ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

8 SETTEMBRE 2021

La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea

di Raffaella Brighi
Professoressa associata di Informatica giuridica
Alma Mater Studiorum - Università di Bologna

e Pier Giorgio Chiara
Dottorando di ricerca in Diritto delle nuove tecnologie
Università del Lussemburgo | LAST-JD-RIoE

La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*

di Raffaella Brighi
Professoressa associata di Informatica giuridica
Alma Mater Studiorum - Università di Bologna

e Pier Giorgio Chiara
Dottorando di ricerca in Diritto delle nuove tecnologie
Università del Lussemburgo | LAST-JD-RIoE

Abstract [It]: Il presente contributo si propone di illustrare come e fino a che punto i recenti sviluppi legislativi dell'Unione Europea possano sostenere la tesi che vorrebbe identificare la cybersecurity come bene pubblico, con particolare riferimento alla cd. "robustezza dei sistemi". La dottrina economico-giuridica del bene pubblico rivela infatti un interessante quadro di responsabilità condivise, nell'ottica del comune interesse ad avere un soddisfacente grado di sicurezza dei sistemi informatici alla base delle nostre società.

Abstract [En]: The article casts the light on how and to what extent the recent EU legislative developments can uphold the thesis that would identify cybersecurity as a public good, in particular, taking into account systems' robustness. The doctrine of the public good, which is typically an economic concept, in its normative dimension reveals a framework of shared responsibilities, in view of the common interest in having a satisfactory level of security of the information systems at the basis of our societies.

Parole chiave: sicurezza informatica; beni pubblici; UE; strategia; direttiva NIS 2
Keywords: cybersecurity; beni pubblici; UE; strategia; direttiva NIS 2

Sommario: **1.** Verso una definizione del concetto di cybersecurity. **2.** La dottrina della cybersecurity come bene pubblico: una riflessione comparata. **3.** La nuova strategia della Commissione Europea sulla cybersecurity. **4.** La proposta per una Direttiva NIS 2.0. **5.** Conclusione. **6.** Riconoscimenti.

1. Verso una definizione del concetto di cybersecurity

Con l'evoluzione tecnologica e la transizione al digitale, i paradigmi della sicurezza informatica sono mutati fino a confluire nel concetto – ampio e trasversale a discipline diverse – di "cybersecurity". Spesso utilizzato in modo interscambiabile con i termini *computer security* o *information security*, questi ne rappresentano in realtà solo un sottoinsieme[1]: in un panorama di difficile interazione tra sistemi informativi, società e ambiente, pur partendo da obiettivi comuni, la cybersecurity amplia il perimetro dei rischi e degli attori coinvolti con la conseguente individuazione di elementi di protezione nuovi.

A fronte del progressivo aumento quantitativo e qualitativo delle minacce e degli attacchi informatici, la sicurezza informatica ha l'obiettivo di proteggere il sistema informativo di una organizzazione (istituzione o azienda) mediante lo studio, lo sviluppo e l'implementazione di strategie, politiche e piani operativi volti

* Articolo sottoposto a referaggio.
[1] ENISA, *ENISA Overview of cybersecurity and related terminology*, 2017, p. 6.

a prevenire gli incidenti informatici e, nel momento in cui accadono, a fronteggiarli e a superarli[2]. Essa si sforza di assicurare il raggiungimento e il mantenimento delle proprietà di sicurezza degli *asset* dell'organizzazione e dell'utente contro i rischi rilevanti nell'ambiente cibernetico.

L'espressione *computer security* (e le sue evoluzioni che ricomprendono la *network security*) si riferisce a una visione originaria di sicurezza informatica intesa come protezione del computer o, più in generale, del sistema informatico, dei suoi apparati, dei programmi informatici, delle infrastrutture e dei dati elaborati e trasmessi. Successivamente, nella "società dei dati", si è approdati a un concetto di sicurezza maggiormente orientato alla protezione delle informazioni, la c.d. *information security*. La nota triade CIA[3] (RID, in italiano: *riservatezza*, *integrità* e *disponibilità* del sistema o di un suo componente), centrale nella *computer security,* integra in questa accezione ulteriori requisiti di sicurezza per restituire certezza ai rapporti digitali e trasformare in *conoscenza* i flussi continui di dati e informazioni: la *non ripudiabilità*, l'*autenticità*, l'*accountability* e la *verificabilità*[4].

A un alto livello di astrazione, sul profilo tecnico e organizzativo, la sicurezza informatica si estrinseca in tre categorie di misure (o controlli). In primis, la predisposizione di misure in grado di prevenire l'incidente informatico con l'obiettivo di impedire che il rischio si manifesti, controllando i punti di vulnerabilità del sistema e proteggendolo dagli attacchi; in seconda istanza, misure di monitoraggio degli eventi avversi che nel caso si verifichi un incidente di sicurezza siano finalizzate a rilevarne le conseguenze dannose e ad agire sul sistema per migliorare la sicurezza; infine misure di ripristino che in risposta all'evento consentano di minimizzare i danni con la riattivazione tempestiva del sistema e delle sue funzionalità, senza perdita di dati. Ciascun ambito comprende una vasta gamma di strumenti tecnici e misure organizzative: controllo degli accessi, *distaster recovery*, crittografia, hardware e software per la difesa perimetrale, sistemi di rilevamento intrusioni e misure di sicurezza fisica, ecc. La progettazione di sistemi robusti resta un punto cardine della prevenzione.

L'evoluzione del concetto di sicurezza da *computer security* a *information security* trova riscontro, oltre che nella letteratura tecnico-scientifica, anche negli interventi del legislatore comunitario: da principio la sicurezza era orientata a garantire il funzionamento delle reti pubbliche di comunicazione (sin dalla direttiva 90/387/CE sull'istituzione del mercato interno per i servizi delle telecomunicazioni), per arrivare poi a una nuova visione focalizzata sulla protezione dei dati e delle informazioni nella strategia europea

[2] Così la norma tecnica UNI/EN ISO 104559.
[3] La CIA triad è alla base di molteplici norme tecniche per la sicurezza informatica. Si veda, tra tutti, NIST (National Institute of Standards and Technology), *Handbook on Computer security* o anche UNI/EN ISO 27001.
[4] Si rimanda alle definizioni del NIST in M. NIELES, K. L. DEMPSEY, V. Y. PILLITTERI, *An Introduction to Information Security,* in *NIST Special Publication 800-12 Rev 1.,* 2017.

del *Digital Single Market* dove la sicurezza dell'informazione diventa un pilastro per creare un clima di fiducia nell'ambiente digitale[5].

Più di recente, come testimonia lo studio di Veale e Brown[6], nella letteratura scientifica e in generale nel lessico comune, i riferimenti a concetti più tecnici come *computer security* e *information security* sono stati sostituiti dal termine cybersecurity su cui, tuttavia, non pare esserci una convergenza definitoria. Coniato originariamente negli US in riferimento alla capacità di difendere e proteggere il ciberspazio contro la minaccia cibernetica[7], il termine rimanda alla necessaria espansione del perimetro da proteggere non solo con riferimento a una dimensione di sicurezza che diventa sicurezza nazionale e sovranazionale ma anche con riferimento a nuovi valori. Limitare il concetto di sicurezza informatica alla sola protezione delle reti e dei sistemi informativi è oggi fuorviante e anacronistico: il contesto in cui agire e i valori da proteggere sono enormemente più complessi.

Il susseguirsi di attacchi informatici anche di grande entità ha aumentato la consapevolezza della vulnerabilità di soggetti diversi – privati, imprese, enti pubblici, istituzioni, organizzazioni – di fronte alle minacce cibernetiche. Il Rapporto sui rischi globali del *World Economic Forum* già nel 2019 aveva classificato gli attacchi informatici tra i primi dieci rischi globali di maggiore impatto e i dati documentati dai più recenti rapporti di sicurezza lo confermano[8]. La pandemia COVID-19, inoltre, ha imposto cambiamenti così repentini nel panorama tecnologico da indebolire le misure di sicurezza informatica esistenti; i cibercriminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori – come quello della produzione dei presidi di sicurezza e della ricerca sanitaria – per colpire le proprie vittime con vettori di attacco personalizzati. Come è evidenziato dal Rapporto (2020) "L'anno in rassegna" di ENISA (*European Union Agency for Cybersecurity*) la cybersecurity si è trovata di fronte a un paradosso: è stata sia la sfida sia l'opportunità di agevolare la trasformazione in quanto strumento generatore di fiducia nei servizi digitali.

Nella misura in cui la sicurezza riguarda la protezione degli *asset* ("i valori da proteggere") di un'organizzazione da minacce poste da aggressori che sfruttano le vulnerabilità del sistema, predisporre

[5] Su questa linea si collocano, in particolare, il Regolamento Generale sulla Protezione dei Dati, anche noto come GDPR (General Data Protection Regulation, Regolamento UE 2016/679) e il Regolamento UE 91/2014 eIDAS (electronic IDentification Authentication and Signature).

[6] I dati riportati da Vale e Brown evidenziano che dal 2003 si fa sempre più riferimento a questo concetto sia nelle pubblicazioni accademiche che in quelle tradizionali, in campi che includono l'ingegneria del software, le relazioni internazionali, la gestione delle crisi e la sicurezza pubblica, superando lentamente termini più tecnici come computer security, system security o data security (diffuso negli anni '70/80) e information security (diffuso dalla metà degli anni '90). M. VEALE e I. BROWN, *Cybersecurity,* in *Internet Policy Review,* n. 9 vol. 4, 2020.

[7] C. PAULSEN e R.D. BYERS, *Glossary of Key Information Security Terms,* in *NIST Interagency/Internal Report (NISTIR),* 2019.

[8] Si veda, *ex multis,* ENISA, *L'anno in rassegna da gennaio 2019 ad aprile 2020,* 2020;), EUROPOL, *Internet organised crime threat assessment (IOCTA),* 2020; Clusit, *Rapporto Clusit 2021 sulla sicurezza ICT in Italia*, 2021.

un piano di sicurezza significa individuare gli *asset* e ordinarli per gradi, identificare i pericoli e stimare i rischi. I fattori di rischio nel contesto digitale attuale non sono legati esclusivamente alla tecnologia e un attacco può causare non solo danni tecnologici ma, anche, ledere diritti e libertà delle persone, alterare gli equilibri politici di una nazione e, se sono colpite infrastrutture critiche, determinare gravi conseguenze per comunità, istituzioni e imprese.

Procedure, controlli e comportamenti, unitamente alla tecnologia, sono i fondamenti della sicurezza informatica. Essa, infatti, riguarda limitatamente l'adozione dell'ultimo prodotto tecnologico quanto piuttosto la definizione di procedure (regole legislative, amministrative e organizzative), la predisposizione di meccanismi di controllo e la promozione di comportamenti individuali corretti per il controllo del *rischio*[9]. Il rischio non rappresenta solo una condizione individuale, della persona singola che utilizza le ICT ma, in determinati contesti e scenari, diviene di interesse globale e riguarda questioni di sicurezza pubblica.

Tracciare un quadro di minacce che mutano dinamicamente non è semplice. La motivazione dei principali incidenti informatici[10] del 2020 è quella *economica*: il numero di incidenti che hanno portato a furti di informazioni, di dati e di credenziali utente è il più alto nel periodo di riferimento. Le informazioni sottratte vengono vendute nel *dark web* e divengono a loro volta strumento per altri tipi di attacchi, come la frode finanziaria o come lo spionaggio e il sabotaggio, finalizzati ad acquisire informazioni industriali, commerciali o relative al *know how*, decretando il fallimento di aziende e causando danni di immagine e organizzativi. Sempre rilevante è il *crimine informatico* con il modello ormai consolidato del *Crime As a Service*, in base al quale organizzazioni criminali vere e proprie strutturate come aziende offrono *software* pronti all'uso che non necessitano di particolari abilità informatiche per perpetrare attacchi.

Non sono queste, tuttavia, le minacce che destano maggiori preoccupazioni. Una dimensione nuova e problematica è legata alle c.d. *Cyberwar*[11] e alle guerre di informazioni (*information warefare*)[12] dove il conflitto tra gli stati viene condotto con attacchi cyber verso sistemi informatici di varia natura, infrastrutture

[9] Il concetto di rischio permea tutta la disciplina della sicurezza informatica. Il rischio è l'effetto dell'incertezza sugli obiettivi di sicurezza del sistema e, in quanto tale, può essere misurato in termini probabilistici come la combinazione della gravità delle conseguenze di un dato evento pericoloso (impatto) e la probabilità che l'evento stesso accada (ISO 73:2009). Le metodologie per il "controllo del rischio" sono molteplici; fondamentalmente l'attività si sostanzia in diversi passaggi che possono avere perimetri differenti a seconda dello standard di riferimento. In particolare, la ISO 31000 definisce due fasi: (i) la valutazione del rischio che comprende l'identificazione dei pericoli, l'analisi e la ponderazione della gravità e (ii) il trattamento del rischio che ha l'obiettivo di mitigare gli effetti del rischio con la predisposizione di misure adeguate e di verificare il rischio residuo.

[10] Un incidente informatico è un qualsiasi evento di natura dolosa o colposa volto a danneggiare le risorse materiali, immateriali e umane che abbiano *valore* per il sistema o per l'organizzazione. Per incidente informatico, dunque, non si intendono solo "attacchi hacker" o intrusioni esterne ma anche comportamenti inadeguati degli utenti del sistema, rottura di apparecchiature, bug nei *software* o eventi e calamità naturali.

[11] A. BONFANTI, *Attacchi cibernetici e cyber war: considerazioni di diritto internazionale*, in *Notizie di Politeia*, n. XXXIV vol. 132, 2018 pp. 118-127.

[12] F. RUGGE, *Mind hacking: la guerra informativa nell'era cyber,* in *Notizie di Politeia*, XXXIV, 132, 2018 pp. 118-127.

nazionali critiche e servizi il cui malfunzionamento produce disagi. Il *controllo delle informazioni* non riguarda solo l'ambito militare ma anche ambiti come l'economia, la politica e la vita sociale, attraverso *fake news* e *trolls* che propagano informazioni manipolate sulla rete e amplificate dai *social network*[13]. Nuove sfide provengono infine dall'uso malevolo dell'Intelligenza artificiale (IA)[14]. L'IA offre nuovi modi di condurre attacchi cyber, sempre più efficaci, sfruttando la capacità di tali sistemi di identificare vulnerabilità che possono sfuggire a un esperto umano; di automatizzare attacchi di ingegneria sociale personalizzati mediante informazioni raccolte online; di generare immagini e video non distinguibili dalla realtà (i c.d. *deep fake*); di realizzare *malware* autonomi nel mascherarsi e selezionare il proprio target, o ancora di attaccare altri sistemi di IA applicando in modo avverso gli stessi paradigmi del *machine learning*.

Gli attacchi si basano sulle sempre nuove lacune di sicurezza dei sistemi informatici ma trovano altresì la principale vulnerabilità nel fattore umano. La cybersecurity di un paese non dipende solo dalla sicurezza informatica delle organizzazioni del settore pubblico e privato ma anche dalla sicurezza dei singoli utenti che possono fungere da vettori di attacco a istituzioni o infrastrutture critiche.

La vulnerabilità della persona è correlata alla percezione del rischio e al grado di competenza tecnica; spesso viene trascurato il rischio connesso a un uso improprio di dati personali[15] con conseguenze sulla costruzione dell'identità personale[16], sulla reputazione online e sull'esposizione al cibercrimine[17]. I modelli tradizionali di minacce e attaccanti, in questo senso, possono essere limitati. Frequentemente, per esempio, tra i possibili attaccanti non vengono considerati familiari o conoscenti che in un contesto di abusi possono comunque avvantaggiarsi di un accesso facilitato ai dispositivi della vittima. Pochi strumenti informatici sono disegnati per distinguere gli utenti legittimi da utenti autenticati. L'*asset* da proteggere da abusi e manipolazioni diventa dunque la persona[18].

---

[13] Si veda, *ex multis*, G. ZICCARDI, *Tecnologie per il potere*, Raffaello Cortina, 2019.

[14] Per una fotografia delle minacce per l'IA si veda il Rapporto di ENISA del 15 dicembre 2020, *Artificial Intelligence Threat Landscape Report.*

[15] M. MARTONI, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *federalismi.it*, n. 1, 2020, pp. 119 – 136.

[16] M. PALMIRANI, M. MARTONI, *Big data, governance dei dati e nuove vulnerabilità*, in *Notizie di Politeia*, n. 136, 2019, pp. 9 – 22.

[17] R. BRIGHI, *Cibercrimine e anonimato in Rete. Riflessioni su sicurezza, efficacia investigativa e tutela delle libertà personali*, in *Sicurezza e Scienze Sociali,* n. 3, 2017.

[18] Comportamenti lesivi quali molestie, odio, bullismo e *stalking* hanno nella dimensione online un forte potenziale lesivo della reputazione in virtù della persistenza delle informazioni e della loro potenziale diffusione virale. Il furto d'identità, agevolato spesso da lacune di sicurezza, può diventare strumento, oltre che per commettere truffe e frodi, per reati di diffamazione e per diffondere contenuti riservati a scopo di vendetta (*revenge* p*orn*) o di estorsione e ricatto (*sexstortion*) e atti persecutori verso individui vulnerabili. Per un inquadramento del tema si rimanda a G. ZICCARDI, *L'odio online. Violenza verbale e ossessioni in rete,* Raffaello Cortina, 2016; si veda, inoltre, G. CASSANO, *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio*, Ipsoa, 2017; F. DI TANO, *Hate speech e molestie in rete. Profili giuridici e prospettive de iure condendo*, Aracne editrice, 2019; D.K. CITRON, M.A. FRANKS, *Criminalizing Revenge Porn*, in *Wake Forest Law Review*, n. 49 vol. 2, 2014, pp. 345-391; C. SGARBI, *Lo stalking. Dall'evoluzione del fenomeno alle prospettive di intervento*, in T. Casadei (a cura di), Donne, diritto, diritti. Prospettive del giusfemminismo, Giappichelli, 2015, pp. 131-154; A. VERZA, "*Mascolinità*

Un ulteriore esempio dell'espansione dei confini di interazione tra ambiente e sistemi informativi è dato dall'Internet delle cose, o *Internet of Things* (IoT)[19]. Tali sistemi, che svolgono un ruolo sempre più importante sia nella dimensione pubblica - ad es. nelle infrastrutture critiche – che in quella privata – da intendersi sia nel senso dell'iniziativa privata (si pensi al caso della cd. industria 4.0) che della dimensione domestica, sono dispositivi in grado di interagire in modo continuo con il mondo fisico in cui operano, attraverso sistemi di sensori e attuatori tra loro connessi. In ragione di ciò, l'IoT implica un cambio di paradigma nell'approccio alla sicurezza: ogni cyberattacco ai sistemi IoT ha un impatto diretto su tutti gli oggetti fisici (inter)connessi[20]. La sicurezza dei sistemi, intesa nel senso di *security,* acquista così un legame ancora più stretto con la sicurezza intesa come *safety*[21]*,* cioè quella dimensione volta a proteggere l'integrità della vita dalla minaccia di un pericolo imminente[22].

L'esigenza di sicurezza, in ambienti complessi di interazione tra persone, software e servizi, rimanda dunque a una dimensione olistica di controllo del rischio che comporti la protezione in modo coordinato dei molti valori in gioco. Questo giustifica la ragione per cui a differenza di termini più tecnici quali *computer security* e *information security*, del concetto di cybersecurity non esistano nozioni condivise e tantomeno confini definiti sia a livello scientifico che a livello politico e dottrinale.

A contribuire a una nuova concettualizzazione della cybersecurity è l'approccio che l'Unione europea ha messo in atto a partire dal 2013, con il documento "Strategia dell'Unione europea per la cybersecurity: un ciberspazio aperto e sicuro" (la c.d. *Cybersecurity Strategy*): con un approccio *top down,* l'Unione ricorda come un alto livello di sicurezza informatica sia necessario, non solo per mantenere i servizi essenziali e per il funzionamento della società e dell'economia, ma anche per salvaguardare l'integrità fisica dei cittadini.

Il progetto di un'Unione più resiliente alle minacce cibernetiche viene rilanciato con una serie di misure proposte dalla Commissione nel 2017 al fine di colmare le lacune delle regole già esistenti e rafforzare la strategia del 2013 nell'ottica di rendere la cybersecurity una materia armonizzata a livello comunitario. In particolare, viene adottato il *Cybersecurity Act* (Regolamento UE 2019/881)[23], entrato in vigore il 27 giugno

tossica" sul web: la "cultura" dell'odio anti-femminista online, in A. Verza, S. Vida (a cura di), Postfemminismo e neoliberalismo, Roma, Aracne, 2020, pp. 157-196.

[19] A. RAYES e S. SALAM, *Internet of Things: from Hype to Reality,* Springer, seconda edizione, 2019, p. 2.

[20] Si veda, *ex multis,* C. CAMARA, P. PERIS-LOPEZ, e J. TAPIADOR, *Security and privacy issues in implantable medical devices: A comprehensive survey,* in *Journal of biomedical informatics,* n. 55, 2015, pp.272-289; si veda, inoltre, C. MILLER e C. VALASEK, *Remote exploitation of an unaltered passenger vehicle,* in *Black Hat USA,* n. 91, 2015.

[21] A. VEDDER, *Safety, security and ethics,* in A. VEDDER, J. SCHROERS, C. DUCUING e P. VALCKE (a cura di) *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Intersentia, p. 15.

[22] M. DURANTE, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks,* in D. BERKICH e M. V. D'ALFONSO (a cura di) *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, Springer Nature, 2019, p. 372.

[23] REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie

2019, composto di due parti. Nella prima viene specificato e potenziato il ruolo dell'ENISA. L'ENISA – che ricopriva un ruolo di mera consulenza tecnica nei confronti degli Stati membri in caso di attacchi o incidenti informatici – assume un ruolo operativo nella gestione di tali minacce, facendo in modo che la risposta agli attacchi di questa natura, che è sempre stata appannaggio degli Stati membri, abbia rilevanza comunitaria e sia gestita a livello sovranazionale. Nella seconda parte il Regolamento introduce la creazione di un quadro comune europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali, con l'obiettivo di facilitarne lo scambio nella UE e di aumentare la fiducia dei consumatori.

In questo scenario il Cybersecurity Act propone una definizione di cybersecurity volutamente molto più ampia delle precedenti che include tutte le "attività necessarie per proteggere i sistemi di rete e di informazione, gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche". In questo modo il legislatore europeo comprende un ampio perimetro di rischi senza limitazioni concettuali[24].

La nuova strategia per la cybersecurity dell'UE, presentata dalla Commissione a dicembre 2020, completa il percorso con l'introduzione di diverse proposte per il dispiegamento di un quadro giuridico, politico e di investimenti unitario e all'altezza delle sfide attuali.

Nel presente contesto, in cui molti obiettivi della cybersecurity coincidono con l'interesse comune ad abitare una "società sicura", nella sua dimensione *onlife*[25], le sezioni che seguono analizzeranno la possibilità di estendere la dottrina dei beni pubblici alla cybersecurity, con particolare riferimento alla dimensione della robustezza dei sistemi. Da un punto di vista metodologico, il contributo analizza diverse teorie per la cybersecurity come bene pubblico al fine di estrapolare diversi indicatori, ritenuti significativi dagli Autori, per la costruzione di un indipendente impianto teorico. Tale modello fornirà un'originale chiave di lettura ai recenti sviluppi legislativi dell'Unione Europea in materia di cybersecurity, come la nuova strategia della Commissione Europea e la proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) COM(2020) 823 final, al fine di determinare se e fino a che punto l'approccio europeo alla cybersecurity integri elementi fondamentali della dottrina del bene pubblico.

dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 «regolamento sulla cibersicurezza».

[24] Art. 2, Regolamento UE 2019/881.

[25] L. FLORIDI, *The Onlife Manifesto,* Springer, 2015.

2. La dottrina della cybersecurity come bene pubblico: una riflessione critica

Una dottrina che caratterizzi la cybersecurity come bene pubblico non è certamente una novità teorica. Come premessa essenziale, al fine di giustificare tale impostazione, è bene chiarire i confini concettuali, di stampo economico-giuridico, di "bene pubblico". Nella teoria economica, un bene è definito pubblico quando il suo consumo presenti le caratteristiche della non-rivalità e non-escludibilità. Nel primo caso, la fruizione del bene potrà avvenire ad opera di più agenti simultaneamente; nel secondo, da tale consumo non potrà essere escluso alcun membro della società perché l'esclusione implicherebbe un costo eccessivo[26]. Quest'ultima connotazione comporta tuttavia la possibilità di usufruire il bene in questione senza sostenerne i costi: tale fenomeno è detto *free-riding*. Senza voler entrare nel merito, basti qui sottolineare il lavoro della *Commissione Rodotà* - nel primo decennio del 2000 - per una riforma del regime giuridico italiano dei beni pubblici[27].

Soprattutto negli Stati Uniti, da circa vent'anni, diversi studiosi elaborano modelli teoretici volti a giustificare l'equazione tra cybersecurity e bene pubblico, tracciando analogie ora con la difesa nazionale, ora con la tutela della salute pubblica. Taluni hanno infatti sostenuto come gli obiettivi, e non anche gli istituti, della salute pubblica, indiscusso bene pubblico, possono fondare una solida base per un ragionamento analogicamente applicabile alla cybersecurity. La salute pubblica e la cybersecurity mirano entrambe a raggiungere un esito positivo (salute o sicurezza) in un contesto tendenzialmente connesso ma altamente interdipendente. Tale metafora esplicherebbe principalmente due effetti. In primo luogo, nel bilanciare gli interessi collettivi contro quelli individuali, l'accento verrebbe posto sul primato della collettività. In secondo luogo, la gestione dell'insicurezza di sistemi e reti verrebbe gestita in misura crescente dall'intervento pubblico, attraverso incentivi e obblighi[28].

Per quanto intrigante e, per certi versi, intuitiva, tale metafora solleva non pochi problemi teorici, quindi pratici. Innanzitutto, un'applicazione *tout court* della dottrina del bene pubblico al contesto della cybersecurity, composto da persone, hardware e software, e non pertanto riconducibile ad un unico aspetto, impone una riflessione per compensare la sottoproduzione di tali beni in uno scenario di fallimento di mercato. Tale strategia combina tendenzialmente tre approcci: i) persuasione attraverso l'educazione, ideologie e norme sociali; ii) monitoraggio attraverso una raccolta e scambio di informazioni che sia trasparente; e iii) intervento dello Stato nelle scelte dei privati. Soprattutto l'ultimo aspetto evidenzia il fatto che se la società vuole trattare molti, se non tutti gli aspetti di cybersecurity come bene pubblico, allora ciò che le metafore di salute pubblica dimostrano è che potrebbe essere necessario

[26] R. MARCHIONATTI e F. MORNATI, *Principi di Economia Politica,* Giappichelli Editore, Torino, 2010, p. 171.
[27] U. MATTEI, E. REVIGLIO, S. RODOTÀ (a cura di), *Invertire la rotta: Idee per una riforma della proprietà pubblica,* il Mulino, Bologna, 2007.
[28] D.K. MULLIGAN e F.B. SCHNEIDER, *Doctrine for Cybersecurity,* in *Daedalus*, n. 140 vol. 4, 2011, pp. 70-92.

accettare un livello più alto di coercizione sul comportamento rispetto a quello a cui la società iperstoriche[29] dell'informazione sono abituate[30].

Nella sezione introduttiva si è già evidenziato come non ci sia, sia a livello politico che dottrinale, un consenso stabile sui confini concettuali del termine. Eppure, è pacifico che la cybersecurity non si sostanzi in una singola dimensione, e tantomeno in un singolo prodotto, capace di fare fronte, in un'ottica olistica, a tutti i diversi casi di minacce informatiche (virus, malware, ransomware, DDoS ecc.); piuttosto, è un insieme di vari beni e processi. Infatti, molti prodotti e soluzioni di cybersecurity, come schemi crittografici avanzati, software antivirus e sistemi di rilevamento delle intrusioni[31], non sono beni pubblici: comprati e venduti tra attori del settore privato, sono rivali, perché il loro uso influenza altri attori, ed escludibili, poiché il loro proprietario può limitare il loro uso da parte di altri. Adottando questo approccio, Rosenzweig argomenta come la cybersecurity sia un bene pubblico solo ed esclusivamente nella sua dimensione di scambio di informazioni circa vulnerabilità e minacce[32].

Similmente, è stata proposta una teoria facente perno sulla tripartizione classica della sicurezza informatica di tre ambiti distinti ma al tempo stesso fortemente connessi tra loro: i) progettare sistemi robusti e in grado di resistere agli attacchi; ii) progettare metodi e sistemi di rilevamento delle minacce e delle anomalie per garantire la resilienza di un sistema; iii) definire le risposte del sistema agli attacchi. Taddeo sostiene che solo il primo dominio – la robustezza del sistema, e quindi il grado di divergenza tra il comportamento attuale e quello desiderato dal sistema – debba essere ricompreso nella cornice di tutela accordata ai beni pubblici; di converso, tale dottrina non sarebbe suscettibile di essere applicata alle restanti aree della cybersecurity, seppur per motivi diversi. Infatti, la *resilienza* – intesa nella dimensione del rilevamento delle minacce – impone un delicato bilanciamento tra il grado di sicurezza desiderato e diritti fondamentali, quali il diritto alla privacy e alla protezione dei dati; similmente, facilitare la *responsività* potrebbe non portare ad un miglioramento globale e collettivo della cybersecurity. Al contrario, è probabile che porti ad una intensificazione degli attacchi informatici[33]. Questo impianto teorico non si propone tanto di trovare una giustificazione di matrice economica, quanto di fondare, da un punto di vista filosofico, le basi per una riflessione sulla necessità di trattare come bene pubblico il requisito di *robustezza* dei sistemi, che di per sé sfugge da questo inquadramento, in virtù dell'interesse pubblico

[29] L. FLORIDI, *Il Verde e il Blu – Idee ingenue per migliorare la politica,* Raffaello Cortina Editore, 2020, pp. 85-91.
[30] S. WEBER, *Coercion in cybersecurity: What public health models reveal,* in *Journal of Cybersecurity*, n. 3 vol. 3, 2017, pp. 173-183.
[31] C. THELIOS, G. THOLIS e M. ATHANATOS, *A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions,* in A. FOURNARIS et al. (a cura di) *Computer Security: IOSEC 2019, MSTEC 2019, FINSEC 2019*, Springer, 2019.
[32] P. ROSENZWEIG, *Cybersecurity and Public Goods: The Public/Private "Partnership*", in *Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, Praeger Security International, 2012, pp. 7-9; cfr. N.E. WEISS, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis, Congressional Research Service Report*, 2014.
[33] M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machines*, n. 29, Springer, 2019, p. 354.

sottostante e del ruolo cruciale che riveste nelle società. A fronte di una crescita esponenziale di attacchi e minacce informatiche, l'approccio non-rivale ma esclusivo (ossia, l'accesso è regolato dal costo) di questo aspetto della cybersecurity continuerebbe a rivelarsi inefficace[34]. In generale, infatti, sviluppare sistemi robusti ha costi elevati: spesso gli aspetti di sicurezza vengono concepiti in un trade-off con il costo finale del prodotto. Per rendere le cose ancora più complicate, si consideri, per esempio, il settore dell'IoT: la maggioranza di questi dispositivi connessi sono limitati in termini di potere computazionale (*resource-constrained devices*)[35]. Di conseguenza, potrebbero non avere un'adeguata capacità di elaborazione e memorizzazione per incorporare dei software di sicurezza o per eseguire tecniche come la crittografia[36]. Una prima conseguenza diretta dell'applicazione della teoria dei beni pubblici imporrebbe il confronto con le esternalità positive e negative del bene privato, la cybersecurity, cui si vorrebbe estendere tale trattamento.

La prima esternalità negativa da analizzare è *l'effetto diversivo*: alcune tecnologie di cybersecurity, come i *firewall*, appartenenti alla dimensione della *resilienza*, sviano semplicemente gli attacchi da un obiettivo più impenetrabile ad uno più facilmente attaccabile, il che significa che il miglioramento della sicurezza di un attore può determinare uno stato di sicurezza inferiore per i sistemi[37], piuttosto che un innalzamento del livello globale di sicurezza. In questo contesto, circoscrivere la dottrina dei beni pubblici alla sola dimensione della *robustezza,* e non alla cybersecurity *tout court,* risponde a tale esternalità, dal momento che la *ratio* stessa di questo impianto teoretico risiede nel migliorare il livello globale di cybersecurity.

Una seconda esternalità negativa della cybersecurity è *l'esternalizzazione dei costi*: quando un software non riesce a prevenire un'intrusione o un fornitore di servizi non riesce a bloccare un attacco *malware*, non c'è alcun meccanismo attraverso il quale ritenere tali attori privati responsabili per i costi di questi fallimenti. I costi sono sostenuti interamente dagli utenti finali[38]. In questo secondo caso, la robustezza del sistema non dovrebbe essere necessariamente gratuita per gli utenti finali, piuttosto, è essenziale che i suoi costi non diventino un fattore discriminante, determinandone l'accesso. Attraverso un'equa ripartizione dei costi tra i vari attori di mercato, si dovrebbe garantire a tutti gli utenti l'accesso alle tecnologie digitali adeguatamente sicure[39]. Come risultato, verrebbero favoriti approcci sistemici, o olistici[40], che si

[34] *Ibid.*, 350.
[35] T. STAPKO, *Practical Embedded security: Building Secure Resource-Constrained Systems,* Newnes, 2008, p. 85.
[36] Agenzia dell'Unione Europea per i Diritti Fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati,* 2018.
[37] P. ROSENZWEIG, *Cybersecurity and Public Goods: The Public/Private "Partnership"*, *op. cit.,* p. 9.
[38] *Ibid.*, p. 10.
[39] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 351.
[40] In letteratura, il cd. "approccio olistico" in cybersecurity raccoglie sempre più consensi, seppur non abbia un'univoca interpretazione. *Ex multis,* cfr. L. FLORIDI e A. STRAIT, *Ethical Foresight Analysis: What it is and Why it is Needed?,* in *Minds & Machines*, n. 30, 2020; C. RAAB, *Information privacy, impact assessment, and the place of ethic*, in *Computer law and security review*, n. 37, 2020; A. MANTELERO, *AI and big data: a blueprint for a human rights, social and ethical impact assessment,* in *Computer law and security review*, n. 34 vol. 4, 2018.

concentrerebbero cioè sulle relazioni tra le diverse tecnologie di cybersecurity e, soprattutto, sul risultato di queste ultime in termini di impatto sull'ecosistema in cui operano[41].

La gestione della robustezza del sistema come bene pubblico richiede inoltre la collaborazione tra il settore privato e quello pubblico per assicurare un alto livello di sicurezza, attraverso una ripartizione bilanciata di competenze e responsabilità. Da una parte, il pubblico dovrà stabilire gli standard, la certificazione e i test, le procedure di supervisione, per garantire che sia mantenuto un livello sufficiente di sicurezza per proteggere e promuovere l'interesse pubblico e che ci siano misure di riparazione e compensazione quando le responsabilità non sono assolte correttamente[42]. In questo senso, il già citato Cybersecurity Act[43] definisce un quadro europeo di standard certificativi della cybersecurity, volto ad attestare che i prodotti, servizi e processi ICT siano conformi "a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita"[44].

D'altra parte, il settore privato ha la responsabilità di progettare sistemi robusti, sviluppare e migliorare i metodi per favorire la robustezza dei servizi e dei prodotti che offre, e collaborare con il settore pubblico per i meccanismi di controllo e di prova[45].

In generale, la necessità di strutturate intersezioni tra pubblico e privato è testimoniata dal numero crescente di iniziative e dichiarazioni politiche che sottolineano il valore dei partenariati pubblico-privato (PPPs) per fornire o aumentare la cybersecurity, soprattutto nel campo delle infrastrutture critiche[46]. Le aeree di intersezione, ad un più alto livello d'astrazione, sono prevalentemente quattro: (1) la fornitura affidabile dell'accesso a Internet e alle infrastrutture TIC; (2) la co-regolamentazione degli aspetti tecnici della sicurezza informatica e del trattamento dei dati; (3) lo scambio di informazioni sulle minacce e la vulnerabilità; e (4) l'assistenza reciproca nell'affrontare minacce o contenuti illegali nel ciberspazio[47].

In questo contesto di redistribuzione delle diverse responsabilità a tutti coloro i quali possano essere determinanti nell'ottenere un soddisfacente livello di robustezza dei sistemi, nell'ottica di proteggere un

[41] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 350.
[42] *Ibid.*, 351.
[43] Regolamento UE 2019/881
[44] Art. 46(2), Regolamento UE 2019/881; cfr. B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità e competitività e diritti individuali,* in *Federalismi.it*, n. 14, 2020.
[45] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 351.
[46] F. CAPPELLETTI e L. MARTINO, *Achieving robust European cybersecurity through public-private partnerships: Approaches and developments,* in *Elf discussion papers*, n. 4, 2021. Si veda inoltre, COMMISSIONE EUROPEA, *Public consultation on the public-private partnership on cybersecurity and possible accompanying measures*; ENISA, *Public Private Partnerships (PPP): Cooperative models*, 2017.
[47] R. BOSSONG e B. WAGNER, *A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union,* in O. BURES e H. CARRAPICO (a cura di) *Security Privatization*, Springer, 2018, p. 227.

interesse comune, alcune responsabilità dovranno necessariamente ricadere anche sugli utenti, con particolare riferimento alla loro cd. "igiene informatica"[48]. Da un punto di vista strettamente giuridico, tale conclusione implicherebbe non facili considerazioni sui vari titoli di responsabilità che si potrebbero configurare in capo agli utenti. In ottica comparatistica, negli Stati Uniti, in un incontro organizzato dal NIST circa la cybersecurity dei dispositivi IoT, è emerso – *inter alia* – che la sicurezza di tali sistemi debba essere una responsabilità condivisa tra produttori e utilizzatori[49]. Senza dilungarci in una riflessione sulla disciplina consumeristica dell'ordinamento giuridico italiano, che andrebbe al di là dell'oggetto del presente articolo, si potrebbe valutare l'adeguatezza dell'articolo 122 del Codice del Consumo, segnatamente al comma secondo, come base giuridica per tale cornice di responsabilità[50]. In termini meno controversi, la cd. "igiene" del computer si potrebbe pertanto sostanziare in *best practices* di cybersecurity che dovrebbero diventare parte delle competenze quotidiane di ogni utente di Internet[51]. Sullo sfondo di queste riflessioni, tuttavia, rimangono le criticità connesse al *digital divide*[52], o *Onlife divide* – ossia, non esclusione dalla sola dimensione della connessione, ma dalla vita sociale e dalla conoscenza[53]– benché sia stato dimostrato che l'età non sia sempre un fattore di vulnerabilità quando si tratti di percepire l'importanza di tali pratiche[54].

Tale ampliamento e redistribuzione delle responsabilità, unitamente alla necessità di considerare le esternalità scaturenti dalla produzione di beni di cybersecurity, favorirebbe la collaborazione e lo scambio di informazioni sulle vulnerabilità dei sistemi[55]. Se, da una parte, l'aspetto della collaborazione è certamente il punto privilegiato per considerare una teoria della cybersecurity come bene pubblico, in forza della sua natura non-rivale e non-esclusiva[56], dall'altra, potrebbe essere sbagliato ritenere che la

[48] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 352.
[49] NIST, *Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop,* NISTIR 8322, 2021, pp. 9-10: "eighty-two percent of responses to one poll question agreed that the responsibility for securing IoT devices is shared between manufacturer and customer. […] Customers, then, are responsible for implementing IoT devices in accordance with manufacturer guidance, ensuring devices have connectivity to receive updates, and monitoring devices to ensure continued security".
[50] Articolo 122, comma 2, del Codice del Consumo (D.lgs. 6 settembre 2005, n. 206): "[i]l risarcimento non è dovuto quando il danneggiato sia stato consapevole del difetto del prodotto e del pericolo che ne derivava e nondimeno vi si sia volontariamente esposto."
[51] L. PUPILLO, *EU Cybersecurity and the Paradox of Progress,* in *CEPS policy paper*, 2021, pp. 6-7.
[52] A. SULTAN, *Improving Cybersecurity Awareness in Underserved Populations,* in *Berkley Center for Long-Term Cybersecurity White Paper Series*, 2021.
[53] L. FLORIDI e M. SIDERI, *Piramide Onlife,* in *Corriere Innovazione*, 28 maggio 2021, p. 2.
[54] S.M. DEBB, D.R. SCHAFFEN, D.G. COLSON, *A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults,* in *International Journal of Cybersecurity Intelligence & Cybercrime*, n. 3 vol. 1, 2021.
[55] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 352.
[56] P. ROSENZWEIG, *Cybersecurity and Public Goods: The Public/Private "Partnership"*, *op. cit.*

condivisione delle informazioni circa le vulnerabilità e le minacce generi un impatto positivo per tutti i soggetti coinvolti[57].

In primo luogo, la vulnerabilità del software è un argomento sensibile che interseca gli interessi confliggenti della cybersecurity (e, unitamente, di privacy e protezione dei dati personali) e della sicurezza nazionale: le forze dell'ordine e le agenzie di intelligence, sfruttando le cd. vulnerabilità *zero-days*[58], riescono più agevolmente ad installare *malware* nei sistemi informatici ai fini di contrasto[59], al prezzo però di esporre gli utenti del sistema in questione agli attacchi di attori malevoli[60]. Pertanto, è agevolmente comprensibile il motivo per cui gli Stati membri siano reticenti a cedere le loro prerogative in tema di segnalazione delle vulnerabilità[61].

In secondo luogo, le imprese che sono a conoscenza di vulnerabilità informatiche o che hanno subito attacchi[62] sono riluttanti a svelarli per timore di ricadute reputazionali o di eventuali responsabilità, anche civili, dell'evento[63]. Infatti, il costo della divulgazione di un incidente o di una minaccia è soprattutto privato, in quanto sostenuto interamente dall'azienda, mentre i benefici di una migliore divulgazione sono pervasivi. Lo squilibrio tra i costi sostenuti da un'azienda e i benefici collettivi genera un fallimento del mercato.

Se, da una parte, questo spiega la tentazione di passare dallo strumento del partenariato ad un modello di governance più marcatamente *topdown*, consistente in processi istituzionalizzati che regolino un "dovere di notifica"[64], seppur in contesti che garantiscono riservatezza e reciprocità come quelli individuati nei *computer emergency response teams* (CERT) e *computer security incident response teams* (CSIRT)[65], dall'altra risulta quindi chiaro che sia necessario un nuovo approccio concettuale alla cybersecurity per rendere il

---

57 R. BOSSONG e B. WAGNER, *A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union*, *op. cit.,* p. 228.

58 Una falla nella sicurezza che non sia ancora conosciuta agli sviluppatori/produttori di un sistema informatico e, *a fortiori*, agli utenti del sistema stesso.

59 B.-J. KOOPS e E. KOSTA, *Looking for some light through the lens of "cryptowars" history: policy options for law enforcement authorities against "going dark",* in *Computer Law & Security Review*, n. 34, 2018, p. 898; cfr. G. ZICCARDI, *Lo studio del Parlamento Europeo sull'attività di hacking delle Forze dell'Ordine: un'analisi informatico-giuridica (e di politica legislativa)*, in *Archivio Penale*, n. LXIX vol. 2, 2017, pp. 512-537.

60 P.N. STOCKTON e M. GOLABEK-GOLDMAN, *Curbing the market for Cyber Weapons,* in *Yale Law and Policy Review*, n. 32 vol. 1, 2013, p. 239.

61 S. FANTIN, *Weighting the EU Cybersecurity Act: progress or missed opportunity?,* in KU Leuven Citip blog, 2019.

62 Non anche, ovviamente, i soggetti rientranti nell'ambito di applicazione della Direttiva EU 2016/1148 (NIS): gli operatori di servizi essenziali devono notificare, senza ingiustificato ritardo, all'autorità competente NIS (il CSIRT) gli incidenti con impatto "rilevante" sui servizi forniti; i fornitori di servizi digitali devono invece notificare quegli incidenti aventi un impatto "sostanziale".

63 BANCA D'ITALIA, *Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass,* Gruppo di coordinamento sulla sicurezza cibernetica (GCSC), 2018, p. 14; cfr. A. NOLAN, *Cybersecurity and information sharing: Legal challenges and solutions,* in *Congressional Research Service Report,* 2015, p. 5.

64 R. BOSSONG e B. WAGNER, *A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union*, *op. cit.,* p. 228.

65 BANCA D'ITALIA, *Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass*, *op. cit.*, pp. 14-15.

comportamento di tutti gli attori di questo mercato più compatibile con gli incentivi[66]. La dottrina del bene pubblico, in questo senso, è una risposta a tale esigenza.

Concludendo, l'analisi dell'impianto teorico proposto da Taddeo è funzionale a delineare un modello costituito da diversi indicatori, i quali serviranno come guida nell'analisi normativa dei recenti documenti e proposte legislative della Commissione. Ad un alto livello d'astrazione, la *redistribuzione delle responsabilità, cooperazione* e *scambio di informazioni* sono elementi cardine per la dottrina della cybersecurity come bene pubblico. Tuttavia, va preliminarmente sottolineato come sia nella nuova Strategia, sia nel pacchetto di misure legislative proposto dalla Commissione Europea in materia di cybersecurity, i termini *robustezza* o *robusto* non compaiano o siano marginali, rispetto ai ben più citati *resilienza* o *resiliente*. In questo contesto, la dimensione della robustezza, che sola giustificherebbe un impianto teorico per considerare la cybersecurity come bene pubblico, si estrinsecherebbe nella predisposizione di misure in grado di prevenire l'incidente informatico con l'obiettivo di impedire che il rischio si manifesti, controllando i punti di vulnerabilità del sistema e proteggendolo dagli attacchi. Questa prospettiva, secondo gli Autori, coincide per larghi tratti con il più ampio concetto di "resilienza" adottato dalla Commissione nelle sue attività, ricomprendente in tal senso il requisito della "robustezza" dei sistemi.

3. La nuova strategia della Commissione Europea sulla Cybersecurity

Il 16 dicembre 2020, la Commissione Europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la nuova Strategia Europea sulla Cybersecurity, componente chiave, integrata e coerente con il piano europeo di transizione digitale[67], il Recovery Plan[68] e la Strategia Europea sulla Sicurezza di luglio 2020[69]. La Commissione aspira infatti a migliorare ulteriormente la prevenzione, resilienza e le capacità di risposta agli incidenti di enti pubblici e privati, delle autorità competenti, e l'Unione nel suo complesso, nel campo della cybersecurity. Questo importante e ambizioso obiettivo si concretizza in due proposte legislative: la revisione della Direttiva NIS, o "NIS 2.0", del non lontano 2016[70] e una nuova Direttiva sulla resilienza delle Entità Critiche[71]. La rapida azione della Commissione in questo settore evidenzia la sempre maggiore centralità delle questioni di cybersecurity nell'agenda comunitaria.

---

[66] L. PUPILLO, *EU Cybersecurity and the Paradox of Progress, op. cit.,* p. 7.
[67] COMMISSIONE EUROPEA, *Shaping EU's Digital Future*, testo consultabile sul sito della Commissione.
[68] COMMISSIONE EUROPEA, *Recovery Plan per l'Europa,* testo consultabile sul sito della Commissione.
[69] COMMISSIONE EUROPEA, *Strategia Europea sulla sicurezza,* 2020.
[70] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[71]COMMISSIONE EUROPEA, *Proposta di direttiva del Parlamento Europeo e del Consiglio sulla resilienza delle infrastrutture critiche* COM(2020) 829 final.

Come già ricordato nella prima sezione, la strategia del 2020 assurge programmaticamente il concetto di cybersecurity a bene meritevole di tutela in sé e, contemporaneamente, a bene strumentale per la tutela e il godimento di diritti fondamentali. Questa prospettiva strumentale, identificata da alcuni come *infraetica*[72], trova la sua ragione d'essere nella natura essenziale della dimensione di robustezza dei sistemi[73], da una parte, per creare fiducia o, in termini meno problematici[74], fare affidamento sull'ambiente digitale; dall'altra, per garantire e promuovere diritti e libertà fondamentali, quali il diritto alla privacy e alla protezione dei dati personali, la libertà di espressione e di informazione[75].

La strategia definisce tre settori di intervento dell'UE, per un'accresciuta protezione dei cittadini, delle imprese e delle istituzioni, attraverso il dispiegamento di strumenti normativi, di investimento e politici. Queste tre aree di azione riguardano: 1) resilienza, sovranità tecnologica e leadership, 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta e 3) promozione di un ciberspazio globale e aperto.

Alcune iniziative strategiche della prima area di azione (resilienza, sovranità tecnologica e leadership) sono volte ad incentivare una redistribuzione delle responsabilità e la cooperazione pubblico-privato, integrando così due elementi cardine della dottrina della cybersecurity come bene pubblico. La Commissione si propone innanzitutto di portare a termine il processo di riforma della Direttiva NIS, per aumentare livello di cyber resilienza "di tutti i settori pertinenti, pubblici e privati, che svolgono una funzione importante per l'economia e la società"[76]. Inoltre, in un contesto di proliferazione di dispositivi connessi in rete (IoT), l'aumento vertiginoso di vecchie e nuove vulnerabilità rivela preoccupanti superfici di attacco: la Commissione, da una parte, sta valutando, in linea con le conclusioni del Consiglio[77], nuove norme orizzontali volte a migliorare la cybersecurity dei prodotti connessi e servizi associati (ad es., un nuovo dovere di diligenza da parte dei produttori); dall'altra, per incentivare prodotti e servizi sicuri,

---

[72] L. FLORIDI, *Infraethics–on the Conditions of Possibility of Morality,* in *Philosophy & Technology*, 2017, p. 30; si veda inoltre P.G. CHIARA, *The balance between security, privacy and data protection in IoT data sharing: A critique to traditional "security & privacy" surveys,* in *European Data Protection Law Review*, n. 7 vol.1, 2021.

[73] La resilienza dei sistemi, invece, impone dei trade-off tra sicurezza e diritti; si veda M. TADDEO, *Cyber security and individual rights, striking the right balance*, in *Philosophy & Technology*, n. 26 vol. 4, 2013, pp. 353–356.

[74] A. JOBIN, *AI and reflections in 2020,* in *Nature Machine Intelligence*, n. 3, 2021, pp. 6-7: M. Taddeo, intervistata dall'autrice, afferma: "[they] used the definition I previously introduced for trust — a second-order property that is qualified by the delegation of a task and the lack of monitoring over the way in which the task is performed — to distinguish trust from reliance, which envisages some form of control over the execution of a given task. This 'trust and forget' dynamic is problematic, because it may lead to the erosion of human control on the impact that digital technologies have on our societies". Cfr. M. TADDEO, *Trust in technology: A distinctive and a problematic relation,* in *Knowledge, Technology & Policy*, n.23 vol. 4, 2010.

[75] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale* JOIN(2020) 18 final, p. 5.

[76] *Ibid.*, 6.

[77] CONSIGLIO DELL'UNIONE EUROPEA, *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, 13629/20, 2020.

promuove la certificazione a norma del Cybersecurity Act e propone di sviluppare uno standard europeo per la conformità alla cybersecurity dei prodotti che sia armonizzato con l'attuale quadro di conformità della famiglia ISO 27000 e i requisiti stabiliti dal GDPR e dalla Direttiva NIS[78]. Per quanto concerne il piano di investimenti nei rapporti pubblico-privato, la Commissione pianifica un intervento finanziario del settore pubblico, per un valore fino a 4,5 miliardi di euro, a favore dell'intera *supply chain* digitale facendo "affidamento sugli strumenti forniti dal quadro normativo degli appalti pubblici dell'UE, nonché sugli importanti progetti di comune interesse europeo. Esso può inoltre sbloccare investimenti privati attraverso partenariati pubblico-privati (anche sulla base dell'esperienza del partenariato pubblico-privato contrattuale sulla cybersecurity e la sua attuazione attraverso l'Organizzazione europea per la cybersecurity), capitali di rischio a sostegno delle PMI o alleanze industriali e strategie sulle capacità tecnologiche"[79]. In questo contesto, il Centro Europeo di Competenza sulla Cybersecurity (CCCN) avrà un ruolo centrale nel gestire la sintesi tra investimenti degli Stati membri e sforzi analoghi dell'industria, nello sviluppo della sovranità tecnologica dell'UE nella cybersecurity riducendo così la dipendenza da paesi terzi per le tecnologie cardine[80]. Parallelamente, la Commissione propone di creare una rete di centri operativi di sicurezza al fine di sostenere il miglioramento di quelli esistenti, quali gli ISAC (condivisione e analisi delle informazioni), SOC (centri operativi di sicurezza) e CSIRT, "nel permettere lo scambio di informazioni sulle minacce informatiche tra più portatori di interessi", coinvolgendo anche le PMI[81]. Il fine ultimo della cooperazione, di sviluppare una conoscenza collettiva e condividere le migliori pratiche è il *fil rouge* che unisce la prima aerea di intervento alla seconda e, contestualmente, richiama un ulteriore indicatore individuato nella sezione precedente: lo *scambio di informazioni*.

La seconda area di azione ("sviluppo capacità operative volte alla prevenzione, alla dissuasione e alla risposta") è suscettibile di essere letta attraverso le lenti della dottrina del bene pubblico nella sola dimensione della prevenzione, che nella nostra ricostruzione è in parte sovrapponibile al requisito della robustezza. La *Joint Cyber Unit* (unità congiunta per il ciberspazio), primo strumento analizzato dalla Commissione in questo settore, sarebbe l'interfaccia eletta per la cooperazione tra le diverse comunità (civili, diplomatiche, delle forze dell'ordine e della difesa) europee di cybersecurity, colmando un'ulteriore lacuna nella governance delle crisi informatiche a livello tecnico e operazionale. "L'unità dovrebbe consentire agli Stati membri e alle istituzioni, agli organismi e alle agenzie dell'UE di utilizzare appieno le

[78] COMMISSIONE EUROPEA, *Rolling Plan for ICT Standardization*, 2021, pp. 30-32.
[79] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *op. cit.,* pp. 12-13.
[80] *Ibid.*
[81] *Ibid.*, pp. 7-8. Ulteriori propositi della Commissione, in questa prima macroarea, riguardano: lo sviluppo di un servizio di risoluzione DNS dell'UE quale alternativa aperta e sicura di accesso a Internet per i cittadini, le imprese e l'amministrazione pubblica dell'UE; e, il completamento dell'attuazione del pacchetto di strumenti del 5G.

strutture, le risorse e le capacità esistenti, nonché promuovere il principio della "*necessità di condividere*" (enfasi aggiunta). Essa […] fornirebbe anche l'opportunità di rinforzare ulteriormente la cooperazione riguardo all'architettura del programma e di sfruttare i progressi compiuti, in particolare all'interno del gruppo di cooperazione NIS e la rete CyCLONe"[82]. Come è stato giustamente evidenziato da Cappelletti, un partenariato pubblico-privato rafforzato dai già menzionati standard predefiniti avrebbe un impatto positivo sulla relazione tra il settore pubblico e quello privato in termini di *condivisione delle informazioni*, rafforzando ulteriormente la loro cooperazione e evitando anche le asimmetrie informative: ironicamente, è proprio la capacità di condividere facilmente informazioni tra i settori (cioè pubblico e privato) ad essere stata infatti identificata come punto debole della strategia di sicurezza informatica dell'UE[83]. Le capacità operative di dissuasione e risposta, richiamate dalla Commissione nella seconda area di azione, sono invece riconducibili alla dimensione di resilienza e risposta, e non quindi suscettibili di applicazione della dottrina del bene pubblico. In particolare, sono: i) contrastare la criminalità informatica nell'ambito della strategia per l'Unione della sicurezza; ii) pacchetto di strumenti della diplomazia informatica dell'UE, tra cui figura l'istituzione di un gruppo di lavoro di intelligence informatica degli Stati membri all'interno del Centro UE di situazione e di intelligence (INTCEN), unitamente alla promozione della posizione sulla dissuasione informatica dell'Unione; iii) rivedere il quadro strategico e le capacità di ciberdifesa, facilitando lo sviluppo di una "visione e strategia militari dell'UE sul ciberspazio come dominio operativo" per le missioni e le operazioni militari della politica di sicurezza e difesa comune (PSDC)[84].

Infine, la terza area di intervento della Commissione propone di insistere sulla cooperazione e collaborazione con i partner internazionali "per promuovere un modello politico e una visione del ciberspazio fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici che generino sviluppo sociale, economico e politico a livello globale e contribuiscano a un'Unione della sicurezza"[85]. Questa promozione del modello di normazione *a là européen*, con al centro cioè la dignità dell'uomo, i diritti e le libertà fondamentali[86], avente il proprio baricentro sull'articolo 3 comma 5 del Trattato sull'Unione Europea, deve avvenire nelle sedi internazionali di standardizzazione, affinché le norme tecniche siano allineate ai valori dell'Unione[87]. Il rafforzamento dei dialoghi con i paesi

[82] *Ibid.*, p. 15.
[83] F. CAPPELLETTI, *Free market and cybersecurity in Europe: The need for strategic public-private partnerships,* in *Elf discussion papers*, n. 4, 2021, p. 21.
[84] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *op. cit.,* pp. 16-20.
[85] *Ibid.*, 22.
[86] L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach,* in *Philosophy & Technology,* Springer, 2021, p. 4.
[87] A. CHRISTOFI, P. DEWITTE, C. DUCUING, P. VALCKE, *Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment up to (GDPR) standard?,* in *IGI Global,* 2020; cfr. E. LACHAUD, *ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification,* in *European Data Protection Law Review*, n. 7 vol. 2, 2020.

terzi in materia di ciberspazio, con particolare riferimento al tema della cybersecurity, si inserirebbe nel più ampio contesto di un modello "multi-partecipativo" per la governance di internet: tale approccio inclusivo intende rafforzare gli scambi strutturati con organizzazioni regionali, quali l'Unione africana, il Forum regionale dell'ASEAN, l'Organizzazione degli Stati americani e l'Organizzazione per la sicurezza e la cooperazione in Europa, e organizzazioni internazionali come la NATO[88].

La bontà della scelta del legislatore eurounitario di rafforzare ulteriormente il quadro giuridico di rifermento è confermata dalla stretta regolamentativa adottata dalla presidenza Biden negli Stati Uniti, a seguito dell'attacco "Solarwind" del febbraio 2021. L'Ordine Esecutivo del 12 maggio 2021, e non quindi atto del Congresso, mira a rafforzare il livello generale delle difese cibernetiche del paese, incoraggiando le aziende private ad adottare le migliori pratiche cyber, in mancanza delle quali verrebbero estromesse dai contratti d'appalto federali[89]. Ai fini del presente articolo, poi, preme evidenziare come gran parte del provvedimento sia incentrato attorno agli aspetti della *cooperazione pubblico-privato* e della *condivisione delle informazioni*. In primo luogo, si riconosce come la cybersecurity richieda più dell'azione del governo: "[p]rotecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace"[90]. In secondo luogo, la Casa Bianca ritiene che la rimozione delle barriere contrattuali alla condivisione delle informazioni su minacce, incidenti e rischi da parte dei fornitori di servizi *information technology* (IT)e *operational technology* (OT) verso le agenzie federali sia un passo necessario per accelerare gli sforzi di deterrenza, prevenzione e risposta agli incidenti e per permettere una difesa più efficace dei sistemi[91].

Inoltre, nel dibattito geopolitico, ogni attore internazionale lavora nell'ottica di accrescere – o costruire – la propria autonomia strategica in questo campo[92]. In Europa, ciò trova conferma nelle ragioni alla base della creazione del CCCN. Inoltre, si pensi, nuovamente, al caso degli Stati Uniti e all'NDAA del 2019 (legge McCain), con cui il Congresso ha vietato a tutte le agenzie federali di acquistare qualsiasi apparecchiatura, sistema o servizio che utilizzi prodotti o servizi di telecomunicazione prodotti da Huawei o ZTE come componente sostanziale o essenziale di qualsiasi sistema[93]. Peraltro, tali divieti in ambito di

[88] COMMISSIONE EUROPEA E ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *op. cit.,* pp. 24-25.
[89] GOVERNO DEGLI STATI UNITI D'AMERICA, *Executive Order on Improving the Nation's Cybersecurity*, 2021.
[90] D. E. SANGER e J. E. BARNES, *Biden Signs Executive Order to Bolster Federal Government's Cybersecurity,* in *The New York Times*, 12 maggio 2021.
[91] GOVERNO DEGLI STATI UNITI D'AMERICA, *Executive Order on Improving the Nation's Cybersecurity*, *op. cit.*
[92] COMMISSIONE EUROPEA, *Una nuova strategia industriale per l'Europa* COM(2020) 102 final, p. 14; cfr. P. TIMMERS e F. DEZEURE, *Strategic Autonomy and Cybersecurity in the Netherlands, Draft study commissioned by the Cyber Security Council (CSR)*, 2021.
[93] J. DEMPSEY, *Bans on Foreign Equipment in U.S. Critical Infrastructure,* in *Lawfare,* 19 maggio 2020.

procurement federale nei confronti delle tecnologie cinesi hanno radici lontane, essendo le prime restrizioni del 2013[94]. L'Italia, dal canto suo, non ha adottato delle norme per poter escludere dalle gare d'appalto in materia di telecomunicazioni determinati fornitori, come Huawei e ZTE: in Parlamento, è tuttavia acceso il dibattito circa l'opportunità di adottare una legislazione in tal senso[95].

4. La proposta per una direttiva NIS 2.0

La direttiva (UE) 2016/1148[96], nota come direttiva NIS "Network and Information Security", è il primo atto legislativo europeo in materia di cybersecurity. Nel perimetro NIS rientrano gli attori classificabili come "operatori di servizi essenziali"[97] operanti nei principali settori strategici[98] e "fornitori di servizi digitali"[99]; agli Stati membri è chiesto di garantire che questi attori rispettino, secondo il criterio della valutazione del rischio, gli obblighi in materia di misure di sicurezza e di notifica degli incidenti[100], adottando un approccio differenziato al livello di armonizzazione relativo ai due gruppi di soggetti[101]. L'Italia ha recepito la direttiva con il decreto legislativo n. 65 del 2018, adottando un approccio prudente e poco incisivo sulle dinamiche di mercato[102].

La relazione della proposta per la cd. "NIS 2"[103] riconosce, da una parte, che la direttiva NIS ha contribuito a migliorare le capacità di cybersecurity a livello nazionale, richiedendo agli Stati membri di adottare strategie nazionali e di nominare – ove necessario – le autorità competenti NIS, e ad aumentare

94 A. SELYUKH e D. PALMER, *U.S. law to restrict government purchases of Chinese IT equipment,* in *Reuters,* 28 marzo 2013.
95 M. LUDOVICO, *5G, gara da un miliardo per le Forze di polizia: ammesse anche le cinesi Huawei e Zte,* in *Il Corriere della Sera*, 26 maggio 2021; cfr. M. MAYER, *Cina, 5G, perimetro cyber. I rischi per il Paese (e il Pd) secondo Mayer,* in *Formiche*, 28 giugno 2020; G. POMPILI, *Conte e la videosorveglianza cinese a Palazzo Chigi*, in *Il Foglio,* 9 aprile 2021; G. CARRER, *5G, Draghi stoppa (di nuovo) la Cina. Il Dpcm su Vodafone,* in *Formiche,* 31 maggio 2021.
96 Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.
97 Ai sensi dell'art. 5 della direttiva NIS, gli Stati membri devono identificare, per ciascun settore (allegato II), gli operatori di servizi essenziali con una sede nel loro territorio, secondo i criteri delineati dal secondo comma dello stesso articolo.
98 Energia, trasporti, banche, infrastrutture del mercato finanziario, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali.
99 L'identificazione dei fornitori di servizi digitali opera invece automaticamente, secondo la tripartizione definita dall'allegato III: servizi di mercato online; motori di ricerca; servizi di cloud computing.
100 Il capo IV (artt. 14 e 15) della direttiva NIS è dedicato alle misure di sicurezza degli operatori di servizi essenziali, mentre il capo V (artt. 16, 17 e 18) riguarda i fornitori di servizi digitali.
101 I considerando 57 e 60 della direttiva NIS chiariscono il cd. "light-touch" a favore dei prestatori di servizi digitali in quanto, secondo il legislatore europeo, la natura transnazionale di questi e, di converso, il collegamento diretto con le infrastrutture fisiche degli operatori di servizi essenziali sarebbero argomenti idonei a giustificare un'imposizione di requisiti più rigorosi di quelli previsti dalla presente direttiva in capo agli operatori. Infatti, l'articolo 17 comma 1 statuisce che gli Stati membri, se necessario, adottino misure di vigilanza *ex post*, semplificate e reattive, quando ottengono la prova che un fornitore di servizi digitali non rispetta gli obblighi di notifica e in materia di sicurezza di cui all'articolo 16.
102 B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali, op.cit.*, p. 14.
103 COMMISSIONE EUROPEA, *Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)* COM(2020) 823 final.

la cooperazione a livello dell'Unione, istituendo vari forum volti a facilitare lo scambio di informazioni strategiche e operative. Dall'altra, la valutazione del funzionamento della direttiva ha evidenziato diversi e significativi problemi.

In primo luogo, l'ambito di applicazione della NIS è troppo limitato. Il maggior grado di interconnessione (si pensi all'aumento di dispositivi IoT) e di digitalizzazione determina l'esclusione di settori strategici e attori che forniscono servizi chiave per la società. Inoltre, l'ambiguità circa l'ambito di applicazione ha dato luogo ad una frammentazione del mercato interno: alcuni tipi di operatori di servizi essenziali non sono stati identificati in tutti gli Stati membri, non vi è chiarezza circa le competenze nazionali sui fornitori di servizi digitali, vi sono significative discrepanze circa i requisiti di sicurezza e di segnalazione degli incidenti per gli operatori di servizi essenziali, derivanti – probabilmente – dal diverso grado di preparazione degli Stati membri in materia di cybersecurity[104]. Una ulteriore causa di indeterminatezza è data dalla potenziale sovrapposizione di obblighi di notifica ai sensi della direttiva NIS con altri doveri di segnalazione di violazioni in materia di cybersecurity ai sensi di altre leggi dell'UE, ad esempio il GDPR[105].

In terzo luogo, il regime di supervisione e di applicazione della direttiva è stato valutato inefficace, dal momento che gli Stati membri sono stati molto riluttanti nell'applicazione delle sanzioni[106]. Infine, nonostante la direttiva riconosca al rilievo della cooperazione strategica e dello scambio di informazioni l'intero capo III, la Commissione riconosce il fallimento dell'obiettivo di condivisione sistematica ad ogni livello: tra gli Stati membri, tra soggetti privati, e tra soggetti pubblici e privati[107].

In questo contesto, vediamo ora se e come la *redistribuzione delle responsabilità,* la *cooperazione pubblico-privato* e lo *scambio di informazioni,* gli elementi cardine per una dottrina della cybersecurity come bene pubblico, vengano modellati dal legislatore europeo nella proposta per la revisione della direttiva NIS.

Preliminarmente, per quanto concerne l'ambito di applicazione della direttiva NIS 2, la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali verrebbe sostituita, all'articolo 2, da una classificazione dei soggetti, pubblici e privati, tra essenziali (allegato I) e importanti (allegato II). L'ampliamento del perimetro di protezione è ravvisabile anche nella deroga, ex articolo 2 comma 2, alla esclusione di micro e piccole imprese, qualora integrino certi requisiti.

Il capo II, "quadri normativi *coordinati* in materia di cibersicurezza" (enfasi aggiunta), rivela già dalla parola chiave "coordinati" un cambio di passo rispetto alla NIS attualmente in vigore. Se infatti la maggior parte

[104] R. H. WEBER e E. STUDER, *Cybersecurity and the Internet of Things: Legal Aspects,* in *Computer Law & Security Review*, n. 36, 2016, p. 726.
[105] M. D. COLE e S. SCHMITZ-BERNDT, *The Interplay between the NIS Directive and the GDPR in a Cybersecurity threat landscape,* in *University of Luxembourg Law Working Paper*, 2019, p. 20; cfr. S. SCHMITZ-BERNDT e S. SCHIFFNER, *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR,* in *International Review of Law, Computers & Technology,* 2021.
[106] COMMISSIONE EUROPEA, Proposta di direttiva NIS 2, p. 6.
[107] *Ibid.*

degli articoli del presente capo risulta arricchita di obiettivi e misure strategiche e normative rispetto alla versione precedente[108], è l'articolo 6 che introduce la prima grande novità, disegnando una cornice normativa per la divulgazione delle vulnerabilità. Ogni Stato membro dovrà designare un CSIRT come coordinatore ai fini della divulgazione coordinata delle vulnerabilità: il CSIRT agirà da intermediario di fiducia agevolando, se necessario, l'interazione tra il soggetto che effettua la segnalazione e il fabbricante o fornitore di servizi o prodotti ICT[109]. Spetta invece all'ENISA istituire e aggiornare un "registro europeo delle vulnerabilità", contenente informazioni che illustrino la vulnerabilità, i prodotti o i servizi ICT interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata, la disponibilità di relative *patch* e, qualora queste non fossero disponibili, orientamenti rivolti agli utenti dei prodotti e dei servizi vulnerabili sulle possibili modalità di attenuazione dei rischi[110]. Osserviamo, dunque, come l'intenzione del legislatore europeo sia quella di favorire un approccio sempre più stretto di cooperazione tra i soggetti privati e pubblici, in ragione dei rischi e delle vulnerabilità aventi un impatto sulla società intera.

Il capo III è dedicato, come nella attuale NIS, alla "cooperazione", in merito alla quale – nella valutazione dell'impatto della direttiva – la Commissione ha riconosciuto un fallimento di sistema. Mentre gli articoli 12 (gruppo di cooperazione)[111] e 13 (rete di CSIRT)[112] sono simili nella loro essenza ai predecessori, un primo rilievo quantitativo evidenzia i tre articoli aggiunti dal progetto di revisione: l'articolo 14, sulla "rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)"; l'articolo 15 sulla "relazione sullo stato della cibersicurezza nell'Unione"; e, l'articolo 16, "revisioni tra pari". Sotto il segretariato assicurato dall'ENISA, la rete CyCLONe è pensata per garantire una gestione coordinata a livello operativo delle crisi di cybersecurity su vasta scala e di garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE[113]. Oltre a tali poteri *ex post*, EU-CyCLONe avrà il compito di aumentare il livello di preparazione per la gestione di crisi e incidenti su vasta scala e di sviluppare una consapevolezza [114]. In questo quadro di ampliamento dei poteri dei soggetti già esistenti (gruppo di cooperazione e rete di CSIRT) e, dall'altra, di ulteriore creazione di una rete di

[108] Particolarmente rilevante è l'articolo 5 della Proposta di direttiva NIS 2, per il quale ogni Stato membro dovrà adottare una strategia nazionale per la cybersecurity con obiettivi e adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di sicurezza.
[109] Art. 6, Proposta di direttiva NIS 2.
[110] Art. 6 comma 2, Proposta di direttiva NIS 2.
[111] Una novità è data dal comma quinto, per cui il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati.
[112] L'articolo 13, comma 3, lettera b, include esplicitamente tra i compiti della rete di CSIRT lo scambio di informazioni "pertinenti sugli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità", uscendo dall'ambiguità e dalla natura volontaria della lettera dell'articolo 12 ora vigente.
[113] Art. 14, commi 1 e 2, Proposta di direttiva NIS 2.
[114] Art. 14, comma 3, lettere a e b, Proposta di direttiva NIS 2.

condivisione (EU-CyCLONe), sarà cruciale definire sostanzialmente e proceduralmente le rispettive competenze, assicurando al tempo stesso fecondo dialogo tra i vari attori[115].

Il capo IV, concernente gli obblighi in materia di gestione e segnalazione dei rischi di cybersecurity, riscrive i capi IV e V della direttiva attualmente in vigore. Innanzitutto, è bene evidenziare come la NIS 2 voglia enucleare dei requisiti di base in materia di misure tecniche e organizzative di gestione del rischio – come analisi dei rischi e politiche di sicurezza dei sistemi informatici, gestione degli incidenti, continuità operativa e gestione delle crisi, sicurezza della supply chain e uso della crittografia e cifratura – lasciando quindi meno discrezionalità agli Stati membri[116]. Per quanto attiene alla dimensione olistica della gestione del rischio, nella sua accezione di estendere lo standard di protezione a tutti gli attori rilevanti in una prospettiva coordinata, la proposta della direttiva NIS 2 crea nuovi obblighi per i soggetti rientranti nell'ambito di applicazione in relazione a tutti i fornitori della *supply chain*. I soggetti NIS dovranno tener conto, da una parte, delle vulnerabilità specifiche e, dall'altra della qualità complessiva dei prodotti e delle pratiche di cybersecurity per ogni fornitore di prodotti e servizi, comprese le loro procedure di sviluppo sicuro[117]. Inoltre, il gruppo di cooperazione, in concerto con la Commissione ed ENISA, ha il potere di "effettuare valutazioni coordinate dei rischi per la sicurezza" di specifiche e critiche *supply chain* di servizi, sistemi o prodotti ICT[118]. Infine, per quanto concerne i novellati obblighi di segnalazione, molto più dettagliati da un punto di vista procedurale, una novità sostanziale è data dall'obbligo di notifica, da parte dei soggetti NIS, di "qualunque minaccia informatica significativa che secondo tali soggetti avrebbe potuto causare un incidente significativo"[119].

Infine, il capo V, intitolato "condivisione delle informazioni", novità assoluta della proposta legislativa, integra perfettamente uno degli elementi cardine della dottrina per la cybersecurity come bene pubblico. Gli Stati membri dovranno provvedere affinché i soggetti NIS possano scambiarsi informazioni relative a minacce informatiche, vulnerabilità, indicatori di compromissione, tattiche, tecniche e procedure, allarmi e strumenti di configurazione[120]. È interessante notare come il legislatore inserisca due condizioni alla condivisione di informazioni: queste devono prevenire, rilevare o attenuare gli incidenti o a rispondervi; e, aumentare il livello di cybersecurity, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento delle minacce,

[115] All'articolo 14, i commi 5 e 6 fondano la base giuridica per il dovere di cooperazione dell'EU-CyCLONe rispettivamente con il gruppo di cooperazione e la rete di CSIRT.
[116] Art. 18, comma 2, Proposta di direttiva NIS 2.
[117] Art. 18, comma 3, Proposta di direttiva NIS 2.
[118] Art. 19, comma 1, Proposta di direttiva NIS 2.
[119] Art. 20, comma 2, Proposta di direttiva NIS 2.
[120] Art. 26, comma 1, Proposta di direttiva NIS 2.

strategie di attenuazione o fasi di risposta e recupero[121]. Queste previsioni normative saranno essenziali per il settore privato per garantire la robustezza del sistema e imparare dai pari[122]. Inoltre, nell'ottica della cybersecurity come interesse comune, viene fatta salva la possibilità per i soggetti che non rientrino nell'ambito di applicazione della direttiva di poter trasmettere, su base volontaria, notifiche di incidenti significativi, minacce informatiche o quasi incidenti[123]. Al fine di tutelare gli interessi privati e di incentivare tali pratiche, altrimenti scoraggiate – come osservato nella seconda sezione del presente articolo, lo scambio di informazioni dovrà avvenire "nell'ambito di comunità fidate di soggetti essenziali e importanti. Tale scambio è attuato mediante accordi di condivisione delle informazioni che tengono conto della natura potenzialmente sensibile delle informazioni condivise"[124].

5. Conclusione

La sicurezza nel ciberspazio è rilevante non solo come valore in sé, ma nell'ottica del bene comune della sicurezza nazionale, della protezione delle infrastrutture critiche, dello sviluppo del mercato digitale e della tutela del sistema di diritti e libertà fondamentali. Perché si realizzi un tale livello di protezione, a fronte di sfide che sono globalizzate e minacce sempre più transnazionali, l'Unione promuove, come si è illustrato nel corso dell'articolo, un approccio strategico di tipo globale, fondato sulla cooperazione internazionale e sulla condivisione di informazioni a tutti livelli, redistribuendo responsabilità tra settore pubblico e privato. Soprattutto questi aspetti richiamano e fondano le basi per una riflessione europea sulla dottrina della cybersecurity come bene pubblico, nella sua dimensione della robustezza.

Nelle società che dipendono dall'infrastruttura digitale per funzionare, la solidità dei sistemi è un requisito essenziale e richiede una progettazione accurata, verifiche del codice, collaudi e test continui per le vulnerabilità. La robustezza dei sistemi gestita nell'interesse pubblico, in un quadro d'insieme caratterizzato dalla centralità dei diritti fondamentali, può avere effetti diretti e effetti indiretti sullo sviluppo della società: dal funzionamento delle infrastrutture critiche alla protezione delle attività che i cittadini conducono online.

Una cooperazione, che superi quindi il paradigma della collaborazione, tra il settore pubblico e quello privato è auspicabile per la creazione di un clima di fiducia reciproca che favorisca, nel pubblico interesse, il requisito della solidità dei sistemi. La cybersecurity è una responsabilità condivisa. È compito del settore pubblico stabilire norme, procedure di certificazione, collaudo e verifica in grado di garantire un livello sufficiente di sicurezza, dall'altra parte, il settore privato è responsabile della progettazione di sistemi

[121] Art. 26, comma 1, lettere a e b, Proposta di direttiva NIS 2
[122] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 352.
[123] Art. 27, comma 1, Proposta di direttiva NIS 2.
[124] Art. 26, comma 2, Proposta di direttiva NIS 2.

robusti e dello sviluppo e del miglioramento di nuovi metodi di sicurezza[125]. Ai cittadini dovrà invece essere attribuita la responsabilità di adottare comportamenti consapevoli. Si rende necessaria, dunque, per tutte le organizzazioni, l'adozione di paradigmi "di comunità" o "olistici" per la cybersecurity, come sottolineato recentemente in una conferenza dal professor Baldoni[126] – già vice-direttore del Dipartimento delle Informazioni per la Sicurezza (Dis) con delega alla cybersecurity e fresco di nomina di direttore per la nascente Agenzia italiana per la cybersicurezza nazionale – che promuovano la consapevolezza dei requisiti di conformità cui fare riferimento in ambito di prodotti, processi e sicurezza, al fine di garantire idonei livelli di gestione del rischio in un contesto sempre più variegato e complesso.

Proprio nell'ottica di migliorare la robustezza, e quindi il livello globale di cybersecurity, dei dispositivi connessi contro gli attacchi informatici, l'approccio normativo adottato dalla Commissione, e incoraggiato dal Consiglio dell'Unione Europea[127], è incentrato sull'inclusione di requisiti minimi di cybersecurity nelle direttive e nei regolamenti del cd. "New Legislative Framework" (NLF) del 2008[128], attraverso l'adozione di atti delegati della Commissione. Il primo strumento all'esame di Bruxelles è la Direttiva 2014/53/UE sulle apparecchiature radio e indossabili[129].

Al centro dell'approccio europeo vi è l'analisi preventiva dei rischi, la notifica degli incidenti da parte degli operatori pubblici e privati, la verifica dei livelli di sicurezza dei prodotti attraverso sistemi di certificazioni e standard. In particolare, al fine di dimostrare il rispetto delle misure di gestione del rischio cyber, gli Stati membri potranno richiedere ai soggetti essenziali e importanti di certificare determinati prodotti, servizi e processi ICT nell'ambito di specifici sistemi europei di certificazione di cybersecurity adottati a norma dell'articolo 49 del regolamento (UE) 2019/881[130]. Inoltre, con il medesimo obiettivo di *compliance* con gli obblighi della direttiva NIS, l'adozione di standard tecnici europei o internazionali verrà incoraggiata, senza imporre o discriminare a favore dell'uso di un particolare tipo di tecnologia[131].

[125] M. TADDEO, *Is Cybersecurity a Public Good?*, *op. cit.*, p. 351. Così anche Laura Carpini, Capo Unità per le politiche e la sicurezza dello spazio cibernetico presso presso il Ministero degli Affari Esteri e Cooperazione Internazionale (MAECI), nella conferenza *Cyber - The New Frontier of Security. The EU Approach,* SIOI, Ambasciata di Romania in Italia e Formiche.net, 23/06/2021.

[126] *Cyber - The New Frontier of Security. The EU Approach,* SIOI, Ambasciata di Romania in Italia e Formiche.net, 23/6/2021.

[127] CONSIGLIO DELL'UNIONE EUROPEA, *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, *op. cit.*, p. 4.

[128] Il Nuovo Quadro Legislativo è stato adottato nel 2008 per migliorare il mercato interno delle merci e rafforzare le condizioni per l'immissione di una vasta gamma di prodotti nel mercato UE. Si tratta di un pacchetto di misure atte a migliorare la sorveglianza del mercato e ad aumentare la qualità delle valutazioni di conformità (es., marchio CE).

[129] Direttiva 2014/53/UE del Parlamento Europeo e del Consiglio 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.

[130] Art. 21, Proposta di direttiva NIS 2.

[131] Art. 22, Proposta di direttiva NIS 2.

In questo contesto, l'Italia vuol essere esempio virtuoso nella comunità europea. I tre DPCM di attuazione del Perimetro Nazionale di Sicurezza Cibernetica[132] e la costituzione dell'Agenzia per la cybersicurezza nazionale (Acn) testimoniano, da una parte, l'esigenza di "tutela rafforzata avvertita in relazione ad ambiti ritenuti maggiormente sensibili ed afferenti alla sicurezza degli apparati dello Stato non "coperti" dalla direttiva NIS in tutte le componenti essenziali"[133] e, dall'altra, la volontà dell'esecutivo e del Parlamento di dotare la nazione di una Autorità nazionale avente personalità giuridica di diritto pubblico volta a ricomprendere il *Computer security incident response team* italiano (CSIRT) e il Centro di valutazione e certificazione nazionale (CVCN)[134].

In conclusione, l'impianto teorico proposto da questo contributo, facente perno sulla natura di bene pubblico della dimensione della robustezza dei sistemi della cybersecurity, trova conferme nell'approccio delineato dalle proposte del legislatore europeo. Incidenti informatici che, mossi da ragioni economiche, nei primi sei mesi del 2021 hanno colpito infrastrutture civili di molti Paesi occidentali[135], tra cui nel nostro paese l'attacco *ransomware* ai sistemi informativi della Regione Lazio - infrastruttura critica che rientra nel perimetro della Direttiva NIS, rendono evidente quanto la sicurezza delle tecniche utilizzate sia il fianco scoperto di tutti i processi di informatizzazione e ponga sfide specifiche che debbono essere affrontate globalmente, al servizio degli interessi generali ma utili per ciascun cittadino. Una strada non semplice, non breve, che ridisegnerà gli equilibri nei rapporti economici tra gli attori di mercato pubblici e privati ma che riteniamo essere l'unica via per creare sistemi e infrastrutture robuste al fine di garantire a milioni di cittadini la non chimerica promessa di abitare società sicure.

6. Riconoscimenti

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" grant agreement No 814177.

Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambi gli Autori. Tuttavia, nel dettaglio, ai fini della stesura del contributo, Raffaella Brighi è autrice dei §§ 1 e 5, mentre Pier Giorgio Chiara è autore dei §§ 2, 3 e 4.

[132] Decreto legge n.105 del 2019, poi convertito in legge (legge 8 del 28 febbraio 2020): "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica".

[133] B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali, op.cit.*, p. 20.

[134] G. CARRER, *Con il sì del Senato, l'Agenzia cyber in rampa di lancio,* in *Formiche.net,* 03/08/2021.

[135] Uno dei maggiori distributori di benzina in Nordamerica, agenzie governative Usa, uno dei maggiori produttori mondiali di carne e, a fine maggio, il blitz hacker contro l'Health Service Executive ovvero l'intero sistema sanitario dell'Irlanda.