una norma internazionale o europea, nel qual caso è sufficiente una semplice informazione sulla norma stessa, ove sono anche tenuti a comunicare brevemente i motivi che rendono necessario adottare tale regola tecnica, a meno che ciò non risultino già dal progetto[292].

In questo caso all'informativa fornito dallo Stato membro, segue la comunicazione da parte della Commissione agli altri Stati membri del progetto di regola tecnica e tutti i documenti che le sono stati trasmessi.

All'art. 6 è invece disciplinato l'obbligo di rinviano all'adozione del progetto di regola tecnica di tre mesi da parte dello Stato membro, a decorrere dalla data in cui la Commissione ha ricevuto la comunicazione di cui all'art. 5.

2.7.3 Segue. I recenti adattamenti e modifiche al Regolamento (UE) 1025/2012

Tra il 2022 e il 2023 la disciplina europea sulla normazione tecnica è stata oggetto di ulteriori attenzioni da parte del legislatore. Si tratta di interventi che sono andati in alcuni casi a modificare, in altri ad adattare il Regolamento (UE) 1025/2012.

a) Il Regolamento (UE) 2022/2480

Il primo di questi interventi è il Regolamento (UE) 2022/2480, il quale è andato ad apportare modifiche alla disciplina del 2012 per quanto riguarda le decisioni delle organizzazioni europee di normazione relative alle norme europee e ai prodotti della normazione europea[293], ossia all'art. 10 del Regolamento del 2012 relativo alle richieste di normazione della Commissione alle organizzazioni europee di normazione.

A nostro modo di vedere, il recente intervento si muove nel solco già tracciato nel Regolamento 1025/2012, ove il legislatore europeo si è mostrato consapevole dell'impatto della normazione tecnica sulla società in generale (e quindi oltre i soggetti per i quali le norme tecniche sono prodotte). Come si apprende dal considerando 4, l'esigenza di modifica è stata dettata dai cambiamenti nella prassi

[289] *Ibidem*.
[290] Art. 2, Dir. 1535/2015.
[291] Cfr. art. 4 Dir. 1535/2015.
[292] Cfr. art. 5 Dir. 1535/2015.
[293] Regolamento (UE) 2022/2480, del Parlamento europeo e del Consiglio del 14 dicembre 2022 recante modifica del regolamento (UE) n. 1025/2012 per quanto riguarda le decisioni delle organizzazioni europee di normazione relative alle norme europee e ai prodotti della normazione europea.

delle organizzazioni europee di normazione per quanto riguarda la *governance* interna e le procedure decisionali ove si è stata notata un'intensificazione della cooperazione con i soggetti interessati internazionali ed europei. Cambiamento che tuttavia necessita, quando le organizzazioni europee di normazione eseguono richieste di normazione a sostegno della legislazione e delle politiche dell'Unione, che «le loro decisioni interne tengano pienamente conto degli interessi, degli obiettivi politici e dei valori dell'Unione, nonché degli interessi pubblici in generale [enfasi aggiunta]»[294].

In questa sede il legislatore europeo si è quindi preoccupato del coinvolgimento della tutela degli interessi pubblici generali e dei valori dell'Unione nelle procedure decisionali presso gli enti di normazione tecnica.

Al considerando 5, è invece tornato sulla garanzia di una rappresentanza equilibrata degli interessi dei soggetti interessati, compresi qu3elli che rappresentano, le PMI e gli interessi ambientali, sociali e dei consumatori, ribadendo che le opinioni e i contributi di tali soggetti dovrebbero essere presi in considerazione in seno alle organizzazioni europee di normazione. E che inoltre, le opinioni espresse nell'ambito delle consultazioni nazionali condotte dagli organismi nazionali di normazione dovrebbero essere prese in considerazione al momento di adottare decisioni riguardanti le norme europee armonizzate[295].

Si delineano pertanto due piani, da una parte l'attenzione verso tali interessi nelle procedure di formazione delle norme tecniche presso gli organismi europei, le ESOs; dall'altra il rilievo degli interessi emersi durante le consultazioni pubbliche a livello nazionale (per quanto riguarda l'Italia, per esempio, le consultazioni indette dall'UNI v. *infra* 2.6.2).

Alla luce di ciò, il considerando 6, pone particolare attenzione proprio sugli enti di normazione nazionali in quanto ritenuti «nella posizione migliore per far sì che gli interessi, gli obiettivi politici e i valori dell'Unione, nonché gli interessi pubblici in generale, siano debitamente presi in considerazione presso le organizzazioni europee di normazione». La modifica del 2022 si pone pertanto nell'ottica di rafforzare il ruolo degli organismi nazionali all'interno degli organi decisionali delle organizzazioni europee di normazione quando questi adottano decisioni riguardanti le norme europee armonizzate «senza pregiudicare il ruolo importante svolto dalla base più ampia dei soggetti interessati nella preparazione di norme efficaci che rispondano alle esigenze dell'interesse pubblico e del mercato»[296].

Il nuovo sistema di formazione delle norme armonizzate tracciato dal legislatore europeo è pertanto orientato su meccanismi di rappresentanza indiretta degli interessi sociali nazionali in sede europea. Stando a quanto si apprende dal considerando, in tali sedi, sono gli organismi di normazione nazionali a farsi portatori di tali interessi risultanti dai meccanismi di consultazione pubblica.

Resta tuttavia fermo l'obbligo per le organizzazioni di normazione europee di incoraggiare di facilitare la rappresentanza e l'effettiva partecipazione di tutti i soggetti interessati - per la formazione di tutte le norme in generale siano esse armonizzate od europee - sebbene ciò «non comporta alcun diritto di voto per tali soggetti interessati, a meno che tale diritto di voto non sia previsto dal regolamento interno delle organizzazioni di normazione europee [enfasi aggiunta]»[297].

Sulla scorta di tali considerazioni, alla lettera dell'art. 10 del Regolamento 1025/2012 è stato introdotto il paragrafo 2 *bis*, ove è disposto che fatti salvi altri pareri consultivi, ciascuna

[294] Cfr. cons. 4, Reg. 2022/2480.
[295] Cfr. cons. 5, Reg. 2022/2480.
[296] Cfr. cons. 6, Reg. 2022/2480.
[297] Cfr. cons. 23 Reg. (UE) 1025/2012.

organizzazione europea di normazione garantisce che le decisioni relative alle norme europee armonizzate siano adottate «esclusivamente dai rappresentanti degli organismi nazionali di normazione in seno all'organo decisionale competente di tale organizzazione [enfasi aggiunta]», e tali decisioni sono relative: all'accettazione e al rifiuto delle richieste di normazione; all'accettazione dei nuovi lavori necessari per soddisfare la richiesta di normazione; e all'adozione, alla revisione e al ritiro di norme europee o di prodotti della normazione europea.

Si tratta pertanto di un cambiamento radicale che pone maggior potere sugli organismi nazionali di normazione piuttosto ché sulle ESOs, le quali assumono quindi da una parte il ruolo di piattaforme di raccordo tra le esigenze nazionali e quelle europee, e dall'altro quello di promotori degli interessi interni negli organismi internazionali. soprattutto del mercato globale, dato che, come ricordato, sono tenute a mediare tali interessi[298]. Precisiamo tuttavia che tale particolare enfasi per la rappresentanza degli interessi sociali presso gli organismi di normazione tecnica interessa solo la formazione delle norme armonizzate, mentre per la formazione delle norme europee, resta fermo il solo obbligo per le organizzazioni di normazione europee di incoraggiare e facilitare la rappresentanza e l'effettiva partecipazione di tutti i soggetti interessati.

b) Il Regolamento (UE) 2023/988

La riforma del 2023 ha invece toccato solo alcuni aspetti del Regolamento 1025/2012 dato che questa è stata perlopiù diretta a novellare la disciplina sulla sicurezza generale dei prodotti (*General Product Safety Regulation* - GPSR)[299].

In particolare, la modifica in questo caso è stata diretta a fare in modo che la Commissione, qualora ritenga necessaria l'elaborazione di una norma europea che garantisca la conformità di determinati prodotti all'obbligo generale di sicurezza previsto dal GPSR, la Commissione deve applicare le disposizioni pertinenti del Regolamento del 2012 per richiedere a una o più organizzazioni di normazione europee di elaborare o individuare una norma adatta «a garantire che i prodotti ad essa conformi siano considerati sicuri»[300].

Secondo nostra opinione, si tratta di un ulteriore passo avanti nella disciplina della normazione europea in quanto il legislatore europeo è andato ad imporre il rispetto del requisito di sicurezza dei prodotti nella formazione di tutte le norma tecniche europee da parte delle ESOs, affinché gli operatori economici immetteranno o metteranno a disposizione sul mercato soltanto prodotti sicuri.

In particolare, secondo la disciplina del Regolamento GPSR, la sicurezza dei prodotti deve essere valutata tenendo conto di alcuni criteri, quali: le caratteristiche del prodotto, quali progettazione, caratteristiche tecniche, composizione, imballaggio e istruzioni; l'effetto su altri prodotti; la

[298] Cfr. cons. 6, Reg. 2022/2480, ove è precisato che lo spazio lasciato agli organismi nazionali di normazione tecnica per far valere le istanze sociali (nazionali) non deve comunque «pregiudicare il ruolo importante svolto dalla base più ampia dei soggetti interessati nella preparazione di norme efficaci che rispondano alle esigenze dell'interesse pubblico e del mercato».

[299] Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio. In breve, il RGPD impone che tutti i prodotti di consumo presenti sui mercati dell'UE siano sicuri e stabilisce obblighi specifici per le imprese al fine di garantirla. Si applica ai prodotti non alimentari e a tutti i canali di vendita. Il RGPD fornisce una rete di sicurezza per i prodotti o i rischi non regolamentati da altre normative dell'UE. Questa funzione di rete di sicurezza significa che i consumatori dell'UE sono sempre protetti dai prodotti pericolosi, sia ora che in futuro.

[300] Cfr. cons. 28 Reg. 2023/988.

presentazione del prodotto, l'etichettatura, le avvertenze e le istruzioni e informazioni sulla sicurezza; le categorie di consumatori che utilizzano il prodotto; l'aspetto del prodotto, in particolare gli aspetti legati all'imitazione di prodotti alimentari o all'attrattività per i bambini; le caratteristiche di cibersicurezza e tutte le funzionalità evolutive, di apprendimento e predittive del prodotto.

Il Regolamento prevede inoltre casi in cui si presume che un prodotto sia sicuro. Tali casi includono prodotti conformi alle norme europee pertinenti citate nella Gazzetta ufficiale dell'Unione europea. Altri elementi che possono essere presi in considerazione per valutare la sicurezza di un prodotto sono le norme nazionali e internazionali, i sistemi di certificazione volontaria, i codici di buona condotta e le ragionevoli aspettative dei consumatori.

Così è stato ritenuto necessario oltre all'adattamento del Regolamento (UE) n. 1025/2012, anche introdurre una procedura specifica per l'adozione dei requisiti specifici di sicurezza con l'assistenza del comitato specializzato[301], nonché la modifica di alcune disposizioni per tenere conto delle specificità del GPSR, in particolare la necessità di determinare i requisiti specifici di sicurezza prima di inviare la richiesta all'organizzazione europea di normazione[302].

Nello specifico, sulla scorta di tali esigenze, è stato modificato l'art. 10 del Regolamento del 2012 facendo precedere all'obbligo per la Commissione di pubblicare in Gazzetta ufficiale dell'UE la norma armonizzata prodotta, il parametro della conformità non solo alla disciplina in generale e alle indicazioni della Commissione stessa ma anche ai requisiti specifici di sicurezza[303].

Ulteriori modifiche sono state apportate anche sul diritto di opposizione degli Stati membri o del Parlamento alla pubblicazione o al mantenimento di una norma armonizzata di cui all'art. 11[304]. In particolare, modificando i primi tre paragrafi, la nuova disciplina prevede che, qualora uno Stato membro o il Parlamento europeo ritenga che una norma armonizzata o una norma europea elaborata a sostegno del GPSR non soddisfi completamente le prescrizioni cui intende riferirsi e che sono stabiliti nella pertinente legislazione dell'Unione in materia di armonizzazione o nello stesso Regolamento (UE) 2023/988, esso ne informa la Commissione fornendo una spiegazione dettagliata. La Commissione, previa consultazione del comitato, laddove esista, o del comitato istituito dal GPSR, o previe altre forme di consultazione di esperti del settore, decide: di pubblicare, non pubblicare o di pubblicare con limitazioni i riferimenti alla norma armonizzata o alla norma europea in questione elaborata a sostegno di detto regolamento nella Gazzetta ufficiale dell'Unione europea; ovvero di mantenere, mantenere con limitazioni o di ritirare i riferimenti alla norma armonizzata o alla norma europea in questione elaborata a sostegno del GPSR.

La Commissione pubblica sul proprio sito web le informazioni relative alle norme armonizzate e alle norme europee elaborate a sostegno del Regolamento (UE) 2023/988 che sono state oggetto della decisione.

La Commissione informa l'organizzazione di normazione europea interessata della decisione e, all'occorrenza, richiede la revisione delle norme armonizzate o delle norme europee in questione elaborate a sostegno del regolamento (UE) 2023/988.

2.7.4 Le norme (tecniche) armonizzate e le norme volontarie europee

[301] Cfr. cons. 30 Reg. 2023/988.
[302] Cfr. cons. 103 Reg. 2023/988.
[303] Art. 48, par. 1, Reg. 2023/988.
[304] Art. 48, par. 2, Reg. 2023/988.

Ai sensi dell'art. 2, n. 1, lett. c) del Regolamento 1025/2012, per norma armonizzate si intende «una norma europea adottata sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione», mentre alla lett. b) la norma europea è definita quale qualsiasi «norma adottata da un'organizzazione europea di normazione [ESOs]»[305].

Come abbiamo già avuto modo di trattare, le prime sono frutto di un processo di formazione che pone maggiore rilievo alla partecipazione tra istituzioni pubbliche, europee e nazionali, e parti private del mondo industriale, ove le seconde sono invece frutto di un processo di formazione autoregolato dagli stessi organismi (le ESOs) ma, come si è evidenziato, influenzato dalla disciplina dettata dal Regolamento del 2012 nella parte in cui impone l'obbligo per queste organizzazioni di normazione europee di incoraggiare e facilitare la rappresentanza e l'effettiva partecipazione di tutti i soggetti interessati. Inoltre, aggiungiamo che il Direzione generale per il mercato interno, l'industria, l'imprenditorialità e le PMI (anche noto come DG GROW)[306], è responsabile della gestione delle relazioni tra la Commissione e le ESOs fornendo strumenti, *database* e orientamenti su come utilizzare le norme europee volontarie per sostenere la legislazione e le politiche dell'Unione[307]. Pertanto, anche in questo caso, troviamo un elemento di eterodirezione della normazione tecnica europea verso la realizzazione dei fini dell'Unione. Sulla scorta della riforma del 2022, si è anche avuto modo di notare come sia stata ribadita dal legislatore l'importanza della rappresentanza equilibrata degli interessi dei soggetti interessati, compresi i soggetti che rappresentano, tra l'altro, le PMI e gli interessi ambientali, sociali e dei consumatori, nelle procedure decisionali di tali organismi.

Tuttavia, a nostro modo di vedere, riteniamo che il maggiore *effort* alla tutela degli interessi pubblici generali sia stato maggiormente garantito nella disciplina per la formazione delle norme armonizzate.

A tal proposito, abbiamo anche avuto modo di trattare della procedura di formazione di tali norme armonizzate (art. 10 Reg. 1025/2012), tenendo conto anche delle eventuali opposizioni (art. 11), anche alla luce delle recenti modifiche sul punto. In sostanza la grande differenza tra le due è che la norma armonizzata viene prodotta dagli organismi di normazione europea sulla scorta di indicazioni circa il contenuto e i requisiti della Commissione europea, mentre le norme europee sono prodotte da detti organismi senza alcuna indicazione istituzionale. Le norme europee possono pertanto essere facilmente qualificate come norme volontarie, non cogenti ma tali da produrre rilevanti effetti giuridici.

---

[305] Artt. 2, n. 1, lett. b) e c), Reg. 1025/2012.

[306] Come si apprende dal sito ufficiale, la DG GROW sostiene la competitività, la crescita e la resilienza dell'economia dell'UE, facilitando allo stesso tempo una ripresa trasformativa dalla crisi del coronavirus. Si concentra sul rafforzamento della leadership delle industrie europee attraverso diversi ecosistemi industriali, sfruttando il potere del Mercato Unico e affrontando le dipendenze strategiche nelle nostre catene di approvvigionamento. Inoltre, implementa politiche che sostengono l'imprenditorialità e la crescita, in particolare a vantaggio delle piccole e medie imprese (PMI), facilitando l'accesso al finanziamento e ai mercati globali per le imprese dell'UE. Per ulteriori si rinvia al link ufficiale:<https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/internal-market-industry-entrepreneurship-and-smes_it>.

[307] Commissione "Better regulation Toolbox: Tool 17 - The choice of policy instruments", sec. 3.2, box 4 "European standards", 2023, reperibile al link:<https://commission.europa.eu/document/download/c0561a9c-d112-4d20-b1ec-145748e2c61c_en?filename=BRT-2023-Chapter%202-How%20to%20carry%20out%20an%20impact%20assessment_0.pdf>.

Diversamente, problemi di qualificazione sorgono invece sulla natura della norma armonizzata. Come evidenziato da una certa dottrina, il "dilemma" pare riconducibile al contrasto tra i diversi orientamenti interpretativi delle principali istituzioni europee[308].

Precisiamo tuttavia che tali dubbi sono stati sollevati già sulla natura delle norme tecniche (volontarie) in generale. Con il Regolamento 1025/2012 e il caso *Fra.bo*[309], fu ritenuto, per via normativa e giurisprudenziale, che i processi di normazione europea si fossero «giuridificati»[310] ma, nonostante ciò, questi restavano immuni al controllo giudiziario, sollevando le osservazioni critiche della dottrina sull'ipotetica violazione del principio di tutela giurisdizionale effettiva[311]. Inoltre, sempre nel caso *Fra.bo* la Corte stabilì che in determinate circostanze le organizzazioni di normalizzazione volontaria (SSO) devono essere considerate esercitanti poteri pubblici ma, l'accesso a queste norme resta a titolo oneroso in quanto protette dal *copyright* della SSO che le ha prodotte, ponendosi quindi l'astratta violazione con i parametri di pubblicità propri della legge[312].

I dilemmi interpretativi relativi alla natura delle norme armonizzate sono invece iniziati dopo la sentenza *James Elliot*[313] del 2016, ove la Corte di giustizia ha dichiarato che la norma armonizzata è parte dell'ordinamento europeo nella misura in cui implementa o applica un atto legislativo dell'Unione. La Commissione ha affermato all'interno di documenti ufficiali che le norme tecniche armonizzate sono pienamente giustiziabili nella loro «validità e interpretazione»[314]. Secondo il Parlamento Europeo invece «[...] gli standard non possono essere considerati come diritto dell'UE, poiché la legislazione e le politiche riguardanti il livello di tutela del consumatore, della salute, della sicurezza, dell'ambiente, della protezione dei dati e del livello di inclusione sociale sono determinate dal legislatore»[315]. Perplessità sulla natura e collocazione delle norme tecniche che possiamo riscontrare anche nelle argomentazioni dell'Avvocato generale Saugmandsgaard Øe a proposito del caso *Stichting Rookpreventie* ove, tra i punti delle conclusioni vi è stata anche la questione se le norme tecniche (seppur in questo caso quelle volontarie internazionali dell'ISO) possano essere considerate come «atti legislativi» o come meri «elementi» di un atto legislativo[316].

Secondo tali opposte ricostruzioni la norma armonizzata può quindi acquisire carattere regolatorio (*Fra.bo*), essere considerata parte del diritto dell'Unione come misura di attuazione o applicazione di

---

[308] R. VALLEJO, *The private administrative law of technical standardization*, in *Yearbook of European Law*, vol. 40, 2021, pp. 172–229, reperibile al link:<https://doi.org/10.1093/yel/yeab011>.

[309] CGUE, Causa C-171/11, *Fra.bo SpA c. Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein*, 2012, ECLI:EU:C:2012:453.

[310] H. SCHEPEL, *The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law*, in *Maastricht Journal of European and Comparative Law*, vol. 20, n. 4, 2012, pp. 521-533. reperibile a:<doi:10.1177/1023263x1302000404>.

[311] M. ELIANTONIO, *Judicial Control of the EU Harmonized Standards: Entering a Black Hole?*, in *Legal Issues of Economic Integration*, vol. 44, n. 4, (2017), 44, pp. 395-407, reperibile al link:<https://kluwerlawonline.com/journalarticle/Legal+Issues+of+Economic+Integration/44.4/LEIE2017022>.

[312] R. VALLEJO, *The private administrative law of technical standardization …op.cit.,* p. 190.

[313] M. ELIANTONIO, M. MEDZMARIASHVILI, *Hybridity under scrutiny: How European standardization shakes the foundations of EU constitutional and internal market law*, in *Legal Issues of Economic Integration*, vol. 44, n. 4, 2017, pp. 323-335, reperibile al link:<https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\LEIE\LEIE2017017.pdf>.

[314] Commissione "*Better regulation Toolbox: Tool 18 - The choice of policy instruments*", sec. 3.2, 2017, pp. 114 ss.

[315] Parlamento europeo, *Draft Report - on a standardisation strategy for the Single Market*, (2022/2058(INI)), del 14 novembre 2022, p. 4, reperibile al link:<https://www.europarl.europa.eu/doceo/document/IMCO-PR-737208_ EN.pdf>.

[316] Conclusioni dell'Avvocato generale Henrick Saugmandsgaard Øe, presentate il 15 luglio 2021, *Stichting Rookpreventie Jeugd e a. c. Staatssecretaris van Volksgezondheid, Welzijn en Sport. Domanda di pronuncia pregiudiziale proposta dal Rechtbank Rotterdam*, 2021, ECLI:EU:C:2021:618.

un atto di diritto derivato (*James Elliot*) ma, resta comunque un tipo di normativa diversa dagli atti legislativi di diritto (Parlamento europeo) non assimilabile a quella applicabile alle agenzie amministrative dell'UE, né alle parti private nelle loro relazioni puramente private[317].

Contrasto che la dottrina maggioritaria ha tentato di chiarire con la già menzionata teoria della "giuridificazione" da cui deriva, da una parte l'"agenzificazione" degli organismi di normazione, ossia la loro assimilazione alle agenzie amministrative europee per via di "delega" (ossia il mandato conferito dalla Commissione europea) che li renderebbe soggetti ai requisiti della dottrina *Meroni*[318], e dall'altra, la conseguente giudiziarizzazione delle norme armonizzate.

Altro aspetto che rende tali strumenti di *soft law* particolarmente vicini alla norma giuridica riguarda gli effetti giuridici prodotti dalla norma armonizzata, distinti dalla dottrina in: i) obblighi nei confronti delle organizzazioni nazionali di standardizzazione; ii) onere nei confronti degli operatori economici; iii) obbligazione *de facto* nei confronti degli operatori economici[319].

Il dibattito sulla norma armonizzata europea non sembra quindi diverso da quello che abbiamo già affrontato alla luce della dottrina italiana a cui si rinvia (Pt. III, Cap. I, 2.2 e 2.3).

Nel proseguo tenteremo tuttavia di ricostruire i termini del dibattito alla luce della giurisprudenza della Corte di giustizia sul punto al fine di meglio comprendere il rapporto tra le norme tecniche ed armonizzate e l'ordinamento europeo.

2.7.5 *Segue*. Il caso *James Elliot* sulle norme armonizzate

Nella causa C-613/14, la Corte di giustizia veniva adita in via pregiudiziale su una controversia relativa alla fornitura, ad opera della Irish Asphalt Limited, di aggregati rocciosi alla James Elliott Construction Limited. La vicenda è stata occasione per la Corte di pronunciarsi per la prima volta sulla collocazione delle norme armonizzate nell'ordinamento europeo.

Come già precisato, con tale sentenza il giudice europeo ha riconosciuto che la norma armonizzata «rientra nel diritto dell'Unione» (par. 40), pur essendo emanata da «un organismo di diritto privato» (par. 43), ossia da soggetti che «non possono essere qualificati come "istituzioni, organi o organismi dell'Unione"» (par. 34).

Motivo per cui le norme armonizzate non possono essere assimilate ad un atto giuridico di diritto derivato ma sono da intendersi come «misure di attuazione o di applicazione di un atto di diritto dell'Unione» (par. 34), e che conferiscono concreta forma «a un livello tecnico dei requisiti essenziali» definiti dagli atti di diritto (par. 36) a cui questi si devono conformare.

Sulla scorta di tali considerazioni, il Giudice europeo approdava pertanto alla conclusione che la norma armonizzata (o comunque le norme tecniche in generale) sono atti diversi dalla norma giuridica, ma di cui non è possibile negare la loro rilevanza per l'ordinamento giuridico europeo. A tal proposito, la Corte argomenta sul valore giuridico di tali strumenti a partire dell'analisi della loro formazione. Le norme armonizzate sono infatti elaborate sulla scorta di un preciso atto di mandato della Commissione verso l'organismo di normazione europeo, (par. 44), il quale, se accetta, elabora

---

317 R. VALLEJO, *The private administrative law of technical standardization …op.cit.*

318 CGUE, C-9/56, *Meroni & Co., Industrie metallurgiche, SAS c Alta Autorità della Comunità europea del carbone e dell'acciaio*, sentenza del 13 giugno 1958, ECLI:EU:C:1958:7.

319 A. VOLPATO, *The Legal Effects of Harmonised Standards in EU law*, in P.L. LÁNCOS, N. XANTHOLIUS, L.A. JIMÉNEZ (a cura di), *The Legal Effects of EU Soft Law Theory, Language and Sectoral Insights*, Elgar Studies in European Law and Policy, 2023, 193-212.

tale norma che consiste in «una misura di attuazione necessaria e strettamente regolamentata dei requisiti essenziali definiti [dall'atto Ue], realizzata su iniziativa e sotto la direzione nonché il controllo della Commissione, e i suoi effetti giuridici sono soggetti alla previa pubblicazione da parte di quest'ultima dei suoi riferimenti nella Gazzetta ufficiale dell'Unione europea» (par. 43).

Il Giudice precisa che la Commissione svolge un monitoraggio dettagliato durante la fase di elaborazione e un controllo di conformità sul progetto finale di norma armonizzata prima della pubblicazione dei riferimenti nella Gazzetta ufficiale dell'Unione europea; inoltre, l'organismo di armonizzazione è anche tenuto all'obbligo di relazionare regolarmente verso di questa (par. 45).

Solo dopo la pubblicazione di tali riferimenti nella Gazzetta ufficiale la norma armonizzata produce effetti giuridici (par. 37) che tuttavia non consistono nella cogenza della norma, che resta volontaria (par. 35), ma in un mero «beneficio di una presunzione di conformità ai requisiti essenziali» prescritti nell'atto di diritto europeo (par. 38-39, 41 e 46).

La Corte ha inoltre avuto occasione di pronunciarsi circa la sua giurisdizione su tali norme. Considerato che la norma armonizzata non può essere considerata una norma giuridica, ma essendo parte dell'ordinamento europeo in quanto misura di attuazione o di applicazione di un atto di diritto dell'Unione, ne deriva che anche la giurisdizione del Giudice europeo su di queste non possa essere piena ma limitata: la Corte di giustizia si arresta infatti ad una giurisdizione di interpretazione (ossia in via pregiudiziale) sulle norme armonizzate (par. 34), anche se queste sono prive di effetti obbligatori (par. 35)[320].

I punti salienti appena ripercorsi ci paiono fornire maggiore chiarezza sul punto, tuttavia, resta il problema di come sia possibile giustificare il perseguimento di interessi generali con strumenti non giuridici, originati da processi che non assicurano le medesime garanzie dei processi giuridico-politici dei Parlamenti e su cui non sussiste la piena giurisdizione dei giudici.

Secondo la dottrina a cui abbiamo fatto riferimento, i dilemmi di cui prima, riconducibili alla questione di legittimità degli organismi di normazione e delle norme tecniche possono essere interpretati alla luce del c.d. *private administrative law*[321]. Come già argomentato, il Regolamento 1025/2012 ha imposto alle ESOs (anche nel caso di produzione di norme non armonizzate) il rispetto dei principi della trasparenza, partecipazione e razionalità, nonché anche di opposizione che sono ben noti nel diritto amministrativo[322].

Aggiungiamo inoltre che tale processo di ispirazione (diverso dalla "giuridicizzazione") del sistema di normazione tecnica europeo agli strumenti e principi giuspubblicistici non avviene solo per eterodirezione delle istituzioni europee ma anche per attività assunte da tali organismi su base volontaria (come l'adozione di linee guida etiche, codici di condotta, ecc.) che ci portano a ritenere che, o per spirito di convenienza, o per presa di coscienza di tali soggetti circa la rilevanza sociale dei loro prodotti, possa parlarsi di una vera e propria convergenza.

2.7.6 *Segue.* Il caso *Stichting Rookpreventie* sull'accesso e opposizione alle norme volontarie (internazionali)

[320] Cfr. *Ivi*, p. 218.
[321] Cfr. *Ivi*, pp. 176 e 190.
[322] *Ivi*, p. 208.

Quanto espresso nel precedente paragrafo trova conferma nel recente caso *Stichting Rookpreventie,* causa C-160/2020[323], ove la Corte di giustizia si è trovata a doversi pronunciare su una questione relativa alla trasparenza e libero accesso alle norme tecniche da parte dei singoli.

La Corte è stata adita in via pregiudiziale sull'interpretazione dell'art. 4, par. 1, della Direttiva 2014/40/UE, sul ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla lavorazione, alla presentazione e alla vendita dei prodotti del tabacco e dei prodotti correlati, nella parte in cui prevede che i livelli massimi di emissioni di catrame, nicotina e monossido di carbonio delle sigarette sono misurati sulla base di tre norme tecniche elaborate dall'ISO indicate dal disposto della Direttiva (rinvio fisso).

Le ricorrenti avevano adito il Tribunale dei Paesi Bassi evidenziando, tra i diversi punti del ricorso, che tali norme non fossero liberamente accessibili al pubblico e che la loro consultazione sarebbe stata possibile solo dietro pagamento, sollevando così il dubbio interpretativo del Giudice nazionale «se una siffatta modalità di regolamentazione sia compatibile con il regime di pubblicità degli atti legislativi dell'Unione e con il principio di trasparenza» (pt. 22).

La Corte di giustizia ha così argomentato la sua decisione ricordando le basi legali del principio di trasparenza, quali l'art. 10, par. 3, TUE, l'art. 15, par. 1, e dall'art. 298, par. 1, TFUE, l'art. 42 della Carta dei diritti fondamentali dell'Unione europea, nonché l'art. 297, par. 1, TFUE il quale prevede che tutti gli atti legislativi, sia che siano stati adottati sulla scorta della procedura ordinaria, sia speciale, sono «pubblicati nella Gazzetta ufficiale dell'Unione europea [ed] entrano in vigore alla data da essi stabilita oppure, in mancanza di data, il ventesimo giorno successivo alla pubblicazione».

Sulla scorta di ciò, il Giudice europeo sosteneva, in accordo con la precedente giurisprudenza, che se una disposizione non prescrive un metodo o procedimenti concreti non significa che quest'ultima violi il principio della certezza del diritto e pertanto, non è necessario che un atto legislativo fornisca esso stesso precisazioni di natura tecnica, in quanto il legislatore dell'Unione può ricorrere a un quadro giuridico generale che deve essere, eventualmente, precisato successivamente (pt. 43).

Motivo per cui, tenuto conto dell'ampio margine di discrezionalità di cui dispone il legislatore dell'Unione nell'ambito dell'esercizio delle competenze ad esso demandate quando la sua azione implica scelte di natura politica, economica e sociale, e quando è chiamato ad effettuare valutazioni complesse questi «può legittimamente rinviare, negli atti da esso adottati, a norme tecniche stabilite da un organismo di normalizzazione, quale l'Organizzazione internazionale per la standardizzazione (ISO)» (pt. 44), purché tale rinvio sia «chiaro, preciso e prevedibile nei suoi effetti, affinché gli interessati possano orientarsi nelle situazioni e nei rapporti giuridici rientranti nell'ordinamento giuridico dell'Unione» (pt. 45).

Così la Corte concludeva sulla questione statuendo che «norme tecniche stabilite da un organismo di normalizzazione, quale l'ISO, e rese obbligatorie da un atto legislativo dell'Unione sono opponibili ai singoli in generale solo se sono state a loro volta oggetto di pubblicazione nella Gazzetta ufficiale dell'Unione europea [enfasi aggiunta]» (pt. 48), ed inoltre, anche ove queste «siano state oggetto di modifiche da parte di siffatto organismo, tale principio comporta altresì la conseguenza di rendere opponibile ai singoli in generale soltanto la versione di dette norme che sia stata pubblicata» (pt. 49).

2.7.7 *Segue*. Il caso *Public.Resource.Org Inc. et al.* sull'interesse pubblico all'accesso alle norme armonizzate

[323] CGUE, Causa C-160/2020, *Stichting Rookpreventie Jeugd …,* pt. 1.

Il 5 marzo 2024 la Grande Sezione della Corte di giustizia si è pronunciata sulla causa C-588/21[324], improntata dalla Public.Resource.Org Inc. e la Right to Know CLG, due organizzazioni senza scopo di lucro la cui missione principale è quella di rendere il diritto liberamente accessibile a tutti i cittadini, le quali nel 2018 avevano avanzato una domanda di accesso pubblico alla Commissione europea relativa a quattro norme armonizzate adottate dal CEN ai sensi del Reg. (UE) 1025/2012.

La Commissione era stata destinataria di tale richiesta ai sensi del Regolamento n. 1049/2001 (relativo all'accesso ai documenti detenuti dalle istituzionali dell'Unione), sulla scorta del precedente giurisprudenziale secondo cui le norme armonizzate rientrano nel diritto dell'Unione e pertanto, secondo le ricorrenti, da ciò sarebbe dovuto derivare anche l'applicazione del principio di trasparenza e libero accesso ai documenti detenuti dalle istituzioni europee.

La Commissione rifiutava tuttavia di accogliere la domanda in virtù dell'art. 4, par. 2, primo trattino, del Reg. (UE) 1049/2001, ritenendo che tale divulgazione avrebbe leso la tutela degli interessi commerciali degli enti di normazione, nonché anche la proprietà intellettuale delle norme in questione.

Le interessate ricorrevano così al Tribunale della Corte di giustizia, il quale si pronunciava nel 2021 respingendo il ricorso in tutte le sue motivazioni, e quindi: confermando la sussistenza di un limite al diritto di accesso alle norme armonizzate in quanto protette dal diritto d'autore, e negando la sussistenza di un interesse pubblico prevalente al loro accesso.

La Grande Sezione con la pronuncia del 2024 ha ribaltato la sentenza del Tribunale riproponendo tre argomentazioni di fondo. Innanzitutto, veniva ricordando che «il diritto di accesso ai documenti delle istituzioni, degli organi e degli organismi dell'Unione, a prescindere dal loro supporto, è garantito a qualsiasi cittadino dell'Unione e a qualsiasi persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro dall'articolo 15, paragrafo 3, TFUE nonché dall'articolo 42 della Carta dei diritti fondamentali dell'Unione europea» (pt. 66).

Altro argomento riguardava il ruolo centrale svolto dalla Commissione nella procedura di elaborazione delle norme armonizzate ai sensi del Reg. (UE) 1025/2012, ove concordando con quanto sostenuto dall'Avvocato generale Medina nelle conclusioni[325], sebbene l'elaborazione di tali norme sia affidata a un organismo di diritto privato, «solo la Commissione ha il potere di richiedere l'elaborazione di una norma armonizzata al fine di attuare una direttiva o un regolamento. [...], essa stabilisce i requisiti relativi al contenuto che la norma armonizzata di cui è chiesta l'elaborazione deve rispettare e un termine per la sua adozione. Detta elaborazione è supervisionata dalla Commissione, che provvede altresì a un finanziamento [inoltre], essa decide di pubblicare, di non pubblicare o di pubblicare con limitazioni i riferimenti alla norma armonizzata in questione sulla Gazzetta ufficiale dell'Unione europea» (pt. 73).

Infine, veniva ricordato come sebbene il rispetto delle norme armonizzate non sia obbligatorio, i prodotti che rispettano tali norme giovano di una presunzione di conformità alle prescrizioni fondamentali relative a tali prodotti stabilite dalla pertinente legislazione dell'Unione sull'armonizzazione (pt. 74). Questo effetto giuridico costituisce un utile beneficio per gli operatori economici che troverebbero svantaggioso dimostrare tale conformità ricorrendo a procedure alternative (pt. 74), comportando inoltre una inversione della prova per «qualsiasi persona fisica o

[324] CGUE, C-588/21, *Public.Resource.Org and Right to Know v Commission and Others*, ECLI:EU:C:2024:201.

[325] Cfr. Conclusioni dell'Avvocato generale Laila Medina, presentate il 22 giugno 2023, ECLI:EU:C:2023:509, di cui al link:<https://curia.europa.eu/juris/document/document.jsf?text=&docid=274881&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=1411271>.

giuridica che intenda contestare utilmente tale presunzione in relazione a un determinato prodotto o servizio [dovendo] dimostrare che quest'ultimo non soddisfa tale norma o che detta norma è inadeguata» (pt. 76).

Sulla scorta di tali argomenti, la Grande Sezione concludeva che, sebbene il rispetto delle norme armonizzate non è obbligatorio, nel caso di specie la norma prodotta dal CEN è «manifestamente obbligatoria» poiché utile come metodi di prova per dimostrare la conformità dei prodotti (pt. 79). Ed inoltre, andando oltre la questione oggetto della decisione, il Giudice europeo approdava inoltre alla considerazione generale secondo cui «una norma armonizzata è idonea a specificare diritti conferiti ai singoli nonché obblighi ad essi incombenti e tali specificazioni possono essere loro necessarie per verificare se un determinato prodotto o servizio sia effettivamente conforme alle prescrizioni di una siffatta legislazione» (pt. 82).

Concludeva così che nel caso di specie vi era un interesse pubblico prevalente di cui all'art. 4, par. 2, ultima parte di frase, del Reg. 1049/2001 che giustifica la divulgazione delle norme armonizzate richieste.

2.7.8 Considerazioni sulla natura delle norme armonizzate alla luce degli approdi giurisprudenziali della Corte di giustizia

Secondo l'ultima pronuncia, le norme armonizzate acquistano quindi i tratti della obbligatorietà e della trasparenza (accesso al pubblico), quando specificano diritti ed obblighi dei singoli. Tuttavia, come osservato dal CEN e CENELEC in un comunicato, la Grande Sezione non si è espressa sulla soggezione delle norme armonizzate al diritto d'autore, ma, contrariamente a quanto argomentato nelle conclusioni dall'Avvocato generale, non ha neppure prospettato una esclusione generale del diritto d'autore su tali norme[326].

La precisazione non è di secondario rilievo in quanto consente di approfondire il rapporto tra normazione tecnica (nel caso di specie normazione armonizzata) e ordinamento giuridico.

Come già evidenziato, tale rapporto è spesso oggetto di orientamenti interpretativi riconducibili alle tesi moniste che intendono assimilare la normazione tecnica a quella giuridica degli Stati, o dell'Unione europea (*infra* 2.3). Dall'altro si pone invece l'orientamento pluralista che invece riconosce capacità normativa anche a soggetti diversi dal legislatore, ossia ai privati.

Sebbene nelle pronunce della Corte di giustizia nei casi esaminati, nonché nelle conclusioni degli Avvocati generali, sia assista spesso ad argomentazioni a favore delle tesi moniste[327], le conclusioni dei giudici europei paiono sempre aderire alla tesi pluralista riconoscendo la giuridicità delle norme armonizzate nel solo caso di specie e in circostante determinate.

Ad oggi non vi sono state pronunce che equiparano la norma armonizzata, e neppure quella tecnica volontaria, ad un atto legislativo (perché non sono vincolanti, e perché il loro processo di formazione non è giuridico-politico come quello legislativo). Sempre per la giurisprudenza, è pacifico che la norma armonizzata i cui riferimenti siano stati pubblicati nella Gazzetta ufficiale dell'Unione europea, rientra nel diritto dell'Unione (caso *James Elliott*).

---

[326] CEN-CENELEC, *Copyright protection of Harmonized Standards not in question – however, there is an overriding public interest in their disclosure*, 5 Marzo 2024, reperibile al link:<https://www.cencenelec.eu/news-and-events/news/2024/brief-news/2024-03-05-ecj-case/>.

[327] Ne sono prova le considerazioni sul preminente peso della Commissione nella formazione delle norme armonizzate rispetto al ruolo degli enti di normazione europei, nonché la vincolatività *de facto* di tali norme data dal beneficio della presunzione di conformità dei prodotti o dei servizi alla disciplina legislativa per chi ne rispetta il contenuto.

Tuttavia, nella recente giurisprudenza il giudice europeo è andato a riconoscere i tratti della giuridicità di tali norme quando queste non svolgono un ruolo meramente accessorio e funzionale all'applicazione della disciplina legislativa, ma specifichino esse stesse diritti ed obblighi per i singoli. In quest'ultimo caso pare quindi che la distanza tra normazione tecnica e ordinamento giuridico si restringa conferendo alle prime alcuni tratti delle norme giuridiche.

Non possiamo escludere che questo scarto possa tendere a ridursi ancora di più in futuro, dato il sempre maggiore utilizzo della normazione tecnica non tanto per scopi di tipo economico-commerciali, quanto piuttosto per obiettivi di interesse sociale diffuso, tra cui anche quello alla cybersicurezza.

2.8 Gli organismi europei di normazione tecnica

L'armonizzazione e la standardizzazione delle norme tecniche hanno giocato un ruolo fondamentale nella costruzione del mercato unico europeo. A questo scopo, a partire dal ricordato "Nuovo approccio" del 1985, sono stati istituiti gli organismi di normazione europea per promuovere l'adozione di norme tecniche comuni in tutto il territorio dell'Unione. Questi organismi sono l'*European Committee for Standardization* (CEN), l'*European Committee for Electrotechnical Standardization* (CENELEC) e l'*European Telecommunications Standards Institute* (ETSI).

In particolare, per quanto riguarda il CEN e il CENELEC, si tratta di due associazioni belghe di diritto privato[328].

Circa i rapporti tra le istituzioni europee e tali enti, una certa dottrina ha già evidenziato che questi prendono spunto dal modello tedesco[329]. Difatti la Commissione europea ha concluso un accordo di cooperazione con il CEN e il CENELEC nel 1984[330], successivamente rinnovato ed esteso nel 2003 anche all'ETSI.

Si tratta di documenti ove emerge la strategia europea di coniugare nella normazione tecnica diversi interessi che non riguardano solo lo sviluppo e consolidamento del mercato unico ma anche la rappresentanza di interessi pubblici che rende le norme tecniche sempre meno neutrali e sempre più di rilevanza politica[331].

In particolare, secondo quanto stabilito nell'ultimo documento del 2003, viene previsto che «il sistema europeo di normalizzazione deve tener conto di tutti gli interessi: industria, lavoratori, consumatori, ambiente, poteri pubblici; di conseguenza, non può agire in base a interessi particolari»; fare in modo che gli interessi dell'Europa siano tutelati anche nell'ambito della normazione internazionale; e che il sistema di normalizzazione europeo risponda rapidamente e in modo adeguato alle diverse esigenze del mercato, ma sempre nell'osservanza dei principi di trasparenza, di accesso, di apertura, di efficacia, di coerenza e di volontariato[332].

---

328 A. ZEI, *Tecnica e diritto …op.cit.,* pp. 290 ss.

329 *Ibidem.*

330 L'accordo raggiunto nel 1984 è all'origine degli orientamenti generali per la cooperazione tra la Commissione europea, il CEN e il Cenelec, adottati il 13 novembre 1984 e pubblicati come parte 1 del *memorandum* CEN/Cenelec n. 4.

331 V. Orientamenti generali per la cooperazione tra il CEN, il CENELEC e l'ETSI e la Commissione e l'Associazione europea di libero scambio, del 29 marzo 2003 (2003/C 91/04).

332 *Ivi*, pt. 4. Si tenga inoltre conto di quanto riferito dalla parlamentare europea Barbara Weiler (PSE) nell'interrogazione scritta alla Commissione (P-2522/01) dell'11 settembre 2001, a proposito della normalizzazione tecnica di cui al link:<https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A92001E002522>.

Diversamente dagli organismi di normazione internazionale, notiamo quindi che, in virtù di tali accordi, le ESOs subiscono un forte condizionamento da parte della Commissione europea circa il perseguimento di principi di democraticità, nonché quelli tipici del procedimento amministrativo, ma nonostante ciò, ricordiamo che tali soggetti mantengono natura privata e il prodotto della loro attività resta volontario e non cogente (fino a quando non sia oggetto di incorporazione o rinvio da parte del legislatore).

a) L'*European Committee for Standardization* (CEN) e l'*European Committee for Electrotechnical Standardization* (CENELEC)

Nella presente sezione tratteremo dei due organismi europei di standardizzazione CEN e CENELEC, utilizzando lo schema espositivo già adottato per l'analisi degli organismi internazionali e italiani. Tuttavia, considerata la progressiva convergenza delle attività dei citati due organismi, nonché la similare organizzazione interna (rimarcata anche dagli stessi Statuti) abbiamo deciso di analizzarli in una trattazione unica il cui punto di vista sarà lo Statuto del CEN, riservandoci poi, nella sezione successiva (b), di analizzare nel dettaglio la disciplina delle rappresentanze sociali che trovano espressione nelle "*Partner Organizations*".

L'*European Committee for Standardization* (CEN) è stato fondato il 30 ottobre 1961 da un gruppo di rappresentanti di organismi di standardizzazione nazionali provenienti da diversi Paesi europei nell'ambito della Conferenza delle Commissioni nazionali per la normazione della Comunità economica europea e della zona di libero scambio a Parigi[333].

In un primo periodo, fino al 1970, il suo ruolo si limitava perlopiù alla presentazione di proposte per l'armonizzazione delle norme tecniche nazionali e alla redazione di documenti di "unificazione", volti a promuovere l'adozione volontaria del sistema di qualità basato sulle norme ISO.

L'*European Committee for Electrotechnical Standardization* (CENELEC) venne fondato nel 1973, ma la storia di questo organismo prende avvio già nel 1959, anno in cui venne fondato il CENELCOM su volere del Belgio, Paesi Bassi, Francia, Germania e Italia[334]. Nel 1960, i membri di CENELCOM insieme al Lussemburgo e ai paesi dell'AELS (in quel momento) Norvegia, Svezia, Danimarca, Regno Unito, Svizzera, Austria e Portogallo crearono la cooperazione CENEL per discutere gli standard IEC e per verificare, mediante questionari, fino a che punto questi standard venivano uniformemente implementati nei tredici paesi. Nel 1973, il CENEL e il CENELCOM si fusero dando origine al CENELEC. Successivamente altri paesi presero parte a questa Commissione, pare tuttavia interessante osservare come la maggior parte di questi Paesi abbia ancora una propria rappresentanza del CENELEC accanto all'organismo membro di CEN (nel caso dell'Italia il riferimento è al Comitato elettrotecnico italiano - CEI).

Il grande cambiamento avviene con l'emanazione della "Direttiva bassa tensione" del 1985, che ha reso i due organismi non più meri recettori e adattatori delle norme internazionali ma questi assunsero per la prima volta la funzione di provvedere essi stessi alla redazione di specifici standard europei.

---

[333] Cfr. A. ZEI, *Tecnica e diritto …op.cit.,* p. 292, nota 41.

[334] H.J. DE VRIES, *Governance of electrotechnical standardisation in Europe*, Rotterdam, 2015, pp. 20-21. Lo studio è reperibile al link:<https://repub.eur.nl/pub/78344/Metis_209630.pdf>.

L'attuale versione dello Statuto del CEN è del 2023[335], mentre quello del CENELEC è del 2021[336]. Come abbiamo anticipato, data la similità tra i due organismi, prenderemo in considerazione lo Statuto del CEN. Questo prevede innanzitutto che il Comitato è impegnato in una serie di attività, tra cui lo sviluppo di norme volontarie europee, il sostegno allo sviluppo e all'adozione delle norme internazionali e l'armonizzazione delle norme nazionali sostenendo l'adozione di norme europee e internazionali e il ritiro delle norme in conflitto[337].

L'Associazione è composta dai membri (ossia gli organismi di normazione nazionali[338]), dagli organi di governo (l'Assemblea Generale; il Consiglio Amministrativo; e il Comitato Presidenziale, il Direttore Generale; il Consiglio Tecnico; i Comitati Tecnici; e la Commissione di Appello) e dalle funzioni (il Presidente; tre Vicepresidenti; e il Presidente Eletto) e un organo di gestione nel caso di collaborazioni con il CENELEC[339], che prende il nome di CEN-CENELEC[340].

Tra questi, i Comitati tecnici sono gli organi responsabili della creazione delle norme tecniche, ma la loro disciplina è articolata nel relativo Regolamento interno[341]. Mentre nello Stato è regolato il Consiglio Tecnico che, nell'ambito delle politiche stabilite dagli Organi Corporativi pertinenti, è responsabile di decidere su tutte le questioni riguardanti l'organizzazione, le procedure di lavoro, la coordinazione e la pianificazione del lavoro normativo, nonché il monitoraggio e controllo dei progressi del lavoro normativo dei Comitati Tecnici, in stretta collaborazione con il Centro di Gestione CEN-CENELEC. Tra i poteri del Consiglio c'è anche quello di istituire o sciogliere gli organismi tecnici, come i Comitati Tecnici.

Il Regolamento parte 2, rubricato *Common Rules For Standardization Work*, prevede che i membri di un Comitato Tecnico sono costituiti dai Membri del CEN e/o del CENELEC, e normalmente, non più di tre rappresentanti di uno stesso Membro dovrebbero partecipare contemporaneamente a una riunione di un Comitato Tecnico[342]. Duranti tali lavori questi soggetti non sono esenti da responsabilità. In particolare, nel formare e informare la sua delegazione per la riunione presso un Comitato Tecnico, il Membro deve innanzitutto assicurarsi che «la delegazione trasmetta il punto di vista nazionale che tenga conto di tutti gli interessi che possano essere coinvolti dal lavoro»[343]. Sono

---

335 *The Statutes of CEN*, 2023 (d'ora in poi Stat. CEN). La documentazione del CEN può essere reperita dal sito ufficiale alla sezione "*reference documents*" di cui al link:<https:// boss.cen.eu/reference-material/refdocs/pages/>.

336 *The Statutes of CENELEC*, 2021. La documentazione del CENELEC può essere reperita dal sito ufficiale alla sezione "*reference documents*" di cui al link:<https://boss.cenelec.eu/reference-material/refdocs/pages/>.

337 Art. 5 Stat. CEN.

338 In particolare l'art. 7 Stat. CEN prevede che i Membri devono soddisfare i seguenti criteri: a) Adottare a livello nazionale le Norme Europee e ritirare norme nazionali in conflitto; b) Essere Membro (pieno o corrispondente) dell'ISO; c) Aderire ai principi di standardizzazione dell'OMC; d) Essere l'Organismo Nazionale di Standardizzazione di uno Stato UE/EFTA, con le seguenti relazioni: Membro Blu: SEE; Membro Rosso: EFTA (non Blu), o candidato all'UE; Membro Giallo: accordo con l'UE e convergenza regolamentare. 7.2 Un Organismo Nazionale di Standardizzazione candidato è ammesso se: Invia domanda al Direttore Generale; Conforma alle regole statutarie e interne; Ottiene il consenso dell'Assemblea Generale con tre quarti dei voti. 7.3 Non può esserci più di un Membro per paese. 7.4 L'ammissione è effettiva alla data fissata dall'Assemblea Generale.

339 Art. 6 Stat. CEN.

340 L'art. 24 Stat. CEN, prevede che il Centro di Gestione CEN-CENELEC, guidato dal Direttore Generale, è composto da personale dell'Associazione e di CENELEC necessario per gestire e sostenere l'ambito dell'Associazione e di CENELEC. Ha un ruolo attivo nella gestione quotidiana dell'Associazione ed è responsabile del collegamento e del dialogo con le istituzioni europee e le associazioni. L'organizzazione e la struttura del Centro di Gestione CEN-CENELEC rientrano nelle competenze del Comitato Presidenziale, come previsto nei Regolamenti Interni.

341 In questo caso il riferimento è all'Internal Regulations Part. 2, Common Rules For Standardization Work, July 2023 (d'ora in poi anche Int. Reg. 2).

342 Pt. 3.2.2 Int. Reg. 2.

343 Pt. 3.2.3.1 Int. Reg. 2.

inoltre stabiliti dei limiti di tempo per l'invio dei commenti nazionali sui documenti del Comitato Tecnico che devono essere osservati rigorosamente, in modo che, per quanto possibile, siano rispettati i tempi per la produzione della norma. Nell'eventualità di obiezioni e voti contrari, devono sempre essere fornite ragioni[344].

b) Le rappresentanze sociali nelle *Partner Organizations* del CEN e del CENELEC

Relativamente alla partecipazione delle rappresentanze sociali nei processi decisionali del CEN e/o del CENELEC, questa è regolata dalla disciplina delle "*Partner Organizations*", assetti in cui tali categorie possono trovare espressione.

Innanzitutto, il Regolamento interno 2 definisce tali *Partner* come organizzazioni settoriali indipendenti, europee o internazionali, con sede in Europa, nonché organizzazioni europee pan-settoriali che rappresentano, all'interno del loro ambito di competenza, un settore, un sottosettore o una categoria definita di portatori di interesse (ad esempio, PMI, consumatori, portatori di interessi sociali ed ambientali) e che hanno un interesse a cooperare a livello politico e tecnico generale con il CEN e/o il CENELEC.

Il citato Regolamento prevede inoltre che lo *status* di Organizzazione Partner deve essere concesso dall'Assemblea Generale del CEN e/o del CENELEC, e questo comporta per l'Organizzazione Partner la possibilità di designare un osservatore alle riunioni del Consiglio Tecnico, il quale svolgerà la sua funzione a titolo personale e con consapevolezza delle posizioni nazionali sul tema al fine di minimizzare il rischio di respingere la bozza di norma in una fase successiva[345].

Tuttavia, maggiori indicazioni sulla disciplina di tali Organizzazioni sono fornite nel *CEN-CENELEC Guide 25 "The concept of Cooperation with European Organizations and other stakeholders"*[346], il quale riconosce innanzitutto che tale forme organizzativa si adatta bene alle rappresentanze di interessi sociali (in particolare quelle coperte dall'Allegato III del Regolamento 1025/2012) «poiché hanno un interesse generale - o molto ampio - nel lavoro di CEN e CENELEC», ma, allo stesso tempo, anche «le organizzazioni legate al mondo degli affari con interessi significativi nella standardizzazione in settori multipli potrebbero anche trovare prezioso questo livello di partnership»[347].

Inoltre, oltre ai criteri già previsti dal Regolamento interno 2, la Guida prevede ulteriori condizioni affinché un'organizzazione possa costituirsi come *Partner* nei processi decisionali del CEN e del CENELEC, ossia che l'organizzazione:

- è in grado di rappresentare una parte molto significativa dei gruppi di interesse europei legati alla sua area di competenza definita, su tutto il territorio di CEN e CENELEC;
- è disposta e in grado di fornire in modo attivo contributi rilevanti al lavoro di uno o più organi tecnici di CEN e/o CENELEC nello sviluppo di norme o di altri deliverable tecnici;
- è disposta e in grado di contribuire attivamente, come appropriato, con contributi e proposte nel dialogo con gli organi aziendali di CEN e/o CENELEC e i loro gruppi di lavoro o *advisory*;
- è aperta all'adesione di organizzazioni nazionali adeguatamente qualificate nei paesi dai quali provengono i membri di CEN e CENELEC;

---

344 *Ibidem.*

345 Cfr. pt. 3.4.2 Int. Reg. 2.

346 CEN-CENELEC *Guide 25* (d'ora in poi CC G25). Il documento, nella sua ultima versione aggiornata al 2023, è reperibile sul sito ufficiale del CEN-CENELEC ove sono raccolte tutte le Guide, al link:<https://www.cencenelec.eu/european-standardization/european-standards/types-of- deliverables/cen-cenelec-guides/>.

347 Pt. 1.1 CC G25.

- ha un interesse legittimo nella standardizzazione europea in generale, o per quanto riguarda il settore/sottosettore della sua attività; Non svolge attività considerate in conflitto o in competizione con le attività di CEN e CENELEC;
- può sostenere in modo efficace e rappresentativo gli obiettivi di CEN e CENELEC attraverso il contributo dei suoi membri e delle loro organizzazioni interne, anche a livello nazionale[348].

La Guida prevede che le *Partner Organizations* possano prendere parte nelle procedure decisionali e delibere dei due organismi in diversi modi[349].

Possono riceve inviti a partecipare alle Assemblee Generali e alle riunioni aperte di alto livello, consentendo così all'Organizzazione di apprendere informazioni sulle principali questioni politiche e strategiche che influiscono sulle comunità di standardizzazione del CEN e/o CENELEC, nonché anche di contribuire attivamente al dibattito svolto durante tali incontri[350].

Oppure l'Organizzazione *Partner* può individuare la necessità di avere un dialogo su una questione di rilevanza politica e strategica. In tal caso, può inviare una richiesta per iscritto al Direttore Generale con una breve descrizione dell'argomento che desidera discutere con il Comitato Presidenziale. Dopo la conferma da parte del Presidente del Comitato Presidenziale, l'Organizzazione Partner interessata sarà invitata a presentare le proprie opinioni al Comitato Presidenziale e a contribuire al dibattito su tale questione. Altri gruppi di lavoro o *advisory* L'Organizzazione Partner può anche partecipare in qualità di osservatore a Gruppi di Lavoro, Gruppi Consultivi, *Task Force*, Piattaforme, ecc., di CEN, CENELEC o CEN-CENELEC, che trattano questioni di rilevanza politica e aziendale, qualora tale partecipazione sia prevista nei Termini di Riferimento del Gruppo pertinente o su invito del Presidente. La partecipazione a tali incontri avviene senza diritto di voto[351].

Infine, le Organizzazioni *Partner* ha accesso ai documenti dei Consigli Tecnici (*Technical Boards* - BTs) di CEN e/o CENELEC e partecipa in qualità di osservatore alle riunioni delle BTs[352].

La partecipazione di tali Organizzazioni nei corpi tecnici del CEN e/o del CENELEC è possibile solo in qualità di osservatori: *status* che può essere richiesto dall'Organizzazione in qualsiasi momento su cui prendono decisione i Consigli Tecnici dei due Enti, conformemente ai Regolamenti Interni e su consiglio dei corpi o gruppi tecnici interessati quando appropriato[353].

L'Organizzazione *Partner* beneficia di alcuni vantaggi in termini di informazioni quando partecipa nei corpi tecnici come:

a) l'accesso a documenti di lavoro e a inchieste pubbliche. In particolare, possono presentare commenti sui progetti di norme europee in fase di inchiesta pubblica, associati ai corpi tecnici per i quali è stata concessa la partecipazione. Inoltre, le Organizzazioni Partner che rappresentano consumatori, interessi ambientali e sociali nelle attività di standardizzazione europea e coperte dall'Allegato III del Regolamento 1025/2012, hanno anche il diritto di: presentare commenti su progetti di norme europee sottoposti ad approvazione formale, presentare pareri su progetti di norme europee sottoposti a inchiesta pubblica o presentati per approvazione formale.

[348] Pt. 1.3 CC G25. Da notare che la Guida fa espresso riferimento al concetto di "*legitimate interest*" nella standardizzazione europea.
[349] Cfr. pt. 1.2.1 CC G25.
[350] *Ibidem.*
[351] *Ibidem.*
[352] *Ibidem.*
[353] Cfr. pt. 1.2.2 CC G25.

b) In ogni caso, la partecipazione ai corpi tecnici del CEN e/o del CENELEC (sempre in qualità di osservatori), comporta per le Organizzazioni: assenza di diritto di voto; la possibilità di proporre documenti tecnici con l'obiettivo della loro possibile conversione in "*deliverables*"[354]; la possibilità di introdurre lavori preparatori a supporto delle attività di standardizzazione in corso; la possibilità di presentare contributi tecnici alle riunioni del corpo e per corrispondenza; la possibilità di formulare consigli sui programmi di norme attuali e futuri.

Tuttavia, è anche possibile che lo *status* di osservatore, e i relativi benefici da questo derivanti, possa essere revocato. Per motivi di efficienza nell'amministrazione delle attività del corpo tecnico, il Consiglio Tecnico può infatti richiedere al Presidente del corpo tecnico interessato di fornire valutazioni sul contributo dell'Organizzazione Partner. Se necessario, il Consiglio Tecnico si riserva il diritto di revocare la partecipazione dell'Organizzazione Partner in un corpo tecnico quando emerga chiaramente che l'Organizzazione Partner non stia contribuendo al lavoro corrispondente[355].

Infine, le Organizzazioni Partner saranno tenute al pagamento delle tasse annuali al fine di coprire i costi amministrativi legati alla partecipazione dei loro rappresentanti nei corpi del CEN e/o del CENELEC, nei loro gruppi di lavoro o comitati consultivi e nei lavori tecnici dei corrispondenti organi tecnici, il cui tariffario da applicare verso dette Organizzazioni è deciso annualmente dalle Assemblee Generali dei due Enti.

c) L'*European Telecommunications Standards Institute* (ETSI)

L'*European Telecommunications Standards Institute* (ETSI) è stata istituita nel Gennaio 1988 dalla Conferenza Europea delle Amministrazioni Postali e delle Telecomunicazioni (CEPT) in risposta alle proposte della Commissione Europea, relativamente allo specifico settore delle telecomunicazioni[356].

Diversamente dai primi due organismi di normazione europei, l'ETSI è stata quindi fondata dopo l'emanazione della Direttiva "bassa tensione" e dell'avvio al "Nuovo approccio" alla standardizzione, e su iniziativa dell'allora Comunità europea. In particolare, si tratta di un'associazione non profit di diritto francese istituita in conformità con la legge francese del 1° luglio 1901 e il decreto dell'16 agosto 1901.

Solo due anni dopo la sua fondazione viene siglato il primo accordo cooperativo tra le tre organizzazioni europee (1990), e nel 1994, su previsione della Direttiva 94/10/EC (che modificava la Direttiva 83/189/EC sulla procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche), l'ETSI, il CEN e il CENELEC sono ufficialmente riconosciuti come organizzazioni di normazione europea[357].

Il citato Regolamento 1025/2012, che ha sostituito la Direttiva 98/34/CE, ha poi ufficialmente confermato l'ETSI come organizzazione europea di normazione, potendo quindi essere incaricata dall'Unione europea di produrre norme e specifiche per soddisfare le esigenze politiche dell'Unione.

---

[354] Sul punto si rinvia alla sezione "*Type of Deliverables*", di cui al link:<https://www.cencenelec.eu/european-standardization/european-standards/types-of-deliverables/>.

[355] *Ibidem.*

[356] Tali informazioni possono essere reperite nella sezione "*About ETSI*" del sito ufficiale dell'Ente, di cui al link:<https://www.etsi.org/about>.

[357] Cfr. Allegato I, alla Direttiva 94/10/CE del Parlamento Europeo e del Consiglio del 23 marzo 1994 recante seconda modifica sostanziale della direttiva 83/189/CEE che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche.

Tutta la documentazione istituzionale dell'Organismo è raccolta all'interno delle "*Directives*", attualmente aggiornate alla versione del 2023[358].

Innanzitutto, come già anticipato, l'ETSI è competente nella normazione del settore delle telecomunicazioni a livello europeo. Lo Statuto specifica i settori ricompresi in tale attività[359], ossia: telecomunicazioni, ICT e altre reti e servizi di comunicazione elettronica; aree comuni a telecomunicazioni, ICT e altre reti e servizi di comunicazione elettronica e tecnologie dell'informazione in coordinamento con il CEN e il CENELEC; aree comuni a telecomunicazioni, ICT e altre reti e servizi di comunicazione elettronica e *broadcasting* (in particolare questioni audiovisive e multimediali) in coordinamento con CEN, CENELEC e l'*European Broadcasting Union* (EBU)[360].

L'Istituto contribuisce anche alla standardizzazione di tali settori anche a livello mondiale al fine di produrre e gestire la manutenzione degli standard tecnici e di altri risultati richiesti dai suoi membri, ed inoltre, l'ETSI è «aperto alla collaborazione con altre organizzazioni quando opportuno»[361]. Precisazione quest'ultima di non secondario rilievo se consideriamo che tra queste organizzazioni possono esservi anche quelle rappresentative di interessi generali che vedremo meglio a breve come possono prendere parte alle attività decisionali dell'Istituto.

Difatti lo Statuto prevede che sono membri dell'ETSI[362]: le Amministrazioni; le Altre istituzioni governative; le Organizzazioni nazionali di standardizzazione; il Gruppo delle Organizzazioni nazionali di standardizzazione (NSOG); gli Operatori di rete; i Produttori; gli Utenti; i Fornitori di servizi; gli Enti di ricerca; le Università; le Società di consulenza/partnership; e gli «Altri, a condizione che rispettino l'Articolo 3 sopra indicato», ossia le "altre organizzazioni menzionate"[363].

Tali membri possono partecipare in qualità di: membro effettivo; membro associato o membro osservatore. In particolare, quest'ultimo *status* può essere ottenuto dai richiedenti che soddisfano le condizioni per diventare membri effettivi o associati, ma scegliendo di non avere il diritto di partecipare pienamente alle attività dell'Istituto. Il requisito minimo comune è che tutti i membri dimostrino «il loro interesse nelle attività dell'Istituto e [accettino] di conformarsi alle Direttive ETSI e ad altre decisioni prese dall'Assemblea generale», ed inoltre tutti i membri godono del diritto di partecipare alle riunioni dell'Assemblea generale[364].

L'ETSI è strutturato in un'Assemblea generale, un Consiglio, il Gruppo di organizzazioni Nazionali di normazione, un'Organizzazione tecnica (composta da Comitati tecnici, Progetti ETSI e Progetti di partnership ETSI), Comitati speciali, Gruppi di specifiche industriali, Gruppi di sviluppo *software*, Gruppi di coordinamento e un Segretariato guidato da un Direttore generale[365].

---

[358] Queste possono essere accedute alla sezione "*ETSI Directives*" del sito ufficiale di cui al link:<https://portal.etsi.org/Resources/ETSI-Directives>.

[359] Art. 3 Statuto dell'ETSI (d'ora in poi Stat. ETSI).

[360] L'*European Broadcasting Union* (EBU) è l'alleanza leader a livello mondiale dei media pubblici. Con 112 organizzazioni membri in 56 paesi e 31 associazioni supplementari in Asia, Africa, Australasia e nelle Americhe. I membri EBU gestiscono quasi 2.000 canali e servizi televisivi, radiofonici e online, offrendo una ricchezza di contenuti su altre piattaforme. Per altre informazioni si rinvia al link ufficiale:<https://www.ebu.ch/home>.

[361] Art. 3 Stat. ETSI.

[362] Art. 6 Stat. ETSI.

[363] *Ibidem*.

[364] *Ibidem*.

[365] Art. 10 Stat. ETSI.

Tra questi poniamo attenzione sull'Organizzazione tecnica, quale articolazione dell'Istituto responsabile della «preparazione di standard e altri *deliverables* rilevanti dell'Istituto»[366] e la cui disciplina di dettaglio è contenuta nel "Rules of procedures", aggiornato alla sua versione del 2023[367]. Qui è previsto che l'Organizzazione tecnica è definita nelle Procedure tecniche di lavoro in modo tale da essere aperta e trasparente per tutti i membri ETSI, nonché per tutte le altre organizzazioni con cui l'ETSI mantiene relazioni di lavoro. Essa è supportata dal Segretariato, e l'Assemblea generale garantisce che questa sia mantenuta in linea con i requisiti dei membri ETSI per garantire una standardizzazione efficace, orientata al mercato e che l'Organizzazione tecnica sia in grado di rispondere alle esigenze normative basate sugli standard. In particolare, è stabilito che quando l'Organizzazione lavora in risposta a una richiesta di standard (SReq), «l'Assemblea generale dovrebbe prestare particolare attenzione all'interesse pubblico oltre agli obiettivi politici chiaramente indicati nella richiesta della Commissione Europea»[368].

Il medesimo documento fornisce inoltre la dettagliata disciplina delle procedure di formazione degli standards europei - cc.dd. European Norms (ENs) - (diverse da quelle prodotte su richiesta c.d. SReq, ossia le norme armonizzate), e degli standards e guide dell'ETSI.

Relativamente alle prime la procedura è scandita dalle fasi dell'"*EN Approval Process"* - ENAP, che possiamo distinguere in necessarie, quali: il periodo di *standstill*; l'inchiesta pubblica; l'istituzione della posizione nazionale per il voto per l'adozione o il ritiro di una EN (tranne quelle in risposta a una "*standard request*" - SReq); ed eventuali, ossia: la trasposizione nazionale delle EN sopra menzionate; o il ritiro nazionale delle stesse[369].

In particolare, relativamente all'inchiesta pubblica, tale fase è contemplata dal Regolamento come obbligatoria prima che un progetto di norma europea (EN) sia presentato per l'adozione. L'inchiesta è condotta dai membri del Gruppo degli Organismi Nazionali di Standardizzazione (NSOG) sotto la responsabilità del Direttore Generale, e gli «eventuali commenti ricevuti dai membri del NSOG e dalle Organizzazioni dell'Allegato III durante il periodo stabilito saranno attentamente presi in considerazione da ETSI»[370].

Procedura simile che l'Istituto adotta anche per l'elaborazione dei *deliverables* dietro richiesta della Commissione[371].

Per quanto riguarda i secondi, ossia gli standard e le guide ETSI, tali documenti sono redatti dai Comitati tecnici, dai Progetti ETSI, dai Comitati speciali o dai Progetti di partnership ETSI e, successivamente all'approvazione ove sono sottoposti al Direttore Generale per l'applicazione del processo di approvazione da parte dei membri, come stabilito nelle Procedure Tecnico-organizzative[372].

Tutti i membri effettivi e associati hanno il diritto di votare per l'adozione di tali documenti, e questi sono adottati per il loro uso in Europa se almeno il 71% dei voti ponderati espressi dai membri effettivi sono positivi e possono comunque essere ritirati con apposita procedura.

---

366 Art. 14 Stat. ETSI.

367 V. Rules of procedures -Version adopted by the Specially Convened Meeting of the General Assembly#82 (d'ora in poi Rul. Proc. ETSI). Si tratta di un documento contenuto nelle citate *Directives.*

368 Art. 6 Rul. Proc. ETSI.

369 Art. 13 Rul. Proc. ETSI.

370 Art. 13.4 Rul. Proc. ETSI.

371 Per la disciplina di dettaglio si rinvia all'art. 21 Rul. Proc. ETSI.

372 Art. 14 Rul. Proc. ETSI.

Altra procedura è inoltre prevista per l'elaborazione delle norme armonizzate (nel documento SReqs). In particolare, in questo caso il documento ci offre uno spaccato di dettaglio sul processo di formazione di tali norme. Prevede infatti che «[l]e bozze di SReq sono redatte dalla CE [Commissione europea] attraverso un processo di consultazione con un ampio gruppo di parti interessate, tra cui partner sociali, consumatori, piccole e medie imprese (PMI), associazioni industriali, organizzazioni europee di standardizzazione riconosciute (ESOs) e paesi dell'UE»[373].

Relativamente al coinvolgimento dell'ETSI, durante la redazione da parte della Commissione di una nuova SReq di interesse per l'Istituto, è previsto che la CE consulti e coinvolga l'ETSI nel processo per commentare e/o proporre modifiche al testo della bozza di SReq. Allo stesso modo, l'ETSI è responsabile del coinvolgimento dei suoi appropriati Gruppi tecnici, il Gruppo NSBG, il Gruppo NSOG e le Organizzazioni dell'Allegato III del Regolamento 1025/2012.

Al termine del processo di consultazione interna, ed elaborazione da parte della CE della bozza di lavoro della SReq, e prima della sua presentazione al Comitato per gli Standard (CoS) per l'approvazione, la CE faccia notifica all'ETSI, che a sua volta notificherà i suoi appropriati Gruppi Tecnici, il Gruppo NSBG, il Gruppo NSOG e le citate Organizzazioni dell'Allegato III.

Notiamo pertanto da subito come nei diversi processi di formazione poc'anzi tratteggiati - seppur brevemente - emerge il coinvolgimento delle c.d. rappresentanze sociali. Si tratta innanzitutto di un aspetto che è parte dei valori dell'Istituto[374], e dei principi generali a cui sono ispirate le procedure decisionali dell'ETSI[375].

Precisiamo inoltre che, dalla lettura della documentazione istituzionale, l'ETSI, diversamente del CEN e il CENELEC, si dimostra maggiormente aperta a favorire la partecipazione di tali soggetti che non è limitata solo a quelli indicati nell'Allegato III del Regolamento 1025/2012, ma anche agli "*users*" in generale. Questi sono espressamente ricompresi dallo Statuto tra i membri dell'ETSI e l'Annex I alle *Rules of procedures* li definisce come «Organizzazioni che utilizzano servizi nel campo delle comunicazioni elettroniche e settori correlati, il cui principale interesse nelle norme delle comunicazioni elettroniche è in tale capacità»[376]. Medesimo documento che prevede anche che in occasione della nomina di uno di Vicepresidenti «dovrebbe essere data preferenza a un candidato che rappresenti la categoria di membri Utenti se il Presidente non appartiene alla categoria Utenti»[377].

Tuttavia, come anticipato, le rappresentanze sociali sono ricomprese dei documenti istituzionali dell'Istituto nella categoria degli "*Others*" ove nello specifico, l'Annex I alle *Rules of procedures* vi colloca: il 3SI Advocate, ossia la persona nominata dalle Organizzazioni dell'Allegato III al Regolamento 1025/2012 per sostenere l'interesse comune dei loro rappresentanti ed esperti, e le Organizzazioni dell'Allegato III stesse[378].

---

[373] Art. 20.1 Rul. Proc. ETSI.

[374] Cfr. "*Technical standardisation"*, in ETSI Values, Version adopted by the Extraordinary Meeting of the General Assembly#81a, ove è previsto che i documenti ETSI sono progettati per sostenere il commercio e la connettività globali e promuovere una concorrenza leale, e questi rispondono alle esigenze di mercato e, se opportuno, ai requisiti normativi o alle esigenze della società. I documenti ETSI possono essere mezzi per sostenere specifici obiettivi normativi e politiche.

[375] Pt. 34 Powes and functions delegated to the board - Version adopted by the Ordinary Meeting of the General Assembly#81, ove sono prese in considerazione le «modalità per promuovere ulteriormente l'inclusività in ETSI con programmi e iniziative specifiche e consigliando l'Assemblea Generale e il Direttore Generale su modi per facilitare e massimizzare la partecipazione di tutte le parti interessate rilevanti, inclusi le PMI e gli attori sociali, nelle attività di standardizzazione».

[376] Pt. 1, Annex I Rul. Proc. ETSI.

[377] Art. 4.3 Rul. Proc. ETSI.

[378] Art. 5 Rul. Proc. ETSI. Altre definizioni ricomprese in questo articolo sono quelle di «Consensus: Un accordo generale, caratterizzato dall'assenza di opposizione sostenuta su questioni sostanziali da parte di una parte importante

Tuttavia, nonostante le garanzie di partecipazione delle rappresentanze sociali appena evidenziate, riteniamo che il sistema pecchi ancora di una profonda criticità di cui diremo nel successivo paragrafo.

2.9 Le criticità dei sistemi di normazione tecnica e la via europea

Ad un esame degli statuti, documenti e altre pubblicazioni prodotte dagli Enti di normazione sin qui analizzati di livello nazionale, europeo e internazionale, è possibile concludere, in linea generale, che il processo di normazione presso tali soggetti avvenga nel rispetto del principi dettati dall'Organizzazione mondiale del commercio (OMC) nel 2000[379], ossia: coerenza (gli standards coprono diverse discipline tecniche, è importante che sia assicurata la coerenza e la coesione tra queste), trasparenza e apertura (tutte le proposte di standard e gli standard in bozza vengono resi pubblici per i commenti prima che la versione finale venga pubblicata. Ogni obiezione deve essere discussa con la persona che l'ha sollevata), consenso (il contenuto degli standard è definito sulla base di un mutuo accordo), applicazione volontaria (gli standard non sono obbligatori), indipendenza da interessi particolari ed efficienza.

Di riflesso, le norme tecniche prodotte per mezzo di tali processo hanno quattro caratteristiche fondamentali: consensualità (sono approvate con il consenso di coloro che hanno partecipato ai lavori e costituiscono il risultato di una verifica tecnica professionale, e non di scelte di tipo discrezionale); democraticità (le parti economiche e sociali interessate possono partecipare ai lavori e di formulare osservazioni fino a quando la norma non sia stata approvata); trasparenza (gli organismi di standardizzazione segnalano le tappe fondamentali dell'iter di approvazione del progetto di norma, tenendolo a disposizione degli interessati); volontarietà (la loro osservanza non è obbligatoria).

Tuttavia, sebbene tali principi lascino ben sperare che il processo di formazione di queste norme, non giuridiche e prodotte da enti di natura privata, sia guidato da considerazioni e modelli di ispirazione giuspubblicistica, sono note le criticità evidenziate dalla dottrina, di cui ne abbiamo già avuto modo di argomentare, soprattutto in riferimento all'aspetto della partecipazione delle rappresentanze sociali a livello internazionale (*infra*, 2.9.1)[380].

Alla luce di ciò pare allora utile soffermarci sul modello che sta tracciando il legislatore europeo e per farlo riteniamo utile analizzare quanto sin qui trattato sulla normazione europea alla luce degli obiettivi politici affermati nel documento "Una strategia dell'UE in materia di normazione Definire

---

degli interessati e da un processo che cerca di prendere in considerazione le opinioni di tutte le parti coinvolte e di conciliare eventuali argomenti in conflitto. Il consenso non implica necessariamente l'unanimità. Counsellors: La Commissione europea (CE) e la segreteria dell'Associazione europea di libero scambio (EFTA). Capo della Delegazione Nazionale: La persona nominata da una Delegazione Nazionale, e notificata al Direttore Generale, per ricoprire il ruolo. Il Capo della Delegazione Nazionale deve essere scelto tra i rappresentanti delle organizzazioni che compongono la Delegazione Nazionale. Delegazione Nazionale: Il gruppo formato dai rappresentanti delle organizzazioni Full member registrate nello stesso paese. Organismo Nazionale di Standardizzazione: Un Organismo Nazionale di Standardizzazione che è elencato dalla CE nella Gazzetta Ufficiale dell'Unione Europea (OJEU). Gruppo NSB (NSBG): l'organo decisionale di ETSI composto dagli Organismi Nazionali di Standardizzazione. Gruppo NSO (NSOG): l'organo decisionale di ETSI composto dagli Organismi Nazionali di Standardizzazione, dai paesi CEPT, che hanno firmato l'Accordo ETSI-NSO».

[379] Si tratta di sei principi concordati dal Comitato TBT nel 2000 con l'obiettivo di guidare i Membri nello sviluppo dei processi di standardizzazione e sono reperibili alla pagina ufficiale dell'OMC al link:<https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm>.

[380] sul punto v. anche N. HACHEZ, J. WOUTERS, *A Glimpse at the Democratic Legitimacy of Private Standards: Assessing the Public Accountability of GlobalG.A.P.*, in *Journal of International Economic Law*, vol. 14, n. 3, 2011, pp. 677–710, reperibile al link:<https://doi.org/10.1093/jiel/jgr026>.

norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale" pubblicato dalla Commissione europea nel febbraio 2022[381].

Si tratta del documento da cui sono poi scaturite le modifiche e gli adattamenti del Regolamento 1025/2012 poc'anzi affrontati (*infra* 2.9.3), e da cui possiamo rintracciare la citata consapevolezza dell'Unione europea circa il valore politico e sociale delle norme tecniche. In tale occasione la Commissione ha infatti osservato che «[o]ggi più che mai le norme non possono limitarsi a trattare unicamente la questione dei componenti tecnici, ma devono anche integrare i valori democratici fondamentali e gli interessi dell'UE e i principi ecologici e sociali» - facendo inoltre specifico riferimento alla «dimensione strategica» delle norme in materia di cibersicurezza o resilienza delle infrastrutture critiche - e ritenendo pertanto opportuno che il sistema di normazione europeo delle ESOs rispetti e promuova i valori e gli interessi europei[382].

Tra queste la Commissione evidenziava preoccupazione circa i processi decisionali in seno all'ETSI, ove pare siano stati conferiti a determinati interessi societari un potere di voto non equilibrato: alcune multinazionali hanno infatti acquisito più voti degli organismi che rappresentano l'intera comunità dei portatori di interessi[383].

Maggiori dettagli sono forniti nella Relazione relativa all'attuazione del Regolamento 1025/2012 dal 2016 al 2020[384]. Dal documento emerge che, mentre nel 2017, gli organismi del CEN e CENELEC adottavano una modifica alla governance interna per cui le organizzazioni che non appartengono all'industria di cui all'Allegato III (ANEC, CES ed ECOS) possono presentare pareri formali sui progetti di norme (il cosiddetto "diritto di parere"), l'ETSI preferiva lanciare il "Programma 3SI" per coinvolgere le organizzazioni di cui all'Allegato III. Il programma prevede tavole rotonde con i funzionari dell'ETSI e un rappresentante dei soggetti interessati (il "3SI Advocate") all'interno dell'ETSI per discutere le questioni relative all'inclusività, ma senza il conferimento di un diritto formale di parere in capi ai primi[385].

In considerazione di ciò, nella Strategia la Commissione proponeva l'adozione di «principi amministrativi e di buona governance per le situazioni in cui le organizzazioni europee di normazione rispondono a richieste di normazione a livello europeo ed elaborano norme che saranno utilizzate per dimostrare la conformità a disposizioni giuridiche adottate nell'interesse dei cittadini dell'UE» e invitando le ESOs ad inviare alla stessa «entro la fine del 2022 proposte intese a modernizzare la loro governance».

Come già osservato (*infra* 2.9.3 a), questo obiettivo ha poi trovato concreta attuazione nell'obbligo per le organizzazioni di normazione europee di facilitare la rappresentanza e l'effettiva partecipazione di tutti i soggetti interessati - per la formazione di tutte le norme in generale siano esse armonizzate od europee - sebbene ciò «non comporta alcun diritto di voto per tali soggetti interessati, a meno che tale diritto di voto non sia previsto dal regolamento interno delle organizzazioni di normazione europee [enfasi aggiunta]»[386]. La *ratio* di tale limitazione ci è chiara. Le ESOs mantengono autonomia e indipendenza dalle istituzioni europee, e viceversa: gli Organismi europei di normazione possono rifiutarsi di adempiere ad una richiesta della Commissione; la Commissione dall'altra può decidere di

[381] Comunicazione, *Una strategia dell'UE in materia di normazione Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, COM (2022) 31 final, 2.2.2022.
[382] *Ivi*, p. 4.
[383] *Ivi*, p. 4-5.
[384] Relazione relativa all'attuazione del Regolamento (UE) n. 1025/2012 dal 2016 al 2020, COM (2022) 30 final.
[385] *Ivi*, p. 3. Tale scelta ha inoltre sollevato la diffusa insoddisfazione delle principali rappresentanze sociali.
[386] Cfr. cons. 23 Reg. (UE) 1025/2012.

non pubblicare la norma che ritiene non conforme ai requisiti dalla stessa dettati o quando questa sia contraria ai principi europei.

Dall'analisi dei documenti istituzionali dell'ETSI ci si sarebbe aspettati tuttavia una maggiore convergenza verso il modello adottato dal CEN e dal CENELEC, ossia l'adozione volontaria di strumenti (della ricordata *private administrative law*[387]) che assicurino maggiore democraticità nei processi decisionali, soprattutto sotto il profilo dell'effettiva partecipazione della società civile a tale processo[388].

Come già anticipato, le organizzazioni della società civile di cui all'Allegato III al Regolamento partecipano nell'ETSI come membri "user", e lo Statuto dell'Istituto nel riconosce la qualifica di *full member*, consentendogli quindi di partecipare ai lavori con gli stessi diritti degli altri membri.

Sulla scorta della citata strategia l'ETSI ha attuato diverse riforme alla sua governance. Già nel 2020 il Regolamento interno veniva modificato affinché una copia della bozza di norma matura fosse sistematicamente inviate alle organizzazioni rappresentative sociali, mentre nel 2023 veniva istituito il citato "programma 3SI". Si tratta di iniziative che hanno certamente contribuito ad avviare un dialogo più ravvicinato tra l'ETSI e le organizzazioni sociali, ma l'impressione è che non sia abbastanza.

Il mandato conferito al *3SI Advocate* risulta vago, impodendo a questo strumento di controbilanciare lo squilibrio che caratterizza il sistema di voto nell'ETSI.

Le decisioni dell'Istituto sono adottate all'unanimità dei partecipanti: ossia quando vi è il consenso di tutti e non vi sono opposizioni. Un primo limite a tal proposito riguarda il fatto che l'eventuale azione di contestazione può essere o meno ritenuta come opposizione al voto secondo l'interpretazione discrezionale dei Presidenti delle Commissioni.

Altro limite riguarda invece il caso in cui la contestazione sia riconosciuta come opposizione e in questo caso il processo decisionale prosegue secondo tre iter: i) il voto individuale ponderato, ii) il voto individuale ponderato da parte dei membri a pieno titolo, iii) il voto nazionale ponderato. In tutti questi casi le organizzazioni civili hanno a disposizione un voto ciascuna e pertanto la loro effettiva influenza nel processo decisionale è minima rispetto al peso del voto riconosciuto alle grandi imprese e gruppi industriali di settore che vi prendono parte[389].

Il dato è di particolare rilievo, non solo sotto il profilo giuspubblistico generale, ma anche per tutte le questioni in cui le garanzie di diritto pubblico trovano applicazione nel contesto delle ICT, data la competenza dell'Istituto.

A tal proposito pare allora d'interesse evidenziare come, in determinati settori, tra cui anche quelli dell'Intelligenza artificiale e di cybersicurezza (conformemente alla proposta di Regolamento *Cyber Resilience Act* di cui dopo), la Commissione ha il potere di adottare specifiche tecniche comuni mediante atti di esecuzione, per garantire la tutela dell'interesse pubblico nei casi in cui non vi siano norme armonizzate o quelle esistenti siano insufficienti[390]. Riteniamo pertanto che si tratti di un intervento "di forza" delle istituzioni dell'Unione che incide sul sistema di normazione tecnica per ragioni che trascendono gli interessi economico-commerciali.

---

[387] R. VALLEJO, *The private administrative law of technical standardization …op.cit.*

[388] A. VOLPATO, M. ELIANTONIO, *The participation of civil society in ETSI from the perspective of throughput legitimacy, Innovation*, in *The European Journal of Social Science Research*, 2024, reperibile al link:<https:// doi.org/ 10.1080/13511610.2024.2321852>.

[389] Ivi, p. 9 ss.

[390] Comunicazione, *Una strategia dell'UE in materia di normazione …cit.,* p. 5-6.

3 Il sistema di accreditamento

La parola "accreditamento" deriva da "credo", mentre "certificazione" proviene dalla parola latina *certus* che significa "certo", e quindi certificare significa "rendere certo" un qualcosa[391]. Accreditamento e certificazione sono due attività poste a supporto della normazione tecnica in quanto la certificazione indica che un prodotto, un sistema o una persona è conforme alla norma tecnica, l'accreditamento è invece una forma indipendente e autorevole di attestazione della terzietà, competenza, imparzialità e adeguatezza degli organismi di valutazione della conformità (organismi di certificazione, ispezione e verifica e laboratori di prova e taratura), che assicura quindi che l'organismo di certificazione abbia la credibilità e la competenza necessarie per condurre tale attività.

L'attività di accreditamento è disciplinata a livello europeo e internazionale, rispettivamente, dal Regolamento (CE) n. 765/2008 e dalla norma tecnica ISO/IEC 17011:2018 (la ISO/IEC 17025 si riferisce ai laboratori che svolgono attività di prova e taratura e non sarà trattata), e in Italia è svolta da Accredia, l'ente unico nazionale designato dal Governo.

Avremo modo di trattare all'interno del presente paragrafo l'analisi della disciplina appena menzionata, senza trascurare, seppur brevemente, alcune questioni dibattute in dottrina circa la natura degli organismi di accreditamento e dell'attività di accreditamento in sè.

3.1 Gli enti di accreditamento nel multilivello

Anche l'attività di accreditamento, così come quella certificazione, fortemente correlate alla normazione, sono volte a promuovere lo sviluppo e l'armonizzazione delle regole e procedure dei rispettivi sistemi di accreditamento e certificazione.

Considerati gli sviluppi della normazione tecnica, ciò significa che tale azione deve avvenire nel più ampio multilivello (internazionale, europeo e nazionale) attraverso strumenti di coordinamento e di garanzia dell'armonizzazione in tal senso.

Relativamente al primo profilo, sono presenti organismi di accreditamento nei tre paini considerati. Tra i principali enti di accreditamento a livello internazionale[392] troviamo sicuramente l'*International Accreditation Forum* (IAF), associazione mondiale degli Enti di accreditamento degli organismi di certificazione[393] e l'*International Laboratory Accreditation Cooperation* (ILAC), associazione mondiale degli Enti di accreditamento degli organismi di ispezione e dei laboratori di prova e di taratura[394], mentre a livello europeo è presente l'*European co-operation for Accreditation* (EA), l'associazione europea degli Enti di accreditamento degli organismi di certificazione, ispezione e verifica e dei laboratori di prova e taratura[395]. In Italia invece troviamo quale unico ente di

[391] Cfr. R.J. RUSHDOONY, *Accreditation and certification*, in Chalcedon Position, n. 5, 1979, p. 1.

[392] Altri enti sono l'*International Accreditation Service* (IAS), l'organizzazione di accreditamento internazionale con sede negli Stati Uniti, che fornisce servizi di accreditamento a diversi settori, tra cui costruzioni, sicurezza e industria manifatturiera (per ulteriori si rinvia al link:<https://www.iasonline.org/>); l'*Asia Pacific Accreditation Cooperation* (APAC), l'organizzazione che coordina l'accreditamento nella regione Asia-Pacifico, promuovendo il riconoscimento reciproco delle competenze tra gli enti di accreditamento della zona (per ulteriori si rinvia al link:<https://www.apac-accreditation.org/>); l'*Inter-American Accreditation Cooperation* (IAAC), lorganizzazione che coordina l'accreditamento nelle Americhe, promuovendo la cooperazione e l'accettazione globale delle competenze di accreditamento nella regione (per ulteriori si rinvia al link:<https://www.iaac.org.mx/index.php/en/>).

[393] Per ulteriori si rinvia al sito ufficiale di cui al link:<https://iaf.nu/en/home/>.

[394] Per ulteriori si rinvia al sito ufficiale di cui al link:<https://ilac.org/>.

[395] L'EA, la cooperazione europea per l'accreditamento, è un'associazione senza scopo di lucro registrata nei Paesi Bassi e formalmente designata dalla Commissione europea nel Regolamento (CE) n. 765/2008 per sviluppare e mantenere un

accreditamento su tutto il territorio l'Ente italiano di accreditamento (Accredia), quale associazione originariamente costituita dalla fusione di SINAL e SINCERT, ed ha lo scopo di adeguare il sistema di accreditamento italiano al Regolamento (CE) n. 765/2008.

Per quanto riguarda gli strumenti che consentono di garantire l'armonizzazione delle regole e procedure dei sistemi di accreditamento dal livello internazionale a quello nazionale troviamo gli Accordi multilaterali di mutuo riconoscimento (MLA) che vengono stipulati tra i diversi enti, al fine di garantire l'equivalenza e quindi l'accettazione delle attestazioni di conformità accreditate su scala europea e internazionale.

Tuttavia deve essere fatta una fondamentale distinzione. I membri dell'IAF e dell'EA, esclusivamente persone giuridiche singole o collettive, sono nella quasi totalità Organismi di accreditamento operanti nel c.d. settore volontario, ossia di conformità alle norme tecniche volontarie. Diverso è invece l'accreditamento svolto dalle pubbliche amminsitrazioni ed organi tecnici degli Stati che svolgono tale attività nel c.d. settore cogente, ossia il rilascio di autorizzazioni ad emettere attestazioni di conformità alle norme tecniche obbligatorie (c.d. regole tecniche)[396].

3.2 Il Regolamento CE 765/2008

Il 9 luglio 2008, l'allora legislatore comunitario ha emanato il Regolamento (CE) n. 765/2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti, al fine di stabilire norme comuni per l'accreditamento di organismi che assicurino la conformità dei prodotti non alimentari nell'Unione europea a determinati requisiti, e stabilendo i principi generali della marcatura CE. Precisiamo che per effetto del Regolamento (UE) 2019/1020, sono stati rimossi gli articoli del Reg. CE n. 765/2008 che in precedenza affrontavano aspetti legati alla vigilanza del mercato (collocati nel Capo III).

Come si apprende dal testo del Regolamento l'esigenza che intende soddisfare l'atto è quella di

> assicurare che i prodotti che beneficiano della libera circolazione dei beni all'interno della Comunità soddisfino requisiti che offrano un grado elevato di protezione di interessi pubblici come la salute e la sicurezza in generale, la salute e la sicurezza sul luogo di lavoro nonché la protezione dei consumatori, la protezione dell'ambiente e la sicurezza pubblica, assicurando che la libera circolazione dei prodotti non sia limitata in misura maggiore di quanto consentito ai sensi della normativa comunitaria di armonizzazione o altre norme comunitarie in materia [enfasi aggiunta][397].

In particolare, facendo chiarezza sulla natura dell'accreditamento, con tale intervento il legislatore comunitario ha previsto tra i principi generali di tale attività che «[q]ualora l'accreditamento non sia effettuato direttamente dalle stesse autorità pubbliche, gli Stati membri incaricano il proprio organismo

---

accordo multilaterale di reciproca riconoscibilità (l'EA MLA), basato su un'infrastruttura di accreditamento armonizzata. Attualmente, l'EA conta 49 membri. I membri dell'EA sono Organismi Nazionali di Accreditamento (ONA) ufficialmente riconosciuti dai rispettivi governi nazionali per valutare e verificare, secondo gli standard internazionali, le organizzazioni che svolgono attività di valutazione di conformità come certificazione, verifica, ispezione, prova e taratura. Le organizzazioni che verificano la conformità rispetto agli standard devono avere la competenza tecnica e l'integrità per svolgere tali servizi di valutazione. L'EA valuta i suoi membri, che sono Organismi Nazionali di Accreditamento, i quali a loro volta valutano organismi di certificazione e ispezione, laboratori di prova, laboratori medici e di taratura, nonché organismi di validazione e verifica. Se un Organismo di Valutazione di Conformità è accreditato da uno dei membri della rete EA, i suoi clienti possono avere fiducia nella competenza, indipendenza e imparzialità del lavoro di valutazione di conformità. Per ulteriori si rinvia al sito ufficiale di cui al link:<https://european-accreditation.org/>.

[396] A.L. FAZZARI, *Sistemi di gestione per la qualità*, Torino, Giappichelli, 2012, p. 26.

[397] Cons. 1, Regolamento (CE) n. 765/2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti (d'ora in poi Reg. CE 765/2008).

nazionale di accreditamento di effettuare l'accreditamento quale attività di autorità pubblica e gli conferiscono un riconoscimento formale [enfasi aggiunta]»[398]. Sul punto tornera tuttavia a breve.

Ai sensi del Regolamento sono inoltre definiti i concetti di «organismo nazionale di accreditamento» come «unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento»[399], e di attivita di «accreditamento» come «attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità»[400].

Tuttavia, il legislatore europeo ha anche contemplato l'ipotesi secondo cui qualora uno Stato membro decida di non fare ricorso al sistema di accreditamento, fornisca alla Commissione e agli altri Stati membri tutte le prove documentali necessarie per la verifica della competenza degli organismi di certificazione che sceglie per l'applicazione della normativa comunitaria di armonizzazione in questione[401].

I rapporti tra organismi di accreditamento e organismi di valutazione della conformità, nonché tra organismi di accreditamento nel territorio europeo (e non solo), deve essere ispirato al principio della non concorrenza[402]. A tal proposito, anche al fine di un miglior coordinamento, il legislatore comunitario ha previsto che ciascun organismo nazionale di accreditamento informa gli altri organismi nazionali di accreditamento circa le attività di valutazione della conformità relativamente alle quali esegue l'accreditamento e circa le modifiche di tali attività[403]. Inolre è riconosciuta la possibilità agli organismi nazionali di accreditamento di poter essere autorizzati a svolgere la loro attività oltre frontiera, sul territorio di un altro Stato membro[404].

Affinché un organismo nazionale di accreditamento possa operare in quanto tale, è tenuto a rispettare una serie di principi contemplati dal Regolamento[405], il cui rispetto è verificato mediante una

---

398 Art. 4, par. 5 Reg. CE 765/2008.

399 Art. 2, n. 11 Reg. CE 765/2008.

400 Art. 2, n. 10 Reg. CE 765/2008.

401 Art. 5, par. 2 Reg. CE 765/2008.

402 Art. 6, parr. 1 e 2 Reg. CE 765/2008.

403 Art. 12, Reg. CE 765/2008.

404 Art. 6, par. 3 Reg. CE 765/2008. In particolare ciò è possibile nelle ipotesi di cui all'art. 7 del medesimo ove è previsto, ai parr. 1 e 2, che «qualora chiedano l'accreditamento, gli organismi di valutazione della conformità si rivolgono all'organismo nazionale di accreditamento dello Stato membro in cui sono stabiliti o all'organismo nazionale di accreditamento al quale tale Stato membro è ricorso in conformità dell'articolo 4, paragrafo 2. Tuttavia, gli organismi di valutazione della conformità possono chiedere l'accreditamento ad un organismo nazionale di accreditamento diverso da quelli indicati nel primo comma in una delle seguenti situazioni: a) qualora lo Stato membro in cui sono stabiliti abbia deciso di non istituire un organismo nazionale di accreditamento e non sia ricorso all'organismo nazionale di accreditamento di un altro Stato membro in conformità dell'articolo 4, paragrafo 2; b) qualora gli organismi nazionali di accreditamento di cui al primo comma non effettuino l'accreditamento relativamente alle attività di valutazione della conformità per le quali viene chiesto l'accreditamento; c) qualora gli organismi nazionali di accreditamento di cui al primo comma non abbiano superato positivamente la valutazione inter pares ai sensi dell'articolo 10 relativamente alle attività di valutazione della conformità per le quali viene chiesto l'accreditamento. 2. L'organismo nazionale di accreditamento il quale riceva una richiesta ai sensi del paragrafo 1, lettera b) o c), ne informa l'organismo nazionale di accreditamento dello Stato membro in cui è stabilito il richiedente organismo di valutazione della conformità. In tali casi, l'organismo nazionale di accreditamento dello Stato membro in cui è stabilito il richiedente organismo di valutazione della conformità può partecipare come osservatore».

405 Art. 8, Reg. CE 765/2008, in particolare questi sono «[g]li organismi nazionali di accreditamento soddisfano le seguenti condizioni: 1) sono organizzati in modo che ne sia garantita l'indipendenza dagli organismi di valutazione della conformità da essi valutati, siano sottratti alle pressioni commerciali e non entrino in conflitto d'interesse con gli organismi di valutazione della conformità; 2) sono organizzati e gestiti in modo che sia salvaguardata l'obiettività e

particolare procedura di "valutazione *inter pares*", organizzata dall'*European co-operation for Accreditation* (EA), e per il quale gli Stati membri devono assicurare che i loro organismi nazionali di accreditamento vi si sottopongano regolarmente[406]. Tuttavia affinché si possano presupporre soddisfatte le prescrizioni cui sono sottoposti gli organismi nazionali di accreditamento, non è solo necessario che tali organismi superino con successo la valutazione *inter pares*, ma devono dimostrare anche la loro conformità ai criteri stabiliti nella pertinente norma armonizzata[407].

L'EA è il primo organismo riconosciuto ai sensi del Regolamento, in virtù della conclusione di un accordo con la Commissione europea[408]. Atto che assume quindi particolare rilievo, in quanto sottopone tale organismo al controllo e la direzione della Commissione europea che per via di questo «specifica dettagliatamente i compiti dell'organismo, le disposizioni in materia di finanziamento e le disposizioni relative alla sua vigilanza»[409]. Tuttavia, in quanto accordo, sia la Commissione, sia l'EA hanno la facoltà di risolvere l'accordo *ad nutum*, con un ragionevole periodo di preavviso definito nell'accordo stesso[410].

Inoltre la Commissione, previa consultazione del Comitato permanente in materia di norme tecniche composto da rappresentanti designati dagli Stati membri[411], può chiedere all'EA di contribuire allo sviluppo, al mantenimento e all'attuazione dell'accreditamento nella Comunità[412]. In virtù di tale procedura, la la Commissione può: a) chiedere all'organismo riconosciuto di codificare i criteri e le procedure per la valutazione inter pares e di elaborare programmi settoriali di accreditamento; b) accettare ogni programma di questo tipo eventualmente esistente che codifichi già i criteri e le procedure per la valutazione *inter pares*.

La Commissione assicura anche che i programmi settoriali individuino le specificazioni tecniche necessarie per soddisfare il livello di competenza richiesto dalla normativa comunitaria di armonizzazione nei campi in cui sono imposte prescrizioni specifiche in materia di tecnologia, salute e sicurezza o ambiente ovvero relative a qualsiasi altro aspetto della protezione dell'interesse pubblico.

---

l'imparzialità delle loro attività; 3) operano in modo che ogni decisione riguardante l'attestazione di competenza sia presa da persone competenti diverse da quelle che hanno effettuato la valutazione; 4) adottano disposizioni atte a salvaguardare la riservatezza delle informazioni ottenute; 5) individuano le attività di valutazione della conformità per le quali sono competenti a effettuare l'accreditamento, rinviando, se del caso, alle pertinenti legislazioni e norme comunitarie o nazionali; 6) istituiscono le procedure necessarie per assicurare l'efficienza della gestione e l'adeguatezza dei controlli interni; 7) dispongono di un numero di dipendenti competenti sufficiente per l'esecuzione adeguata dei loro compiti; 8) documentano le funzioni, le responsabilità e i poteri del personale che potrebbe influenzare la qualità della valutazione e dell'attestazione di competenza; 9) istituiscono, applicano e aggiornano procedure per controllare le prestazioni e la competenza del personale; 10) verificano che le valutazioni della conformità siano eseguite in modo adeguato, evitando oneri inutili per le imprese e tenendo debitamente conto delle dimensioni, del settore e della struttura delle imprese, del grado di complessità della tecnologia dei prodotti e del carattere di massa o seriale del processo di produzione; 11) pubblicano annualmente resoconti oggetto di revisione contabile, in conformità dei principi di contabilità universalmente accettati».

406 Art. 10, Reg. CE 765/2008.

407 Art. 11, Reg. CE 765/2008.

408 Art. 14, par. 6, Reg. CE 765/2008. Si faccia inoltre riferimento alle *General guidelines for the Cooperation between the European co-operation for Accreditation and the European Commission, the European Free Trade Association and the competent national authorities* (2009/C 116/04).

409 Art. 14, par. 2, Reg. CE 765/2008.

410 Art. 14, par. 2, Reg. CE 765/2008.

411 Si tratta del Comitato di cui all'art. 5 della Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche.

412 Art. 13 Reg. CE 765/2008.

3.3 La norma tecnica UNI CEI EN ISO/IEC 17011:2018

La norma ISO/IEC 17011 è lo standard internazionale fondamentale che delinea i requisiti generali per gli organismi che offrono servizi di accreditamento[413]. Pubblicato dall'*International Organization for Standardization* (ISO) e dall'*International Electrotechnical Commission* (IEC), questo standard, attualmente aggioranto alla versione del 2018, stabilisce criteri chiari e precisi che gli organismi di accreditamento devono seguire per garantire la competenza, l'imparzialità e l'affidabilità dei servizi che forniscono.

La norma pone alcuni principi fondamentali a garanzia dell'integrità del processo di accreditamento, e questi sono l'indipendenza, l'imparzialità, la competenza tecnica, la trasparenza e l'efficienza[414].

La norma dettaglia inoltre gli specifici requisiti che gli organismi di accreditamento devono rispettare per dimostrare la loro competenza e imparzialità nell'esecuzione delle attività di accreditamento. Ciò comprende la definizione di criteri per il personale[415], la gestione degli *audit*[416], la documentazione e la gestione dei reclami[417]. La norma fornisce inoltre orientamenti per la gestione degli accordi di mutuo riconoscimento tra gli organismi di accreditamento[418], agevolando così il riconoscimento reciproco dei risultati di accreditamento tra Paesi e promuovendo il commercio internazionale.

Tuttavia tali requisiti devono essere garantiti per tutto l'esercizio degli accreditatori. Sono infatti previste valutazioni periodiche e la sorveglianza degli organismi di accreditamento al fine di garantire il mantenimento degli standard di competenza e imparzialità nel tempo.

L'ISO/IEC 17011 è progettata per essere utilizzata in sinergia con altre norme ISO/IEC relative all'accreditamento, come la ISO/IEC 17025 per i laboratori di prova e taratura o la ISO/IEC 17020 per gli organismi di ispezione. Questa norma rappresenta quindi uno strumento fondamentale per garantire che gli organismi di accreditamento operino secondo standard elevati, contribuendo all'affidabilità e alla coerenza dei risultati di valutazione di conformità a livello internazionale.

3.4 La natura giuridica dell'accreditamento e degli enti accreditatori: alcune considerazioni alla luce della dottrina italiana e su Accredia

L'attività di accreditamento si caratterizza per un difficile inquadramento dal punto di vista giuridico. Il tema è stato a dire il vero poco esplorato dalla dottrina italiana, lasciando il passo alle chiarificazioni della giurisprudenza sul punto.

I nodi della questione attengono perlopiù la natura giuridica dei soggetti accreditatori, in quanto esercenti un ruolo di interesse generale, basti ricordare quanto già evidenziato a proposito del Regolamento CE 675/2008 circa l'obiettivo di tale attività di garantire «un grado elevato di protezione di interessi pubblici», nonché la natura giuridica dei loro atti, ossia l'accreditamento in sè.

Anche in questo caso, riteniamo che la questione sia stata oggetto di interpretazioni riconducibili al citato dibattito tra teorie moniste e teorie pluraliste già tratteggiato (*infra* 2.3).

---

[413] ISO/IEC 17011:2018 - Conformity assessment. Requirements for accreditation bodies accrediting conformity assessment bodies.

[414] Cfr. pt. 4.3, 4.4 e 4.5 ISO/IEC 17011:2018.

[415] Cfr. pt. 6, 6.1, 6.2, 6.3, 6.4 ISO/IEC 17011:2018.

[416] Cfr. pt. 5.7 ISO/IEC 17011:2018.

[417] Cfr. pp.tt. 7 ss. ISO/IEC 17011:2018.

[418] Cfr. pp.tt. 8 ss. ISO/IEC 17011:2018.

Secondo una certa dottrina[419], l'accreditamento, così come la certificazione, sono attività inquadrabili nella teoria degli "atti di certezza pubblica" con il quale il Giannini intendeva indicare «il contenuto di un atto che ha particolare autorevolezza perché promanante da pubbliche autorità, [il cui scopo] non è quello di fondare una verità, ma di fornire un'utilità che possa essere accettata, in quanto è plausibile che sia rispondente alla realtà»[420]. Distinti dagli di "certezza privata" con il quale il privato «non può istituire qualificazioni giuridiche che si impongano all'osservanza della generalità, e quindi non può creare certezze efficaci nei confronti di terzi [...]»[421].

Tuttavia gli enti di accreditamento (nonché anche quelli di normazione e di certificazione), non sono pubbliche autorità ma organismi di natura privata che svolgono, ai sensi del ricordato art. 4, par. 5 Reg. (CE) 765/2008, «attività di autorità pubblica», attribuitagli, perlomeno nel territorio euroepeo, in forza di un atto di diritto derivato.

Secondo Alcuni, tale circostanza risponde ad un modello del tutto consolidato di esercizio privato di pubbliche funzioni, ben noto nella dottrina classica giuspubblicistica, e che quindi non vi sono dubbi che l'attività di accreditamento, «costituisca espressione di un *munus* pubblico esercitato da un soggetto privato»[422]. Difatti tali riscostruzioni ritengono che il problema del soggetto, sia esso pubblico o privato, che svolge la funzione amministrativa di accreditamento è questione destinata a divenire recessiva rispetto alla natura oggettivamente pubblica delle funzioni esercitate, ovvero di contro, intrinsecamente privata ed affidata all'autonomia dei singoli[423].

Così, sulla scorta di tale criterio oggettivo, che tiene conto solo della natura della funzione esercitata, tale dottrina è allora proponsa nel ritenere che gli atti di accreditamento siano atti amministrativi, anche se posti in essere da privati nell'esercizio di pubbliche funzioni, senza escludere la concorrenza degli interessi privati con quelli pubblici[424], e in quanto tali soggetti al sindacato del giudice amministrativo.

Tali ricostruzioni non trovano tuttavia il conforto del dato reale, soprattutto della stessa giurisprudenza amministrativa. In particolare, le ambiguità interpretative sul punto, hanno portato Accredia nel 2016, sotto la direzione del Dott. Emanuele Riva, ad impostatare una riflessione organica su questo tema, costituendo a tale scopo un team di avvocati. Dal breve editoriale prodottto sulla scorta della ricerca, sono stati evidenziati dubbi e "punti fermi" sulla questione che riteniamo essere utili per definire i contorni dell'attività di accreditamento[425].

Innanzitutto, come si apprende dallo Statuto dell'Ente, anche nella sua ultima versione del 2021, Accredia è «un'Associazione senza scopo di lucro, ai sensi degli articoli 14 e seguenti del Codice Civile, che opera con il riconoscimento dello Stato e sotto la vigilanza istituzionale del Ministero dello Sviluppo Economico, nonché delle altre Pubbliche Amministrazioni che hanno contribuito alla sua designazione, secondo le rispettive competenze»[426] e, ai sensi del ricordato art. 4, par. 5 Reg. (CE) 765/2008, svolge «attività di autorità pubblica».

---

[419] A. MOSCARINI, *L'accreditamento nel Regolamento CE n. 765/2008 e le "fonti" di produzione privata*, in *Rivista di diritto alimentare*, n. 1, 2012, reperibile al link:<http://www.rivistadirittoalimentare.it/rivista/2012-01/MOSCARINI.pdf>.

[420] M.S. GIANNINI, voce *Certezza pubblica*, in *Enc. giuri*., vol. VI, p. 771.

[421] *Ivi*, pp. 774-775.

[422] Così A. MOSCARINI, *L'accreditamento nel Regolamento CE n. 765/2008 ...op.cit*., p. 6.

[423] *Ivi*, p. 2.

[424] *Ivi*, p. 3.

[425] Cfr. E. RIVA, *Natura giuridica delle attività di accreditamento*, Editoriale Accredia, 2016. Il documento è disponibile alla pagina ufficiale di Accredia al link:<https://www.accredia.it/2016/11/15/15-11-2016- una-riflessione -sulla-natura-giuridica-delle-attivita-di-accreditamento/>.

[426] Lo Statuto è disponibile al link:<https://www.accredia.it/documento/st-00-statuto-accredia/>.

Inoltre, in base all'attuale classificazione operata da ANAC sugli enti privati interessati alla normativa anticorruzione, Accredia risulta essere un ente partecipato (e non quindi un Ente sotto controllo pubblico) e, in quanto tale, è esonerata dal rispetto degli obblighi previsti dalla normativa anticorruzione per gli enti controllati dalla Pubblica Amministrazione, ma è comunque tenuta ad adottare su base volontaria una serie di protocolli di legalità connessi all'effettivo rischio di corruzione riferibile alla sua attività, sotto la vigilanza del MISE e ANAC[427].

La giurisprudenza amministrativa è tuttavia concorde nel ritenere «la nozione di servizio pubblico nel suo significato giuridico potenzialmente più vasto, [è] attività, di qualsiasi natura, connessa alla cura di interessi collettivi, sia essa svolta da Soggetti pubblici o privati».

La forzatura delle richiamate interpretazioni è infatti nella qualificazione pubblica dell'accreditamento che renderebbe quindi tali atti soggetti al sindacato del giudice amministrativo, secondo un'interpretazione fatta automaticamente discendere dal fatto che gli enti di normazione, anche se privati, svolgono una funzione pubblica.

Sulla questione si è espresso il Tribunale amministrativo del Lazio in una sentenza del 2016 ove il Giudice ha statuito che i rapporti tra l'Ente e i soggetti accreditati sono di natura contrattuale, difatti «l'accreditamento di Accredia non costituisce un provvedimento amministrativo», e che, comunque, alla revoca dell'autorizzazione (quale atto amministrativo) non segue automaticamente la perdita dell'accreditamento[428].

Tuttavia, tra autorizzazione ed accreditamento sussiste una relazione. Come argomentato in sentenza, «a seguito della designazione dell'Ente unico, i competenti Ministeri dello Sviluppo Economico e del Lavoro hanno conferito ad ACCREDIA apposita delega per la funzione di accreditamento (che costituisce il presupposto dell'autorizzazione) con Convenzioni stipulate il 13 e 22 giugno 2011, rinnovate nel 2013 [enfasi aggiunta]»[429].

Pare pertanto potersi concludere che la giurisprudenza amministrativa mantiene distinti il sistema di accreditamento, quale funzione pubblica svolta da privati, da quello di autorizzazione, espressione di un potere pubblico per mezzo di un atto giuridico. Tra i due atti vi è tuttavia un rapporto di presupposizione, ove l'atto presupposto, l'accreditamento, «rende possibile o doverosa l'adozione di un atto successivo o che, pur essendo richiesto per legge ai fini dell'adozione di un provvedimento successivo, eserciti comunque su di esso la propria influenza, assumendo le caratteristiche di antecedente logico», l'atto presupponente (o "successivo"), l'autorizzazione, è quello il cui contenuto viene investito dall'effetto condizionante del primo[430]. Ed in particolare la richiamata giurisprudenza ha ritenuto che alla revoca del secondo non consegua automaticamente la perdita dell'accreditamento, così come, secondo recente pronuncia del Consiglio di Stato, la perdita dell'accreditamento non comporta l'automatica revoca dell'autorizzazione, essendo quest'ultimo un'atto rimesso alle valutazioni dell'amministrazione pubblica[431].

---

[427] Sul punto si rinvia al *Piano triennale 2021/2023 per la trasparenza e l'anticorruzione allegato al modello organizzativo* di Accredia, di cui al link:<https://www.accredia.it/app/uploads/2018/10/Piano-triennale-trasparenza-e-anticorruzione-2021-2023_rev-15-10-2021.pdf>.

[428] T.A.R. Lazio, sez. I *ter*, 4 marzo 206, n. 2849, capo 4 in diritto.

[429] *Ivi*, capo 9 in diritto. Sul punto specifichiamo che il richiamato documento di Accredia prevede che tra i punti della sentenza vi sia anche l'affermazione che «l'atto di ACCREDIA può essere considerato un atto preparatorio non autoritativo ponendosi, rispetto a quello autenticamente provvedimentale, come presupposto». Tuttavia il virgolettato non è corretto poiché il Giudice non si è espresso in questi termini ma in quelli da noi riportati.

[430] Cfr. F. ANCORA, *L'individuazione dell'atto amministrativo presupposto*, in *Giur. Amm.*, 2009, p. 41.

[431] Cfr. Cons. Stato., sez. III, 21 ottobre 2020, n. 6371.

Pertanto, gli organismi di accreditamento sono soggetti che conservano la natura privata e i cui atti non possono essere considerati atti amministrativi. Questione che ha portato la dottrina ad interrogarsi sugli strumenti volti a «garantire che il perseguimento degli interessi rappresentati dagli organismi privati di produzione delle norme tecniche coincida effettivamente con l'interesse generale»[432].

L'esercizio di pubbliche funzioni pone infatti tali enti, e nel caso specifico Accredia, sotto un duplice controllo, sia *ex ante*, per via della vigilanza del Ministero delle Imprese e del Made in Italy, sia *ex post*, da parte del giudice civile, il quale è competente nelle controversie relative ai processi di certificazione ed accreditamento dato che interessano diritti soggettivi e non interessi legittimi.

Il richiamato documento di Accredia evidenzia inoltre anche un altro aspetto. Sebbene l'atto di accreditamento non sia un atto amministrativo, Accredia osserva le prescrizioni della Legge n. 241 del 1990 sui criteri ed i principi da del procedimento amministrativo, la quale trova applicazione anche nei confronti dei soggetti privati che operano in regime di pubblico servizio. L'Ente deve inoltre rispettare anche la norma tecnica ISO/IEC 17011[433]. Se non lo facesse, preferendo conformarsi solo ai principi richiamati dalla legge n. 241 del 1990, perderebbe il riconoscimento di EA, condizione essenziale per essere ritenuto Ente Unico nazionale di Accreditamento[434].

La conclusione è che la natura privatistica dell'Ente non si pone in contrasto con l'interesse pubblico al corretto svolgimento dell'attività di accreditamento, dato che il rispetto della normativa tecnica internazionale non contrasta con i principi del procedimento amministrativo

Inoltre, proprio al fine di un miglior perseguimento di obiettivi di interesse generale, oltre al recepimento delle indicazioni Anac e del Ministero vigilante, ha rafforzato, su base volontaria, il controllo interno, attraverso regole, lo studio di nuovi schemi di accreditamento e linee guida, al fine di conferire maggiore imparzialità e affidabilità al processo di accreditamento.

Quello del potenziamento delle procedure interne di tali soggetti privati (siano essi normatori, accreditatori o certificatori) con l'introduzione di meccanismi di ispirazione giuspubblicistica, su base volontaria, è un punto su cui torneremo anche più avanti.

4 Il sistema di certificazione

In termini generali, per certificazione si intende «l'attività di verifica e di accertamento del rispetto delle norme tecniche nei singoli prodotti, sistemi o servizi immessi sul mercato»[435] da parte di un organismo di certificazione (OdC) accreditato, relativamente ad un certo oggetto (prodotto, processo, servizio, persona o sistema) sottoposto a valutazione della conformità rispetto a requisiti contenuti in una norma tecnica o in un disciplinare specifico, eventualmente anche contenuti in una norma giuridica.

Il citato Regolamento 765/2008 definisce tale attività come «la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo siano state rispettate»[436].

---

[432] A. MOSCARINI, *L'accreditamento nel Regolamento CE n. 765/2008 ...op.cit.*, p. 15.

[433] E. RIVA, *Natura giuridica delle attività di accreditamento …op.cit.,* p. 4.

[434] *Ibidem.*

[435] G. CAIA, F.A. ROVERSI-MONACO, *Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *op.cit.*, p. 13.

[436] Art. 2, par. 1, n. 12 Reg. 765/2008.

Tuttavia, tale attività deve essere distinta tra certificazioni in senso proprio, ossia produttive di certezza legale, e certificazioni in senso improprio, produttive solo di certezza in senso informativo[437], come in questo caso.

La certificazione di un prodotto o di un servizio consente infatti di colmare le asimmetrie informative che secondo le teorie economiche ostacolano lo spontaneo funzionamento del mercato[438], in virtù del fatto che tali «meccanismi della "certezza" [...] consentono di ritenere veri determinati assunti "in via sostitutiva" rispetto a processi di verifica e di apprendimento personali»[439]. Si tratta pertanto di un attributo che caratterizza i processi di normazione e che acquista particolare rilevanza oggigiorno nei mercati globali.

La produzione di certezze è sempre stata una funzione dal carattere pubblico, propria dello Stato[440]. Tuttavia, il tempo e soprattutto con gli sviluppi del mercato e della tecnica, tale attività è stata sempre più affidata a soggetti professionisti di natura privata. In particolare a partire dagli anni Ottanta del secolo scorso, la certificazione diventa attività autonoma, e non più ausiliaria, rispetto a funzioni e atti della pubblica amministrazione[441]. Soprattutto la normazione comunitaria impone agli Stati membri di dismettere i compiti di certificazione (così come quelli di normazione e accreditamento) in favore di organismi privati, consentendogli tuttavia di conservare funzioni di indirizzo e supervisione[442].

Nonostante non esista ancora una disciplina generale sull'attività di certificazione[443], sia a livello interno, sia europeo, al giorno d'oggi possiamo distinguere due tipi di certificazione: obbligatoria e volontaria[444].

Le certificazioni obbligatorie (o cogenti) sono quegli attestati che riguardano i prodotti e servizi che rientrano nel campo applicativo di fonti giuridiche che impongono il rispetto di requisiti minimi variamente afferenti alla sicurezza, alla qualità o altre specifiche che tali prodotti o servizi devono garantire, le quali si ritengono presuntivamente rispettate se è stata raggiunta l'apposita certificazione.

Da queste si distinguono le certificazioni volontarie, o "di mercato", quale sistema interamente rimesso alla regolazione privata e vi è volontaria adesione degli attori di mercato a tali certificati[445].

---

[437] A. STOPPANI, voce *Certificazione*, in *Enc. dir.*, vol. VI, Milano, Giuffrè, 1960, pp. 799-800, secondo l'A. le certificazioni in senso proprio sono quelle che riproducono fatti già rappresentati, mediante un atto di certezza, in pubblico registro o in un documento ufficiale, mentre quelle improprie costituiscono il risultato di una attività di accertamento compiuta, prima della loro emanazione, da pubbliche autorità o da altri soggetti equiparati.

[438] Si rinvia si noti scritti di G.A. AKERLOF, *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism*, in *The Quarterly Journal of Economics*, vol. 84, no. 3, 1970, pp. 488–500, reperibile al link:<https://www.jstor.org/stable/1879431>; M. SPENCE, *Job Market Signaling*, in *The Quarterly Journal of Economics*, vol. 87, no. 3, 1973, pp. 355–74, reperibile al link:<https://www.jstor.org/stable/1882010> nonché J.E. STIGLITZ, *Monopoly, Non-Linear Pricing and Imperfect Information: The Insurance Market*, in *The Review of Economic Studies*, vol. 44, no. 3, 1977, pp. 407–30, reperibile al link:<https://www.jstor.org/stable/2296899>.

[439] A. BENEDETTI, *Certezza pubblica e certezze private: poteri pubblici e certificazioni di mercato*, Milano, Giuffrè, 2010, p. 26.

[440] U. BORSI, *Le funzioni del comune italiano*, in V.E. ORLANDO, *Trattato di diritto amministrativo italiano*, vol. II, Soc. ed. libraria, Milano, 1915, p. 225, ove l'A. evidenzia che la potestà pubblica di certificazione è espressione di una «discrezionalità non del dovere ma del conoscere». Sul punto v. anche G. SALA, *Certificati e attestati*, in *Dig. disc. pubbl.*, Utet, Torino, 1987, p. 538.

[441] E. BELLISARIO, *Certificazione di qualità e responsabilità civile*, Milano, Giuffrè, 2011, p. 16.

[442] *Ibidem.*

[443] Si ricorda infatti che il già menzionato Regolamento 765/2008 disciplina l'attività di accreditamento degli organismi di certificazione e non l'attività di certificazione.

[444] F. ANCORA, *Normazione tecnica, certificazione di qualità e ordinamento giuridico*, Torino, Giappichelli, 2000, pp.38 ss.

[445] A. GENTILI, *La rilevanza giuridica della certificazione volontaria*, in *Europa e dir. priv.*, 1999, p. 60.

Altra particolare categoria di certificazioni volontarie sono quelle regolamentate, con il quale l'autorità pubblica, sia essa nazionale od europea, elabora essa stessa un determinato sistema di certificazione indicando le norme tecniche di riferimento i prodotti e servizi, ma lasciando il loro rispetto alla libera adesione degli attori di mercato (è il caso del sistema di certificazione europeo di cybersicurezza che sarà analizzato in Parte III, Cap. III, 4.1.1).

L'obbligatorietà o meno della certificazione è quindi eventualmente determinata dal legislatore ma ciò non incide anche sulle modalità di selezione e qualificazione degli organi di certificazione.

Sia che si tratti del settore cogente o di quello volontario, il sistema resta comunque imperniato su un'autorità di accreditamento, responsabile dell'abilitazione degli organismi di valutazione della conformità, per l'appunto gli enti certificatori, i quali sono scelti dal soggetto che intende certificarsi, sia che questo abbia l'obbligo giuridico di raggiungere detta certificazione ovvero non ne sia gravato.

La pluralità di organismi di certificazione che opera sul mercato, permette la realizzazione di meccanismi di premialità o sanzionatori che inducono tali soggetti a conformarsi alle buone pratiche nell'esercizio delle loro funzioni, pena la revoca dell'accreditamento.

Pertanto, al pari della normazione tecnica e dell'accreditamento, anche la certificazione è un'attività svolta da soggetti privati che, per l'esercizio di detta funzione, sono tenuti a conformarsi ad altre norme di natura privata, la ISO/IEC 17021-1 (attualmente aggiornata alla versione del 2015)[446].

La procedura di certificazione è condotta alla luce di tale norma ove è articolata in diverse fasi. L'organizzazione deve aver predisposto la documentazione richiesta dalla norma tecnica per il quale si richiede la certificazione, oggetto di valutazione preliminare da parte dell'organismo di certificazione. In caso di esito positivo della documentazione fornita, l'organismo predispone il programma di audit, ossia il processo con il quale soggetti valutatori raccolgono evidenze sul luogo e valutano con obiettività gli elementi utili ad attestare l'effettiva implementazione della norma tecnica per il quale si chiede la certificazione.

I soggetti valutatori (*auditor*) possono tuttavia segnalare in tale sede eventuali "non conformità" dell'organizzazione ai requisiti della norma tecnica da certificare, che devono essere sanate prima della formulazione del rapporto finale.

Il rilascio del certificato avviene da parte dell'organismo di certificazione che, per mezzo di un organo interno composto da soggetti diversi da coloro che hanno svolto l'*audit* sul luogo, determina se alla luce del rapporto finale di valutazione (tenuto anche conto delle eventuali azioni sananti delle non conformità), attesta il rispetto dei requisiti della norma tecnica di cui l'organizzazione ha chiesto la certificazione.

Tale attività ha un necessario risvolto anche sul piano giuridico, stante il fatto che tra l'organismo di valutazione e l'organizzazione che intende certificarsi intercorre un contratto che, se inadempiuto potrà essere il presupposto per l'esercizio di poteri di sospensione o revoca del certificato. L'organismo di certificazione, sempre sulla base di accordi contrattuali, potrà infatti svolgere attività di verifica (c.d. *audit* di sorveglianza), per il rinnovo del certificato[447].

---

[446] ISO/IEC 17021-1:2015 Conformity assessment Requirements for bodies providing audit and certification of management systems.

[447] Sul punto v. ad esempio E. BIVONA, *Le certificazioni di qualità: vizi del prodotto e responsabilità dell'ente certificatore*, in *Contr. impresa*, 2006; M. STRUKUL, *La certificazione di qualità come strumento di tutela del consumatore. Profili contrattuali e di responsabilità*, in *Obbl. e contratti*, 2009; R. SAIJA, *Stanards e contratti di certificazione*, in *Riv. dir. alim.*, anno VII, n. 1, 2013, reperibile al link:<http://www.rivistadirittoalimentare.it/rivista/2013-01/SAIJA.pdf>.

Relativamente alla natura del certificato, la dottrina è concorde nel ritenere che si tratti di una fornte di certezza informativa, non legale[448], ma comunque di rilievo pubblico e facente fede fino a prova contraria, indipendentemente dal fatto che questa sia rilasciata da autorità pubbliche o soggetti privati[449].

[448] E. GARGALE, *Amministrazione Pubblica e privati nella certificazione di qualità dei prodotti industriali*, in *Informatica e diritto*, XIX annata, vol. II, n. 1, 1993, pp. 243-304.
[449] E. BELLISARIO, *Certificazione di qualità e responsabilità civile …op.cit.,* p. 44.

CAPITOLO II

QUALITÀ E SICUREZZA DELLE "COSE" NELLA NORMAZIONE E CERTIFICAZIONE TECNICA

SOMMARIO: 1. Introduzione - 2. La sicurezza delle "cose" a partire dalla definizione di attività di polizia amministrativa di Oreste Ranelletti e similitudini con il concetto di resilienza - 3. *Segue*. La relazione tra normazione tecnica e sicurezza

1. Introduzione

Nel capitolo II si è fatto riferimento alla cybersicurezza come forma di sicurezza mediata, in quanto persone fisiche-Stato-mercato possono essere sia vittime di azioni malevole o malfunzionamenti delle risorse informatiche, sia allo stesso tempo, beneficiari delle azioni di cybersicurezza e cyberesilienza da parte di attori pubblici o privati, sempre per il mezzo del cyberspazio (inteso nelle sue dimensioni logica e fisica).

Al capitolo I abbiamo invece introdotto il "cyberspazio merceologico", quale proposta di scomposizione e reinterpretazione di tale dimensione come insieme prodotti, servizi e processi appartenenti alle tecnologie dell'informazione e comunicazione (beni ICT) scambiati nel mercato, - per l'appunto "merci" - 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 originati per decisione degli stessi operatori di mercato.

Ciò ha consentito di individuare il legame tra il cyberspazio e il mercato liberalizzato, dettato da obiettivi comuni: 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. Ed è vero anche il contrario: possono infatti realizzarsi mercati chiusi, così come - pare astrattamente ipotizzabile - creare spazi digitali limitati, e non più globali, per volontà politica degli Stati[1].

Dal punto di vista della sicurezza, è evidente che l'esigenza di sicurezza "nel" e "del" cyberspazio non possa che realizzarsi prima di tutto attraverso la messa in sicurezza del complesso di beni ICT che compongono questa dimensione (o potremmo meglio dire "mezzo"[2]). Ciò porta a riflettere sul rapporto tra sicurezza e mercato, ed in particolare sulla soddisfazione dell'esigenza sicurezza non più garantita per esclusiva mano pubblica, ma anche attraverso il mercato ove, secondo Alcuni, si sono

[1] É il caso di RuNet, v. ad esempio M. RISTOLAIMEN, *Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West*, in *Journal of Information Warfare*, vol. 16, n. 4, 2017, pp. 113–31, reperibile al link:<https://www.jstor.org/stable/26504121>.

[2] Cfr. G. FINOCCHIARO, *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, vol. 17, 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».

originate forme di sicurezza complementare o partecipata, in virtù del principio di sussidiarietà orizzontale[3].

In questa sede ci soffermeremo sui tratti evolutivi della sicurezza delle "cose" tra ordinamento italiano ed europeo, al fine di meglio comprendere e contestualizzare la sicurezza dei beni ICT che sarà affrontata nel prossimo capitolo.

2. La sicurezza delle "cose" a partire dalla definizione di attività di polizia amministrativa di Oreste Ranelletti e similitudini con il concetto di resilienza

Nonostante l'irrompere di idee e innovazioni dello Stato liberale abbia comportato una drastica rottura con la precedente forma di stato, questo ha tuttavia conservato uno dei tratti dello Stato assoluto proprio nelle politiche di sicurezza ed in particolare nel fine di polizia. Come noto, la differenza è che nello Stato liberale l'ordinamento è connotato sulla garanzia delle libertà individuali piuttosto ché sul potere dell'autorità[4].

Secondo la dottrina italiana, confrontando l'amministrazione dell'assolutismo e quella liberale, il fine di polizia mantiene «una parziale identità nel significato più circoscritto di conservazione della sicurezza interna dello stato», quale elemento di continuità che caratterizzerà anche lo Stato costituzionale ove sopravvive il concetto di polizia[5].

Quest'ultima era intesa da Vittorio Emanuele Orlando, come parte integrante l'attività giuridica dello Stato e diretta espressione del potere sovrano[6].

Tale accezione sovrana sembrava tuttavia attenuarsi nell'analisi dell'attività dei Comuni italiani ed in particolare nell'erogazione dei servizi[7]. Altre dottrine interpretarono infatti la sicurezza anche come forma di prevenzione del prodursi di danni all'integrità fisica delle persone, la quale trovava espressione in diversi ambiti come nell'attività sanitaria, nel caso della vigilanza igienza e la polizia mortuaria, o nella vigilanza sulla salubrità delle attività economiche[8]. Medesima dottrina che ricomprendeva nella vigilanza generale di sicurezza diverse attività di controllo, ad esempio della statica degli edifici, la circolazione dei pedoni, il controllo sugli animali o sui velivoli.

La dottrina amministrativa andava così a individuare i tratti distintivi di tale attività[9]. In particolare, Ranelletti, distinguendo le diverse attività di polizia in giudiziaria, amministrativa e di sicurezza, definiva quest'ultima come quell'attività che

> protegge i vari interessi del tutto sociale e delle sue singole parti *direttamente e immediatamente* in quanto possono essere lesi dall'attività di una persona; difende cioè, direttamente ed immediatamente l'esistenza, la libertà, l'onore, ecc., dell'uomo, la vita, la funzione dello Stato, in breve tutti i diritti reali e patrimoniali

---

[3] A. BENEDETTI, *La sicurezza attraverso privati e la rilettura della nozione di ausiliarietà ai pubblici poteri*, in F. PIZZOLATO, P. COSTA (a cura di), *Sicurezza, stato e mercato*, Milano, Giuffrè, 2015, pp. 203 ss.

[4] M.S. GIANNINI, *Il pubblico potere*, Bologna, Il Mulino, 1986, p. 95.

[5] A. CHIAPPETTI, *Polizia (dir. pubbl.)*, in *Enc. dir.*, XXXIV, Milano, 1985, pp. 124-125.

[6] V.E. ORLANDO, *Introduzione al diritto amministrativo*, in *Primo trattato completo di diritto amministrativo italiano*, vol. I, Milano, Soc. ed. libraria, 1900, p. 71.

[7] A. BENEDETTI, *La sicurezza attraverso privati …op.cit.,* 206.

[8] U. BORSI, *Le funzioni del Comune italiano*, in *Primo trattato completo di diritto amministrativo italiano*, vol. II, Milano, Soc. ed. libraria, 1915, pp. 508 ss.

[9] Il riferimento principale è alla distinzione tra polizia amministrativa e polizia di sicurezza di cui v. S. ROMANO, *Il diritto pubblico italiano*, Milano Giuffrè, 1988v, pp. 300 ss.; E. PRESUTTI, *Polizia di pubblica sicurezza e polizia amministrativa*, in *Arch. giur.,* LXV, p. 1900; P. VIRGA, *La potestà di polizia*, Milano, 1954; G. CORSO, *L'ordine pubblico*, Bologna, 1979.

contro i pericoli che possono provenire immediatamente dall'attività umana, cioè da atti illeciti delle singole persone[10].

Mentre la polizia amministrativa era definita dalla magistrale dottrina come

> l'insieme di quelle attività di polizia, che sono immanenti ai singoli rami dell'amministrazione, e che servono alla difesa dei vari speciali interessi comuni, i quali vengono curati in questi singoli rami: essa mira ad assicurare determinati rami di attività dello Stato, e costituisce la funzione negativa per ogni ramo dell'amministrazione. Così si ha una polizia sanitaria come la polizia dell'amministrazione sanitaria, la polizia delle strade come la polizia dell'amministrazione delle strade ecc.[11]

Rannelletti individuava tuttavia un tratto di indipendenza di tale attività dai singoli rami dell'amministrazione. Difatti, secondo tale dottrina, la polizia amministrativa non ha solo valore accessorio rispetto ai singoli rami dell'amministrazione, ma in quanto la polizia è funzione essenziale dello Stato se «anche l'amministrazione non avesse una funzione diretta e positiva, non *curasse*, cioè, la sanità pubblica, non per questo verrebbe meno la poliza sanitaria. Anche là, difatti, dove l'amministrazione non *cura* l'edilizia, fuori, cioè, dal perimetro dell'abitato, in cui valgono prescrizioni dei regolamenti edilizi, resta egualmente la polizia ediliza»[12].

Alla luce di tali considerazioni, Raneletti sintetizzava allora

> osservando i campi nei quali agisce la polizia amministrativa si rivela subito che essa protegge i vari interessi del tutto sociale e delle singole, i quali si collegano con i vari rami dell'attività dell'ammministrazione pubblica solo *mediatamente*, cioè attraverso la protezione della esistenza, conservazione e funzione di una data cosa (strada, fiume, porto, abitazione, alimenti, ecc.). Provvedendo perché la cosa esista, sia conservata e funzioni bene, cioè limitando o regolando l'attività dei singoli, ed eventualmente, se è necessario, per mezzo della coazione, affinché la cosa risponda nella sua esistenza e nella sua funzione allo scopo, per quale esiste, essa tutela indirettamente e mediante tutti gli interessi che possono essere danneggiati o non soddisfatti da una cattiva esistenza o da una mala funzione della cosa medesima[13].

La polizia amministrativa era pertanto intesa come un'attività diretta alla sicurezza delle "cose", intese come «cose o atttività che hanno una funzione sociale [...]» ossia una funzione che «deve interessare la società, in modo da permettere a questa di raggiungere alcuni suoi scopi di conservazione o di perfezionamento, se funziona bene; e in modo da danneggiare o non soddifare la società medesima, se funziona male», tale per cui «[l]a funzione della cosa o l'attività, quindi, viene qui tutelata come un *fatto* sociale, non come un diritto»[14].

L'attività di polizia amministrativa così definita ci sembra quindi molto vicina a quella che oggi che è solitamente definita "resilienza" e di cui abbiamo già avuto modo di argomentare nella Parte II dell'elaborato.

La difesa dell'esistenza, dell'integrità e funzione delle "cose" «*al solo fine che queste cose, malamente esistendo o funzionando, non danneggino l'ordine giuridico esistente*»[15], non paiano infatti essere attività dissimili dalla capacità di un "sistema" di "resistere", "adattarsi", "riprendersi"

---

[10] O. RANELLETTI, *La polizia di sicurezza*, in V.E. ORLANDO (a cura di), *Primo trattato completo di diritto amministrativo italiano,* vol. IV, Milano, Soc. ed. libraria, 1904, p. 279. Per una interpretazione critica a tale orientamento si rinvia a A. CHIAPPETTI, *L'attività di polizia*, XXXIV, Cedam, Padova, 1973, pp. 122 ss.

[11] *Ivi*, p. 301.

[12] *Ivi*, p. 302.

[13] *Ivi*, p. 304.

[14] *Ivi*, p. 305.

[15] *Ivi*, p. 308, corsivo nello scritto.

alle "perturbazioni", "shock" o "crisi" in maniera tale da preservare la sua esistenza o la sua "continuità". Il ragionamento è pertanto che la garanzia dell'integrità, sicurezza e funzionamento dei beni, singolarmente considerati, è a sua volta condizione per la sicurezza della collettività o di un "sistema" considerato. Non è un caso se la proposta di Regolamento europeo sulla protezione dei beni (cose) ICT è anche nota come *cyber "resilience" act.*

Altra dottrina ha definito la polizia amministrativa in altri termini come «l'attività preventiva contro cause prevedibili dei turbamenti sociali qualunque ne sia la natura»[16], o anche come attività «diretta a prevenire i danni sociali che [...] possono derivare dall'attività privata»[17]. Secondo la maggioritaria dottrina liberale la polizia amministrativa si sarebbe quindi posta come attività preventiva, a volte imponendo il limite che non deve essere superato dai privati[18].

Oggi la nozione di polizia amministrativa vive quindi sotto altre forme. Con il passaggio allo Stato democratico, questa è stata infatti assorbita nell'ambito delle funzioni di gestione ordinaria che riguardano in un certo senso tutti i settori della vita sociale. Ulteriore tratto che quindi avvicina detta funzione a quella di "sistema" che viene spesso utilizzata per indicare l'oggetto su cui insistono le attività di resilienza. La dottrina ne individua alcuni nel settore sanitario, nell'assistenza pubblica, e nella tutela beni culturali, ma questa trasformazione si è realizzata anche in altri settori in cui questa si esplicava tradizionalmente come quello urbanistico, o anche la disciplina della produzione[19].

Ambito quest'ultimo in cui rientra non solo la disciplina della produzione in sé, come ad esempio i piani di programmazione economica, le concessioni di attività, gli orientamenti settoriali, ma anche la disciplina della fabbricazione, ossia a fasi particolari dell'attività di produzione, tra cui rientra la produzione standardizzata[20].

3. *Segue*. La relazione tra normazione tecnica e sicurezza

Nel precedente paragrafo si è individuata una continuità tra quella che la dottrina liberale ha definito polizia amministrativa, quale sicurezza delle "cose", e l'attuale concetto di resilienza. Inoltre, si è anche evidenziato come con il passaggio allo Stato costituzionale, tale attività di sicurezza, prima di derivazione pubblica e limitativa dei privati, viva oggi in attività tipiche dei privati che operano nel mercato, tra cui anche la produzione di norme tecniche.

Difatti durante lo Stato liberale, la ricordata sicurezza interna dello Stato, quale *proprium* delle attività di polizia, si manifestava anche attraverso la normazione tecnica, finalizzata alla salvaguardia dell'ordine, dell'igiene e dell'incolumità pubbliche, la cui produzione era essenzialmente affidata allo Stato, in particolare al Governo e alla pubblica amministrazione[21].

Come già anticipato, oggi queste norme sono prodotte da organismi di normazione, quali soggetti di natura privata i cui componenti sono perlopiù operanti nel settore di mercato della norma in questione. Il mercato si è quindi costituito come nuovo attore capace di fornire risposte alle domande di sicurezza.

---

[16] G.E. GARELLI, *Il diritto amministrativo italiano*, ed. VII, Torino, 1885, p. 212.
[17] S. ROMANO, *Principi di diritto amministrativo*, ed. II, Milano, 1906, p. 225.
[18] A. CHIAPPETTI, *L'attività di polizia …op.cit*., p. 126.
[19] A. CHIAPPETTI, *Polizia (dir. pubbl.) …op.cit.,* pp. 153 e 155-156.
[20] Cfr. M.S. GIANNINI, *Produzione (disciplina della)*, in *Enc. dir.*, XXXVI, Milano, 1987, pp. 1019 e 1021.
[21] F. SALMONI, *Le norme tecniche*, Milano, Giuffrè, 2001, p. 147.

Una certa dottrina si è tuttavia chiesta entro quali limiti possa allora essere prodotta la sicurezza secondo i meccanismi di mercato[22].

Riprendendo la distinzione tra polizia di sicurezza e polizia amministrativa poc'anzi introdotta, secondo tale ricostruzione la sfera della polizia di sicurezza è rimasta ancorata al potere pubblico, mentre la polizia amministrativa, quale forma di sicurezza riconducibile alle "cose", è stato l'ambito che ha visto il venir meno della riserva pubblica e lo sviluppo del mercato, al punto che oggi

> [l]'incolumità fisica delle persone che è riconducibile alla sicurezza delle cose passa dunque, in misura sempre maggiore, attraverso l'attività normativa ed esecutiva di soggetti privati qualificati, che competono nei mercati aperti e rispetto ai quali gli ordinamenti statali svolgono prevalentemente attività di controllo e/o di qualificazione[23].

Quella che nello Stato liberale era la c.d. attività di polizia amministrativa, sembra quindi trovare oggi continuità nella normazione tecnica sui processi produzione, e sulla fabbricazione di beni ed erogazione di servizi, i quali devono garantire i requisiti di qualità e sicurezza[24].

Pare tuttavia ragionevole chiedersi se in tale contesto, ove la norma tecnica parla il linguaggio del mercato piuttosto che quello del diritto, la sicurezza conservi gli stessi tratti della sicurezza giuridica.

Riteniamo che se la normazione nasce per rispondere all'esigenza di creare modelli di produzione uniformi, e la certificazione, invece, nasce per rispondere all'esigenza di riscontrare la conformità dei prodotti e dei sistemi produttivi a tali modelli, nella dimensione del mercato, la sicurezza assume allora da una parte il significato di certezza, di fiducia volta a favorire gli scambi (funzione del certificato), dall'altra, non potendo essere intesa come assoluta e quindi restrittiva di detti scambi, diventa «insicurezza sostenibile» per mezzo della disciplina di valutazione del rischio insita nella normazione tecnica[25].

---

[22] A. BENEDETTI, *La sicurezza attraverso privati …op.cit.,* p. 208.

[23] *Ivi*, p. 218. Secondo tale dottrina, tuttavia anche nell'altro ambito di sicurezza, che resta "fuori dal mercato", ossia la polizia di sicurezza (riconducibile alla sicurezza dei rapporti), i privati partecipano comunque a tale attività in via ausiliaria rispetto ai pubblici poteri, quindi attraverso partenariati, collaborazioni attive dal carattere complementare, nella definizione di compiti che nel campo della polizia di sicurezza restano intangibili (p. 222). Senza operare la suddetta distinzione tra le attività di polizia che sono state attratte o meno dal mercato, la dottrina risalente aveva già osservato l'avvicinamento tra le funzioni di polizia e la disciplina economica ritenendo che «l'attività di polizia nelle sue molteplici specificazioni (di sicurezza, sanitaria, igienica, urbanistica, sociale, ecc.), a volte incide in maniera tanto sensibile sullo svolgimento di attività economiche da poter in pratica trarre in inganno sulla sua "causa"» sul punto v. V. SPAGNUOLO VIGORITA, *Attività economica privata e potere amministrativo*, Napoli, Morano, 1962, p. 75.

[24] Cfr. G. VESPERINI, *Il controllo della "sicurezza" e della "qualità" …op.cit.*, p. 131. Sul punto v. anche A. CROSETTI, *"Stato di sicurezza" e controlli conformativi: la legge sulla prevenzione incendi n. 818 del 1984*, in *La gestione pubblica dell'economia* (contributi in materia coordinati da C. Ferrari), Milano, 1988, p. 15.

[25] Cfr. A. BENEDETTI, *Certezza pubblica e certezze private …op.cit.*, p. 26-27.

CAPITOLO III

LA NORMAZIONE E CERTIFICAZIONE TECNICA DI CYBERSICUREZZA TRA ITALIA E UNIONE EUROPEA

SOMMARIO: 1. Introduzione alla normazione tecnica nel settore delle ICTs - 2. La normazione europea e il settore ICT - 3. La standardizzazione di cybersicurezza tra *self* e *co-regulation* - 4. La normazione e certificazione europea di cybersicurezza - 4.1 Il *Cybersecurity Act*. Il sistema europeo di certificazione e valutazione di cybersicurezza - 4.1.1 *Segue*. L'*European Cybersecurity Scheme on Common Criteria* (EUCC) e il Regolamento (UE) 2024/482 - 4.2 La definizione dei requisiti essenziali di cybersicurezza e gli obblighi per gli attori della *supply chain* dei beni ICT nella proposta *Cyber Resilience Act* - a) I requisiti essenziali dei beni ICT e le norme armonizzate di cybersicurezza - b) Gli obblighi per gli attori della *supply chain* dei beni ICT in relazione ai livelli di rischio - c) La cybersicurezza dei consumatori: il ruolo del sistema di vigilanza del mercato e della Commissione europea - d) Indiscrezioni dal trilogo tra i colegislatori del dicembre 2023 - 4.3 La specializzazione degli enti di normazione europei nell'ambito della cybersicurezza - a) Il CEN-CLC/JTC 13 *Cybersecurity and Data protection* - b) L'ETSI TC *Cyber* - c) Gli enti di normazione di cybersicurezza diversi da quelli tradizionali - 5. Il controllo sul *procurement* informatico alla luce della disciplina sul Perimetro di Sicurezza Nazionele Cibernetica: il ruolo del CVCN - 5.1 Il Decreto legislativo del 3 agosto 2022 n. 123 e il ruolo dell'ACN nella certificazione rispetto ad Accredia - 5.2 Il sistema di certificazione italiano per motivi di sicurezza interna

1. Introduzione alla normazione tecnica nel settore delle ICTs

Nella Parte I è stato introdotto il concetto di cyberspazio "merceologico", inteso come complesso di beni, servizi e processi afferenti alle tecnologie dell'informazione e comunicazione (cc.dd. beni ICT) e abbiamo implicitamente inteso che tali "cose" fossero in qualche modo collegate al fine di consentire al cyberspazio di esistere (ossia di funzionare).

Ciò è reso possibile grazie all'interoperabilità dei tanti sistemi, reti, mezzi, applicazioni o componenti informatiche[1]. Tuttavia, affinché tale capacità trovi concreta realizzazione è necessaria l'elaborazione di comuni specifiche e interfacce, sotto forma di standard, che consentano di sviluppare e progettare beni ICT interoperabili in tutto il mondo. Nello specifico queste norme tecniche regolano diverse funzioni: descrivono metodi applicati nei *devices* elettronici e consentono

[1] L'Enciclopedia Treccani Informatica, ed. 2013 definisce l'"interoperabilità" come «[c]apacità di due o più sistemi, reti, mezzi, applicazioni o componenti di scambiare informazioni tra loro e di essere poi in grado di utilizzarle. In una società globalizzata che vede una sempre crescente diversità di sistemi e di applicazioni, l'i. rende possibile lo sviluppo di mercati e sistemi globali, prevenendo gli indesiderabili effetti della frammentazione; in stretta sintesi è la chiave di un sano sviluppo della globalizzazione. Essa può essere di tipo tecnico e/o di tipo concettuale. Quella di tipo tecnico è la più nota: basti pensare al mondo delle telecomunicazioni, al software e alla continua evoluzione dei sistemi di calcolo. L'impiego domestico delle tecnologie informatiche ci mette ogni giorno di fronte all'esigenza di i. fra i diversi sistemi di cui disponiamo. Quella di tipo concettuale fa invece riferimento al modo razionale con cui sistemi complessi, privati e pubblici, nazionali e sovranazionali, sono in grado di cooperare sinergicamente: per esempio le grandi strutture e agenzie di servizi (amministrazioni dello Stato a tutti i livelli, banche, assicurazioni, trasporti, ecc.). Un classico campo in cui si possono e si devono ormai coniugare contemporaneamente questi due tipi di i. è senza dubbio quello della difesa e della sicurezza. Le capacità operative che un paese deve esprimere in questo settore hanno una loro utilità ed efficacia soltanto nella misura in cui ogni forza armata sia in grado di esprimere capacità operative e tecnologiche di qualità, interoperabili con quelle delle collaterali forze armate e dei principali partner nazionali (si pensi all'azione di coordinamento compiuta dalla protezione civile in casi di emergenza) e alleati. Pertanto, in tale ambito si tratta non soltanto di i. tecnica, ma anche di standardizzazione delle dottrine e delle procedure [enfasi aggiunta]» (p. 618).

le connessioni tra reti, interfacce, e prodotti di diversi venditori, nonché coordinano le radiofrequenze e applicano la crittografia ai *software*, o consentono la trasmissione dati in Internet[2].

Ad esempio, si faccia riferimento ai vari protocolli di rete (o di comunicazione)[3]. Tra questi ricordiamo i più noti per lo scambio di dati via Internet, come il *Secure Sockets Layer* (SSL) e il *Transport Security Layer* (TLS), o quelli per la protezione dei *Web service Extensible Markup Language* (XML), tra cui *Web Services Security* (WS-Security), *XML Encryption* (XMLENC) e *XML Signatures* (XMLDSIG).

Se dal piano informatico passiamo a quello economico, ed in particolare tornando sulla natura di "merceologica" del cyberspazio, comprendiamo come l'interoperabilità sia possibile solo quando vi sia un approccio collaborativo dei produttori e sviluppatori nella realizzazione di tali norme tecniche[4]. Non solo. Oltre agli interessati alla normazione, particolare rilievo è assunto anche dai soggetti che dettano le specifiche in questo settore, che non sempre coincidono con gli organismi di normazione sin qui analizzati.

È il caso, ad esempio, dell'*Institute of Electrical and Electronics Engineers* (IEEE)[5], impegnato nei settori dei campi elettrici, elettronici e informatici, e l'*Organization for the Advancement of Structured Information Systems* (OASIS)[6], competente in diverse attività tecniche, nonché l'*European Computer Manufacturers Association* (ECMA)[7]. Ovvero, l'*Internet Engineering Task*

---

[2] O. KANEVSKAIA, *The law and practice of global ICT standardization*, Cambridge, Cambridge university press, 2023, pp. 14-15.

[3] L'Enciclopedia Treccani Informatica, ed. 2013 definisce il "protocollo di comunicazione" come «[i]nsieme di regole formali e di procedure che consentono di stabilire una connessione e mettere in comunicazione due o più entità, in particolare due apparati elettronici. Un p. di c. definisce le modalità per scambiare informazioni tra entità distinte - sovente non eterogenee, come computer o stampanti - e comprende regole di segnalazione, autenticazione, rilevazione e correzione di errori. [...] Un p. di c. definisce quindi l'insieme delle regole attraverso il quale creare, letteralmente, un linguaggio comune per il tramite di messaggi scambiati tra le apparecchiature, messaggi che devono potersi interpretare inequivocabilmente per funzionare correttamente [...]» (p. 958).

[4] H. TSILIKAS, *Collaborative Standardization and Disruptive Innovation: The Case of Wireless Telecommunication Standards*, in *IIC - International Review of Intellectual Property and Competition Law*, vol. 48, n. 2, 2017, pp. 151–178, reperibile al link:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2783372>.

[5] L'IEEE è un'organizzazione dedicata all'avanzamento dell'innovazione e all'eccellenza tecnologica a beneficio dell'umanità. È la più grande società tecnica e professionale del mondo. È progettata per servire i professionisti coinvolti in tutti gli aspetti dei campi elettrici, elettronici e informatici, nonché nelle aree correlate di scienza e tecnologia che sottendono la civiltà moderna. Le radici dell'Istituto risalgono al 1884, quando l'elettricità iniziò a diventare una grande influenza nella società. Per ulteriori si rinvia al link:<https://www.ieee.org/>.

[6] L'*Organization for the Advancement of Structured Information Systems* (OASIS) è stata fondata con il nome "SGML Open" nel 1993. Ha iniziato come consorzio di fornitori e utenti dedicato allo sviluppo di linee guida per l'interoperabilità tra prodotti che supportano lo *Standard Generalized Markup Language* (SGML). Il consorzio ha cambiato il suo nome in "OASIS" nel 1998 per riflettere una gamma più ampia di attività tecniche. Si rinvia alla pagina ufficiale di cui al link:<https://www.oasis-open.org/>.

[7] Si tratta di un'Associazione con sede a Ginevra fondata nel 1961 quando i dirigenti delle aziende più longeve nel campo dell'elaborazione dati in Europa (Compagnie des Machines Bull, IBM World Trade Europe Corporation e International Computers and Tabulators Limited) invitarono rappresentanti di varie aziende informatiche a una riunione. Durante l'incontro, fu deciso di formare un'associazione di produttori di computer chiamata ECMA. Un comitato fu incaricato di preparare la costituzione dell'associazione, redigere statuti e regolamenti. L'obiettivo principale era coordinare gli sforzi nel campo dell'informatica in Europa. Si rinvia al sito per ulteriori al link:<https://ecma -international.org/>.

Force (IETF)[8] e il *World Wide Web Consortium* (W3C)[9], quali organizzazioni internazionali impegnate nella produzione di standard di Internet.

Altro esempio sono i consorzi di produttori come la *Wi-Fi Alliance*[10], il *Liberty Alliance Project*[11] e la *Trusted Computing Group*[12].

Oppure le agenzie governative che producono standards come negli Stati Uniti il *National Institute of Standards and Technology* (NIST)[13], il *National Computer Security Center* (NCSC) britannico[14], o l'*Institute of Standardization of the State Science and Technology Commission* (oggi *National Institute of Standardization*) in Cina[15].

2. la normazione europea e il settore ICT

Nel paragrafo 2.9.1 (c) abbiamo già avuto modo di affrontare il tema delle ICTs nella normazione tecnica europea relativamente all'art. 13 del Regolamento 1025/2012 che consente alla Commissione di identificare le specifiche tecniche delle ICT cui è possibile fare riferimento negli appalti pubblici.

Considerato che molte delle più comuni specifiche in tale settore sono elaborate nell'ambito dei consessi e consorzi privati poc'anzi ricordati, il legislatore del 2012 ha preferito affidare alla

---

[8] L'*Internet Engineering Task Force* (IETF), è stata fondata nel 1986 ed è la principale organizzazione di sviluppo degli standard (c.d. SDO) per Internet. L'IETF crea standard volontari che sono spesso adottati dagli utenti di Internet, dagli operatori di rete e dai fornitori di apparecchiature, contribuendo così a plasmare la traiettoria dello sviluppo di Internet. Tuttavia, in nessun modo l'IETF controlla, o sorveglia, Internet. Per ulteriori si rinvia al sito ufficiale di cui al link:<https://www.ietf.org/>.

[9] Il *World Wide Web Consortium* (W3C) venne fondato da Tim Berners-Lee nel 1994 per garantire la crescita a lungo termine della Rete. Fin dall'inizio, il W3C è stata una comunità internazionale *multi-stakeholder* in cui organizzazioni membri, personale a tempo pieno e il pubblico lavorano insieme per sviluppare standard web aperti. Maggiori informarmazioni sono disponibili alla pagina ufficiale di cui al link:<https://www.w3.org/>.

[10] Il *Wi-Fi Alliance* nasce nel 1999 per volere di diverse aziende che si sono unite per formare un'associazione globale no-profit con l'obiettivo di migliorare l'esperienza dell'utente, indipendentemente dal marchio, utilizzando una nuova tecnologia di rete wireless. Il sito ufficiale può essere raggiunto dal link:<https://www.wi-fi.org/>.

[11] Si tratta di un consorzio globale sull'dentità fondato nel 2001 da circa 30 organizzazioni con l'obiettivo di sviluppare standard aperti tecnici, commerciali e sulla privacy per la gestione dell'identità federata. Vedi la pagina ufficiale di cui al link:<https://www.projectliberty.org/>.

[12] L'11 ottobre 1999 è stata costituita la *Trusted Computing Platform Alliance* (TCPA), un consorzio di varie aziende tecnologiche, tra cui Compaq, Hewlett-Packard, IBM, Intel e Microsoft, con l'obiettivo di promuovere la fiducia e la sicurezza nella piattaforma di elaborazione personale. Nel 2003, la TCPA è stata sostituita dal *Trusted Computing Group*, con un maggiore impegno sui dispositivi mobili. Per ulteriori si rinvia al link ufficiale:<https://trusted computinggroup.org/>.

[13] Il *National Institute of Standards and Technology* (NIST) è stato fondato nel 1901 ed è ora parte del Dipartimento del Commercio degli Stati Uniti. Il NIST è uno dei laboratori di scienze fisiche più antichi della nazione. Il Congresso istituì l'Agenzia per ragioni di competizione industriale rispetto alle capacità del Regno Unito, della Germania e di altri rivali economici. Vedi il sito ufficiale per ulteriori al link:<https://www.nist.gov/>.

[14] Lanciato nell'ottobre 2016, il NCSC ha sede a Londra e ha riunito competenze provenienti da CESG (il braccio per l'assicurazione dell'informazione di GCHQ), il *Centre for Cyber Assessment*, CERT-UK e il *Centre for Protection of National Infrastructure* (divenuto *National Protective Security Authority*, NPSA, nel marzo 2023). Vedi il link:<https://www.ncsc.gov.uk/>.

[15] L'Istituto Nazionale di Standardizzazione della Cina (noto come Istituto di Standardizzazione della Commissione per la Scienza e la Tecnologia dello Stato quando è stato istituito nel 1963) è direttamente subordinato all'Amministrazione Statale per la Regolamentazione del Mercato (SAMR). Come istituzione nazionale di servizio sociale dedicata alla ricerca sulla standardizzazione, si occupa principalmente delle questioni di standardizzazione a livello globale, strategico e completo nell'economia nazionale e nello sviluppo sociale della Cina. Sul punto si rinvia alla pagina ufficiale al link:<https://en.cnis.ac.cn/>.

Commissione europea - nel caso degli appalti pubblici - il ruolo di "selezionatrice" delle specifiche tecniche ICT ritenute dalla stessa conformi ai valori e principi europei.

Ciò, tuttavia, non significa che l'Unione rinunci alla promozione e allo sviluppo di norme tecniche europee in questo ambito. Nel 2011 infatti è stata istituita la Piattaforma multilaterale europea delle parti interessate sulla normalizzazione delle ICT (o *Multistakeholder Platform on ICT Standardisation* - MSP)[16]. Si tratta di uno strumento costituito da ampie rappresentanze: le autorità nazionali degli Stati membri e dei paesi EFTA, le organizzazioni di parti interessate rappresentanti l'industria, le piccole e medie imprese, i consumatori e altre parti sociali interessate nonché gli organismi europei e internazionali di normalizzazione e altre organizzazioni senza scopo di lucro che siano enti professionali, associazioni industriali o commerciali o altre organizzazioni associative attive in Europa che sviluppano standard nel settore delle ICT[17], al fine di assistere la Commissione su questioni riguardanti l'attuazione della politica di normalizzazione nel campo delle ICT.

Nello specifico, la piattaforma svolge perlopiù funzioni di consiglio e consulenza verso la Commissione europea circa diversi aspetti che interessano la normazione delle ICT[18], tra queste riteniamo d'interesse menzionare che l'MSP si occupa di «individuare potenziali future esigenze in tema di normalizzazione delle ICT a sostegno della legislazione, delle politiche e degli appalti pubblici in ambito europeo», nonché di «raccogliere informazioni sui programmi di lavoro delle organizzazioni che si occupano di elaborare le norme TIC al fine di concorrere al coordinamento ed evitare una inutile duplicazione o frammentazione degli sforzi»[19]. Il Centro comune di ricerca può inoltre fornire pareri scientifici e servizi nel proprio settore di competenza.

Relativamente al suo funzionamento interno, la piattaforma è presieduta dalle Direzioni generali di "Imprese e industria" e di "Società dell'informazione e media"[20]. Previo consenso del rappresentante della Commissione la piattaforma ha la facoltà di istituire sottogruppi per esaminare questioni specifiche, sulla base di un mandato definito dalla piattaforma stessa, i quali sono poi sciolti non appena espletato il mandato. Il rappresentante della Commissione può invitare esperti con competenze specifiche su argomenti all'ordine del giorno a partecipare al lavoro della MSP a seconda delle necessità. Il rappresentante della Commissione può inoltre conferire lo *status* di osservatore a persone fisiche o organizzazioni quali definite nelle regole orizzontali per i gruppi di esperti nonché a Paesi candidati all'adesione.

Nel 2016, sulla scorta del parere fornito dalla MSP, sono stati selezionati cinque "settori prioritari" relativi a elementi tecnologici essenziali del mercato unico digitale, ossia le comunicazioni 5G, il *cloud computing*, l'Internet delle cose (IoT), le tecnologie di dati e di big data e la cybersicurezza, verso cui l'Unione europea avrebbe dovuto dare priorità nella normazione delle ICT[21]. Come si comprenderà tali tecnologie sono ancora oggi al centro di diverse normative europee, mentre altre, allora ancora non considerate, se ne sono aggiunte, come l'intelligenza artificiale.

Per quel che qui interessa ci concentreremo sulla normazione tecniche nell'ambito della cybersicurezza, ma prima, come sarà argomentato nei prossimi paragrafi, occorre analizzare cosa

[16] Decisione, che istituisce la piattaforma multilaterale europea delle parti interessate sulla normalizzazione delle tecnologie dell'informazione e della comunicazione (TIC), 28 novembre 2011, 2011/C 349/04 (d'ora in poi Dec. MSP).
[17] Art. 4 Dec. MSP.
[18] Artt. 2 e 3 Dec. MSP.
[19] Cfr. art. 2, lett. c) ed h) Dec. MSP.
[20] Art. 5 Dec. MSP.
[21] Comunicazione, *Priorità per la normazione delle ICT per il mercato unico digitale*, 9 aprile 2016, COM (2016) 176 final.

significa regolazione tecnica per l'ordinamento europeo, ed in particolare come si pone la regolazione tecnica europea di cybersicurezza nel più ampio contesto internazionale.

3. *Self* e *co-regulation* nella standardizzazione di cybersicurezza

In precedenza abbiamo avuto modo di introdurre brevemente alcuni aspetti di *governance* del cyberspazio (*infra* Parte I) caratterizzati dalla 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[22].

Come rileva una certa dottrina di diritto internazionale dell'economia, tale contrapposizione di assetti 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*[23].

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)[24].

E' il caso del *Cybersecurity Framework* (CSF), sviluppato dal *National Institute of Standards and Technology* (NIST) degli Stati Uniti nel 2013[25], e il cui ultimo aggiornamento è atteso per il 2024[26], il quale costituisce una "regola" volontaria di riferimento anche in altri Paesi[27]. 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[28].

La predetta distinzione, tuttavia, non è sempre così agevole, soprattutto perché *top-down* e *bottom-up* sono due concetti che indicano da quale parte proviene l'iniziativa regolamentare (dai governi la

---

[22] M. RAYMOND, L. DENARDIS, *Multistakeholderism: anatomy of an inchoate global institution*, in "International Theory", 2015, pp. 572–616.

[23] S.Y. PENG, *Private Cybersecurity Standards: Cyberspace Governance, Multistakholdersim, and the (Ir)Relevance of TBT Regime*, in *Cornell International Law Journal*, 51, n. 2, 2018, pp. 445-470.

[24] S.J. SHACKELFORD, S. RUSSELL, J. HAUT, *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks*, in *UC Davis Business Law Journal*, n. 16-2, 2016.

[25] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 febbraio 2014.

[26] M. TEPLINSKY, *A Review of NIST's Draft Cybersecurity Framework 2.0*, in *LawFare*, 13 settembre 2023.

[27] Per quanto riguarda l'Italia si rinvia al *Framework Nazionale per la Cybersecurity e la Data Protection* elaborato dal CIS-Sapienza Research Center of Cyber Intelligence and Information Security Sapienza Università di Roma e il CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica, reperibile nella sua ultima versione 2019 al link:<https://www.cybersecurityframework.it/>, il quale è stato elaborato sulla base del *Cybersecurity Framework* sviluppato dal NIST (p. 8).

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

prima, dai privati la seconda) e questa può accomunare tanto i modelli di regolazione spontanea privata, ossia la *self-regulation*, sia anche quelli a partecipazione pubblico-privata di co-regolazione[29].

La regolazione privata e la coregolazione sono considerate dall'ordinamento dell'Unione come forme di "regolazione alternativa" rispetto a quella tradizionale (o "di base") del legislatore europeo. I due concetti sono infatti parte delle politiche sulla "Migliore regolazione"[30] europea che ha trovato concreta applicazione per mezzo di accordi interistituzionali ex art. 295 TFUE, di cui il più recente del 2016, le linee guida del 2021 e un *toolbox* del 2023, entrambi emanati dalla Commissione europea[31].

Tuttavia, per avere una migliore panoramica sul punto, occorre tornare al previo accordo interistituzionale del 2003, ove è stato evidenziato che, conformemente ai Trattati istitutivi, il ricorso a forme di regolamentazione diverse da quelle tradizionali è possibile solo, in virtù dei principi di sussidiarietà e di proporzionalità, ove opportuno, e qualora i Trattati non prescrivano specificamente il ricorso a un determinato strumento legislativo[32].

Anche qualora il ricorso a detti strumenti sia possibile, la Commissione si assicura che questi siano sempre conformi al diritto europeo e rispettino i criteri della trasparenza (con particolare riguardo alla pubblicità degli accordi) e della rappresentatività delle parti interessate[33]. Sono inoltre fissati anche dei limiti inderogabili, secondo cui tali meccanismi non possono trovare applicazione «se sono in gioco i diritti fondamentali o scelte politiche importanti, oppure nelle situazioni in cui le regole devono essere applicate uniformemente in tutti gli Stati membri»[34].

Fatte queste premesse generali, l'accordo definiva la coregolamentazione come «il meccanismo mediante il quale un atto legislativo comunitario conferisce la realizzazione degli obiettivi definiti dall'autorità legislativa ai soggetti interessati riconosciuti in un determinato settore (in particolare agli operatori economici, alle parti sociali, alle organizzazioni non governative o alle associazioni)»[35]. Si tratta quindi di uno strumento di cui le istituzioni europee conferiscono il suo ricorso al fine di alleggerire il lavoro legislativo, concentrandolo sugli aspetti essenziali e beneficiare dell'esperienza dei soggetti interessati, i quali tuttavia devono attenersi ai criteri definiti nell'atto legislativo in questione ("di base").

---

[29] Così T. TROPINA, C. CALLANAN, *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Springer Cham, 2015, pp. 35 ss., ove gli AA. osservano che «No government can expect "pure" bottom-up approaches in the complex environment. In contrast, "voluntary" does not always mean coming from the industry without any governmental participation. The true collaboration requires efforts and financial contributions from both parties». A tal proposito, per uno studio sulle diverse varianti di *self* e *co-regulation* tra approccio *top-down* e *bottom-up* si rinvia a A.J. SENDEN, E. KICA, K. KLINGER, M.I. HIEMSTRA, *"Mapping Self-and Co-regulation Approaches in the EU Context": Explorative Study for the European Commission, DG Connect*, Utrecht University, RENFORCE, 2015, pp. 31 ss., lo studio è reperibile al link:<https://dspace.library.uu.nl/handle/1874/327305>; nonché, sugli aspetti di legittimazione delle forme di co-regolazione nell'ordinamento europeo si rinvia a P. VERBRUGGEN, *Does Co-regulation Strengthen EU Legitimacy?*, in *European Law Journal*, 2009, pp. 425-441, reperibile al link:<https://cadmus.eui .eu/handle/1814/ 13457>.

[30] Si rinvia alla pagina ufficiale della Commissione europea di cui al link:<https://commission.europa.eu/law/ law-making-process/planning-and-proposing-law/better-regulation_en>.

[31] I due documenti sono reperibili alla pagina ufficiale al link:<https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en>.

[32] Progetto interistituzionale "Legiferare meglio", 2003/C 321/01, pt. 16.

[33] *Ivi*, pt. 17.

[34] *Ibidem*.

[35] *Ivi*, pt. 18.

Come si comprenderà tale atto assume particolare rilievo, dato che al suo interno sono definiti gli obiettivi da raggiungere e i criteri essenziali, mentre la loro realizzazione è rimessa alla discrezionalità dei soggetti interessati[36]. L'atto legislativo di base indica infatti «l'ampiezza possibile della coregolamentazione nel settore interessato»[37]. L'autorità legislativa è responsabile, a monte, dei controlli sullo stesso poiché questa è competente a definire all'interno dell'atto misure appropriate per la verifica della sua applicazione, con riguardo all'ipotesi dell'inosservanza dell'accordo ad opera di una o più parti o dell'insuccesso dell'accordo stesso[38].

L'autoregolamentazione è invece definita come «la possibilità lasciata agli operatori economici, alle parti sociali, alle organizzazioni non governative o alle associazioni, di adottare tra di loro e per sé stessi orientamenti comuni a livello europeo (in particolare codici di condotta o accordi settoriali)»[39].

Come precisato dal documento, tali iniziative autonome, generalmente, non presuppongono una presa di posizione da parte delle istituzioni, specialmente quando intervengono in settori non rientranti nell'ambito dei Trattati o in cui l'Unione non ha ancora legiferato. Tuttavia, la Commissione esamina le prassi di autoregolamentazione al fine di verificarne la conformità con le disposizioni dei Trattati[40], e ne informa il Parlamento europeo e il Consiglio qualora queste siano ritenute compatibili con la realizzazione degli obiettivi dei Trattati, nonché adeguate sotto il profilo della rappresentatività dei soggetti interessati[41].

Tali definizioni trovano conferma anche nel citato *toolbox* di recente emanazione che, nello specifico, riconduce le norme tecniche europee tra gli strumenti alternativi frutto di processi di coregolamentazione[42].

Appurato ciò, possiamo ora passare alla normazione tecnica europea nel contesto della cybersicurezza.

4. La normazione e certificazione europea di cybersicurezza

La politica europea in tema di normazione tecnica e cybersicurezza può essere ben compresa alla luce di quanto delineato nel "*Rolling Plan for ICT standardisation"*. Si tratta di un documento annuale in cui è rappresentato lo stato dell'arte delle attività di standardizzazione delle ICT nel contesto europeo, elaborato dalla Commissione europea grazie al contributo della piattaforma MSP di cui sopra[43].

Il Piano è solitamente articolato in sei capitoli relativi ai "driver di base", i settori "Abilitatori chiave", le "sfide per la società", l'"innovazione per il mercato unico digitale", l'"innovazione per il mercato unico" e tre Allegati su questioni orizzontali ai temi del documento. Nell'attuale versione del 2024 non sono stati aggiunti ulteriori capitoli ma si è provveduto ad una sostanziale revisione del

[36] *Ivi*, pt. 20.
[37] *Ivi*, pt. 21.
[38] *Ibidem*.
[39] *Ivi*, pt. 22.
[40] *Ibidem*.
[41] *Ivi*, pt. 23.
[42] Commissione europea, *"Better regulation" toolbox 2023 -tool#17*, sec. 3.1, 2023, p. 124, reperibile al link:<https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en>.
[43] Si rinvia alla pagina ufficiale di cui al link:<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation>.

documento. Diversamente nel 2023 sono stati aggiunti i capitoli relativi al Metaverso e alle tecnologhe quantistiche.

Per quanto riguarda la presente trattazione, ci concentremo sul piano delle politiche di standardizzazione relative alla cybersicurezza[44]. Il documento ha il pregio di ricapitolare gli interventi legislativi fino ad ora adottati in questo settore, ma soprattutto consente anche di apprendere quelli che saranno i "passi successivi" della strategia europea sul punto.

È infatti previsto che dopo l'adozione della proposta di Regolamento (UE) 2022/272 (anche nota come *Cyber Resilience Act* - CRA) (COM/2022/454 final), che tra le altre questioni disciplina anche i requisiti essenziali di cybersicurezza dei beni ICT, la Commissione europea preparerà una richiesta formale di normazione per sostenere l'attuazione del CRA.

Dobbiamo pertanto presumere che la Commissione avvierà una richiesta di normazione ad una delle ESOs per l'elaborazione della prima norma armonizzata di cybersicurezza, la quale dovrà essere elaborata conformemente ai requisiti essenziali stabiliti dal CRA (e quindi non ai requisiti definiti dalla Commissione stessa come previsto dall'art. 10 Reg. 1025/2012).

Ulteriore rilevanza è posta sul sistema europeo di certificazione della cybersicurezza, la cui preparazione e attuazione è rimessa all'ENISA, e che si struttura in un sistema di criteri comuni (*European Cybersecurity Scheme on Common Criteria* - EUCC) e in sistemi di certificazione settoriali come quelli dei servizi *cloud* (EUCS) e del 5G (EU5G) attualmente in preparazione.

Avremo modo di affrontare nel dettaglio il citato quadro legislativo nel proseguo, precisando si d'ora che si tratta di un complesso disciplinare in via di attuazione e che quindi ha portato a dover considerare solo quegli atti prodotti fino al momento in cui si scrive, tuttavia, per quanto possibile, non saranno trascurate considerazioni circa successivi provvedimenti non ancora adottati (soprattuto per quanto riguarda le norme armonizzate di cybersicurezza di cui diremo *infra* 4.2 a).

4.1 Il *Cybersecurity Act.* Il sistema europeo di certificazione e valutazione di cybersicurezza

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*)[45]. 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[46] 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[47]. 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

[44] Il *Rolling Plan* relativo a *Cybersecurity / network and information security (RP 2024)* è disponibile al link:<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cybersecurity-network-and-information-security-rp-2024>.

[45] Commissione Europea, *Comunicazione congiunta al Parlamento europeo e al Consiglio, Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN(2017) 450 final (anche nota come "*Cybersecurity package*").

[46] Reg. (EC) 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[47] Cfr. considerando 11, Reg. (EC) 460/2004.

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 cibersicurezza 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[48].

In sostanza il piano di riforma, poi concretamente formulato con la proposta 2017/0225[49], prevedeva che l'ENISA non si limitasse a fornire solo consulenze specialistiche, come prefissato nel 2004, ma che fosse investita anche di 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 cyberiscurezza 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[50]. 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 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[51]. 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)[52]. Si tratta tuttavia di un gruppo che comprende solo 12 Stati membri, più la Norvegia.

---

[48] Relativamente allo scambio di informazioni per il contrasto alle minacce informatiche a livello europeo sia concesso rinviare a F. SERINI, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in *MediaLaws*, n. 3, 2023.

[49] 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 final (proposta Cybersecurity Act).

[50] 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.

[51] 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.

[52] Per ulteriori si rinvia al sito ufficiale del *Senior Officials Group - Information Systems Security*, SOG-IS.

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[53].

La proposta, seppur volta ad innestare 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*"[54], 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 avrebbero dovuto essere non solo l'articolo 114 TFUE, ma anche l'articolo 5 del TUE concernente le questioni di sicurezza[55]; 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»[56].

Altre osservazioni sono invece pervenute dal settore industriale, particolarmente interessato alla regolazione delle certificazioni di cybersicurezza. Tra i pareri avanzati dai diversi stakeholders, 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[57]. Tra queste, l'art. 8 del Regolamento, rubricato "Mercato, certificazione della cybersicurezza 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

---

[53] 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. D.D. STEWART FERGUSON, *European Cybersecurity Certification Schemes and cybersecurity in the EU internal market*, in *Int. Cybersecur. Law Rev.*, vol. 3, 2022, pp. 51–114.

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

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

[56] Si rinvia a par. 10 del documento *ENISA and the new Cybersecurity Act* di cui in nota 105.

[57] Reg. (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 Regolamento (UE) n. 526/2013. Si precisa inoltre che con tale atto, il legislatore europeo ha introdotto per la prima volta, in 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».

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 cybersicurezza (art. 22 par. 2), e il Gruppo europeo per la certificazione della cybersicurezza - ECCG (art. 62).

Il Gruppo dei portatori di interessi per la certificazione della cybersicurezza, copresieduto dai rappresentanti della Commissione e dall'ENISA, è costituito da membri tra 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)[58]; 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)[59].

Il Gruppo europeo per la certificazione della cybersicurezza (ECCG), presieduto dalla 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, per non 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 attuazione e applicazione del programma di lavoro progressivo

[58] 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».

[59] Il diposto 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 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».

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 cybersicurezza (lett. a). Sia verso l'ENISA, in relazione alla preparazione di una proposta di preparazione, adozione e revisione di un sistema europeo di certificazione della cibersicurezza ex art. 49 (lett. b) sui cui poi esprime un parere sulle proposte preparate dall'ENISA (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 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»[60].

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»[61].

L'effetto di tale intervento normativo è stato da una parte 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)[62], 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 rilascio dei certificati siano «rigorosamente separate» dalle attività di vigilanza[63]. Altri profili riguardano invece la collaborazione e cooperazione tra le

---

[60] Cfr. art. 2, n. 9, Reg. (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".

[61] Crf. considerando 69, Reg. (UE) 2019/881.

[62] Cfr. art. 57, Reg. (UE) 2019/881.

[63] 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

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[64].

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 della 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 756/2008, 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[65].

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 porter 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»[66], qualora rispettino determinati criteri, e per un periodo massimo di cinque anni rinnovabile.

Ai sensi dall'art. 58 del Reg. 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.

---

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».

[64] Cfr. art. 58, par. 4, Reg. (UE) 2019/881.

[65] Cfr. art. 2, nn. 10 e 11 Reg. (UE) 756/2008.

[66] Cfr. art. 2, n. 11, del Reg. (UE) 756/2008.

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 definisce 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 prevedendo che «[l]a Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cybersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cyberiscurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di cyberiscurezza 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 europea di conformità che si riferisca al livello di affidabilità "di base" assicura 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»[67].

Un certificato o una dichiarazione europeo di conformità che si riferisca al livello di affidabilità "sostanziale" assicura 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»[68].

Infine, un certificato o una dichiarazione europea di conformità che si riferisca al livello di affidabilità "elevato" assicura 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»[69].

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 ICT, i servizi ICT o i processi ICT 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

[67] Cfr. art. 52, par. 5, Reg. (UE) 2019/881.
[68] Cfr. art. 52, par. 6, Reg. (UE) 2019/881.
[69] Cfr. art. 52, par. 7, Reg. (UE) 2019/881.

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 organismo di valutazione della conformità ma solo in presenza di determinate condizioni[70].

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 Reg. (UE) 765/2008, non tutti gli Stati membri e mondiali sono dotati di un organismo di certificazione della cybersicurezza governativo. In alcuni contesti, tale attività è demandata ad organismi di valutazione della conformità di natura perlopiù privata e pertanto, stando a quanto prescritto dal *Cybersecurity Act*, tali soggetti non possono rilasciare certificati di affidabilità elevata.

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 ove è dimostrato il rispetto ai requisiti previsti dal sistema (par. 2), ma a titolo volontario, salvo diversamente specificato nel diritto dell'Unione o degli Stati membri (par. 4).

4.1.1 *Segue*. L'*European Cybersecurity Scheme on Common Criteria* (EUCC) e il Regolamento (UE) 2024/482

Il 31 gennaio 2024 la Commissione europea ha adottato attuato l'*European Cybersecurity Scheme on Common Criteria* (EUCC), il primo schema di certificazione (generale) europeo di cybersicurezza, con il Regolamento (UE) 2024/482 e i relativi Allegati[71].

Con questo atto il legislatore europeo ha inteso specificare i ruoli, le norme e gli obblighi, nonchè la struttura del sistema europeo di certificazione della cybersicurezza nel rispetto di quanto disposto dal *Cybersecurity Act*. In particolare, lo schema si fonda sull'accordo di reciproco riconoscimento (ARR) dei certificati di valutazione della sicurezza delle tecnologie dell'informazione del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (*Senior Officials Group*

[70] 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».

[71] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) C/2024/560 (d'ora in poi Reg. EUCC).

– *Information Systems Security*, SOG-IS[72]) e si basa sui criteri comuni, comprese le procedure e i documenti del Gruppo[73].

Relativamente alla formazione dello schema di certificazione, conformemente a quanto previsto dal *Cybersecurity Act* (il Regolamento 2019/881), la Commissione ha chiesto all'ENISA di preparare una proposta di sistema europeo di certificazione della cybersicurezza[74]. Proposta che è stata discussa prima dagli Stati membri, per mezzo dell'*European Cybersecurity Certification Group* (ECCG) costituito, ricordiamo, dai rappresentanti delle autorità nazionali di certificazione della cybersicurezza o di altre autorità nazionali competenti, e successivamente dai portatori di interessi riuniti nello *Stakeholder Cybersecurity Certification Group* (SCCG)[75].

A tal fine, l'Agenzia europea ha istituito un Gruppo di lavoro *ad hoc*, e si avvalsa della consultazione di tutti i partecipanti «mediante un processo di consultazione formale, aperto, trasparente e inclusivo»[76], al termine del quale l'ENISA ha redatto lo schema di certificazione definitivo. La Commissione ha dato attuazione a detto schema con il citato Regolamento attuativo, tenendo tuttavia conto di quanto emerso nella consultazione pubblica che si è tenuta nel mese di ottobre 2023[77].

In tal sede alcuni Paesi, extra-europei, hanno voluto evidenziare che l'adozione dell'EUCC non esclude per uno Stato membro l'essere parte degli accordi CCRA (vedi *infra* 4.1)[78],

Per quanto riguarda il contenuto del Regolamento di attuazione, al Capo V è stata dettagliata la disciplina relativa al monitoraggio della conformità al sistema di certificazione da parte dei diversi soggetti coinvolti, attraverso un meccanismo di controllo a cascata.

L'Autorità nazionale di certificazione della cybersicurezza (in Italia l'ACN) è il soggetto responsabile del controllo sul rispetto degli obblighi contemplati dal *Cybersecurity Act* e dallo stesso Regolamento attuativo da parte di tutti i soggetti (e beni) interessati, ossia su: l'organismo di

---

[72] Come si apprende dal sito ufficiale, il Gruppo ha creato il primo Accordo SOG-IS in risposta alla Decisione del Consiglio dell'Unione Europea del 31 marzo 1992 (92/242/CEE) nel campo della sicurezza dei sistemi informativi, e alla successiva Raccomandazione del Consiglio del 7 aprile (1995/144/CE) sui criteri comuni di valutazione della sicurezza delle tecnologie dell'informazione. Si rinvia al sito ufficiale di cui al link:<https://sogis.eu/>, nonché al sito dell'ACN per una panoramica chiara sul Gruppo e sul contenuto dell'Accordo, di cui al link:<https://www.ocsi.gov.it/ index.php/organismo/sogis-mra.html>.

[73] A tal proposito tra le definizioni di cui all'art. 2 Reg. EUCC, vi sono anche quelle di "criteri comuni", «i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione quali definiti nella norma ISO/IEC 15408»; "metodologia comune di valutazione", «la metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione quale definita nella norma ISO/IEC 18045»; "profilo di protezione", «un processo ICT che stabilisce i requisiti di sicurezza per una categoria specifica di prodotti ICT, che affronta le esigenze di sicurezza indipendenti dall'implementazione e che può essere utilizzato per valutare i prodotti ICT rientranti in tale categoria specifica ai fini della loro certificazione».

[74] Cfr. art. 48 Reg. (UE) 2019/881.

[75] Circa lo SCCG si rinvia al link:<https://digital-strategy.ec.europa.eu/en/policies/stakeholder-cybersecurity-certification-group>.

[76] Art. 49, par. 3 e 4 Reg. (UE) 2019/881.

[77] Si rinvia all'apposita pagina di cui al link:<https://digital-strategy.ec.europa.eu/en/news/ have-your-say-european-common-criteria-based- cybersecurity-certification-scheme-eucc>. Dal sito emerge che la consultazione ha raccolto 59 opinioni da parte di diversi soggetti interessati, spesso anche provenienti/stabiliti in Stati non appartenenti all'Unione; tuttavia, alcuni di questi hanno lamentato che la breve finestra di commento per la consultazione pubblica non ha permesso loro di poter ben comprendere e approfondire il contenuto e quindi anche i relativi effetti del Regolamento (vedi ad es. NSA/NIAP).

[78] Vedi a tal proposito le opinioni dello stesso CCRA, nonché del Canada, Polonia, Stati Uniti (Camera di commercio).

certificazione e l'ITSEF, ossia l'organismo di valutazione della conformità competente nella sicurezza delle ICT[79]; i titolari di un certificato EUCC; i prodotti ICT certificati[80].

L'organismo di certificazione invece responsabile del controllo circa il rispetto dei detti obblighi sui titolari di un certificato e sui prodotti ICT[81].

Infine, il titolare del certificato EUCC è responsabile del monitoraggio della conformità del prodotto ICT certificato rispetto ai suoi requisiti di sicurezza.

È inoltre dettagliata la disciplina relativa alle conseguenze della non conformità di un prodotto ICT certificato o di un profilo di protezione[82]; conseguenze della non compliance da parte del titolare del certificato[83]; e le conseguenze della non compliance da parte dell'organismo di valutazione della conformità[84].

Riteniamo tuttavia di particolare interesse la disciplina di cui al Capo VI, relativa alla gestione e divulgazione delle vulnerabilità informatiche riscontrate dal titolare del certificato EUCC. La condivisione di tali informazioni è di fondamentale importanza[85], sia per contribuire a migliorare la postura di sicurezza di altre organizzazioni, sia per i produttori e sviluppatori di beni ICT, al fine di garantire che la produzione di detti beni sia sempre aggiornata a prevenire gli ultimi *trend* di minaccia.

Il Regolamento prevede che, qualora rilevi una potenziale vulnerabilità che interessa un suo prodotto ICT certificato o riceva informazioni in merito, il titolare del certificato EUCC registra tali informazioni ed effettua un'analisi dell'impatto delle vulnerabilità[86]. Se dall'analisi emerge un probabile impatto della vulnerabilità sulla conformità del prodotto, il titolare elabora una relazione[87] e, conformemente all'art. 56, par. 8, del *Cybersecurity Act*, la trasmette senza indebito ritardo all'organismo di certificazione o all'autorità nazionale di certificazione della cybersicurezza[88].

Qualora il documento sia inviato al primo, l'organismo di certificazione è tenuto a fornire dette informazioni all'Autorità nazionale di certificazione della cybersicurezza, includendo tutti gli elementi necessari a quest'ultima per comprendere l'impatto della vulnerabilità, le modifiche da apportare al prodotto e, se disponibili, le eventuali informazioni da parte dell'organismo di certificazione sulle implicazioni più ampie della vulnerabilità per altri prodotti ICT certificati. Il Regolamento precisa, tuttavia, che le informazioni fornite dall'organismo di certificazione «non contengono dettagli sulle modalità di sfruttamento della vulnerabilità», dato che l'Autorità nazionale di certificazione può sempre esercitare i suoi poteri di indagine[89].

La precisazione non è di secondario rilievo poiché interessa il delicato tema della divulgazione delle vulnerabilità non sfruttate, di cui diremo ampiamente in seguito a proposito della proposta di Regolamento *Cyber Resilience Act* - CRA (*infra* 4.1.1, d).

---

[79] Art. 2, n. 7 Reg. EUCC, che lo definisce «una struttura di valutazione della sicurezza delle tecnologie dell'informazione, che è un organismo di valutazione della conformità quale definito nell'articolo 2, punto 13), del regolamento (CE) n. 765/2008, che svolge attività di valutazione».

[80] Cfr. art. 25 Reg. EUCC.

[81] Cfr. art. 26 Reg. EUCC.

[82] Art. 28 Reg. EUCC.

[83] Art. 29 Reg. EUCC.

[84] Art. 31 Reg. EUCC.

[85] Per maggiori dettagli sul punto, sia concesso rinviare a F. SERINI, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in *MediaLaws*, n. 3, 2023.

[86] Art. 33, par. 3, Reg. EUCC.

[87] Art. 35 par. 1, Reg. EUCC.

[88] Art. 35 par. 4, Reg. EUCC.

[89] Art. 37, par. 2, Reg. EUCC.

Tuttavia, come osservato da Alcuni nella consultazione pubblica, tale meccanismo, oltre a non essere allineato alla disciplina CRA[90], potrebbe anche comportare dei rischi[91], o non essere praticabile a livello concreto[92].

4.2 La definizione dei requisiti essenziali di cybersicurezza e gli obblighi per gli attori della *supply chain* dei beni ICT nella proposta *Cyber Resilience Act.*

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»[93], al fine di armonizzare il mercato interno dei beni ICT relativamente ai requisiti di cybersicurezza[94].

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 medico diagnostici 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[95].

Nello specifico, la proposta è volta a stabilire, da una parte, le norme per l'immissione sul mercato dei beni ICT consistenti perlopiù in una serie di obblighi per gli attori della *supply chain* dei beni ICT, dall'altra, detta una disciplina per i requisiti essenziali per la progettazione, lo sviluppo e la fabbricazione di tali beni, nonché i requisiti essenziali per il processo di gestione delle vulnerabilità. Infine, l'ultima parte è dedicata alle norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti di cui sopra.

Come si comprenderà, si tratta di una disciplina particolarmente articolata. Ragione che ha portato alla scelta di suddividerne la trattazione in diverse parti. Inoltre, al momento in cui si scrive, la proposta in questione non è stata ancora promulgata nella sua versione definitiva; pertanto, terremo anche conto di quanto emerso dal trilogo dei co-legislatori europei.

---

[90] Così la Camera di commercio degli Stati Uniti, vedi documento reperibile al link:<https://ec.europa.eu/info/ law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification/F3441440_en>.

[91] È il parere di Huawei, di cui al link:<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/ 13382-Cybersecurity-security-requirements-for-ICT-product-certification/F3441417_en>.

[92] Secondo il parere della Cisco systems, al link:<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certification/F3441404_en>.

[93] Cfr. art. 3, par. 1, proposta CRA.

[94] P.G. CHIARA, *Il Cyber Resilience Act: la proposta di regolamento della Commissioneeuropea relativa a misure orizzontali di cybersicurezza per prodotticon elementi digitali*, in "Rivista Italiana di Informatica e Diritto", fasc. 1, 2023, pp. 151 ss., a cui si rinvia per una trattazione dettagliata della proposta CRA.

[95] Cfr. art. 2, parr. 2 e 3, proposta CRA.

a) I requisiti essenziali dei beni ICT e le norme armonizzate di cybersicurezza

All'istituzione del quadro unico armonizzato di certificazioni di cybersicurezza dei beni ICT, attuato con il *Cybersecurity Act*, ha dovuto necessariamente far seguito une disciplina che dettasse i requisiti che i beni ICT devono possedere affinché possano presuntivamente essere ritenuti cybersicuri (certificandolo) secondo i valori e principi europei.

Nel *Cybersecurity Act* era già stata prevista questa esigenza, ma il Regolamento 2019/881 non venne considerato essere la sede disciplinare opportuna a ciò[96], oltre al riscontro di una obiettiva difficoltà nel «formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi»[97]. Ragione che ha portato all'elaborazione dell'ampia e generale nozione giuridica di cybersicurezza al fine di consentire la certificazione.

Nello stesso Regolamento veniva inoltre precisato che tali requisiti da usare nei sistemi europei di certificazione della cybersicurezza dovessero rispettare i principi dell'Allegato II del Regolamento 1025/2012, e che, in casi debitamente giustificati, le cui motivazioni siano rese pubbliche, il legislatore europeo possa «discostarsi da detti requisiti qualora le specifiche tecniche siano da usare in un sistema europeo di certificazione della cibersicurezza che fa riferimento a un livello di affidabilità elevato»[98].

Il riferimento ci porta quindi a dover tornare sul citato Regolamento 2012 disciplinante la normazione tecnica europea, soprattutto al fine di capire cosa si intenda per requisito tecnico e cosa prevedano i principi dell'Allegato II allo stesso.

Innanzitutto il Regolamento precisa che i requisiti tecnici sono contenuti in un documento che prende il nome di «specifica tecnica», definito infatti come «un documento che prescrive i requisiti tecnici che un determinato prodotto, processo, servizio o sistema deve soddisfare [enfasi aggiunta]» e che stabilisce uno o più elementi relativi alle caratteristiche di un prodotto o di un servizio (esempio i livelli di qualità, le prestazioni, l'interoperabilità, la protezione dell'ambiente, la salute, la sicurezza o le dimensioni)[99].

Tali specifiche, se relative a beni ICT, e se non elaborate da un ente di normazione europeo, nazionale o internazionale, devono rispettare alcuni principi che trovano spazio nell'Allegato II del Regolamento, ossia: devono essere prodotte attraverso processi che soddisfano i criteri di apertura, consenso e trasparenza; e devono soddisfare alcune condizioni quali quelle di manutenzione, disponibilità, rispetto dei diritti di proprietà intellettuale, pertinenza, neutralità e stabilità, qualità.

Conformemente a quanto previsto nel 2019, con la proposta di Regolamento CRA del 2022, il legislatore europeo è andato così a contemplare direttamente i requisiti obbligatori sia per la sicurezza dei prodotti con elementi digitali in via generale (All. I n. 1), non escludendo anche interventi settoriali specifici[100], sia per il processo di gestione della vulnerabilità (All. I n. 2), garantendo un livello adeguato di cybersicurezza in base ai rischi.

Inoltre, se non sono adottate norme armonizzate o se le norme armonizzate non affrontano in misura sufficiente i requisiti essenziali disposti dal Regolamento CRA, la Commissione ha il potere

---

[96] Cfr. cons. 75 Reg. (UE) 2019/881, ove è previsto che «[n]on è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti ICT, servizi ICT e processi ICT nel presente regolamento».
[97] *Ibidem.*
[98] Cons. 75 Reg. (UE) 2019/881.
[99] Cfr. art. 2 nn. 4 e 5, Reg. (UE) 1025/2012.
[100] Cfr. cons. 14 proposta CRA.

di adottare essa stessa specifiche comuni (di cui all'All. I), mediante atti di esecuzione[101]. Al riguardo la proposta specifica che «tra le ragioni per definire tali specifiche comuni, anziché utilizzare norme armonizzate, possono figurare il rifiuto della richiesta di normazione da parte di una qualsiasi organizzazione europea di normazione, ritardi ingiustificati nell'elaborazione di norme armonizzate appropriate o la mancanza di conformità delle norme elaborate ai requisiti del presente regolamento o a una richiesta della Commissione»[102].

Orbene, come già anticipato, nel *Rolling Plan for ICT Standardisation* 2024, è previsto che la Commissione europea, una volta approvato il CRA, preparerà una richiesta formale di normazione per sostenere l'attuazione, che si concluderà con l'eventuale approvazione e pubblicazione della prima norma armonizzata di cybersicurezza conforme ai requisiti essenziali dettati dal Regolamento CRA.

Quest'ultimo aspetto è il motivo che ci ha fatto ritenere che si tratterà di una norma armonizzata formata in maniera difforme rispetto alla procedura ordinaria di cui all'art. 10 del Regolamento 1025/2012, ove è la Commissione che «stabilisce i requisiti relativi al contenuto che il documento deve rispettare e un termine per la sua adozione», requisiti che - ricordiamo - «tengono conto dell'interesse pubblico e degli obiettivi politici chiaramente specificati nella richiesta della Commissione e sono fondati sul consenso».

Analogamente, anche la proposta di Regolamento CRA, come tutti gli atti di diritto derivato, è stata elaborata sulla scorta di valutazioni con i soggetti interessati e in considerazione di un interesse pubblico, quale quello alla sicurezza delle infrastrutture informatiche e dei beni informatici. Tuttavia, il dato che pare d'interesse è che, alla luce di quanto già osservato in precedenza (*infra* 2.9.1 e 2.11), le attuali procedure di formazione delle norme armonizzate, sia dal punto di vista giuridico, sia secondo i documenti istituzionali degli enti europei di normazione, assicurano meccanismi di garanzia sotto gli aspetti della democraticità in quasi tutte le ESOs (eccezion fatta per l'ETSI come già visto *infra* 2.11).

Tale norma, al momento non ancora richiesta dalla Commissione, potrebbe pertanto essere la prima norma tecnica, che trova applicazione in un particolare e delicato ambito quale quello della (cyber)sicurezza, ad essere prodotta in considerazione di interessi che non solo di un certo gruppo di grandi imprese, ma anche della rappresentazione della piccola e media industria, nonché soprattutto delle varie rappresentanze sociali e dell'ambiente.

b) Gli obblighi per gli attori della *supply chain* dei beni ICT in relazione ai livelli di rischio

In questa parte sarà analizzato 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, quali soggetti che sono stati interpretati dalla disciplina come avere un ruolo attivo nella catena di fornitura dei beni ICT.

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

[101] L'art. 19 della Proposta CRA specifica che tale atto di esecuzione è adottato conformemente alla disciplina sulla procedura d'esame, di cui all'art. 5 del Regolamento Regolamento (UE) n. 182/2011 che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione.

[102] cfr. cons. 41 proposta CRA.

Allegati alla proposta[103]. 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»[104].

La seconda categoria include invece "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 vi rientrano i prodotti con elementi digitali critici (ad esempio, reti private virtuali e router)[105] 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)[106].

In base al loro livello di rischio, i suddetti prodotti digitali sarebbero soggetti a procedure di valutazione della conformità più o meno stringenti per dimostrare la conformità agli obblighi di cybersicurezza stabiliti nella proposta di Regolamento. Premettiamo 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 applichino al loro prodotto gli attuali standard armonizzati di cybersicurezza, ad esempio, sviluppati da organizzazioni europee di normazione o schemi di certificazione di cybersicurezza 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 devono invece essere oggetto di valutazione di conformità per opera di terze parti gestita e 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

[103] 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.

[104] Cfr. art. 5, proposta CRA.

[105] Cfr. art. 3, n. 3, proposta CRA.

[106] Cfr. art. 3, n. 4, proposta CRA.

conformi alle norme armonizzate che traducono i requisiti essenziali della proposta in specifiche tecniche dettagliate e che sono adottate conformemente al già ricordato Reg. 1025/2012[107].

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 in d).

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 i primi 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[108], 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[109]. Si è pertanto auspicato di includere anche tali beni tra quelli oggetto di controllo da parte delle competenti autorità pubbliche.

Il *Computer & Communications Industry Association* (CCIA Europe), l'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[110].

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[111].

c) La cybersicurezza dei consumatori: il ruolo del sistema di vigilanza del mercato e della Commissione europea

[107] Cfr. considerando 15 proposta CRA.

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

[109] V. TICcouncil, *TIC Council Welcomes the European Commission's Proposal for a Cyber Resilience Act*, reperibile sul sito ufficiale (ultima consultazione il 17.12.23).

[110] V. CCIA Europe, *New EU Cybersecurity Rules Are Well-intended, but Introduce Unnecessary Red Tape*, del 15 settembre 2022, reperibile sul sito ufficiale (ultima consultazione il 17.12.23).

[111] M. BURRI, Z. ZIHLMANN, *The EU Cyber Resilience Act – An Appraisal and Contextualization*, in "Zeitschrift für Europarecht (EuZ)", n. 2, 2023.

La proposta di Regolamento CRA prevede inoltre il coinvolgimento delle Autorità vigilanti del mercato nel processo di cybersicurezza del mercato unico.

Questo aspetto ci porta a dover considerare un ulteriore punto di vista. Oltre agli obiettivi di cybersicurezza del mercato unico, e di cybersicurezza nazionale, la politica di resilienza dei beni ICT è volta ad assicurare anche la (cyber)sicurezza dei consumatori. Come si comprenderà si tratta di un aspetto riconducibile alle più ampia politica di sicurezza dei prodotti in generale, recentemente aggiornata con il citato Regolamento (UE) 2023/988 (o GPSR).

L'interesse pubblico sotteso a detto sistema è quello di assicurare che i prodotti siano conformi alla normativa di armonizzazione europea in maniera da poter garantire che la loro circolazione non comporti alcun rischio per «la salute e la sicurezza in generale, la salute e la sicurezza sul luogo di lavoro, la tutela dei consumatori, la protezione dell'ambiente, la sicurezza pubblica»[112]. I prodotti non conformi e non sicuri sono infatti sia un rischio per i cittadini, sia per il mercato poiché possono falsare la concorrenza con gli operatori economici che vendono prodotti conformi all'interno dell'Unione.

L'Unione europea ha inteso garantire l'applicazione del complesso di norme (non solo giuridiche) che caratterizzano questa materia attraverso il Regolamento (UE) 2019/1020, volto a disciplinare i poteri e l'azione coordinata delle Autorità di vigilanza del mercato degli Stati membri al fine di coniugare l'esigenza di sicurezza dei consumatori, riflessa nella sicurezza del prodotto, con il buon andamento del mercato unico[113].

È all'interno di questo quadro disciplinare che devono essere lette e interpretate le disposizioni di cui al Capo V, della proposta di Regolamento CRA, rubricato "Vigilanza del mercato e applicazione delle norme", volta ad introdurre una disciplina di dettaglio (ma non speciale) delle procedure di vigilanza del mercato sui beni ICT per ragioni di cybersicurezza.

In tale contesto le Autorità di vigilanza sono infatti chiamate a valutare la conformità dei prodotti con elementi digitali e dei processi messi in atto dai loro fabbricanti ai requisiti essenziali di cui all'Allegato I della proposta[114].

Nello specifico, il CRA prevede due procedure, una a livello nazionale, l'altra a livello europeo, relative ai prodotti con elementi digitali che presentano un rischio di cybersicurezza significativo.

Relativamente alla prima, l'Autorità di vigilanza può effettuare una valutazione del bene ICT, qualora «abbia motivi sufficienti per ritenere che un prodotto con elementi digitali, compresa la relativa gestione delle vulnerabilità, presenti un rischio di cybersicurezza significativo» e, se questa si concluderà con esito negativo, ossia una "non conformità" ai requisiti dettati dal CRA, «chiede senza indugio all'operatore interessato di adottare tutte le opportune misure correttive al fine di rendere il prodotto conforme ai suddetti requisiti oppure di ritirarlo o di richiamarlo dal mercato entro un termine ragionevole e proporzionato alla natura del rischio, a seconda dei casi»[115].

Inoltre, qualora ritenga che la non conformità non sia limitata al territorio nazionale, l'Autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri dei risultati della valutazione e delle azioni che ha chiesto all'operatore economico di intraprendere[116].

---

[112] Cfr. cons. 1, Reg. (UE) 2019/1020.

[113] Cfr. cons. 43 Reg. (UE) 2019/1020.

[114] Art. 42 proposta CRA.

[115] Art. 43 par. 1, proposta CRA.

[116] Art. 43 par. 2, proposta CRA.

Qualora il fabbricante di un prodotto con elementi digitali non adotti misure correttive adeguate entro il termine indicato, l'Autorità di vigilanza del mercato adotta tutte le opportune misure provvisorie per vietare o limitare la messa a disposizione del prodotto sul suo mercato nazionale, per ritirarlo o per richiamarlo, e ne informa, senza indugio, la Commissione e gli altri Stati membri di tali misure[117].

Particolarmente interessante, ci pare inoltre essere la possibilità per l'Autorità di indicare se la non conformità sia dovuta a: «a) mancato rispetto dei requisiti essenziali di cui all'allegato I da parte del prodotto o dei processi messi in atto dal fabbricante; b) carenze nelle norme armonizzate, nei sistemi di certificazione della cibersicurezza o nelle specifiche comuni»[118]. Si tratta di indicazioni che possono infatti avere particolare valore ai fini della correzione o aggiornamento del sistema di normazione e certificazione di cybersicurezza.

Le misure adottate dalle Autorità di vigilanza devono essere comunicate sia alla Commissione, sia agli altri Stati membri. Se entro tre mesi dal ricevimento delle informazioni, alcuno Stato membro o la Commissione non sollevano obiezioni contro la misura provvisoria adottata, tale misura è ritenuta giustificata[119].

Diversamente, ove siano sollevate obiezioni da parte degli Stati, o se la Commissione ritiene che la misura sia contraria alla normativa europea, si apre la "procedura di salvaguardia dell'Unione"[120]. La Commissione consulta senza indugio lo Stato membro interessato e l'operatore economico e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione decide se la misura nazionale sia giustificata o meno, e ne comunica l'esito all'operatore dopo nove mesi dalla notifica.

In linea generale, se la misura è ritenuta giustificata, tutti gli Stati membri adottano le misure necessarie a garantire che il prodotto con elementi digitali non conforme sia ritirato dal loro mercato e ne informano la Commissione. Se la misura nazionale è ritenuta ingiustificata, lo Stato membro interessato provvede a ritirarla.

Tuttavia, è proprio in questo frangente che le indicazioni dell'Autorità di vigilanza nazionale poc'anzi accennate possono essere rilevanti. Difatti se la misura è giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze nelle norme armonizzate, la Commissione applica la procedura di cui all'art. 10 del Reg. 1025/2012. Se invece è attribuita a carenze in un sistema europeo di certificazione della cybersicurezza, la Commissione valuta se modificare o abrogare l'atto di esecuzione che specifica la presunzione di conformità relativa a tale sistema di certificazione. Infine, se la misura nazionale è ritenuta giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze nelle specifiche comuni, la Commissione valuta se modificare o abrogare l'atto di esecuzione che la ha stabilite[121].

La procedura europea prevede invece che se la Commissione «ha motivi sufficienti per ritenere, anche sulla base delle informazioni fornite dall'ENISA», che un prodotto con elementi digitali che presenta un rischio di cybersicurezza significativo non sia conforme ai requisiti del CRA, può chiedere alle autorità di vigilanza del mercato competenti di effettuare una valutazione della

[117] Art. 43 par. 4, proposta CRA.
[118] Art. 43 par. 5, proposta CRA.
[119] Art. 43 parr. 6-7, proposta CRA.
[120] Art. 44, par. 1 proposta CRA.
[121] Art. 44, parr. 3,4,5 proposta CRA.

conformità[122]. Tuttavia, in circostanze eccezionali che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che il prodotto continui a non essere conforme ai requisiti stabiliti dal CRA, la Commissione può chiedere invece all'ENISA di effettuare la valutazione della conformità[123].

A conclusione di tali valutazioni (dell'Autorità di vigilanza nazionale, o dell'ENISA), la Commissione può decidere di adottare una misura più o meno restrittiva[124].

In tutti questi casi, la circolazione dei beni ICT può essere interrotta per motivi di cybersicurezza. La proposta CRA prevede tuttavia che le Autorità nazionali di vigilanza del mercato che, anche nei casi in cui il bene risulti conforme ai requisiti del Regolamento, se «i processi messi in atto dal fabbricante presentino un rischio di cybersicurezza significativo e comportino inoltre un rischio per la salute o la sicurezza delle persone, per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali, per la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali [...] o per altri aspetti della tutela dell'interesse pubblico», questa chiede all'operatore interessato di adottare tutte le misure appropriate a far sì che il prodotto in questione venga immesso nel mercato privo dei predetti rischi, oppure che il prodotto sia ritirato o richiamato[125].

d) Indiscrezioni dal trilogo tra i co-legislatori del dicembre 2023

Da settembre 2023, la proposta è passata all'esame congiunto della Commissione, del Parlamento europeo e del Consiglio (c.d. trilogo)[126]. Secondo quanto riportato dagli organi di stampa[127], 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 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

---

[122] Art. 45, par. 1 proposta CRA.

[123] Art. 45, par. 2 proposta CRA.

[124] Art. 45, par. 3 proposta CRA.

[125] Art. 46 proposta CRA.

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

[127] Per i temi discussi nei vari trilogi, si rinvia agli articoli di Euractiv firmati da Luca Bertuzzi, di cui in particolare: L. BERTUZZI, *EU Commission pitches double reporting of open security loopholes in cybersecurity law*, in "Euractiv", 15 novembre 2023; ID, *EU policymakers prepare to close on cybersecurity law for connected devices*, in "Euractiv", 30 novembre 2023; ID, *EU institutions finalise agreement on cybersecurity law for connected products*, in "Euractiv", 5 dicembre 2023 (ultime consultazioni 13.12.23).

stata effettuata da un attore su un sistema senza il permesso del proprietario del sistema»[128]. 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 originaria 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[129].

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 cybersicurezza, 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[130].

Da quanto si apprende dall'ultimo trilogo il 30 novembre 2023[131], sembra che questo problema sia stato bilanciato giungendo a soluzioni restrittive che probabilmente faranno parte del testo finale del CRA[132]. 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 dibattutto 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[133]. 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[134].

4.2 La specializzazione degli enti di normazione europei nell'ambito della cybersicurezza

[128] Art. 3, n. 39, proposta CRA.

[129] 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.

[130] L. BERTUZZI, *EU Commission pitches double reporting … op. cit.*

[131] 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.

[132] L. BERTUZZI, *EU institutions finalise agreement …op. cit.*

[133] Parte del documento è stato riportato da Euractiv. Il frammento interessato citato da L. BERTUZZI, *EU Commission pitches double reporting … op. cit.* 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».

[134] *Ibidem.*

L'esigenza di cybersicurezza, particolarmente avvertita a livello europeo, ha avuto l'effetto di specializzare le tre ESOs attraverso l'istituzione di gruppi e nuove Commissioni tecniche di lavoro focalizzate in questo settore. Proponiamo di seguito una breve panoramica a partire dal *Rolling Plan for ICT Standardisation* 2024 che ne fa una accurata elencazione aggiornata.

a) Il CEN-CLC/JTC 13 *Cybersecurity and Data protection*

Nel 2011 è stato istituito il CEN-CENELEC *Focus Group on Cybersecurity* (CSCG), inizialmente come "*Cybersecurity Coordination Group*", per fornire consulenza strategica sulla standardizzazione nel campo della sicurezza informatica, sicurezza delle reti e delle informazioni e cybersicurezza.

Più nello specifico, il Gruppo è 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 dei portatori di interessi in diversi standard e ha così prodotto un documento sulla definizione di tale concetto[135].

La vera specializzazione dei gruppi di lavoro delle norme tecniche in ambito cybersicurezza è tuttavia avvenuta nel 2017 quando il CEN-CENELEC ha istituito una apposita *Joint Technical Committee* (JTC)[136], il CEN-CLC/JTC 13 *Cybersecurity and Data protection*.

Obiettivo principale della JTC è di trasporre gli standard internazionali rilevanti come standard europei (EN) nel settore delle Tecnologie dell'Informazione (IT)[137]. Mentre il Comitato tecnico CLC/TC 65X *Industrial-process measurement, control and automation*, l'altro principale fornitore di standard correlati alla sicurezza informatica, svolge la medesime funzione nel settore della Tecnologia Operativa (OT)[138].

Nello specifico la JTC Commissione ha partecipato attivamente alla elaborazione di quadri organizzativi e metodologie; sistemi di gestione informatica; linee guida sulla protezione dei dati e sulla *privacy*; schemi di valutazione dei processi e dei prodotti; linee guida tecniche per la sicurezza delle ICT e la sicurezza fisica; tecnologia intelligente, oggetti, dispositivi informatici distribuiti, servizi di dati, sicurezza dei prodotti, sostegno al sistema di certificazione 5G dell'UE, nonché a livello legislativo alla formulazione della Direttiva sulle apparecchiature radio (Direttiva 2014/53/UE) e il *Cyber Resilience Act*.

In quest'ultimo caso, il CENELEC JTC 13 ha istituito un gruppo di lavoro speciale per l'occasione, il CEN/CLC/JTC 13/WG 9, per avviare la preparazione alle esigenze di normazione dell'agenzia di rating del credito. Questo gruppo di lavoro si basa sull'esperienza del gruppo di lavoro speciale RED Standardization Request (CEN/CLC/JTC 13/WG 8).

A livello di normazione tecnica, le norme ISO/IEC 27000, i criteri comuni per la valutazione delle tecnologie dell'informazione di cui ISO/IEC 15408 e la metodologia comune per la valutazione delle tecnologie dell'informazione ISO/IEC 18045 sono adottati come norme europee da questo comitato tecnico misto.

---

[135] CSCG, *Recommendation #2 – Definition of Cybersecurity*, ver. 01.08, 2017.

[136] Al pari delle altre JTC del CEN-CENELEC, la Commissione segue le disposizioni dei documenti istituzionali interni di cui si rinvia al link:<https://boss.cen.eu/technicalstructures/pages/jointcenclctcs/>.

[137] Per ulteriori si rinvia al sito ufficiale CEN-CLC/JTC 13 Cybersecurity and Data protection.

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

b) L'ETSI TC *Cyber*

Nel 2014, l'Organismo ETSI ha istituito l'ETSI TC CYBER[139], il centro di competenza che produce standard per l'ecosistema di cybersicurezza, IoT, dispositivi per i consumatori, protezione dei dati personali e della comunicazione, sicurezza della rete, strumenti e guide per la cybersicurezza e svolge attività di supporto alla legislazione europea nel digitale (esempio GDPR, CSA, RED, NIS)[140].

Il Centro è inoltre competente, per mezzo di altre Commissioni, in diversi settori, tra cui, il TC CYBER QSC sulla crittografia quantistica; l'ISG QKD (*Quantum Key Distribution*) che lavora per sostenere l'industrializzazione della tecnologia QKD per proteggere le reti ICT; l'ISG MEC (*Multi-access Edge Computing)*, che ha guidato la pubblicazione di un Libro bianco dal titolo "*MEC security: Stato di supporto degli standard ed evoluzioni future*", ed altri ancora[141].

c) Gli enti di normazione di cybersicurezza diversi da quelli europei

Il citato Piano annuale ci offre anche una panoramica delle norme tecniche di cybersicurezza prodotte da altri organismi, consorzi privati o enti. Tale quadro ci pare interessante non solo per il valore meramente informativo ma soprattutto perché - lo ribadiamo - gran parte delle norme tecniche nel settore ICT, ed anche quelle di sicurezza, sono prodotte perlopiù da tali soggetti. Mentre come abbiamo osservato, solo di recente (dal 2022 ad oggi), l'Unione europea ha iniziato a concretizzare gli sforzi nel settore della normazione tecnica di cybersicurezza.

Tra i diversi standard citati, ci sembra utile soffermarci sull'*OASIS Cyber Threat Intelligence (CTI) TC* che definisce l'insieme di rappresentazioni e protocolli di informazione utili nella condivisione automatizzata delle informazioni per la consapevolezza situazionale della sicurezza informatica, la difesa della rete in tempo reale e l'analisi sofisticata delle minacce (sul punto P.te II, Cap. II, 1), per mezzo dei linguaggi *Structured Threat Information eXpression* (STIX), che fornisce un insieme comune di descrittori per le minacce alla sicurezza e gli eventi, *Trusted Automated Exchange of Indicator Information* (TAXII), che specifica fornisce comuni modelli di scambio di messaggi.

Si tratta dello standard utilizzato nei sistemi di *cyber threat sharing* che consentono alle vittime di condividere informazioni sull'attacco informatico subito, sia verso altri soggetti operativi nel settore interessato (es. i circuiti ISACs), sia verso le competenti autorità nazionali od europee[142].

5. Il controllo sul *procurement* informatico alla luce della disciplina sul Perimetro di Sicurezza Nazionale Cibernetica: il ruolo del CVCN

Il controllo sui prodotti ICT in Italia è stato disciplinato all'interno del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), istituito con decreto-legge del 21 settembre 2019, n. 105, convertito con modificazioni in legge 18 novembre 2019 n. 133, e successivamente, dal Decreto legislativo del 3 agosto 2022, n. 123, per quanto riguarda l'adeguamento dell'Italia al sistema di certificazione di cybersicurezza europeo (di cui si dirà *infra* 5).

---

[139] Si rinvia al sito ufficiale dell'ETSI TC CYBER.

[140] I programmi di lavoro del Centro possono essere consultati dalla pagina "*TC Cyber roadmap*" al link:<https://www.etsi.org/cyber-security/tc-cyber-roadmap>.

[141] Si rinvia al citato *Rolling Plan for ICT Standardisation* del 2024 sul punto.

[142] Per maggiori informazioni sul punto, anche in alcuni aspetti di dettaglio sul piano giuridico, sia concesso rinviare a F. SERINI, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in *MediaLaws*, n. 3, 2023.

Relativamente al primo intervento, si tratta di una disciplina con il 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 [...]»[143].

In particolare, l'art. 1 co.1, del decreto-legge 105/2019 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, è istituito il perimetro di sicurezza nazionale cibernetica».

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[144].

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, affidando poi tale compito – come per la direttiva NIS – ad alcune amministrazioni centrali dello Stato. Si tratta di disposizioni con il quale 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[145].

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[146].

---

[143] Cfr. S. MELE, *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*, Milano, 2020, p. 186. Nello specifico, confrontando le due citate discipline, il PSNC comprende anche quei soggetti attivi nei settori interno, difesa, spazio e aerospazio, telecomunicazioni, economia e finanza, servizi digitali, tecnologie critiche.

[144] 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 12.11.2023).

[145] art. 2, lett. a), d.P.C.M. 30 luglio 2020, n. 131.

[146] art. 2, lett. b), d.P.C.M. 30 luglio 2020, n. 131.

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 quale definito da uno Stato membro conformemente al diritto nazionale»[147].

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.

L'aspetto d'interesse in questa sede riguarda l'esercizio dei poteri di controllo sui beni ICT: accertamenti che vengono effettuati 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)[148]. Si tratta di un ente originariamente istituito presso l'Istituto Superiore delle Comunicazioni e Tecnologie Informatiche (ISCTI), del Ministero dello sviluppo economico, ed ora confluito presso l'Agenzia per la Cybersicurezza Nazionale (ACN)[149].

Con il Decreto del Presidente della Repubblica del 5 febbraio 2021, n. 54, emanato in attuazione dell'art. 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, è stata dettagliata la disciplina sul punto. Nello specifico, oltre al CVNC, sono stati introdotti anche i Centri di Valutazione (CV) presso il Ministero dell'interno[150] e del Ministero della difesa (Ce.Va.), nonché i Laboratori accreditati in prova (LAP): tutte strutture accreditate dal CVCN conformemente alle procedure di contemplate dal Decreto del Presidente del Consiglio dei Ministri del 18 maggio 2022, n. 92.

Nello specifico, come si apprende dall'art. 3 del DPCM 92/2022, il CVCV quale Organismo di accreditamento, «opera in conformità ai requisiti della norma UNI CEI EN ISO/IEC 17011 - «"Valutazione della conformità - Requisiti per gli organismi di accreditamento che accreditano organismi di valutazione della conformità"»[151].

---

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

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

149 Il trasferimento è avvenuto in virtù del decreto-Legge n. 82 del 14 giugno 2021, 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. L. PARONA, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in "Giornale di Diritto amministrativo", n. 6, 2021; Sia inoltre concesso rinviare a F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in f*ederalismi.it,* n. 12, 2022;

150 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 decreto-legge 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.

151 In particolare, all'art. 4 sono definiti i compiti del CVCN, ossia «a) accredita i laboratori di prova, in possesso dei requisiti di cui agli articoli 8 e 9, per l'esecuzione dei test di cui all'articolo 5, comma 3, del DPR; b) intraprende iniziative al fine di garantire il mantenimento del livello di qualità dei LAP e la corretta attuazione delle determinazioni tecniche di cui alla lettera e), delle specifiche tecniche e della redazione dei rapporti di prova; c) stabilisce le metodologie di test di cui all'articolo 5, comma 4, del DPR; d) vigila sull'attività dei LAP nel corso delle attività di test effettuando verifiche intermedie o a campione per la verifica del mantenimento dei requisiti di accreditamento; e) adotta, in conformità e in attuazione di quanto previsto dal presente regolamento, specifiche determinazioni tecniche, assicurandone, nell'ambito delle proprie competenze, il rispetto e curandone l'aggiornamento. In particolare, tali determinazioni definiscono: 1) i requisiti tecnici e logistici, tra cui quelli relativi alla dotazione strumentale per l'esecuzione dei test e alla protezione

Il dato è particolarmente importante poiché conferisce funzione accreditante ad un Organismo diverso da Accredia (infra Parte III, Cap. I, 3).

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[152]. 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»[153].

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

---

degli ambienti di test; 2) le specifiche misure di sicurezza informatica; 3) i requisiti di competenza ed esperienza necessari per l'accreditamento dei laboratori di prova ivi comprese le modalità di redazione del curriculum professionale da presentare nella domanda di accreditamento; 4) le aree di accreditamento di cui all'articolo 7; 5) i test da eseguire di cui all'articolo 5, comma 3, del DPR; 6) le attività relative all'esecuzione dei test soggette al divieto di divulgazione di cui all'articolo 13, comma 2; 7) le modalità di notifica delle limitazioni di operatività superiori a 24 ore di cui all'articolo 13, comma 1, lettera f) 8) le modalita' tecniche per l'applicazione dei raccordi di cui all'articolo 21 tra il CVCN e i CV, concordandoli con questi ultimi per gli aspetti di loro competenza; 9) le modalità esecutive delle comunicazioni con i LAP e i termini tecnici e organizzativi mediante i quali i raccordi trovano effettiva applicazione di cui all'articolo 21; f) cura i raccordi con i LAP e i CV, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio; g) redige e aggiorna periodicamente la lista dei beni, sistemi e servizi ICT oggetto di valutazione, per i quali sia stato emesso un rapporto di prova; h) gestisce la piattaforma informatica di cui all'articolo 6, commi 1 e 6, del DPR, anche ai fini di cui all'articolo 21, in particolare per la conservazione e condivisione: 1) di un elenco dei LAP contenente il nominativo del responsabile del laboratorio di prova, del responsabile del sistema di gestione per la qualità e del responsabile per i rapporti con il CVCN, nonchè la durata e l'area dell'accreditamento; 2) della documentazione di sintesi relativa ai rapporti di prova».

[152] L. FIORENTINO, *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. DELLA CANANEA, L. FIORENTINO, *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editoriale scientifica, 2020, p. 57.

[153] Art. 5, co. 9, d.P.R. 54/2021.

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]»[154].

Tra le altre ipotesi, le valutazioni possono infatti costituire un'importante fase preliminare anche per l'attivazione dei poteri speciali da parte del Governo (cc.dd. *golden powers*)[155] 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 d.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 decreto-legge 15 marzo 2012, n. 21, potenziando e ampliandone il loro campo applicativo[156].

In conclusione, il sistema così delineato prevede che nel caso in cui il bene ICT da acquisire presso l'infrastruttura afferente al PSNC risulti avere un parere negativo da parte dei Centri di valutazione, prevale l'interesse nazionale su quello del libero mercato e pertanto l'acquisto e l'installazione di detto bene non saranno consentiti.

5.1 *Segue*. Il Decreto legislativo del 3 agosto 2022 n. 123 e il ruolo dell'ACN nella certificazione rispetto ad Accredia

L'ordinamento italiano si è adeguato al nuovo quadro europeo di certificazione della cybersicurezza, introdotto dal citato *Cybersecurity Act*, con il Decreto legislativo del 3 agosto 2022, n. 123, con il quale il Governo[157] ha dato attuazione alla delega di cui all'art. 18 della Legge di delegazione europea 2019-2020 (Legge 22 aprile 2021, n. 53).

---

[154] art. 4, d.P.R. 54/2021.

[155] 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".

[156] S. MELE, *Il Perimetro di Sicurezza Nazionale …op. cit.,* pp. 204 ss.

[157] Sulla "Prevalenza dell'attività del Governo nella recezione della regolamentazione tecnica comunitaria" si rinvia a A. IANNUZZI, *Caratterizzazioni della normazione tecnica nell'ordinamento italiano. Il campo di analisi e di verifica della materia ambientale*, in "St. parl. pol. cost.", 2006, p. 13.

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 decreto-Legge 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*[158]. Si tratta di una attività che prima era di competenza dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) operando presso il Ministero dello sviluppo economico (MISE), ove era stato istituito, con il DPCM 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[159].

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[160].

Nello specifico, l'art. 5 del decreto legislativo, stabilisce che l'Agenzia svolge la funzione 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'esclusiva competenza di ACN il rilascio dei certificati di cybersicurezza con livello di affidabilità "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.

---

[158] Cfr. art. 4, d.Lgs. n. 123/2022.

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

[160] Sul punto si rinvia al DPCM 9 dicembre 2021, n. 223, Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale.

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[161]), 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.

Il decreto, recependo la disciplina europea, ha quindi istituito un sistema di accreditamento specifico nel settore della cybersicurezza che vede ACN godere di una certa preminenza su Accredia, verso cui in certi casi svolge anche attività di controllo e vigilanza. La ragione è dovuta al fatto che in determinati casi (come la certificazione di affidabilità elevata), le attività di certificazione e accreditamento sono demandate all'esclusiva competenza di organismi di natura pubblica[162].

Ciò tuttavia non esclude il ruolo della seconda in questo ambito. Come si apprende dal sito di Accredia, «alcune attività di certificazione di prodotto [sono] delegate dall'Unione europea all'ACN. Altre, invece, verranno svolte sulla base di un accreditamento e di una collaborazione fra l'Agenzia e Accredia»[163]. Presumiamo infatti che Accredia resti esclusivamente competente in tutti i casi di accreditamento per quanto riguarda l'ambito volontario di cybersicurezza (diversamente da quello cogente che - come poc'anzi osservato - è di competenza dell'ACN).

Si delinea pertanto un sistema di accreditamento e certificazione di cybersicurezza ripartito su tre livelli di competenza di cui: il primo, di esclusiva competenza dell'ACN, relativo ai sistemi di accreditamento cogente (es. per i certificati di affidabilità elevata); il secondo, di collaborazione dell'ACN con Accredia; il terzo, di competenza residuale di Accredia.

5.2 Il sistema di certificazione italiano per motivi di sicurezza interna

L'art. 9 del d.Lgs. 123/2022 dispone che, in assenza di un sistema europeo di certificazione, l'ACN può introdurre sistemi nazionali di certificazione per i beni ICT, previa consultazione dei portatori di interesse. Tuttavia che, al fine di evitare la frammentazione del mercato interno dei sistemi di certificazione, in questo caso lo Stato italiano è tenuto ad informare la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cybersecurity.

Oggi questo disposto non ha più validità considerato che il 31 gennaio 2024 la Commissione europea ha emanato l'*European Cybersecurity Scheme on Common Criteria* (EUCC), il primo schema di certificazione (generale) europeo di cybersicurezza.

Tuttavia la disciplina europea delineata nel *Cybersecurity Act*, conformemente a quanto previsto all'art. 4, c. 2, TUE, prevede che «[n]on si dovrebbe tuttavia impedire agli Stati membri di adottare o mantenere in vigore sistemi nazionali di certificazione della cybersicurezza per motivi di sicurezza nazionale»[164]. Difatti all'art. 1, c. 2 del Regolamento è disposto che sono fatte salve le competenze degli Stati membri «per quanto riguarda le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale».

---

[161] 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 l'Aula Magna del Rettorato dell'Università La Sapienza.

[162] Come abbiamo ampiamente trattato in precedente (Parte III, Cap. I, 3 e 4), i sistemi di certificazione e accreditamento vedono la partecipazione di soggetti privati. Si comprenderà pertanto come la disciplina europea del *Cybersicurity Act* abbia profondamente inciso in questi settori.

[163] Si rivia alla pagina "*Cybersecurity, la certificazione accreditata per gestire i rischi informatici*" del 14 ottobre 2022, di cui al link:<https:// www.accredia.it/ 2022/10/14/ cybersecurity-la-certificazione-accreditata- per-gestire-i- rischi-informatici/>.

[164] Cons. 94, Reg. (UE) 2019/881.

Il punto porta ancora una volta a riflettere sul rapporto tra libero mercato (europeo) e sicurezza nazionale. Nei casi citati, sarà infatti possibile la creazione di un sistema italiano di certificazione per quei beni ICT che rientrano nei settori della pubblica sicurezza, della difesa, della sicurezza nazionale o relativi alle attività dello Stato nell'ambito del diritto penale, e che saranno quindi sottratti al normale regime di mercato[165].

A nostro parere, precisiamo tuttavia che simili misure devono essere interpretate come strumenti di intervento dello Stato, non per motivi di fallimento del mercato, ma come espressione di una capacità di adattamento dello Stato ai mercati globali, che lo hanno portato a dover sviluppare dei meccanismi di "graduazione" degli interessi economici rispetto alle esigenze di sicurezza interna.

[165] Cfr. A. PANSA, *La sicurezza nazionale. Innovazione e nuovi limiti*, in *Gnosis*, n. 1, 2019, pp. 31-32.

CONCLUSIONI

Lo studio ha preso avvio dalle ricordate intuizioni di Reidenberg e Lessig relative all'individuazione di un valido "appiglio" tecno-giuridico attraverso il quale i poteri pubblici avrebbero potuto orientare indirettamente le attività nel cyberspazio (o meglio, la "società informazionale"), incidendo sul «*code*», ossia sullo standard tecnico che governo il funzionamento logico delle reti.

L'assunto di tali ricostruzioni è che, se i tecnologi informatici progettano le caratteristiche di base dell'infrastruttura che crea ed attua le impostazioni predefinite della rete – il «*code*» per l'appunto - che limita di fatto le azioni degli utenti nel cyberspazio, gli Stati possono allora regolare indirettamente i comportamenti umani nel cyberspazio influenzando a monte le decisioni prese dai tecnologi attraverso leggi che impongono restrizioni sulle scelte che questi prendono[1].

Secondo quanto emerso dallo studio questa tesi conserva ancora rilevanza dato che i recenti sviluppi della normazione tecnica, soprattutto nel settore delle ICTs hanno ormai reso nota l'apparentemente neutralità di tali strumenti oramai sempre più politicamente rilevanti.

I sistemi di normazione, accreditamento e certificazione tecnica si sono rivelati essere strumenti che non solo hanno un impatto sul commercio internazionale, ma anche come strumenti che possono contribuire a colmare il vuoto dato dal fallimento del diritto internazionale nella stabilità del cyberspazio aumentando i livelli di sicurezza delle reti e dei sistemi informatici, almeno a livello europeo se non globale[2], attraverso uno strumento flessibile che "parla" il linguaggio del mercato: gli standard tecnici per l'appunto[3].

È interessante notare come la cybersicurezza abbia trovato definizione e regolamentazione in origine proprio all'interno di queste norme tecniche, poiché solo recentemente i pubblici poteri hanno iniziato a prestare attenzione a questa esigenza.

A tal proposito particolare attenzione è stata posta sulla definizione di cybersicurezza introdotta dall'Unione europea nel Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*), all'art. 2, n. 1, come l'«insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

Con questa concettualizzazione il legislatore europeo non ha solo tradotto in termini giuridici un concetto prima di allora conosciuto e formulato all'interno delle norme tecniche di settore, ma con quest'opera di "giuridicizzazione" ne ha anche conferito valore politico e sociale.

La formulazione testimonia tuttavia anche lo stretto legame tra norma giuridica e norma tecnica nel settore della cybersicurezza (per lo meno nell'ordinamento europeo e in quello degli Stati membri), ove al tradizionale riferimento alla garanzia della riservatezza, integrità e disponibilità (c.d. R.I.D.) dell'informazione e del supporto che la contiene quali principali caratteristiche definite nelle norme tecniche di *information* e *computer security*, è stata affiancata la "sicurezza dell'umano",

---

[1] L. LESSIG, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, in *Common Law Conspectus*, n. 5, 1997, reperibile al link:<https://scholarship.law.edu/commlaw/vol5/iss2/5/>.

[2] N. KATAGIRI, *Why international law and norms do little in preventing non-state cyber attacks*, in *Journal of Cybersecurity*, Vol. 7, Issue 1, 2021, reperibile al link:<https://academic.oup.com/cybersecurity/ article/7/1/ tyab009/ 6168044>.

[3] Cfr. N. IRTI, *Norma e luoghi ...op.cit.*, p. 62 e 67, ove Illustre dottrina afferma che «La perdita dei luoghi non consente l'immediata individuazione del diritto applicabile. Il dove giuridico attende nuovi criteri. Lo spazio telematico, sciolto da agganci terrestri, si apre a tutte le soluzioni dell'artificialità. [...] Le risorse dell'artificialità si mostrano infinite, duttili, flessibili. Esse appartengono allo stesso mondo della tecnica e dell'economia, e perciò sono in grado di seguirle e di stringerle».

intesa sia delle persone fisiche che utilizzano l'informatica (gli utenti), ma anche coloro che sebbene non utilizzino tali risorse possono comunque essere impattati dagli effetti negativi della loro mera disfunzione o di ciò che viene veicolato attraverso il cyberspazio (si pensi agli attacchi informatici ma anche alla disinformazione).

La normazione tecnica sembra quindi dirigersi sempre più verso interessi sociali diffusi che trascendono gli affari.

Sulla scorta di tali considerazioni, la nostra riflessione si è concentrata sul modello che sta delineando il legislatore europeo, ove già dalla Strategia europea di cybersicurezza per il decennio digitale presentata nel dicembre 2020[4], si apprende che a fronte del fatto che «[l]a normazione internazionale è sempre più utilizzata dai paesi terzi per far progredire la loro agenda politica e ideologica, che spesso non corrisponde ai valori dell'UE», l'Unione ha da qualche tempo intrapreso un cammino volto a formulare norme internazionali nei settori delle tecnologie emergenti, e dell'architettura di base di Internet, in linea con i valori dell'UE al fine di garantire che Internet rimanga globale e aperta, che le tecnologie siano antropocentriche, attente alla riservatezza, e che il loro uso sia sicuro ed etico e quindi conforme al quadro legislativo europeo al riguardo[5].

Riprendendo un interrogativo già posto in dottrina, sorge spontaneo chiedersi se questo processo, che vede una compartecipazione di norme giuridiche (di diritto derivato) e norme tecniche, porti alla «tecnicizzazione della norma giuridica a contenuto tecnico o [alla] giuridicizzazione della norma tecnica incorporata in quella giuridica»[6].

Il punto ci ha portato a dover ricostruire la dibattuta relazione tra norma tecnica e ordinamento giuridico animata da orientamenti interpretativi vari originati da due quesiti di fondo: le norme tecniche sono parte dell'ordinamento giuridico? ovvero, se ne sono estranee, come si pongono allora rispetto a questo?

Come osservava il Cesarini Sforza, sul punto si frappongono due opposte teorie, quella monista (o statalista), secondo cui non è ammissibile altro diritto (inteso come complesso di norme) se non quello creato o realizzato dallo Stato con manifestazioni di sua volontà, e la teoria pluralista che, contrariamente alla prima, ammette che il diritto possa originarsi anche da esigenze o forze, di carattere individuale o sociale, indipendenti dall'esistenza dello Stato, anche se queste si concretizzano nello Stato e mediante manifestazioni della sua volontà[7].

---

[4] Commissione europea, *Comunicazione congiunta al parlamento europeo e al consiglio. La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN(2020) 18 final.

[5] *Ivi*, p. 20.

[6] F. SALMONI, *Le norme tecniche*, Milano, 2001, pp. 165 ss.

[7] W. CESARINI SFORZA, *Ordinamenti giuridici (pluralità degli)*, in *Novissimo digesto italiano*, vol. XII, 1957, p. 1. Approfondendo le origini del contrasto, il Cesarini Sforza scrive «[s]e bene si osserva, l'affermazione che accanto all'ordinamento giuridico dello Stato possono coesistere altri ordinamenti ugualmente giuridici, ossia l'affermazione che più ordinamenti possono logicamente coesistere, in tanto è possibile in quanto il concetto di "ordinamento" è perso nel senso logico-formale di sistema di rapporti, fra determinati oggetti, stabilito secondo un certo criterio. Variando questo criterio, cambia il sistema, onde gli stessi oggetti possono essere ordinati in modi diversi, il che non toglie che tutti questi ordinamenti siano validi nello stesso modo. Se invece l'ordinamento è concepito non nel suo senso logico, ma come concreta manifestazione di una volontà ordinatrice, ossia come atto ordinatore in base un criterio scelto e applicato, allora non può più accadere che tutti i possibili ordinamenti siano validi allo stesso modo, bensì la validità di uno di essi esclude necessariamente quella degli altri. Il che come dire se si possono "pensare" molteplici ordinamenti per la medesima materia, viceversa non è possibile "ordinare" la medesima materia che in un unico modo alla volta [...]. Ora il contrasto fra le due teorie della pluralità e della statualità deriva essenzialmente dal duplice concetto di ordinamento [così esposto], e perciò, mentre la teoria pluralistica è inattaccabile entro l'ambito del concetto puramente logico o, come potrebbe dirsi, statico, invece gli argomenti che la sostengono non hanno nessun valore, se portati contro l'altra teoria che si basa sul concetto che potrebbe dirsi dinamico; ed è altrettanto vero il viceversa».

La normazione tecnica è un esempio emblematico a tal proposito. Essa è infatti interpretata come uno dei fenomeni che si pone fuori dalla legislazione e quindi in un "altrove" rispetto all'ordinamento giuridico[8].

Nello specifico, la norma tecnica è stata tipicamente ricondotta in quel particolare ambito dell'autonomia privata già individuato dal Romano e che sarà poi definito da Cesarini Sforza come il «diritto dei privati», ossia un diritto parallelo a quello dello Stato che «i privati medesimi creano per regolare determinati rapporti di interesse collettivo in mancanza, o nell'insufficienza, della legge statuale»[9]. Un diritto che per l'appunto si distingue dal diritto privato, ossia il «complesso di *volontà statuali* miranti a regolare rapporti tra persone private»[10], in quanto comprensivo delle regole non emanate dallo Stato ma destinate ad essere osservate da soggetti ulteriori rispetto a quelli che le hanno redatte, tali da produrre effetti *erga omnes* per tutta la categoria (*rectius* corpi sociali compatti[11]) a cui queste si rivolgono[12].

Si comprenderà che il corretto inquadramento della questione necessita di un contemperamento dei due opposti interessi. Secondo Alcuni, le teorie del primo tipo correrebbero il rischio di non cogliere la complessità del sistema della normazione tecnica, la cui origine e sviluppo sono nelle dinamiche spontanee della produzione e innovazione dei privati[13]. Ma, allo stesso tempo, si ammette che la materia non può essere inquadrata in chiave esclusivamente privatistica[14].

---

[8] Cfr. A. ZEI, *Tecnica e diritto. Tra pubblico e privato*, Milano, Giuffrè, 2008, pp. 5-6.

[9] W. CESARINI SFORZA, *Il diritto dei privati*, Milano, Giuffrè, 1963, p. 3.

[10] *Ivi*, p. 4. Sul rapporto tra diritto civile e potere pubblico dello Stato si rinvia alle magistrali parole di Filippo Vassalli secondo cui «Il diritto civile non è mai stato mancipio dello Stato come è avvenuto nella fase più recente. Non lo è stato per l'intrinseca sua natura, né per il suo processo di formazione. Il diritto civile [...] è disciplina di libere determinazioni. Vocazione delle norme che si dicono di diritto privato, perché concernenti codeste materie, è di realizzare certe esigenze di giustizia nei rapporti che si svolgono liberamente tra gli uomini: a tal fine non si richiede necessariamente l'intervento del potere pubblico. Il mirabile monumento del diritto romano è costituito prevalentemente per opera di giureconsulti, cioè di privati [...] e del pretore, cioè del magistrato che deve *ius dicere*, dichiarare ciò che è diritto nei singoli rapporti in contestazione, che ha dunque una funzione ben diversa dalla legislativa [...]. La legge, cioè il diritto dettato dai pubblici poteri, ha avuto uno sviluppo limitato, nell'orbita di codesti rapporti; originariamente segna e assicura i limiti nei quali l'autonomia privata si attua [...]» F. VASSALLI, *Extrastatualità del diritto civile*, in *Rivista italiana di scienze giuridiche,* 1951, pp. 482-483, il frammento è riportato in S. ROMANO, *Ordinamenti giuridici privati (appunti)*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, p. 1379.

[11] Sul punto si rinvia a V. CRISAFULLI, *Lezioni di diritto …op.cit.* p. 6, a proposito del concetto di "gruppo propriamente organizzato" ove il Crisafulli a proposito della teoria di Cesarini Sforza scrive che «uno tra gli elementi differenziali tra collettività "diffuse" e *i veri corpi sociali compatti* (gruppi-"enti") [è] nel carattere autoritario di questi ultimi».

[12] A tal proposito osservava S. ROMANO in *L'ordinamento giuridico …op.cit.*, p. 112, «[i]l diritto privato italiano non conosce alcun potre di supremazia, la cui figura non si rinviene se non nel campo del diritto pubblico. Esso quindi regola i rapporti che ricadono sotto le sue norme [...]. Senonché, ciò non corrisponde a realtà. Tutte le volte che si ha un organismo sociale, di qualche complessità, sia pure lieve, nel suo interno si instaura una disciplina, che contiene tutto un ordinamento di autorità, di poteri, di norme, di sanzioni». Come sintetizzato da Salvatore Romano, «[i]l diritto dei privati regola sì i rapporti tra persone private e talvolta quelli stessi che sono già regolati dal diritto privato e anche pubblico ma non emana dallo Stato nè immediatamente nè mediatamente»; e ancora «[...] formuliamo la domanda se un ordinamento statuale abbia dinnanzi a sè un ordinamento generale dei privati, distinto dalla pluralità degli ordinamenti particolari dei privati stessi. Cediamo debba darsi risposta affermativa a questo quesito [...]» (S. ROMANO, *Ordinamenti giuridici privati (appunti)*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, p. 1382 e 1393). Relativamente all'autonomia privata tracciata nel codice civile v. A.C. JEMOLO, *Lo "spirito di liberalità"*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960, Torino, pp. 973 ss. Sulle due diverse accezioni di fonti dell'autonomia privata in studi recenti si rinvia anche a M. CERIONI, *Prime riflessioni sulle fonti dell'autonomia privata*, in *Annali della Facoltà giuridica dell'Università di Camerino – Nuova Serie*, n.1, 2012, reperibile al link:<https://afg.unicam.it/sites/afg.unicam.it/files/CERIONI_prime_ riflessioni_fonti.pdf>.

[13] Cfr. P. LAZZARA, *La normativa tecnica …op.cit.*

[14] *Ivi*, p. 431.

Il problema si pone in tutti quei casi in cui la norma tecnica entra in relazione con l'ordinamento giuridico[15]. Il che avviene seguendo gli schemi tipici dei criteri di collegamento fra gli ordinamenti, ossia attraverso la presupposizione, quando un ordinamento riconosce la qualificazione di alcuni fatti ad opera di altri ordinamenti, o il rinvio, mediante il quale le norme prodotte dall'ordinamento esterno sono richiamate dall'ordinamento giuridico facendole proprie (rinvio fisso o materiale o recettizio), oppure quando l'ordinamento giuridico «dichiara che certe materie o rapporti rimangano esclusi dalla sua sfera e abbandonati ad altro ordinamento»[16].

Una parte della recente dottrina[17], ha individuato una possibile chiave interpretativa del collegamento tra i due ordinamenti nelle tesi sviluppate da Salvatore Romano, il quale, riprendendo gli studi del padre, Santi Romano, sulla pluralità degli ordinamenti giuridici, ebbe modo di elaborare la teoria degli "ordinamenti giuridici privati".

Secondo questa dottrina,

> la sfera privata rimane, come istituzione originaria sulla base di un principio di separazione [...], coordinata o solo parzialmente subordinata, attraverso la funzione legislativa, all'organizzazione statuale stessa. Questa coordinazione e parziale subordinazione si concreta in "relazioni" con l'ordinamento statuale di vario genere e di varia configurazione[18].

Salvatore Romano, contrapponendosi alle dottrine giuspubblicistiche, ove si registra una «netta tendenza ad accentuare la nota della subordinazione della sfera privata a quella pubblica», proponeva una teoria di «considerazione privatistica», senza tuttavia negare i temperamenti a tale elaborazione[19].

Secondo il Giurista, infatti, quella che viene spesso interpretata come una "linea di demarcazione" tra ordinamenti pubblici e privati, costituisce allo stesso tempo una «linea di rapporto»[20]. A tal proposito, veniva preso in considerazione l'esempio della funzione legislativa ove da una parte, l'ordinamento privato, attraverso le persone fisiche, è operante nella funzione legislativa dello Stato (vedi ad esempio i partitici politici quale espressione del libero associazionismo dei cittadini), e l'ordinamento pubblico deve riconoscerlo a tutti gli effetti, ma dall'altro, la legge, rappresenta anche la «misura all'ingerenza del pubblico che l'ordinamento privato ammette nel suo campo»[21].

---

[15] Secondo la teoria di Santi Romano ciò presuppone una «rilevanza giuridica», ossia l'esistenza o il contenuto o l'efficacia di un ordinamento devono essere condizionate da un altro ordinamento in base ad un titolo giuridico, così S. ROMANO, *L'ordinamento giuridico ...op.cit.*, p. 126.

[16] S. ROMANO, *L'ordinamento giuridico ...op.cit.*, p. 135. Sul punto, il Romano, richiama le tesi di altra magistrale dottrina quale quella di Dionisio Anzillotti in D. ANZILOTTI, *Il diritto internazionale nei giudizi interni*, Bologna, Zanichelli, 1905, pp. 179 ss.

[17] P. LAZZARA, *La normativa tecnica ...op.cit.*, nonché da ultimo, A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione,* Napoli, Editoriale scientifica, 2018.

[18] S. ROMANO, *Ordinamenti giuridici privati (appunti) ...op.cit*., p. 1415.

[19] *Ivi*, p. 1414. Nello specifico, precisa Salvatore Romano «[...] le due sfere si presentano ambedue necessarie. Vedremo anche se, come sfere, non si presentino anche come originarie, tenuto conto di quella dottrina che riconosce carattere originario a quegli ordinamenti del c.d. diritto dei privati concepito fuori da ogni dipendenza dall'ordinamento statuale: questa asserzione potrebbe indurre a considerare sotto lo stesso profilo tutti, e non solo in parte, gli ordinamenti privati. Secondariamente c'è da terner presente un processo storico: da una comunità di privati si è distaccata l'organizzazione dei poteri pubblici [...]. Abbiamo però veduto come l'organizzazione a strato non tolga il carattere di ordinamento alla comunità dei privati, mentre deve ammettersi il riconoscimento della sopravvivenza delle consuetudini, almeno in una certa misura. Si aggiungano le note considerazioni secondo le quali la produzione delle norme è riservata, nell'autonomia, agli stessi privati, mentre l'efficacia è il principale compito dell'ordinamento centrale. Può quindi ripetersi quanto già osservato, e cioè che una società organizzata a Stato conserva tutte le sue caratteristiche di ordinamento giuridico privato».

[20] *Ivi,* p. 1415.

[21] *Ibidem.*

Il pregio di questa teoria è quindi quello di aver fornito ulteriori e più dettagliate argomentazioni sulla separazione dei due ordinamenti, e di aver evidenziato come l'ordinamento privato acquista rilevanza per quello pubblico solo in determinate occasioni, ossia quando i due ordinamenti entrano in relazione. Tuttavia, stando a quanto descritto, resta il dubbio circa alcune questioni, prima fra tutte la qualificazione di tali espressioni dell'autonomia privata come ordinamenti (privati) dotati di giuridicità a tutti gli effetti.

A nostro modo di vedere, maggiori chiarimenti sul punto sono stati forniti da un recente orientamento dottrinario che, proprio a proposito delle regolazioni a contenuto tecnico scientifico, analizzate dalla prospettiva del diritto costituzionale, ha ritenuto che

> [l]'ordinamento tecnico resta [...] un ordinamento separato che non è in grado di acquistare il carattere della giuridicità, ma dei cui prodotti può avvalersi il legislatore per conferire loro specificamente ed occasionalmente forza normativa, in virtù della mediazione necessaria di una fonte imperativa [enfasi aggiunta][22].

Secondo questa teoria le norme tecniche «non acquistano di per sé ed una volta per tutte il carattere della normatività, ma solo per il tramite della legge e per via della "scelta", mai irreversibile, effettuata di volta in volta dall'ordinamento giuridico»[23]. In altre parole, una determinata norma tecnica (volontaria) acquista il tratto della giuridicità, in via occasionale e nel solo caso specifico, per mezzo della «selezione volontaria» operata per il tramite della legge o altra fonte dell'ordinamento giuridico[24]. Pertanto, al dubbio se «quando una norma tecnica diventa il contenuto di una norma giuridica [o è da essa rinviata], non sarebbe la prima a giuridicizzarsi, ma la seconda a [...] tecnicizzarsi», tale teoria si pone a sostegno dell'ipotesi inversa, negando la tecnicizzazione della norma giuridica che la priverebbe di forza e riconoscendo il tratto della giuridicità alla norma tecnica tutte le volte che questa entra in relazione con l'ordinamento giuridico[25].

L'ipotesi è quindi quella di applicare la tesi della separazione al particolare caso del rapporto fra l'ordinamento giuridico e il sistema della normazione tecnica, nel solco della teoria della pluralità, ma senza assumere la pretesa di qualificare l'ordinamento a cui si rinvia come normativo o giuridico[26].

Simile interpretazione consentirebbe inoltre di spostare la riflessione sulla legittimità del potere privato nell'ambito della normazione e regolazione tecnica dalla applicazione delle norme tecniche e al loro rapporto con le norme giuridiche, al momento della loro produzione[27], e quindi sugli specifici procedimenti di formazione di tali norme, sulla qualifica dei soggetti che vi partecipano e con quale rilievo. Questioni queste che sono al centro dell'odierno dibattito sul punto e che non escludono, ma

---

[22] A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione …op.cit*., p. 78.

[23] *Ivi*, p. 77.

[24] *Ivi*, p. 78.

[25] Cfr. F. SALMONI, *Le norme tecniche*, Milano, Giuffrè, 2001, pp. 165 ss. Tesi contrarie nella dottrina italiana hanno invece sostenuto, soprattutto nel caso dell'incorporazione che, «la norma giuridica non potrebbe mai avere un contenuto tecnico se non elementare, essendo in ogni altro caso il dato tecnico solamente un presupposto di fatto, da valutarsi dal giudice; di guisa che le norme di legge (o regolamento) che avessero invece tale contenuto non sarebbero norme aventi per destinatari la generalità dei soggetti dell'ordinamento e i giudici, ma i soli organi (tecnici) dell'amministrazione [...]». Così scriveva Vittorio Bachelet in V. BACHELET, *L'attività tecnica della pubblica amministrazione*, Milano, Giuffrè, 1967, p. 88, a proposito di Arnaldo De Valles, in A. DE VALLES, *Norme giuridiche e norme tecniche*, in A.C. JEMOLO (a cura di), *Diritto amministrativo, diritto costituzionale, diritto internazionale, diritto penale, procedura penale*, Milano, Giuffrè, 1963, pp. 175-188.

[26] *Ivi*, p. 77.

[27] Cfr. F. SALMONI, *Le norme tecniche*, Milano, Giuffrè, 2001, p. 31.

anzi portano ancora una volta a dover concentrare la riflessione sulla legittimazione degli enti di normazione e sulla democraticità delle procedure di formazione delle norme tecniche[28].

Fin qui l'analisi ha tuttavia interessato l'interpretazione della norma tecnica secondo i canoni dell'ordinamento giuridico.

Altra questione, connessa alla prima, riguarda il sistema di formazione delle norme tecniche europee, ed in particolare quelle armonizzate, che riteniamo essere una peculiare forma di co-regolazione che vede l'Unione europea impegnata ad estendere il rispetto dei più ampi principi di democrazia in tutti i processi di formazione di tali norme.

L'analisi del sistema di normazione europeo ci ha infatti permesso di osservare come in questo particolare contesto si stia delineando un efficace meccanismo di convergenza verso il rispetto di principi a vocazione giuspubblicistica, senza passare per la "giuridicizzazione" della norma tecnica o la "pubblicizzazione" degli enti che producono dette norme, che quindi restano di natura privata. Ciò è reso possibile grazie ad una doppia azione, da una parte dell'Unione per mezzo di interventi legislativi di diritto derivato, anche recenti (al riguardo si rinvia all'analisi dei Regolamenti (UE) 2022/2480 e 2023/988), e dall'altra, da parte degli stessi enti di normazione, certificazione ed accreditamento (europei) che hanno scelto di introdurre nei loro spazi di autonomia, attraverso libere iniziative di queste sul punto (*self regulation*), simili principi e meccanismi di funzionamento.

Circa quest'ultimo aspetto, una certa dottrina ha elaborato la teoria della *private administrative law*[29], ossia l'adozione volontaria di strumenti che assicurino maggiore democraticità nei processi decisionali, proprio in quegli spazi di autonomia in cui il potere pubblico non può interferire. Una espressione quindi di quel "diritto dei privati" che non può essere ricondotto «*neither public nor private action, but something different and diverse*»[30] e che possiamo interpretare come un avvicinamento - spontaneo o eterodiretto dai governi - degli enti normatori privati alle dinamiche sociali e non più solo a quelle di mercato.

Tuttavia, nonostante l'*enforcement* a garanzia di maggiore democraticità nei processi decisionali di tali soggetti, dall'analisi delle carte istituzionali delle organizzazioni di normazione europea è emerso come questa convergenza pare non essere stata totalmente accolta dall'*European Telecommunications Standards Institute* (ETSI). Sebbene l'Ente abbia istituito appositi canali di dialogo con le organizzazioni rappresentative interessi sociali (vedi il *3SI Advocate*), non ne ha tuttavia dettagliato le modalità di partecipazione, non apportando alcun miglioramento di fatto alla condizione di tali rappresentanze fortemente svantaggiate dal sistema di voto che riconosce un peso maggiore al voto delle grandi imprese e gruppi industriali di settore che vi prendono parte[31]

Il dato è di particolare rilievo, non solo sotto il profilo giuspubblicistico generale, ma anche per tutte le questioni in cui le garanzie di diritto pubblico trovano applicazione nel contesto delle ICT, data la competenza dell'Istituto.

A tal proposito pare allora d'interesse evidenziare come, in determinati settori, tra cui anche quelli dell'Intelligenza artificiale e di cybersicurezza (conformemente alla proposta di Regolamento *Cyber Resilience Act*), la Commissione ha il potere di adottare specifiche tecniche comuni mediante atti di esecuzione, per garantire la tutela dell'interesse pubblico nei casi in cui non vi siano norme

---

[28] M. ELIANTONIO, C. CAUFFMAN (a cura di), *The legitimacy of standardisation as a regulatory technique: a cross-disciplinary and multi-level analysis*, Cheltenham, Northampton, Edward Elgar, 2020.

[29] R. VALLEJO, *The private administrative law of technical standardization …op.cit.*

[30] R. VALLEJO, *The private administrative law of technical standardization …op.cit.* p. 222.

[31] Ivi, p. 9 ss.

armonizzate o quelle esistenti siano insufficienti[32]. L'intervento dell'Unione in questo frangente è quindi volto ad incidere sul sistema di normazione tecnica per ragioni che trascendono gli interessi economico-commerciali.

Nel complesso la disciplina europea risultante dalle recenti riforme pare quindi aver iniziato un processo di "contaminazione" dei processi decisionali alternativi a quelli giuridico-politici orientando gli enti di normazione a rispettare principi di democraticità e trasparenza. Ciò è quindi particolarmente rilevante per il futuro sistema di normazione e certificazione di cybersicurezza europeo che si sta delineando.

Dal *Rolling Plan for ICT standardisation* 2024 si apprende che, dopo l'adozione della proposta di Regolamento (UE) 2022/272 (anche nota come *Cyber Resilience Act* - CRA) (COM/2022/454 final), che tra le altre questioni disciplina anche i requisiti essenziali di cybersicurezza dei beni ICT, la Commissione europea preparerà una richiesta formale di normazione per sostenere l'attuazione del CRA.

Dobbiamo pertanto presumere che la Commissione avvierà una richiesta di normazione ad una delle ESOs per l'elaborazione della prima norma armonizzata di cybersicurezza, la quale dovrà essere elaborata conformemente ai requisiti essenziali stabiliti dal CRA (e quindi non ai requisiti definiti dalla Commissione stessa come previsto dall'art. 10 Reg. 1025/2012).

Tale norma, al momento non ancora richiesta dalla Commissione, potrebbe pertanto essere il primo standard a trovare applicazione in un particolare e delicato ambito quale quello della (cyber)sicurezza, prodotto in considerazione di interessi che non sono solo di un certo gruppo di grandi imprese, ma anche della rappresentazione della piccola e media industria, nonché soprattutto delle varie rappresentanze sociali e dell'ambiente che troveranno spazio grazie alla recente riforma della disciplina generale sulla normazione tecnica.

Non solo. Pare rilevante osservare anche come assieme all'impulso di garantire maggiore rappresentanza nei processi decisionali degli enti di normazione, stiano prendendo piede anche iniziative volte a promuovere la tutela dei diritti umani quali parametri di formazione di tali norme[33].

In attesa dell'adozione della citata norma armonizzata di cybersicurezza, la riflessione ha avuto perlopiù ad oggetto il sistema di certificazione europea di cybersicurezza, l'*European Cybersecurity Scheme on Common Criteria* (EUCC), attuato per mezzo del Regolamento (UE) 2024/482, entrato in vigore il 31 gennaio 2024.

In conclusione, se consideriamo l'attività normativa come espressione di un esercizio di potere, alla luce di quanto sin qui emerso pare allora poter tentare di capire chi effettivamente detenga potere nel contesto digitale.

Sebbene le riflessioni degli studiosi siano spesso concentrate sullo "strapotere" dei privati nel digitale, dell'analisi dell'attuale disciplina sulla normazione tecnica nel settore della cyberisucrezza l'impressione è che l'Unione europea – sulla scorta dell'esigenza di affermarsi sui mercati e di preservare e diffondere i propri principi – stia fortemente accentrando i poteri sulle amministrazioni pubbliche, ed in particolare nelle mani della Commissione.

In un contesto ove si è soliti notare forme organizzative di c.d. *multistakeholder governance* come in quello digitale si riscontra pertanto una diversa morfologia a livello unionale, ove il processo di

[32] Comunicazione, *Una strategia dell'UE in materia di normazione …cit.,* p. 5-6.

[33] Si rinvia al Report ONU, *Human rights and technical standard-setting processes for new and emerging digital technologies*, 9 giugno 2023, reperibile al link:<https://www.ohchr.org/sites/default/files/ documents/hrbodies/ hrcouncil/ sessions-regular/session53/advance-versions/A_HRC_53_42_AdvanceUneditedVersion.docx>.

regolazione è perlopiù affidato al potere pubblico e centralizzato delle istituzioni europee. A tal proposito si è rilevato come nel particolare caso della sicurezza, tipicamente riservata alla sovrana competenza degli Stati, la cybersicurezza e la cyberresilienza risultino essere in parte definite e regolate a livello unionale.

Ci si chiede allora se nella politica europea digitale siano ancora possibili forme di pura co-regolazione pubblico privata, di cui le norme armonizzate fino a prima della loro riforma nel 2022 erano espressione, o piuttosto dovremo abituarci ad assistere all'affermazione di forme di eterodirezione di un potere sull'altro.

Siamo dell'opinione l'uno o l'altro panorama stimoleranno sempre il giurista a dover leggere e criticare tali assetti secondo lo spettro del costituzionalismo, e quindi della limitazione e del bilanciamento di tutti i poteri, siano essi pubblici o privati.

BIBLIOGRAFIA

ALÌ A., *Il diritto dell'Unione Europea e la tutela della sicurezza nazionale degli Stati membri. Osservazioni a margine di alcuni casi esaminati dalla Corte di giustizia dell'Unione Europe*, in U. GORI, L. MARTINO, *Intelligence e interesse nazionale*, Aracne, 2015, pp. 593-604

ATERNO S., *Sicurezza informatica: aspetti giuridici e tecnici*, Pisa, Pacini giuridica, 2022;

BALDINI V. (a cura di), *Sicurezza e Stato di diritto: problematiche costituzionali*, Cassino, Edizioni dell'Università degli Studi di Cassino, 2005;

BALLADORE PALLIERI G., *Il concetto di rinvio formale e il problema del diritto internazionale privato*, in *Rivista di diritto civile*, XXI, 1929;

BARABÁSI A.L., *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, New York, 2014;

BARAN P., *On distributed communications: Introduction to distributed communications networks*, RAND Corp., Santa Monica (CA), 1964;

BARATTA A., *Diritto alla sicurezza o sicurezza dei diritti?*, in *Democrazia e diritto*, n. 2, 2000;

BARLOW J.P., *A Declaration of the Independence of Cyberspace*, 8 febbraio 1996;

BASSAN F., *Dalla golden share al golden power: il cambio di paradigma europeo nell'intervento dello Stato sull'economia*, in *Studi sull'integrazione eur.*, vol. 9, n. 1, 2014;

BASSI N., *Agenzie nazionali ed europee*, in *Enc. dir., Annali*, II, t. 2, Milano, 2009;

BASSINI M., POLLICINO O., *Verso un internet bill of rights*, Roma, Aracne, 2015;

BASSINI M, *Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica*, in *Diritto costituzionale: rivista quadrimestrale*, vol. 6, n. 1, 2023;

BASSU C., PISTORIO G., STERPA A., *Diritto pubblico della sicurezza*, Napoli, Editoriale scientifica, 2023;

BATTISTELLI F., GALANTINO M.G., *Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk*, in *Current Sociology,* vol. 67, n. 1, 2019;

BELLI L., DE FILIPPI P. (a cura di), *Network Neutrality: an Ongoing Regulatory Debate*, 2014;

BELLISARIO E., *Certificazione di qualità e responsabilità civile*, Milano, Giuffrè, 2011;

BENDIEK A., BOSSONG R. SCHULZE M., *The EU's Revised Cybersecurity Strategy*, in *SWP Comments*, n. 47, 2017;

BENEDETTI A., *Certezza pubblica e certezze private: poteri pubblici e certificazioni di mercato*, Milano, Giuffrè, 2010;

BENKLER Y., *Symposium Overview: Part Iv: How (IF At All) To Regulate The Internet: Net Regulation: Taking Stock And Looking Forward*, in *University of Colorado Law Review*, vol. 71. 2000;

BERGER K.P., *The Creeping Codification of the Lex Mercatoria*, Kluwe law, London, 1999;

BERKICH D., D'ALFONSO M. (a cura di), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence. Philosophical Studies Series*, Springer, Cham, vol 134, 2019;

BERLIN I., *Quattro saggi sulla libertà* (1969), Milano, Feltrinelli, 1989;

BERTUZZI L., *EU Commission pitches double reporting of open security loopholes in cybersecurity law*, in "Euractiv", 15 novembre 2023;

BERTUZZI L., *EU institutions finalise agreement on cybersecurity law for connected products*, in "Euractiv", 5 dicembre 2023;

BERTUZZI L., *EU policymakers prepare to close on cybersecurity law for connected devices*, in "Euractiv", 30 novembre 2023;

BIN R., *L'interesse nazionale dopo la riforma: continuità dei problemi, discontinuità della giurisprudenza costituzionale*, in *Le Regioni, Bimestrale di analisi giuridica e istituzionale*, n. 6, 2001;

BIVONA E., *Le certificazioni di qualità: vizi del prodotto e responsabilità dell'ente certificatore*, in *Contr. impresa*, 2006;

BLACKSTONE E., HAKIM S., MEEHAM B.J., *Handbook on Public and Private Security*, Cham, Springer International Publishing, 2023;

BOBBIO N., *Democrazia e segreto*, Torino, Einaudi, 2011;

BOBBIO N., MATTEUCCI N., PASQUINO G., *Dizionario di politica*, Torino, 1990;

BOBBIO N., *Norma giuridica*, in *Novissimo digesto italiano*, vol. XI, Torino, 1965;

BOMBELLI G., *Su qualche destino della "forma-codice"*, in *Jus*, n. 4, 2023, pp. 97-141;

BOMBELLI G, FARAH P., *The Interlinkages Science-Technology-Law: Information and Communication Society, Knowledge-Based Economy and the Rule of Law*, in *Legal Studies Research Series*, n. 43, 2023, pp. 1-14;

BONETTI P., *Allocazione delle funzioni amministrative e le forme di coordinamento per le materie dell'ordine pubblico, della sicurezza e dell'immigrazione nel nuovo art. 118, della Costituzione*, in *le Ragioni*, n. 5, 2002;

BONZANO C., *La Consulta alza il 'sipario nero': alla ribalta la deprecabile confusione normativa tra prova e fatto*, in *Archivio penale*, 2014;

BOOTH K., *Theory of word security*, Cambridge university press, Cambridge, 2007;

BOURDEAU P., *Resiliencism: premises and promises in securitisation research*, in *Resilience: International Policies, Practices, and Discourses*, vol. 1, n. 1, 2013;

BOURNE M., *Understanding security*, Macmillan Publishing, Londra, 2014;

BRADIMARTE R., CHIANTERA-STRUTTE P., DI VITTORIO P., MARZOCCA O., ROMANO O., RUSSO A., SIMONE A. (a cura di), *Lessico di biopolitica*, Manifestolibri, Roma, 2006;

BRESSAN M., CUZZELLI G., *Da Clausewitz a Putin: la guerra nel XXI secolo*, Milano, Ledizioni, 2022;

BUCHANAN B., *The hacker and the State. Cyber attacks and the new normal of geopolitics*, Harvard, Harvard University Press, 2020;

BURES O., CARRAPICO H. (a cura di), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham, 2018;

BURRI M., ZIHLMANN Z., *The EU Cyber Resilience Act – An Appraisal and Contextualizatio*n, in "Zeitschrift für Europarecht (EuZ)", n. 2, 2023;

BUZAN B., *New Patterns of Global Security in the Twenty-First Century*, in *International Affairs (Royal Institute of International Affairs 1944-)*, vol. 67, n. 3, 1991;

BUZAN B., *Rethinking Security after the Cold War*, in *Cooperation and Conflict*, vol. 32, n. 1, 1997;

BUZAN B., WAEVER O., DE WILDE J., *Security: a new framework for analysis*, London, Lynne Rienner, 1998;

CADOCCI-PISANELLI G., *L'invalidità come sanzione di norme non giuridiche*, Milano, Giuffrè, 1940;

CALDERAI V., *The Privatization of Military and Security Services and the Limits of Contract Law*, in EUI MWP, 2010/31;

CALESINI G., *Diritto europeo di polizia*, Roma, Laurus Robuffo, 2007;

CALIGIURI M., *Intelligence e diritto. Il potere invisibile delle democrazie*, Soveria Mannelli, Rubbettino, 2021;

CALIGIURI M., *Cyber Intelligence. Tra libertà e sicurezza*, Roma, Donzelli, 2016;

CALZOLAIO S., IANNUZZI A., LONGO E., OROFINO M., PIZZETTI F., *La regolazione europea della società digitale*, Torino, Giappichelli, 2024;

CANNIZZARO E., *Diritto internazionale*, ed. II, Torino, Giappichelli, 2014;

CANNIZZARO E., *La sovranità oltre lo Stato*, Bologna, l Mulino, 2020;

CANNIZZARO E., *La sovranità oltre lo Stato*, Il Mulino, Bologna, 2020;

CAPORALE M., *Segreto di Stato, segreto amministrativo e sistema di classificazione delle informazioni*, Libreria Bonomo editrice, Bologna, 2013;

CAPPELLETTI F., MARTINO L., *Achieving Robust European Cybersecurity through Public–Private Partnerships: Approaches and Developments*, in *EU Policy Review,* vol. 1, 2021;

CAPPELO P., *La fenomenologia del rinvio statico e del rinvio dinamico*, 2005;

CAPRIO A., *L'"ultimo atto" della vicenda Abu Omar: cala il sipario ma qualche dubbio resta sulla scena*, in *Forum di Quaderni Cosituzionali*, 2014;

CARAVITA B., *Difesa europea, quali prospettive*, in *federalismi.it*, n. 1, 2019;

CARAVITA B., *In tema di "interesse nazionale" e riforme istituzionali*, in *federalismi.it*, n. 6, 2003;

CARAVITA B., *Sicurezza e sicurezze nelle politiche regionali*, in *federalismi.it*, n. 25, 2004;

CARINGELLA F., IANNUZZI A., LEVITA L. (diretto da), *Manuale di pubblica sicurezza*, Roma, Dike, 2013;

CAROTTI B., *Il sistema di governo di Internet*, Giuffrè, Milano, 2016, p. XIII;

CASINI L., *Le agenzie amministrative*, in *Riv. trim. dir. pubbl*., 2003;

CASSANO G., PREVITI S. (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020;

CASSANO G., SCORZA G. (a cura di), *Metaverso: diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT*, Pacini giuridica, Pisa, 2023;

CASSESE S. (a cura di), *Trattato di diritto amministrativo*, I, II ed., Milano, 2003;

CASSESE S. (a cura di), *Trattato di diritto amministrativo*, vol. IV, 2003;

CASTALDO F., *Dalla cyber defence alla cyber resilience dell'infrastruttura critica. Alcune implicazioni strategiche e organizzative*, in *Rivista di economia e politica dei trasporti*, n. 3, 2019;

CASTEL J.G., *The Internet in Light of Traditional Public and Private International Law Principles and Rules Applied in Canada*, in *Canadian Yearbook of International Law*, n. 39, 2001, pp. 3-68;

CASTELLS M., *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford, 2002;

CCIA Europe, *New EU Cybersecurity Rules Are Well-intended, but Introduce Unnecessary Red Tape*, del 15 settembre 2022;

CEN-CENELC CSCG, *Recommendation #2 – Definition of Cybersecurity*, ver. 01.08, 2013;

Centre for Democracy & Technology, *ITU move to expand powers threatens the Internet: civil society should have voice in ITU Internet debate*, 12 marzo 2012;

CERF V.C., *Internet Access Is Not a Human Right*, in *The New York Times*, 4 gennaio 2012;

CERIONI M., *Prime riflessioni sulle fonti dell'autonomia privata*, in *Annali della Facoltà giuridica dell'Università di Camerino – Nuova Serie*, n.1, 2012;

CERI P., *La società vulnerabile. Quale sicurezza, quale libertà*, Roma-Bari, Laterza, 2003;

CERRINA FERONI G., MORBIDELLI G., *La sicurezza: un valore superprimario*, in *Percorsi Costituzionali*, n. 1, 2008;

CESARINI SFORZA W., *Il diritto dei privati*, Milano, Giuffrè, 1963;

CESARINI SFORZA W., *Ordinamenti giuridici (pluralità degli)*, in *Novissimo digesto italiano*, vol. XII, 1957;

CHEN Z., WANG C., LI G., LOU Z., JIANG S., *New IP Framework and Protocol for Future Applications*, University college, Londono, 2020;

CHIAPPETTI A., *L'attività di polizia*, XXXIV, Cedam, Padova, 1973;

CHIAPPETTI A., *Polizia (dir. pubbl.)*, in *Enc. dir.*, XXXIV, Milano, 1985;

CHIARA P.G., BRIGHI R., *La dimensione della "resilienza" nel diritto UE della cyberscurezza*, in *Ragion pratica*, 2024;

CHIARA P.G., *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;

CHIARA P.G., *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*, fasc. 1, 2023;

CHIARELLI G. *Sovranità*, in *Noviss. dig. it.*, XVII, Torino, 1970;

CHITI E., *Le agenzie europee. Unità e decentramento nelle amministrazioni europee*, Padova, Cedam, 2002;

CHITI E., MATTARELLA B.G., *La sicurezza europea*, in *Rivista trimestrale di diritto pubblico*, vol. 58, fasc. 2, 2008;

CHOUCRI N., MADNICK S., KOEPKE P., *Institutions for cyber security: International responses and data sharing initiative*, Working Paper CISL# 2016–10, Cybersecurity Interdisciplinary Systems Laboratory, MIT, Cambridge, MA, 2016;

CHRISTOU G., *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy,* Londra, Palgrave, 2019;

CLARICH M., MATTARELLA B.G. *L'Agenzia italiana del farmaco*, in G. FIORENTINI (a cura di), *I servizi sanitari in Italia*, Bologna, 2004;

COLLINS A., *Contemporary Security Studies*, Oxford, Oxford University Press, 2022;

COMANDÈ G., PONZANELLI G. (a cura di), *Scienza e diritto nel prisma del diritto comparato. Atti del convegno tenutosi a Pisa il 22-24 maggio 2003;*

CONTRAFFATTO V., *I reati informatici*, Frosinone, Key editore, 2017;

CORASANITI G., *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003;

CORNELI A., *I Servizi d'intelligence e l'interesse nazionale*, in *Per Aspera Ad Veritatem*, n.7, 1997;

CORSI C., *Agenzia e agenzie: una nuova categoria amministrativa?*, Torino, 2005;

CORSI E., *La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale*, in *Research Analysis del Center for Cyber Security and International Relations Studies*, 2018;

CORSO G., *L'ordine pubblico*, Bologna, 1979;

CORTESE E., *Sovranità (storia)*, in *Enc. dir.*, XLIII, Milano, 1990;

COSTA P., PIZZOLATO F. (a cura di), *Sicurezza e tecnologia*, Giuffrè editore, Milano, 2017;

COUTURE S., TOUPIN S., *What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?*, in *GigaNet: Global Internet Governance Academic Network*, Annual Symposium 2017;

CREMONA E., I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti, Edizioni Scientifiche Italiane, Napoli, 2023;

CRISAFULLI V., *Lezioni di diritto costituzionale*, vol. I, Milano, Cedam, 1970;

CRISAFULLI V., *Lezioni di diritto costituzionale*, vol. II, Milano, Cedam, 1970;

CRISTIANO F., BERG B., *Hybridity, conflict, and Global Politics of Cybersecurity*, Rowman & Littlefield, 2023;

DE GREGORIO G., DUNN P., *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, vol. 59, n. 2, 2022;

DE LEONARDIS F., *Soggettività privata e azione amministrativa. Cura dell'interesse generale e autonomia privata nei nuovi modelli di amministrazione*, Padova, Cedam, 2000;

DE SANTIS V., *Star Trek: coraggiosamente oltre i confini per ritrovarsi umani*, in A. LIGUSTRO, R. TARCHI, G.M. RUOTOLO, G. MARTINICO, *La rappresentazione delle tradizioni giuridiche nella pop culture : narrazione e percezione del giuridico tra immagini statiche e immagini dinamiche: atti del primo Seminario annuale dell'Associazione di diritto pubblico comparato ed europeo: Foggia, 23-24 giugno 2022*, Napoli, Editoriale scientifica, 2023, pp. 491-504.;

DELIMATSIS P., BIJLMAKERS S., BOROWICZ M.K., *The Evolution of Transnational Rule-Makers through Crises*, Cambridge, Cambridge University Press, 2023;

DELLA CANANEA G., FIORENTINO L., *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editoriale scientifica, 2020;

DELLA SCALA M.G., *Le valutazioni tecniche nel procedimento amministrativo,* in AA.VV., *L'attività amministrativa,* a cura di Alb. Romano, Torino, 2016, pp. 552-564;

DENNINGER E., *Sovranità dello Stato e tutela dei diritti fondamentali nel confronto dialettico tra autodeterminazione nazionale e intreccio globale*, in *Dirittifondamentali.it*, 29 giugno 2016;

DE VERGOTTINI G., *La persistente sovranità*, in *Recte sapere. Studi in onore di Giuseppe Dalla Torre*, Torino, 2014,

DE VIDO S., *La recente giurisprudenza comunitaria in materia di golden shares: violazione delle norme sulla libera circolazione dei capitali o sul diritto di stabilimento?*, in *Dir. comm. int*., 2007;

DE VRIES H.J., *Governance of electrotechnical standardisation in Europe*, Rotterdam, 2015;

DRAETTA U., PARISI N., RINOLDI D., *Lo spazio di libertà, sicurezza e giustizia dell'Unione europea: principi fondamentali e tutela dei diritti*, Napoli, Editoriale Scientifica, 2007;

DRAKE W.J., CERF V.G., KLEINWACHTER W., *Internet fragmentation: An overview. Davos: World Economic Forum*, 2016;

DUCCI R., OLIVI B., *L'europa incompiuta*, Padova, Cedam, 1970;

DUNN CAVELTY M., ERIKSEN C., SCHARTE B., *Making cyber security more resilient: adding social considerations to technological fixes*, in *Journal of Risk Research*, vol. 26, n. 7, 2023;

DUNN CAVELTY M., THIERRY BALZACQ, *Routledge handbook of security studies*, London, New York, Routledge, 2017;

D'ALBERTI M., *Lezioni di diritto amministrativo*, Torino, 2013;

D'ALBERTI M., *Poteri pubblici, mercati e globalizzazione*, Bologna, 2008;

D'ALOIA A. (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Giuffrè, Milano, 2003;

D'ONGHIA M.V., *Resilienza, una parola alla moda*, in *Treccani*, 16 ottobre 2020;

EICHENSEHR K., *The Cyber-Law of Nations*, in *The Georgetown law journal*, vol. 103, 2015;

ELIANTONIO M., CAUFFMAN C. (a cura di), *The legitimacy of standardisation as a regulatory technique: a cross-disciplinary and multi-level analysis*, Cheltenham, Northampton, Edward Elgar, 2020;

ELIANTONIO M., *Judicial Control of the EU Harmonized Standards: Entering a Black Hole?*, in *Legal Issues of Economic Integration*, vol. 44, n. 4, 2017;

ELIANTONIO M., MEDZMARIASHVILI M., *Hybridity under scrutiny: How European standardization shakes the foundations of EU constitutional and internal market law*, in *Legal Issues of Economic Integration*, vol. 44, n. 4, 2017;

Enciclopedia Treccani Informatica, ed. 2013;

ENDSLEY M.R., *Design and evaluation for situation awareness enhancement*, in *Proceedings of the Human Factors Society annual meeting*, vol. 32, 1988;

ENISA, *Consultation paper – EU ICT industrial policy: Breaking the cycle of failure*, 2019;

ENISA, *Cybersecurity research directions for the Eu's digital strategic autonomy*, 2019;

ENISA, *EISAS (enhanced) report on implementation*, 2011;

ENISA, *EISAS – European Information Sharing and Alerting System*, 2007;

ENISA, *EISAS – European Information Sharing and Alerting System. Deployment Feasibility Study*, 2013;

ENISA, *EP3R 2009-2013 Future of NIS Public Private Cooperation*, 2015;

ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models,* 2018;

ENISA, *Shortlisting network and information security standards and good practices*, 2012;

ENISA, *Threat Landscape for Supply Chain Attacks*, 2021;

ESTERBROOK F., *Cyberspace and the Law of the Horse*, University of Chicago Legal Forum, 1996;

EVEN S., SIMAN-TOV D., *Cyber Warfare: Concepts and Strategic Trends*, Tel Aviv, Memorandum, 2012;

FAZZARI A.L., *Sistemi di gestione per la qualità*, Torino, Giappichelli, 2012;

FERACI O., *L'ordine pubblico nel Diritto dell'Unione europea*, Milano, Giuffrè, 2012;

FICHERA M., KREMER J. (a cura di), *Law and security in Europe: Reconsidering the security constitution*, Intersentia, Cambridge, 2013;

FINOCCHIARO G., *La sovranità digitale?*, in *Dir. pubbl.*, fasc. n. 3, settembre-dicembre 2022;

FINOCCHIARO G., *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, vol. 17, 2001;

FIORENTINO L. (a cura di), *Le amministrazioni pubbliche tra conservazione e riforme*, Milano, 2008;

FJÄDER C., *The nation-state, national security and resilience in the age of globalisation*, in *Resilience: International Policies, Practices, and Discourses*, vol. 2, n. 2, 2014;

FLORIDI L., *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy & Technology*, 2020;

FORNI L., VETTOR T., *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017;

FORTE A., *I poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale*, in *Nomos*, n. 3, 2014;

FRACANZANI M.M., *Adolfo Ravà: fra tecnica del diritto ed etica dello Stato*, Napoli, Edizioni Scientifiche Italiane, 1998;

FRANKE U., BRYNIELSSON J., *Cyber situational awareness – A systematic review of the literature*, in *Computer & Security*, vol. 46, 2014;

FRAU M., *I nodi irrisolti della difesa comune europea. Una prospettiva federalista*, in *federalismi.it*, n. 6, 2022.

FROSINI V., *La democrazia nel XXI secolo* (1997), Macerata, Liberilibri, 2010;

FOUCAULT M., *Sicurezza, territorio, popolazione. Corso al Collège de France* [1977-1978], ed. II, Milano, Feltrinelli, 2020;

GAJA G., ADINOLFI A., *Introduzione al diritto dell'Unione europea*, Roma-Bari, Laterza, 2020;

GALGANO F., *Lex mercatoria*, Il Mulino, Bologna, 2016;

GALIMBERTI U., *Psiche e techne*: l'uomo nell'età della tecnica, Milano, Feltrinelli, 2004;

GALIZIA M. *La teoria della sovranità dal Medio Evo alla rivoluzione francese*, Milano, 1951;

GALLOTTI C., *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Lulu press, 2022;

GARELLI G.E., *Il diritto amministrativo italiano*, ed. VII, Torino, 1885;

GARGALE E., *Amministrazione Pubblica e privati nella certificazione di qualità dei prodotti industriali*, in *Informatica e diritto*, XIX annata, vol. II, n. 1, 1993;

GAROFOLI R., *Golden power e controllo degli investimenti esteri: natura dei poteri e adeguatezza delle strutture amministrative*, in *federalismi.it*, 18 settembre 2019;

GASPARI F., *Libertà di circolazione dei capitali, privatizzazioni e controlli pubblici: la nuova golden share tra diritto interno comunitario e comparato*, Torino, 2015;

GASPARI F. *Poteri speciali e regolazione economica tra interesse nazionale e crisi socioeconomica e politica dell'Unione europea*, in *federalismi.it*, n. 16, 2020;

GAYCKEN S., KRUEGER J., NICKOLAY B. (a cura di), *The Secure Information Society: Ethical, Legal and Political Challenges*, Berlino, Springer Publ., 2021;

GENTILI A., *La rilevanza giuridica della certificazione volontaria*, in *Europa e dir. priv*., 1999;

GIALDINO C.C. (diretto da), *Codice dell'Unione Europea operativo: TUE e TFUE commentati articolo per articolo, con la carta dei diritti fondamentali dell'Unione Europea*, Napoli, Simone, 2012;

GIANNINI M.S., *Il pubblico potere*, Bologna, Il Mulino, 1986;

GIANNINI M.S., *Lezioni di diritto amministrativo*, vol. I, Milano, Giuffrè, 1950;

GIANNINI M.S., *Produzione (disciplina della)*, in *Enc. dir*., XXXVI, Milano, 1987;

GIANNINI M.S., voce *Organi (teoria generale)*, in *Enc. dir.*, XXXI, Milano, 1981;

GIBSON W., *Il Neuromante (1986)*, Ace book, 2018;

GIDDENS A., *Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita*, Bologna, 2000;

GIGANTE M., *Effetti giuridici nel rapporto tra tecnica e diritto: il caso delle «norme armonizzate»*, in *Rivista italiana di diritto pubblico comunitario*, 1997;

GIGANTE M., *Obblighi procedurali comunitari e attività normativa degli Stati membri*, in *Giur. it*., 2002;

GIUPPONI T., *Le dimensioni costituzionali della sicurezza*, Libreria Bonomo Editore, Bologna, 2010;

GIUPPONI T.F., *Il segreto di Stato ancora davanti alla Corte (ovvero del bilanciamento impossibile)*, in *Diritto penale contemporaneo e Forum di Quaderni Costituzionali*, 2014;

GOLDMAN B., *Lex mercatoria,* Kluwer Law International, 1983;

GOLDSMITH J.L., *Against Cyberanarchy*, in *University of Chicago Law Occasional Paper*, vol. 65, n. 40, 1999;

GOLDSMITH J.L., WU T., *Who Controls the Internet?: Illusions of a Borderless World*, Oxford, Oxford University Press, 2006;

GORI U., MARTINO L., *Intelligence e interesse nazionale*, Roma, Aracne, 2015;

GRASSI S., CECCHETTI M., Governo dell'ambiente e formazione delle norme tecniche, Milano, Giuffrè, 2006;

GRASSO G. (a cura di), *Il governo tra tecnica e politica: atti del Seminario annuale dell'Associazione Gruppo di Pisa, Como, 20 novembre 2015;*

GRECO N., *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale*, Roma, Edises, 1999;

GRIGNETTI F., *Gabrielli: "Allarme terrorismo e clan criminali, l'intelligence europea è un controsenso"*, in *La Stampa*, del 23 settembre 2021;

HAAS E., *Beyond the Nation State*, Stanford, 1964;

HAAS E., *The uniting of Europe: Political, Social and Economic Forces*, Londra, 1958:

HACHEZ N., WOUTERS J., *A Glimpse at the Democratic Legitimacy of Private Standards: Assessing the Public Accountability of GlobalG.A.P.*, in *Journal of International Economic Law*, vol. 14, n. 3, 2011;

HAZUCHA B., *International Technical Standards and Essential Patents. From International Harmonization to Competition of Technologies*, in *Society of International Economic Law (SIEL)*, Second Biennial Global Conference, University of Barcelona, luglio 8-10, 2010;

HEIRES M., *The International Organization for Standardization (ISO)*, in *New Political Economy*, 2008;

HOBBES T., *De Cive* (1642), a cura di T. MAGRI, Roma, Editori Riuniti, 2014;

HOBBES T., *Leviatano* (1651), con saggio introduttivo di C. GALLI, Rizzoli, 2011;

HOFFMAN F. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007;

HOFFMANN H., SCHOELLER W.F. (a cura di), *Wendepunkt 11. September 2001: Terror, Islam und Demokratie*, Amsterdam, DuMont Buchverlag, 2001;

HORNEMAN A., *Situational Awareness for Cybersecurity: An Introduction*, in *Carnegie Mellon University, Software Engineering Institute's Insights (blog)*, 2019;

IANNUZZI A., *Caratterizzazioni della normazione tecnica nell'ordinamento italiano. Il campo di analisi e di verifica della materia ambientale*, in "St. parl. pol. cost.", 2006;

IANNUZZI A., *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione,* Napoli, Editoriale scientifica, 2018;

IEC, *Report of preliminary meeting*, Londra, 1906;

INKSTER I., *History of technology,* vol. 28, London, Continuum, 2008;

IRTI N., *L'età della decodificazione* [1989], Milano, Giuffrè, 1999;

IRTI N., *L'ordine giuridico del mercato*, Roma-Bari, Laterza, 2009;

IRTI N., *Norma e luoghi: problemi di geo-diritto*, Roma, Laterza, 2005;

IRTI N., SEVERINO E., *Dialogo su diritto e tecnica*, Roma-Bari, Laterza, 2001;

ITU, *Resilient Pathways: the adaptation of the ICT sector to climate change*, 2014;

ITU-T, *Cybersecurity, data protection and cyber resilience in smart sustainable cities*, n. 3, 2015;

JAJODIA S., LIU P., SWARUP V., WANG C., *Cyber situational awareness*, in *Springer Science & Business*, 2009;

JEAN C., *La politica di sicurezza dell'Italia*, in *Gnosis*, n. 4, 2014;

JEAN C., SAVONA P., *Intelligence economica. Il ciclo dell'informazione nell'era della globalizzazione*, Catanzaro, Rubettino, 2011;

JEMOLO A.C., *Lo "spirito di liberalità"*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960;

JEMOLO A.C. (a cura di), *Diritto amministrativo, diritto costituzionale, diritto internazionale, diritto penale, procedura penale*, Milano, Giuffrè, 1963;

JENKINS D., JACOBSEN A., HENRIKSEN A. (a cura di), *The Long Decade: How 9/11 Changed the Law,* New York, Oxford Academic, 2014;

JIANG S., *New IP Networking for Network 2030*, Fifth ITU Workshop on Network 2030, International Telecommunication Union, ottobre, 2019;

JOHNSON D., POST D., *Law and Borders - the Rise of Law in Cyberspace*, in *Stanford Law Review*, vol. 48, 1996;

JOLLY R., RAY D.B., *The Human Security Framework and National Human Development Reports*, United Nations Development Programme, NHDR Occasional Paper 5, 2006;

KAMARA I., *European Cybersecurity Standardisation: A Tale of Two Solitudes in view of Europe's Cyber Resilience*, in *Innovation: The European Journal of Social Science Research*. p. 20, 2024;

KAMARA I, *Legal aspects of standardisation: Relationship of standards and law in the EU*, Standardisation Training Academy, Vol. Level: Beginner 1, n. Course: 5, European Commission, 2023;

KANEVSKAIA O., *The law and practice of global ICT standardization*, Cambridge, Cambridge university press, 2023;

KATAGIRI N., *Why international law and norms do little in preventing non-state cyber attacks*, in *Journal of Cybersecurity*, Vol. 7, Issue 1, 2021;

KATTLER A., ETTENSPERGER F., *National internal security policies across Europe – a comparative analysis applying big data clustering techniques*, in *Political Research Exchange*, vol. 2, 2020;

KEFALAS A.G., *Cybernetics*, in *Encyclopedia of Information Systems*, 2003;

KELSEN H., *Lineamenti di dottrina pura del diritto* (1934), Torino, Einaudi, 2000;

KELSEN H., *Reine Rechtslehre: Einleitung in Die Rechtswissenschaftliche Problematik* [1934], *Lineamenti di dottrina pura del diritto*, trad. it. R. TREVES, Torino, Einaudi, 2000;

KHANNA P., *Connectography: mapping the global network revolution*, Croydon, Weidenfeld & Nicolson, 2016;

KOTT A., LINKOV I., *Cyber Resilience of Systems and Networks*, Cham, Springer, 2019;

KRAMER F.D., STARR S., WENTZ L.K., *Cyberpower and National Security*, National Defense University Press, Washington (D.C.), 2009;

LACHMAYER K., *A Comparative Analysis of Security as an Element of Constitutional Design: Is Global Terrorism Changing the Conditions of International Constitutional Law?*, Online Paper submitted at the VII World Conference of the International Association of Constitutional Law – Workshop 8: Constitutions and Global Terrorism 2007;

LAENZA U., *Fenomeni di contiguità aerea nel Diritto internazionale*, Napoli, 1961;

LAENZA U., *Il diritto degli spazi internazionali. Parte prima. La tradizione*, Torino, 1999;

LANIER J., *Dawn of the New Everything: Encounters with Reality and Virtual Reality*, Henry Holt and Company, New York, 2017;

LEFFLER M.P., *National Security*, in *The Journal of American History*, vol. 77, n. 1, 1990;

LEPSIUS O., *Liberty, Security, and Terrorism: The Legal Position in Germany*, in *German Law Journal*, n. 5, 2004;

LESSIG L., *Code: and other laws of cyberspace*, Basic books, 1999;

LESSIG L., *Code. Versione 2.0*, Basic books, New York, 2006;

LESSIG L., *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, in *Common Law Conspectus*, n. 5, 1997;

LESSIG L., *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, n. 2, 1999;

LIBICKI M.C., *Cyberdeterrence e cyberwar*, Santa Monica, RAND Corporation, 2009;

LICKLIDER J.C.R., CLARK W.E., *On-Line Man-Computer Communication*, Cambridge, Massachussetts, 1962;

LOCKE J., *Secondo Trattato sul Governo* (1689), Milano, Mondadori, 2018;

LOSANO M., *Il Diritto pubblico dell'informatica. Corso di informatica giuridica*, Torino, Einaudi, 1986;

LUSTGARTEN L., LEIGH I., *In From the Cold: National Security and Parliamentary Democracy*, Oxford, Oxford University Press, 1994;

LÜTHI B., *Perspectives on Security in Twentieth-Century Europe and the World*, in *Contemporary European History*, vol. 20, no. 2, 2011;

MANDEL R., *The Privatization of Security*, in *Armed Forces & Society*, 2001;

MARCHETTI E., *Private Military and Security Companies: il caso italiano nel contesto internazionale*, Roma, Edizioni Nuova Cultura, 2013;

MARCHISIO S., MONTUORO U., *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, Giappichelli, 2019;

MARRANI D., *La cooperazione internazionale per la sicurezza e la stabilità del cyberspace*, Napoli, Editoriale scientifica, 2020;

MARTINO L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, fasc. 1, gennaio-aprile, 2018;

MATTLI W., BÜTHE T., *Setting International Standards: Technological Rationality or Primacy of Power?,* in *World Politics*, vol. 56 , n. 1 , 2003;

MAURO M.R., *Diritto internazionale dell'economia: teoria e prassi delle relazioni economiche internazionali*, Napoli, Edizioni scientifiche italiane, 2019;

MAYER M., MARTINO L., MAZURIER P., TZVETKOVA G., *How would you define cyberspace?*, First Draft Pisa, Experimental online laboratory PhD in Politics, Human Rights and Sustainability, Scuola Superiore Sant'Anna, 19.05.2014;

MAZZAMUTO M., *Poteri di polizia e ordine pubblico*, in *Dir. Amm.*, nn. 3-4, 1998;

MAZZIOTTI DI CELSO M., *Norma giuridica*, in *Enc. giur.*, vol. XXII, 1990;

MCWILLIAM R.C., *The First British Standards: Specifications and Tests Published by the Engineering Standards Committee, 1903–18*, in *Transactions of the Newcomen Society Journal*, vol. 75, Iss. 2, 2005;

MENSI M., *Il 5G e il "nuovo" paradigma di sicurezza dell'Unione europea. Regole a tutela di autonomia tecnologica e sovranità*, Report, del 15.5.2020;

MERLONI F., *Le agenzie nel sistema amministrativo italiano*, in *Dir. pubbl.*, n. 3, 1999;

MICCÙ R. (a cura di), *Un nuovo diritto delle società pubbliche? Processi di razionalizzazione tra spinte all'efficienza e ambiti di specialità*, Napoli, 2019;

MITNICK K.D., *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, Milano, 2002;

MITRANY D., *A working peace system*, Londra, 1943;

MITRANY D., *The progress of international government*, Londra, 1993;

MODUGNO F., *Norma giuridica*, in *Enc. dir.*, vol. XXVIII, Giuffrè, 1978;

MONACO R., *Rinvio nel diritto internazionale privato*, in *Enc. giuri.*, vol. XXXI;

MONTI A., *Digital rights delusion: humans, machines and the technology of information*, Routlege, Londra, 2023;

MONTI A., *National security in the new world order. Government and the technology information*, New York, Routledge, 2022;

MONTI A., *Ordine pubblico, sicurezza nazionale e sicurezza cibernetica: una prospettiva di sistema*, in *Quaderno speciale CASD n. 1 - Scenari globali e interessi nazionali: pandemia, continuità, cambiamento*, 2020;

MONTI A., *Sicurezza e/o democrazia? Le debolezze strutturali nelle norme italiane sulla cybersecurity*, in *La Repubblica*, 3 novembre 2023;

MORTATI C., *Istituzioni di diritto pubblico*, Padova, Cedam, ed. VI, 1962;

MOSCA C., *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova, Cedam, 2012;

MOSCA C., SCANDONE G., GAMBACURTA S., VALENTINI M., *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)*, Milano, Giuffrè, 2008;

MOSCA C., *Valori, modelli e prassi istituzionali*, Napoli, Editoriale scientifica, 2021;

MOSCARINI A., *Fonti dei privati e globalizzazione*, Roma, Luiss University Press, 2015;

MOSCARINI A., *L'accreditamento nel Regolamento CE n. 765/2008 e le "fonti" di produzione privata*, in *Rivista di diritto alimentare*, n. 1, 2012;

NAPOLITANO G., *L'Agenzia per l'acqua*, in *Giorn. dir. amm.*, 2011;

NAPOLITANO G. (a cura di), *Diritto amministrativo comparato*, Milano, 2007;

NAPOLITANO G. (a cura di), *Foreign Direct Investment Screening. Il controllo sugli investimenti esteri diretti*, Bologna, 2020;

NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 febbraio 2014;

ODDENINO A., *Digital standardization cybersecurity issues and international trade law*, in *Questions of International Law*, 2018;

ODDENINO A., *La governance di Internet fra autoregolamentezione, sovranità statale e diritto internazionale*, Giappichelli, Torino, 2008;

OHLIN J.D., GOVERN K., FINKELSTEIN C. (a cura di), *Cyberwar: Law & Ethics for Virtual Conflicts,* Oxford, Oxford University Press, 2014;

ORLANDO V.E., *Introduzione al diritto amministrativo*, in *Primo trattato completo di diritto amministrativo italiano*, vol. I, Milano, Soc. ed. libraria, 1900;

ORLANDO V.E., *Trattato di diritto amministrativo italiano*, vol. II, Soc. ed. libraria, Milano, 1915;

PACE A., *Le due Corti e il caso Abu Omar*, in *Consulta on line*, 2014;

PAGALLO U., *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Torino, Giappichelli, 2014;

PAJNO S., TORCHIA L. (a cura di), *La riforma del governo*, Bologna, 2000;

PANSA A., *La sicurezza nazionale. Innovazione e nuovi limiti*, in *Gnosis*, n. 1, 2019;

PAPA A., *Alcune considerazioni sulla tecnica del rinvio nella produzione normativa*, in *Rassegna Parlamentare*, 1991

PARISI V.E., *Interesse nazionale e globalizzazione: i regimi democratici nelle trasformazioni del sistema post-westfaliano*, Milano, Jaca book, 1998;

PARONA L., *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di Diritto amministrativo*, n. 6, 2021;

PASSAGLIA P., *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in *MediaLaws*, n. 3, 2021;

PASTORE F., *Il coordinamento delle forze di polizia e di sicurezza italiane nella lotta al terrorismo*, in *Dirittifondamentali.it*, fasc. 2, 2021;

PATTI G., *I diritti speciali dello Stato tra libera circolazione dei capitali, golden shares e regole di diritto societario*, in *Europa e dir. priv*., fasc.2, 2011;

PUYVELDE (van) D., BRANTLY A.F., *Cybersecurity. Politics, Governance and Conflict in cyerspace*, Cambridge, Polity press, 2019;

PECES-BARBA G., *Teoria dei diritti fondamentali*, Milano, Giuffrè, 1993;

PEERS S. *National Security and European Law*, in *Yearbook of European Law*, vol 16, Issue 1, 1996;

PELLEGRINI M. (a cura di), *Elementi di diritto pubblico dell'economia*, Padova, 2017;

PENG S.Y., *Private Cybersecurity Standards: Cyberspace Governance, Multistakholdersim, and the (Ir)Relevance of TBT Regime*, in *Cornell International Law Journal*, 51, n. 2, 2018;

PEOPLES C., VAUGHAN-WILLIAMS N., *Critical security studies: an introduction*, London, New York, Routledge, 2021;

PETRONI G., *Nuovi profili organizzativi dell'evoluzione del sistema amministrativo pubblico*, Padova, 1988;

PICCARDI L., *La pluralità degli ordinamenti giuridici ed il concetto di rinvio*, in *Scritti giuridici in onore di Santi Romano*, vol. I, Padova, 1940;

PIRIS J.C., *Il Trattato di Lisbona*, Milano, Giuffrè, 2013;

PISANELLI G., *La sentenza della Corte costituzionale n. 24 del 2014 in materia di segreto di Stato*, in *Federalismi.it*, 6, 2014;

PISTORIO G., *La sicurezza giuridica: profili attuali di un problema antico*, Napoli, Editoriale Scientifica, 2021;

PIZZOLATO F., COSTA P. (a cura di), *Sicurezza, Stato e mercato*, Milano, Giuffrè, 2015;

PIZZORUSSO A., *Delle fonti del diritto*, Bologna, Zanichelli, 1977;

POCAR F., BARUFFI M.C. (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, Cedam, 2014;

POLI S., FAHEY E., *The strengthening of the European Technological Sovereignty and its legal bases in the Treaties*, in *Eurojus*, fasc. 2, 2022;

POLI S., *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in in *I Post di AISDUE, III, 2021, Sezione Atti Convegni AISDUE*, n. 5, 20 dicembre 2021;

POLLICINO O., BASSINI M., DE GREGORIO G., *Internet law and protection of fundamental rights*, Milano, Bocconi University Press, 2022;

POLLICINO O., *Potere digitale*, Estratto da I Tematici, V-2023, Potere e Costituzione, in *Enc. dir.,* 2023;

POWELL R. *Rights as Security: The Theoretical Basis of Security of Person*, Oxford online edn, Oxford Academic, 2019;

PRESUTTI E., *Polizia di pubblica sicurezza e polizia amministrativa*, in *Arch. giur.,* LXV, p. 1900;

QUADRI R., MONACO R., TRABUCCHI A. *Trattato istitutivo della comunità economica europea*, vol. III, Milano, Giuffrè, 1965;

RAINERO R.H. (a cura di), *Storia dell'integrazione europea*, Milano, Marzorati, 1997;

RANELLETTI O., *Principi di diritto amministrativo*, Napoli, 1912;

RAVÀ A., il quale in *Il diritto come norma tecnica*, Cagliari, 1911;

RAYMOND M., DENARDIS L., *Multistakeholderism: anatomy of an inchoate global institution*, in International Theory, 2015;

REED E., DUMPER M. (a cura di), *Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspectives*, Cambridge, Cambridge University Press, 2012;

REIDENBERG J.R., *Lex informatica: The formulation of information policy rules thruogh technology*, in *Texas Law Review*, 76, 3, 1998;

RINOLDI D., *L'ordine pubblico europeo*, Napoli, Editoriale scientifica, 2005;

RISTOLAIMEN M. *Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West*, in *Journal of Information Warfare*, vol. 16, n. 4, 2017;

RIVA E., *Natura giuridica delle attività di accreditamento*, Editoriale Accredia, 2016;

ROBERTS H., COWLS J., CASOLARI F., MORLEY J., TADDEO M., FLORIDI L., *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, in *Internet Policy Review*, 2021;

ROMANO S., *Il diritto pubblico italiano*, Milano Giuffrè, 1988;

ROMANO S., *L'ordinamento giuridico* [1918], Macerata, Quodlibet, 2018;

ROMANO S., *Ordinamenti giuridici privati (appunti)*, in *Studi in memoria di Filippo Vassalli*, vol. II, 1960;

ROMANO S., *Principi di diritto amministrativo*, ed. II, Milano, 1906;

ROMOLOTTI T.E., *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001*, in *Rivista 231*, n. 1, 2020;

ROSSA S., *Cybersicurezza e pubblica amministrazione*, Napoli, Editoriale scientifica, 2023;

ROTHSCHILD E., *What is security?*, in *Daedalus*, vol. 124, n. 3, 1995;

RUFFO A., *La difesa europea (PSDC) e la Costituzione italiana alla prova della Bussola Strategica 2022*, in *federalismi.it*, n. 7, 2024;

RUGGE F., DOMINIONI S. (a cura di), *La gestione dei rischi nello spazio cibernetico*, Dossier ISPI, 2019;

RUOTOLO G.M., *Il sistema dei nomi di dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in *Il diritto dell'informazione e dell'informatica,* 2016;

RUOTOLO G.M., *Internet (dir. internaz.)*, in *Enciclopedia del diritto – Annali*, Milano, 2014;

RUSHDOONY R.J., *Accreditation and certification*, in Chalcedon Position, n. 5, 1979;

SABATINI C. (a cura di), *Human Rights in a Changing World Order*, Londra, Chatham House and Brookings Institution Press, 2023;

SACCO GINEVRI A., *I "golden powers" dello Stato nei settori strategici dell'economia*, in *federalismi.it*, n. 22, 2016;

SAIJA R., *Stanards e contratti di certificazione*, in *Riv. dir. alim.*, anno VII, n. 1, 2013;

SALA G., *Certificati e attestati*, in *Dig. disc. pubbl.*, Utet, Torino, 1987;

SALMONI F., *Le norme tecniche*, Milano, Giuffrè, 2001;

SALMONI F., *Norme tecniche e dottrina giuspubblicistica*, in *Percorsi Costituzionali*, 2017;

SANTANIELLO M., *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, n. 1, 2022;

SARTOR G., *Internet e il diritto,* in *Temi di diritto dell'informatica*, Giappichelli, Torino, 2011;

SASSEN S., *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton, 2008;

SAVINO M., *Solo per i tuoi occhi? La riforma del sistema italiano di intelligence*, in *Giornale di diritto amministrativo*, dicembre 2007;

SBORDONI S., *Web, libertà e Diritto. Aspetti di diritto positivo nella comunità virtuale*, Roma, Istituto poligrafico e Zecca dello Stato, 2014;

SCARCHILLO G., *Dalla* Golden Share *al* Golden Power: *la storia infinita di uno strumento societario. Profili di diritto europeo comparato*, in *Contratto e Impresa – Europa*, 2015;

SCARCHILLO G., *Privatizzazioni e settori strategici: l'equilibrio tra interessi statali e investimenti stranieri nel diritto comparato*, Giappichelli, 2018;

SCHEPEL H., *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets*, Oxford, Hart, 2005;

SCHEPEL H., *The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law*, in *Maastricht Journal of European and Comparative Law*, vol. 20, n. 4, 2012;

SCHMITT C., *Teologia politica* (1922), in *Le categorie del politico*, Bologna, Il Mulino, 2013;

SCHNEIER B., *Inside the Twisted Mind of the Security Professional*, in *Wired*, 20 marzo 2000;

SCHWARCZ S.L., *Private Ordering*, in *Northwestern University Law Review*, 2002;

SCIULLO G., *Alla ricerca del centro*, Bologna, 2000;

SEGURA SERRANO A., *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, vol. 10, The Hague: Brill, 200;

SENDEN A.J., KICA E., KLINGER K., HIEMSTRA M.I., *"Mapping Self-and Co-regulation Approaches in the EU Context": Explorative Study for the European Commission, DG Connect*, Utrecht University, RENFORCE, 2015;

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

SERINI F., *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in *Rivista Italiana di Informatica e Diritto*, fasc. 2, 2023;

SERINI F., *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in f*ederalismi.it,* n. 12, 2022;

SHACKELFORD S.J., RUSSELL S., HAUT J., *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks*, in *UC Davis Business Law Journal*, n. 16-2, 2016;

SHAPIRO C., VARIAN H.R., *The Art of Standards Wars*, in *California Management Review*, vol. 41, n. 2, 1999;

SHIH G., MENN J., *India targets Apple over its phone hacking notifications*, in *The Washington Post*, 27 dicembre 2023;

SILVESTRI G. *La parabola della sovranità. Ascesa declino e trasfigurazione di un concetto*, in *Riv. dir. cost*., 1996;

SIMONCINI A., CREMONA E., *European private law integration through technology: the constitutional dimension*, in *Persona e Mercato*, n. 2, 2021, pp. 244-260.

SIMONCINI M., *La regolazione del rischio e il sistema degli standard: elementi per una teoria dell'azione amministrativa attraverso i casi del terrorismo e dell'ambiente*, Napoli, Editoriale scientifica, 2010;

SINGER P.W., *Corporate Warriors: The Rise of the Privatized Military Industry*, New York, 2008;

SOFSKY W., *Rischio e sicurezza*, Torino, Einaudi, 2005;

SORICELLI G., *Le agenzie amministrative nel quadro dell'organizzazione dei pubblici poteri*, Napoli, 2002;

SORRENTINO F., *Le fonti del diritto*, Padova, 2015;

SPAGNUOLO VIGORITA V., *Attività economica privata e potere amministrativo*, Napoli, Morano, 1962;

SPANG-HASSEN, *Public International Computer Network Law Issues*, Djoef Publishing, Copenhagen, 2006;

SPENCE M., *Job Market Signaling*, in *The Quarterly Journal of Economics*, vol. 87, no. 3, 1973;

SQUARATTI V., *I limiti imposti dal diritto dell'Unione europea all'intervento pubblico nell'economia: la neutralità delle modalità di perseguimento di obiettivi imperativi di interesse generale*, in *Dir. comm. internaz*., 2014;

STERPA A., COIANTE A., *Sicurezza legalità ed economia*, Napoli, Editoriale scientifica, 2020;

STERPA A., *La libertà dalla paura - una lettura costituzionale della sicurezza*, Napoli, Editoriale scientifica, 2019;

STEWART FERGUSON D.D., *European Cybersecurity Certification Schemes and cybersecurity in the EU internal market*, in *Int. Cybersecur. Law Rev.*, vol. 3, 2022;

STIGLITZ J.E., *Monopoly, Non-Linear Pricing and Imperfect Information: The Insurance Market*, in *The Review of Economic Studies*, vol. 44, no. 3, 1977;

STOPPANI A., voce *Certificazione*, in *Enc. dir.*, vol. VI, Milano, Giuffrè, 1960;

STRANO M., BATTELLI F., BOCCARDI M., BRUZZONE R., FIAMMELLA B., MATTIUCCI M., RIGONI A., *Insiede attack. Manuale di ricerca e di intervento sul computer crime nelle organizzazioni*, Roma, 2005;

STRUKUL M., *La certificazione di qualità come strumento di tutela del consumatore. Profili contrattuali e di responsabilità*, in *Obbl. e contratti*, 2009;

SUTTON D., *Cyber Security. A practitioner's guide*, Swindon, BCS, 2017;

SVANTESSON D.J.B., *A legal method for solving issues of Internet regulation; Applied to the regulation of cross-border privacy issues*, in *EUI Working Papers*, n. 18, 2010;

SVANTESSON D.J.B., *Private international law and the Internet*, Alphen aan der Rijn, Wolters Kluwer, 2021;

SVANTESSON D.J.B., *Solving the internet jurisdiction puzzle*, New York, Oxford University Press, 2017;

TAMPONI M., CONFORTINI M., ZIMATORE A., ZACCHEO M., DI GRAVIO V., PALMIERI A., ORLANDI M., MARTUCCELLI S., RUPERTO S., CARLEO R., *Dieci lezioni introduttive a un corso di diritto privato*, Milano, Wolter Kluver, 2006;

TEPLINSKY M., *A Review of NIST's Draft Cybersecurity Framework 2.0*, in *LawFare*, 13 settembre 2023;

TEUBNER G. (a cura di), *Global law without state*, Aldershot, Dartsmouth, 1996;

TIZZANO A. (a cura di), *Trattati dell'Unione europea*, Milano, Giuffrè, 2014;

TOOHEY L. et al. (a cura di), *China In The International Economic Order: New Directions And Changing Paradigms*, Cambridge University Press, 2015;

TOVO C., *Le agenzie decentrate dell'Unione Europea*, Napoli, 2016;

TROPINA T., CALLANAN C., *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Springer Cham, 2015;

TSAGOURIAS N., BUCHAN R. (a cura di), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015;

TSILIKAS H., *Collaborative Standardization and Disruptive Innovation: The Case of Wireless Telecommunication Standards*, in *IIC - International Review of Intellectual Property and Competition Law*, vol. 48, n. 2, 2017;

TUCCARI F., BORGOGNONE G., *La sovranità: trasformazioni e crisi in età contemporanea*, Roma, Carocci, 2021;

URSI R., *La sicurezza pubblica*, Il Mulino, Bologna, 2022;

URSI R., *La sicurezza nel cyberspazio*, Milano, Angeli, 2023;

VALAGUZZA S., *Giurisprudenza comunitaria in tema di goldensharee principio di legalità*, in *Foro amm./CdS*, 2003;

VALENSISE B., *I settori strategici dopo la Riforma*, in DELLA CANANEA G., FIORENTINO L., *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editoriale scientifica, 2020, pp. 101-191;

VALENTINI M., MELIS G., Pro bono communi. *Scritti in onore di Carlo Mosca*, Napoli, Editoriale scientifica, 2023;

VALENTINI M., *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Napoli, Editoriale scientifica, 2017;

VALLEJO R., *The private administrative law of technical standardization*, in *Yearbook of European Law*, vol. 40, 2021;

VARJU M., *5G networks, (cyber)security harmonisation and the internal market: the limits of Article 114 TFEU*, in *European Law Review*, 2020;

VASSALLI F., *Extrastratualità del diritto civile*, in *Rivista italiana di scienze giuridiche,* 1951;

VEDDER A., SCHROES J., DUCUING C., VALCKE P. (a cura di), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, Cambridge, Antwerp, Chicago, 2020;

VEGA L.E.R., SCAFFARDI L., SPIGNO I., *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, Editoriale scientifica, 2021;

VELLANO M., MIGLIO A., *Sicurezza e difesa comune dell'Unione europea*, Milano, Wolters Kluwer, 2023;

VENTURA L., *Stato e sovranità: profili essenziali*, Torino: Giappichelli, 2010;

VERBRUGGEN P., *Does Co-regulation Strengthen EU Legitimacy?*, in *European Law Journal*, 2009;

VERELLEN T.E., *European Sovereignty Now? A Reflection on What It Means to Speak of "European Sovereignty"*. in E*uropean Papers*, n. 5, 2020;

VESPERINI G. (a cura di), *La riforma dell'organizzazione centrale*, Milano, 2005;

VIRGA P., *La potestà di polizia*, Milano, 1954;

VOLGER H., *A concise encyclopedia of the United Nations*, Leiden, Boston, Martinus, Nijhoff, 2010;

VOLPATO A., ELIANTONIO M., *The participation of civil society in ETSI from the perspective of throughput legitimacy, Innovation*, in *The European Journal of Social Science Research*, 2024;

VOLPATO A., *The Legal Effects of Harmonised Standards in EU law*, in P.L. LÁNCOS, N. XANTHOLIUS, L.A. JIMÉNEZ (a cura di), *The Legal Effects of EU Soft Law Theory, Language and Sectoral Insights*, Elgar Studies in European Law and Policy, 2023, pp. 193-212;

VON DER LEYEN U., *A Union that strives for more. My agenda for Europe. Political Guidelines for the next European Commission 2019-2024;*

WALKER J., COOPER M., *Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation*, in *Security Dialogue*, vol. 42, no. 2, 2011;

WANG X., *The Great Firewall of China and Its Implications for Political Information Systems*, 2019;

WIENER N., *Cybernetics: Or Control and Communication in the Animal and the Machine*, MIT University Press, Cambridge, 1948;

WILLIAMS M.C., *Words, Images, Enemies: Securitization and International Politics*, in *International Studies Quarterly*, vol. 47, n. 4, 2003;

WILLIAMS P.D., MCDONALD M., *Security studies: an introduction*, London-New York, Routledge, 2018;

WILLIAMS T.A., GRUBER D.A., SUTCLIFFE K.M., SHEPHERD D.A., ZHAO E.Y., *Organizational response to adversity: Fusing crisis management and resilience research streams*, in *The Academy of Management Annals*, vol. 11, n. 2, 2017;

WINCKLER R., *Electrotechnical Standardization in Europe: A tool for the common market*, CENELEC, Brussels, 1994;

WORLD TRADE ORGANIZATION, *Members debate cyber security and chemicals at technical barriers to trade committee*, 2017;

WU T., *Cyberspace sovereignty? - The Internet and the International system*, in *Harvard Journal of Law & Technology*, vol. 10, n. 3, 1997;

ZEI A., *Tecnica e diritto. Tra pubblico e privato*, Milano, Giuffrè, 2008;