Forum di QUADERNI COSTITUZIONALI
RASSEGNA
ISSN 2281-2113

# L'ordine costituzionale della *cybersecurity*

ANDREA VENANZONI*

**Abstract:** *The essay analyses how the regulatory and conceptual evolution of cybersecurity is affecting the structure of public powers, changing the very form of government. The efficient protection of the digital domain cannot in fact weaken the respect of rights and freedoms; for this very reason, the ways of guaranteeing citizens are becoming increasingly complex and articulated, between the protection of personal data, the respect of national sovereignty, and the guarantee of freedom in the face of the expansive power of large private entities. The 'catalytic' State represents the reticular evolution of this new arrangement.*

**Parole chiave**: *cybersecurity*, Stato, Diritto costituzionale, cyberspazio, sicurezza

**Sommario**



**Data della pubblicazione sul sito**: 26 novembre 2024

**Suggerimento di citazione**

A. VENANZONI, *L'ordine costituzionale della* cybersecurity, in *Forum di Quaderni Costituzionali*, 4, 2024. Disponibile in: www.forumcostituzionale.it

---

* Assegnista di ricerca in Diritto costituzionale e pubblico nel Dipartimento di Giurisprudenza dell'Università degli Studi "Roma Tre". Email: andrea.venanzoni@uniroma3.it.

## 1. Il dominio digitale e la centralità della *cybersecurity:* una introduzione

La digitalizzazione, processo sempre più esteso e capillare, ha prodotto un significativo impatto non soltanto sulle dinamiche di organizzazione degli apparati pubblici e del mondo aziendale ma più in generale sugli elementi costitutivi stessi dei diritti, delle libertà e della loro garanzia[1].

In questo senso, la sicurezza digitale, nelle sue multiformi sfumature, assume funzioni e significati del tutto nuovi rispetto quelli rivestiti fino a pochi anni fa.

Un mondo globale, interconnesso dalle reti digitali, in cui Stati e imprese erogano servizi o implementano e tutelano diritti attraverso strumenti digitali è un mondo che finisce, inevitabilmente, per esporsi a crescenti rischi.

La virale espansione degli strumenti digitali e la diretta incidenza di questi su assetti ordinamentali e su diritti di matrice costituzionale stanno imponendo da tempo ormai anche alla dottrina costituzionalistica una organica riflessione su come e quanto la sicurezza digitale non sia più solo disciplina tecnico-informatica o, al limite, di azione e organizzazione amministrative, nel generale quadro della tecnificazione[2] dei pubblici poteri[3].

Come si diceva infatti, l'espansione della digitalizzazione dello Stato e delle imprese aumenta il campo dei potenziali attacchi cibernetici, ma soprattutto incide in maniera sempre più radicale sui diritti e pone, pertanto, sfide nuove che attengono al nucleo funzionale stesso del costituzionalismo.

Ogni strumento di difesa, simmetricamente, può divenire anche elemento di offesa e di attacco, e a ogni aumento dei perimetri sensibili, in termini infrastrutturali o di dati, aumenta la potenziale vulnerabilità, nel quadro di una necessitata ridefinizione dei codici, giuridici, tecnici e funzionali, della sicurezza digitale, embricata tra dimensione privata e pubblica[4].

---

[1] L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica e Società*, n. 1, p. 62.

[2] La sussunzione di sempre più raffinati e pervasivi strumenti digitali nelle maglie della sfera pubblica ha posto la delicata questione della eventuale modificazione genetica della pubblica amministrazione, della sua organizzazione, della sua azione e del suo modo di relazionarsi con i cittadini, ponendo lo studioso davanti la oggettivamente enorme questione di individuare anche strumenti di adattamento funzionale degli istituti di garanzia, S. CIVITARESE MATTEUCCI, L. TORCHIA, *La tecnificazione dell'amministrazione*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione*, Firenze University Press, Firenze, 2016, specialmente pp. 9 e ss.

[3] R. URSI, *La sicurezza cibernetica come funzione pubblica*, in R. URSI (a cura di), *La sicurezza nel cyberspazio,* FrancoAngeli, Milano, 2023, p. 9.

[4] S. PIETROPAOLI, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Rivista di filosofia del diritto*, 2, 2019, p. 382

Ma all'aumento qualitativo e quantitativo delle libertà e dei diritti che vengono estrinsecati anche attraverso l'utilizzo di strumenti digitali, aumenta del pari la forza distruttiva e dirompente tanto dei poteri privati, su cui sempre più spesso i cittadini e la stessa sfera pubblica devono fare affidamento, quanto dei potenziali attacchi, i quali finiscono per assumere la preoccupante fisionomia della guerra digitale e per colpire non più solo la funzionalità tecnica di un dato apparato ma i diritti e la libertà stessa dei cittadini.

In questa prospettiva, lo Stato, mediante collaborazioni organiche e reticolari con altri soggetti statali e con i privati, appare quasi rimodellarsi, al fine di poter fare fronte a sfide di enorme complessità.

Prospettiva questa che coinvolge il costituzionalismo, appunto.

Non c'è alcun dubbio poi che la *cybersecurity,* soprattutto quando riguardata nella angolazione prospettica statuale, in questi ultimi anni stia andando incontro a un radicale processo di convergenza con la fisionomia della *cyberwarfare* e stia presentando sempre più evidente embricazione con la dimensione della sicurezza nazionale.

Pur formalmente tra loro distinti i due articolati *framework* normativi, quello di *cybersecurity* e quello di sicurezza nazionale digitale, convergono infatti verso la medesima funzione di garanzia dell'ordine costituzionale.

Già nel 2001 il *Quadriennial Defense Review Report* statunitense avvertiva che alla luce degli enormi progressi compiuti negli ultimi anni nel campo della tecnologia informatica e satellitare, e soprattutto in riferimento alla continua evoluzione verso la creazione di un sistema congiunto di forze armate "netcentriche", il dominio cibernetico diventava un potenziale "moltiplicatore" delle minacce per la sicurezza e gli interessi, nel caso analizzato dal *report*, americani[5].

Ma la considerazione è valida per qualunque Stato profondamente digitalizzato.

Proprio questa consapevolezza ha portato a un mutamento significativo del presidio del dominio cibernetico e alla evoluzione della stessa *cybersecurity*[6], da

---

sottolinea un aspetto molto rilevante: il riconoscimento di un linguaggio comune di limitazione della violenza operava storicamente solo tra gli Stati europei, mentre 'oltre', negli spazi privi di sovranità, quella violenza tendeva a espandersi nel modulo brutale della guerra senza regole.

[5] S. PIETROPAOLI, *Un altro modo di fare la guerra. La cyberwar come problema giuridico*, in *Ars Interpretandi*, 1, 2023, p. 63, rileva acutamente come la guerra cibernetica sia guerra reale, solo combattuta con mezzi diversi e su un 'terreno' diverso.

[6] Non solo in Europa, ma anche negli USA. M. SANTANIELLO, *Sunburst. La grande eclissi della cybersecurity Usa*, in *Rivista di Digital Politics*, 1, 2021, p. 182.

mera sicurezza informatica a dispositivo complesso di garanzia dell'ordine costituzionale[7], mediante la riaffermazione ordinamentale della sicurezza digitale, intesa questa nel senso e nei termini che vedremo.

L'Italia è, in assoluto, uno dei Paesi più esposti a livello mondiale agli attacchi informatici, in un quadro di grave peggioramento della insicurezza cibernetica.

Quantitativamente parlando, solo negli ultimi 5 anni la situazione globale ha fatto registrare un andamento incrementale degli assalti *hacker*, dietro i quali sovente si nascondono attori statali ostili, delineando una tendenza pressoché costante e con una impressionante media mensile di attacchi *gravi* passata da 139 a 232[8].

Per attacco grave si intende un attacco capace di alterare significativamente o addirittura irrimediabilmente la funzionalità di infrastrutture delicate e critiche, tanto di ordine statale quanto di attori privati che però erogano servizi e beni di palese importanza per la collettività.

Confrontando i dati del 2019 con quelli del 2023, l'aumento degli attacchi rilevati ricorrendo alla analisi di fonti pubbliche è stato del 60%, con un passaggio da 1.667 a 2.779.

---

Il 13 dicembre 2020, la società *FireEye* comunica la scoperta di una gravissima falla sul sistema Orion a SolarWind e al *Computer emergency readiness team* (Cert) della *Cybersecurity and infrastructure security agency* (Cisa), un'agenzia federale istituita dal Presidente Trump nel 2018 sotto la supervisione del Dipartimento della sicurezza interna degli Stati Uniti d'America (Dhs).

Lo stesso giorno la Cisa emette una direttiva d'emergenza che ordina a tutte le agenzie federali civili di disconnettere Orion dalle proprie reti a causa di un attacco da parte di non meglio specificati *malicious actors*.

Del virus Sunburst si era avveduta una azienda privata, non una agenzia pubblica.

[7] M. MATASSA, *La regolazione della cybersecurity* in Italia, in R. URSI (a cura di), *La sicurezza nel cyberspazio*, FrancoAngeli, Milano, 2023, p. 21, nota come la sicurezza cibernetica sia prerequisito essenziale per garantire l'ordinata convivenza e la sopravvivenza di qualunque organizzazione articolata.

In questo senso, per la sicurezza digitale valgono le medesime considerazioni che la dottrina costituzionalistica ha svolto, e su cui torneremo in seguito, sulla sicurezza come valore super-primario.

[8] Tutti i dati sono tratti dal '*Rapporto 2024 sulla sicurezza ICT in Italia*' di Clusit – Associazione Italiana per la Sicurezza Informatica e sono stati elaborati da dati pubblici, riferibili alle rilevazioni condotte dalla Polizia postale e delle comunicazioni e dal *SOC* di Fastweb.

Il rapporto può essere liberamente consultato, previo *download*, dal seguente link https://clusit.it/rapporto-clusit/.

Nel 2023 gli attacchi sono aumentati dell'11% a livello globale, ma in Italia sono aumentati del 65%.

Che il 2023 sia stato un anno critico per la sicurezza digitale è testimoniato in maniera cristallina dalla *Relazione annuale al Parlamento relativa all'anno 2023*, predisposta dall'Agenzia per la cybersicurezza nazionale (ACN).

La *Relazione* si sofferma anche sul peso dele recenti vicende belliche, tanto nel settore est-europeo quanto in quello mediorientale, precedute e accompagnate spesso da atti ostili digitali, quali furto di dati o immissioni di *malware* finalizzati al blocco o al danneggiamento di infrastrutture critiche[9].

In un quadro del genere, la funzione delle autorità preposte al governo della sicurezza digitale e del digitale *tout court*, dalla citata ACN al Garante per la protezione dei dati personali (GPDP), senza obliare la centralità della Presidenza del Consiglio, aumenta esponenzialmente di valore e di difficoltà, involgendo ormai la tenuta complessiva del Paese, dei diritti e delle libertà dei cittadini.

La sfida, multidimensionale e multidisciplinare, per sua stessa natura si presenta quale globale e liquida, e non può veder impegnati solo i singoli Stati. Come è stato giustamente rilevato[10], la sicurezza digitale vede quali necessari protagonisti gli organismi sovra-nazionali, con una rinnovata spinta dell'Unione Europea: una spinta che si traduce nella necessità di una sempre più marcata integrazione tra Stati membri e di una riconsiderazione dei formanti stessi della sovranità e del concetto di sicurezza.

In tutto questo, il ruolo dei soggetti privati nel generale quadro della sicurezza digitale muta profondamente e la loro presenza tra le maglie dei dispositivi di sicurezza digitale nazionale e internazionale si rende più massiva e rilevante anche in chiave sostanziale.

Il presente saggio si propone quindi di analizzare le implicazioni costituzionalistiche di questo mutamento del paradigma e delle funzioni della

---

[9] La *Relazione*, elaborando i numeri forniti da CSIRT Italia, rileva come gli eventi gestiti nel 2023 da ACN siano stati 1.411, 3.302 i soggetti *target*, mentre nel 2022 erano stati 1.150, 303 gli incidenti con impatto confermato.

In tema di allertamento, le comunicazioni che ACN ha fatto pervenire ai vari attori sono state 20.825, 447 tra *alert* e bollettini apparsi sul portale pubblico, 72 quelli pubblicati sul portale di *collaboration*, 468 le stime di impatto di nuove vulnerabilità e oltre 180.000 gli indicatori di compromissione condivisi.

[10] F. PIZZETTI, *Introduzione alla regolazione europea della società digitale*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 4, sottolinea come e quanto il *framework* normativo sempre più esteso patrocinato dalla UE stia producendo una espansione globale degli interventi della stessa UE, in maniera non dissimile da quanto già sperimentato con il *GDPR*.

*cybersecurity*, soffermandosi anche su questioni di ordine teorico-generale, in un momento storico in cui l'Italia è peraltro chiamata a una notevolissima sfida di concreta implementazione della Direttiva NIS 2, al raggiungimento degli obiettivi PNRR, la cui sostanza digitale è autoevidente, e a raccordare armonicamente la disciplina di sicurezza nazionale cibernetica con quella *cybersecurity*.

## 2. La sovranità digitale e la *cybersecurity*

L'ascesa del lemma 'sovranità digitale' negli ultimi anni ha imposto all'attenzione degli studiosi la intrinseca problematicità[11] di una formula polisemica e strutturalmente ombrosa[12].

Se già il termine sovranità, emendato di ulteriori caratterizzazioni, nella scienza giuridica indica un campo concettuale assai esteso e dalla storia complessa[13], l'aggettivo ulteriore connesso alla digitalizzazione espande l'obliquità definitoria[14].

Si è correttamente sottolineato come nella pluralità potenziale dei significati, spesso la sovranità digitale tenda a confondersi con il concetto di potere digitale[15];

---

[11] P. PASSAGLIA, *Sovranità*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Giuffrè, Milano, 2006, p. 5643, nota come la sovranità sia nozione tra le più controverse e come essa rappresenti uno degli elementi costitutivi dello Stato, designando la somma delle potestà pubbliche che si esercita su un territorio definito e sul corpo sociale che in esso è stanziato.

[12] A. MATTIONI, *Sovranità*, in Digesto delle discipline pubblicistiche, Wolters Kluwer, Milano, 2012, p. 659.

[13] M.S. GIANNINI, *Sovranità (dir. vig.),* in *Enciclopedia del diritto*, XLIII, Giuffrè, Milano, 1990, p. 225, illustra come Jean Bodin abbia raggiunto lo sviluppo teorico-concettuale di un ampio percorso che aveva preso avvio già nel pensiero di canonisti e dottori della scienza feudale, senza che però questi avessero usato la parola sovranità. Ed è con Vestfalia che la sovranità ottiene il proprio riconoscimento e l'apertura di un orizzonte suo proprio.

La nozione ha una sua scaturigine funzionale assai precisa e evidente, quella di emancipare e liberare il sovrano dal vincolo della supremazia imperiale.

[14] Sia consentito il rinvio ad A. VENANZONI, *La sovranità tra ordine costituzionale, digitale e poteri privati*, in A. VENANZONI, M. PROIETTI, *La sovranità digitale tra sicurezza nazionale e ordine costituzionale*, Pacini giuridica, Pisa, 2023, specialmente pp. 43 e ss.

[15] G. FINOCCHIARO, *La sovranità digitale*, in *Diritto pubblico*, 3, 2022, p. 811 per una ampia ricostruzione problematica del lemma.

Sulla forza modificativa del potere da parte del digitale, e delle grandi piattaforme, ampiamente, L. DI MAJO, F. PARUZZO, *Nuovi aspetti del potere nel Metaverso*, in M. CALAMO SPECCHIA (a cura di), *Processi politici e nuove tecnologie*, Giappichelli, Torino, 2024, pp. 200 e ss.

questo perché, al netto di una serie di estrinseche similitudini, mentre il potere può agitarsi nello spazio dei fatti e dei comportamenti e degli effetti, la sovranità abbisogna di connotazioni ulteriori, come ad esempio la legittimità connessa al suo riconoscimento. Sovranità digitale potrebbe però tanto delineare la riaffermazione

ordinamentale dello Stato nel ventre del digitale[16], a fronte di mutamenti[17] quasi genetici della società e delle forme statali sotto la spinta accelerata dei formanti

---

[16] O. POLLICINO, *Potere digitale*, in *Enciclopedia del diritto*, Giuffrè, Milano, 2023, p. 411, il quale si sofferma sulla sovranità digitale come riaffermazione del potere pubblico su dati, *software*, servizi, infrastrutture nell'ecosistema digitale. In questo prisma, territorio e spazio tendono a rendersi evanescenti e interconnessi. E proprio per questo, ai fini di un pieno recupero della sovranità, si scandagliano e analizzano antecedenti storici, dal medioevo alla Frontiera americana, passando per la evoluzione della legge del mare, sempre più presente negli studi giuridici sul digitale e di quelli sulla *cyberwarfare* e sulla corsa allo spazio.

Si può pensare alla centralità assegnata da Carl Schmitt al pensiero di Francisco de Vitoria, quando nella apertura delle grandi rotte coloniali oceaniche si pose la enorme questione giuridica dei titoli di legittimazione di apprensione degli spazi privi, in apparenza, di sovranità e di regolazione dei conflitti in spazi che, appunto, apparivano vuoti di qualunque connessione con il riconoscimento statale. C. SCHMITT, *Il nomos della terra*, Adelphi, Milano, 1991, p. 105, infatti, discutendo dell'opera di Francisco de Vitoria, il trattato *Relectiones de Indis et de jure belli* del 1539, rileva come per concetti espressi e nitore formale, pur saldamente legata a una concettuologia di pensiero della Scolastica, essa si atteggi come vero spartiacque teorico tra pensiero medievale e pensiero post-medievale. D'altronde, Schmitt riconoscerà come nel mondo globalizzato lo spazio si renda campo di energia tale da permeare il mondo stesso, così C. SCHMITT, *Terra e mare*, Adelphi, Milano, 2002, p. 109.

Per un riadattamento alla società digitale della lettura di diritto internazionale contenuta nel *De Indis* di De Vitoria, J. THUMFART, *Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, Digital Communication as a Human Right, Just Cyber-Warfare*, in J.M. BENEYTO, J. CORTI VARELA (a cura di), *At the Origins of Modernity. Francisco de Vitoria and the Discovery of International Law*, Springer, New York, 2017, pp. 197 e ss., il quale si focalizza soprattutto sulla considerazione degli spazi privi di territorio come elementi comuni da preservare, patrocinando un diritto internazionale non dissimile dalla teologia bellica da cui sarebbe evoluto il pensiero alle radici del diritto internazionale, lungo quella direttrice che va da de Vitoria a Grozio.

In questo senso, la giustezza del conflitto acquisitivo diventa parametro di valutazione da adattare allo spazio digitale al fine di evitare la conquista in via di fatto. Già lo stesso Schmitt aveva rammentato la questione medievale della scoperta degli spazi come eventuale titolo giuridico di legittimazione per la appropriazione, C. SCHMITT, *Il nomos della terra*, cit., pp. 111 e ss.

Ed è così che sorge la necessità di definire, *ex ante* e mediante un approccio cyber-vestfaliano, un nucleo minimo di regole per evitare che la corsa alla appropriazione, dagli spazi digitali allo spazio celeste, possa divenire motivo di conflittualità violenta e del pari evitare che nel campo virtuale possano darsi azioni ostili eslegi capaci di colpire i civili e le infrastrutture essenziali di un dato Paese proprio in quanto manifestate nel mondo digitale e non in quello reale.

La legge del mare, come vedremo, ed elementi concettuali affini al pensiero di de Vitoria e di Grozio, punteggiano i documenti NATO in tema di *cyberwarfare*, a partire dal *Manuale di Tallinn*.

Proprio commentando la prima edizione del *Manuale di Tallinn*, che come noto risale al 2013, C. DEMCHAK, P. DOMBROWSKI, *Cyber Westphalia. Asserting State Prerogatives in Cyberspace*, in *Georgetown Journal of International Affairs*, 2014, p. 32, sottolineano come l'approccio di molti Stati tenda a voler riprodurre nello spazio digitale un elemento cyber-vestfaliano, ovvero la determinazione di riconoscimenti mutuali della propria sovranità su porzioni meta-territoriali dello spazio digitale.

Per fare questo però, essi devono governare non solo le emergenti conflittualità native nel e del cyberspazio ma devono anche tenere unito il proprio popolo, evitandone la dispersione e la frantumazione nei particolarismi tecnici, economici e scientifici della logica digitale.

Un aspetto questo che in piana evidenza concerne la dimensione dell'esercizio della sovranità in termini di rappresentanza politico-istituzionale, del circuito elettorale, della formazione dell'opinione pubblica, sovente minacciata da strumentale disinformazione e *fake news*, della garanzia dei diritti e delle libertà costituzionali, come quella di manifestazione del pensiero, sempre più attratta nella sfera delle grandi piattaforme digitali.

Due aspetti qui merita sottolineare: de Vitoria, tra i primi, aveva segnalato una nuova dimensione della forma stessa dei vincoli privatistici, elevati a paradigma del rispetto di diritti ulteriori rispetto quelli meramente proprietari, manifestazione, per dirla con Paolo Grossi, di un avere che si agganciava nel profondo, nella natura stessa del soggetto, elevandolo e realizzandolo nel suo essere e nel suo canone di libertà, così P. GROSSI, *La proprietà nel sistema privatistico della Seconda Scolastica*, in ID. (a cura di), *La Seconda Scolastica nella formazione del diritto privato moderno*, Giuffrè, Milano, 1973, p. 140.

Un aspetto adattabile, senza dubbio alcuno, a uno spazio come quello digitale in cui i vincoli contrattuali e proprietari e genericamente di matrice privatistica continuano ad assumere forte rilevanza, bel al di là del diritto privato, e in cui la spinta innovativa è modello di appropriazione creatrice, di cui si servono anche gli Stati.

Questa latente 'privatizzazione' di vincoli che non sono più solo contrattuali incide su diritti garantiti storicamente dalle Costituzioni e dai meccanismi di garanzia da queste predisposti, e si assiste a una esternalizzazione co-regolatoria e co-gestoria di libertà costituzionali tra grandi piattaforme digitali e Stati e organismi sovra-nazionali.

Sul versante della sicurezza informatica, i privati concorrono in maniera crescente alla strutturazione della difesa digitale degli apparati pubblici, sia mediante i processi di innovazione tecnologica sia attraverso la messa a disposizione degli *output* da loro prodotti o del loro *expertise* professionale.

Convenzioni, protocolli, contratti pubblici legano in maniera sempre più salda società private e amministrazioni pubbliche, quando queste ultime abbiano bisogno di strumenti, servizi o qualificazione che ritengono di non possedere.

In secondo luogo, de Vitoria, Grozio e gli altri, posero la questione, non meno spinosa e parimenti di grande attualità, di cosa avvenga nel caso di incontri di sovranità

asimmetriche o disomogenee, intendendosi per tali quelle sovranità problematicamente riconosciute, A. DEL VECCHIO, *La legge nell'Oceano. Ugo Grozio e le origini dello spazio politico moderno*, Il Mulino, Bologna, 2020, p. 179.

Se all'epoca del colonialismo e delle rotte nautiche ci si era interrogati lungamente sui rapporti da tenere con le popolazioni indigene e poi con le Compagnie commerciali, si pensi alla nota e secolare questione della Compagnia inglese delle Indie Orientali, e tra distinte nazioni europee che dovessero intrecciare i loro percorsi in spazi da colonizzare, nello spazio digitale la prospettiva è similare, sostituendo alle Compagnie i grandi poteri privati e gli spazi in apparenza privi o vuoti di sovranità con il cyberspazio.

Ciò rende del tutto evidente e necessitato un concetto ampio di sovranità digitale, mobile, ricombinante, come vedremo che contenga al tempo stesso il livello assiologico dei principi costituzionali, la dinamica democratico-rappresentativa e i suoi formanti, il pieno funzionamento dei servizi digitali, la sicurezza digitale e la *cybersecurity*.

Questo anche per affrontare un delicatissimo problema attinente all'orizzontalità del diritto internazionale e all'affermazione di sovranità singolo-nazionali, si pensi all'eccezionalismo statunitense, che dovrebbero nel campo digitale allinearsi lungo nuclei assiologici comuni. Sul tema del conflitto tra orizzontalità e sovranità, M. DIAN, *La Cina, gli Stati Uniti e il futuro dell'ordine internazionale*, Il Mulino, Bologna, 2021, specie pp. 97 e ss.

Naturalmente, l'eccezionalismo sovrano continua a essere un paradigma ben presente e rivendicato anche nel digitale, soprattutto partendo dal dato infrastrutturale delle reti le quali sono sempre riconducibili ad un dato Paese, anche in chiave oceanica di cavi sommersi. Proprio per questo, appare sempre più centrale, ai fini di espansione di una visione rispettosa dei diritti e delle libertà, il ruolo degli organismi internazionali e della UE.

Qui va infatti richiamata la riflessione in ambito euro-unitario, in cui si è posta e continua a porsi la necessità di perimetrare e definire i confini concreti, e la misura, di riconoscimento della sovranità intesa come riaffermazione ordinamentale e di applicazione concreta delle norme in snodi virtuali.

Si pensi al noto caso *Schrems*, dal quale emerge la necessità di delimitare i confini della sovranità dell'UE sulle reti di telecomunicazione, V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "Privacy shield"*, Roma Tre Press, Roma, 2016, p. 13.Si veda inoltre, C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello*, ESI, Napoli, 2018, specie pp. 21 e ss.

[17] Per una ampia disamina del modo in cui l'incistamento dell'alta tecnologia finisce per modificare radicalmente la stessa narrazione giuridica e i postulati sottesi alle soggettività,

della globalizzazione[18] e del digitale[19], quanto una sovranità autodeterminata dalle regole tecniche e organizzative del digitale stesso[20].

In realtà, riguardando il tutto nella prospettiva statale, tanto in una dimensione di sovranità interna, ovvero di mantenimento dell'ordine costituzionale davanti l'incedere della logica *disruptive* del digitale[21] o di assalti alla sicurezza da parte di attori privati o pubblici, e di sovranità esterna, ovvero di preservazione della propria sovranità a fronte delle relazioni e dei conflitti che avvengono nel e attraverso il digitale, è possibile da un lato considerare preliminarmente la sovranità digitale come garanzia di tenuta dei principi costituzionali, dei diritti e delle libertà.

Ciò mediante la riaffermazione statale[22] nei confronti di intrusioni, attacchi, sabotaggi portati avanti per via digitale da attori statali o privati, grazie al controllo di dati e *software*, intelligenza artificiale, standard e protocolli, 5G, nomi di dominio, processi, come per i sistemi di *cloud computing*, *hardware*, *server*,

---

A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *Biolaw Journal – Rivista di biodiritto*, 3, 2019, specialmente pp. 24 e ss.

[18] Per una ricostruzione analitica, puntuale e critica delle ideologie della globalizzazione in cui preminente è il mercato, che sarebbe il motore pulsante e l'unico cardine di regolazione e logica razionale possibile della globalizzazione, M. BETZU, *Stati e istituzioni economiche sovranazionali*, Giappichelli, Torino, 2018, pp. 29 e ss. ove partendo dalla teorica di Manfred Steger si rivela come la globalizzazione sarebbe un fenomeno naturale, inevitabile, nato dal mercato e governato dal mercato, e che favorirebbe la democrazia.

[19] Colgono esattamente il punto, A. SIMONCINI, *Sovranità e potere nell'era digitale*, in O. POLLICINO, T.E. FROSINI, E. APA, M. BASSINI (a cura di), *Diritti e libertà in Internet*, Le Monnier, Milano, 2017, p. 24, il quale inferisce una mutazione radicale e rivoluzionaria anche in chiave antropologica che finisce per echeggiare momenti di svolta nel paesaggio umano, come quello di invenzione della scrittura, e L. CASINI, *Lo Stato nell'era di Google*, Mondadori, Milano, 2020, p. 87.

Si veda anche F. PARUZZO, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, ESI, Napoli, 2022, pp. 105 e ss.

[20] Su questa ambivalenza, T. E. FROSINI, *L'ordine giuridico del digitale*, in *Rivista interdisciplinare sul diritto delle amministrazioni pubbliche*, 2, 2023, p. 37.

[21] G. FONTANA, *Sfera pubblica digitale e democrazia nell'Unione europea. Prime considerazioni intorno alla dichiarazione europea sui diritti e i principi digitali*, in R. TORINO, S. ZORZETTA (a cura di), *La trasformazione digitale in Europa – diritti e principi*, Giappichelli, Torino, 2023, p. 34.

[22] M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, 1, 2022, p. 48, snuda una costellazione di iniziative che hanno provato ad articolare un insieme di diritti politici, norme di *governance,* e limitazioni all'esercizio del potere su Internet.

computer, cellulari, tablet, servizi, si pensi ai *social media* o ai siti di *e-commerce*, e infrastrutture[23] quali cavi, satelliti fino a intere città, nel caso delle *smart cities*, e dall'altro lato riaffermare un sistema di regole giuridiche tese alla garanzia dei diritti e delle libertà, dai dati personali alla libertà di espressione[24], alle libertà politiche fino alla tutela dei consumatori e del mercato[25].

Un contemperamento non semplice e soprattutto fisiologicamente e funzionalmente multilivello[26], che vede negli Stati nazionali aderenti all'Unione Europea attori tra loro connessi a ragnatela, in un *network* di *policies* e di regole normative ed etiche spesso esorbitanti dallo spazio della stessa Unione e che finiscono, tra loro cospiranti, per determinare la modellazione teorica di un autentico cyber-giusnaturalismo[27].

---

[23] A. ARESU, *Lo Stato nella competizione tecnologica*, in *Il Mulino*, 2, 2023, pp. 87 e ss., per la guerra dei semi-conduttori che è guerra concettuale, normativa e 'fisica'.

[24] M. BASSINI, *Internet e libertà di espressione*, Aracne, Roma, 2019, p. 165, rileva come sia soprattutto rispetto a questo diritto fondamentale, la libertà di espressione, che la rete sembra aver provocato conseguenze di non secondario momento.

[25] G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE online*, 1, 2023, p. 348.

[26] G. SMORTO, *Il ruolo della comparazione giuridica*, cit., p. 49, valorizza un modello di intervento regolativo che mira a contemperare, da un lato, le esigenze dello sviluppo economico del settore digitale e la capacità di innovazione del tessuto imprenditoriale europeo, e, dall'altro, gli interessi economici e politici dell'Unione.

[27] Si pensi, in questa prospettiva, all'avvicinamento tra *cybersecurity* e *cyberwarfare* soprattutto in area NATO.

Con la pubblicazione nel 2017 della nuova edizione del '*Manuale di Tallinn*', pietra angolare NATO in tema di legge e *cyberwarfare*, questo aspetto è emerso in maniera sempre più significativa.

In particolare, la *cybersecurity* diviene complementare funzionalmente alla *cyber-defense* soprattutto nella gestione, nella protezione e nella prevenzione degli attacchi a infrastrutture critiche e a obiettivi squisitamente civili, si veda M.N. SCHMITT, *Tallinn Manual 2.0 on the International Laws Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, pp. 401 e ss.

Nella nuova edizione del *Manuale*, ancora più centrali sono i richiami espressi alla 'legge del mare', alla 'legge del cielo' e alla 'legge dello spazio', ma soprattutto al concetto groziano di '*due diligence*' applicato al diritto internazionale, come antecedente storico-funzionale dei processi di giuridificazione degli spazi liquidi e fluidi e dei rapporti tra Stati e attori non statali, a confermare un approccio cyber-giusnaturalista debitore del pensiero di de Vitoria e di Grozio, in questo senso C. PATRICK, *Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations*, in *Washington International Law Journal*, vol. 28, 2, 2019, pp. 586 e ss.

Sicuramente può dirsi che la sovranità digitale passi tanto dal lato di permanenza statale sul versante infrastrutturale[28] quanto su quello concettuale e assiologico dei codici tecnici[29], in questo caso al fine di respingere le logiche centripete dei grandi signori del digitale le cui scelte e le cui decisioni sono sempre più impattanti sugli stessi Stati[30].

Proprio per la radicalità delle conseguenze della rivoluzione digitale[31], è apparso lungo la linea dell'orizzonte un approccio epistemologico nuovo conosciuto come costituzionalismo digitale[32], a cui si è opposta, in sede critica, l'accusa di palesare una qual certa irenicità[33].

Al che si è però replicato[34] opportunamente che la formula costituzionalismo digitale indica che, in estrema sintesi, è stato il processo politico a riprendere in

---

[28] S. MANGIAMELI, *La sovranità digitale*, in *Diritti fondamentali*, 3, 2023, p. 284 per la considerazione del riconoscimento endiadico della sovranità digitale tra rete infrastrutturale e singolo ordinamento, sottolineandone la tendenza unificatrice globale.

Se ciò è indubbio avendo riguardo alla rete come infrastruttura fisica, le cose cambiano quando si ascende al livello dell'ecosistema digitale, degli spazi sociali digitali e soprattutto dei servizi offerti dalle piattaforme.

È certamente vero che un governo nazionale potrebbe oscurare la fruizione di internet o limitarla, come avviene in Cina, affermando con ciò in maniera *tranchant* la propria sovranità; ma del pari, ed è quanto empiricamente avvenuto durante la pandemia quando si rese necessaria la sincronizzazione dei sistemi operativi *IoS* e *Android* per poter fruire della *app Immuni*, spesso sono anche gli Stati a dover scendere a patti con i giganti del digitale.

O si pensi, molto più recentemente, al collasso dei sistemi *cloud* Microsoft che hanno drammaticamente impattato sui sistemi aeroportuali di mezzo mondo, incidendo sulla mobilità globale.

[29] G. CAVANI, *Nuovi poteri, vecchi problemi. Il costituzionalismo alla prova del digitale*, in *DPCE*, 1, 2023, p. 236, sulla applicazione del diritto delle piattaforme.

[30] L. AMMANATI, *I signori nell'era dell'algoritmo*, in *Diritto pubblico*, 2, 2021, specie pp. 385-386, per il passaggio dalla piattaforma all'eco-sistema.

[31] T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. Inf.*, 2020, p. 478, sulla trasformazione della democrazia sotto il peso del digitale.

Si veda anche L. TORCHIA, *Lo Stato digitale*, Il Mulino, Bologna, 2023, pp. 20 e ss.

[32] G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, Cambridge, 2022.

[33] M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, 3, 2021, pp. 746-747, per una ricostruzione fortemente critica del costituzionalismo digitale.

[34] O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, p. 582.

mano il pallino relativo alle modalità espressive della sovranità digitale di reazione al contenimento del nuovo potere privato.

In buona approssimazione, si può definire la sovranità digitale quale il livello costituzionale dei principi e dei diritti fondamentali e della loro tenuta, declinato in chiave comprensiva di qualunque connessione tra sistema ordinamentale, diritti fondamentali e sfera digitale, da opporsi a soggetti privati o a attori pubblici ostili.

Essa opera in maniera biunivoca e connessa tra livello nazionale, livello europeo e transnazionale: sicurezza europea, nazionale, tutela dei dati, tutela della concorrenza[35], ma anche etica comportamentale e raccordo istituzionale ne costituiscono il portato sostanziale che in chiave strumentale passa per un approccio multidisciplinare sempre più conosciuto come cyber-resilienza.

In questa chiave di lettura incarna la tenuta assiologica a fronte dei radicali rivolgimenti importati dal digitale; la sicurezza digitale e la *cybersecurity*, come vedremo, ne sono gli strumenti basici, concettuali nel caso della sicurezza, empirici in quello della *cybersecurity*, di attuazione e preservazione di quella storica traiettoria che connette sovranità e Stato[36].

### *2.1 La sicurezza digitale*

Nessun ordinamento può sopravvivere se non attraverso la modulazione empirica di un sistema di sicurezza, e proprio per questo si è correttamente inferita la natura di valore super-primario[37] della sicurezza stessa.

Condizione necessitata affinché un ordinamento possa preservarsi; una condizione riferita tanto allo Stato-apparato, quanto allo Stato-comunità e che dispiega i propri elementi e le proprie caratterizzazioni in maniera diversa, spesso seguendo le aggettivazioni che meglio la dettagliano.

Le aggettivazioni, in realtà, oltre a seguire una linea didascalica funzionale a perimetrare un dato ambito settoriale di intervento della sicurezza, snudandone le

---

[35] E. BRUTI LIBERATI, *Poteri privati e nuova regolazione pubblica*, in *Diritto pubblico*, 1, 2023, p. 297, nota che il contrasto al potere di mercato delle grandi piattaforme digitali non può essere più lasciato alla sola disciplina antitrust.

[36] A. MORRONE*, La sovranità*, in *Rivista AIC*, 3, 2017, p. 9, sottolinea come la sovranità operi da attributo costitutivo dello Stato moderno: essa ne segue necessariamente la traiettoria storica. Quella che è stata definita la "parabola della sovranità" non è che metafora delle trasformazioni della forma politica statuale riguardata attraverso la categoria della sovranità.

[37] G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, 2008, pp. 31 e ss.

singole caratteristiche di disciplina, sono anche il portato della natura eminentemente relazionale della sicurezza stessa[38].

Detto in altri termini, non può darsi una sola sicurezza ma tante quanti saranno gli ambiti in cui essa è chiamata ad operare.

Se la sicurezza deve farsi scudo rispetto minacce di vario ordine e grado, appare evidente come essa debba atteggiarsi quale ontologica risposta al palesarsi di fratture, falle e vulnerabilità che possano presentarsi.

Non per caso il tema della 'vulnerabilità[39]" nel dominio digitale è uno dei più avvertiti dal legislatore.

Il *corpus* normativo dell'Unione Europea dedicato alla sicurezza cibernetica, sia di diritto vincolante, che di *soft law*, fa sempre più di frequente riferimento alla "vulnerabilità" delle reti, dei sistemi, di tutto quel supporto materiale o digitale che regge l'intero universo cibernetico.

Per dare l'idea di alcuni di questi atti, basta citare i più recenti e rilevanti: l'ultima *Strategia per la sicurezza cibernetica in Europa*, adottata nel 2020, la c.d. Direttiva NIS 2 (Dir. n. 2022/2555), il regolamento DORA, Reg. n. 2022/2554 relativo alla "*resilienza operativa digitale per il settore finanziario*", il Regolamento n. 2021/784 sul contrasto alla diffusione di contenuti terroristici *online*, il Regolamento *Cyber Resilience Act,* proposto nel 2022, approvato dal Consiglio il 10 ottobre 2024, disponendo questo il paradigma di un'autentica '*cybersecurity by design'* gravante sui produttori e sugli erogatori di servizi digitali connessi e, da ultimo, la proposta di Regolamento *Cyber Solidarity Act*, che ha ricevuto il primo voto favorevole da parte del Consiglio nel gennaio 2024 e poi quella del Parlamento nel marzo seguente, consistendo nella modellazione di un cyber-scudo europeo basato su reticolari vincoli di resilienza digitale tra attori pubblici e privati.

Fra questi, la direttiva NIS 2 contiene una definizione di vulnerabilità, che l'art. 6, n. 15 identifica come "*un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica*".

La sua essenzialità è cristallina, posto che considerata la natura del digitale, la sua dinamica iper-relazionale, una singola vulnerabilità potrebbe tramutarsi in una frattura ordinamentale.

L'idea di fondo sottesa al variegato *framework* normativo di sicurezza digitale è che per preservare l'ordine democratico europeo, il suo spazio giuridico di libertà e soprattutto il mercato unico occorre approntare un elevatissimo livello di

---

[38] Sul portato relazionale della sicurezza, sul suo atteggiarsi a elemento fluido, contenutisticamente complesso, G. PISTORIO, *La sicurezza giuridica. Profili attuali di un problema antico*, ESI, Napoli, 2022, p. 17.

[39] G. D'ANGELO, G. GIACOMELLO, *Cybersicurezza*, Il Mulino, Bologna, 2023, p. 254.

protezione tecnica delle reti, identificando e eliminando le vulnerabilità in queste presenti.

Non può essere trascurato come questa evoluzione faccia sempre più spesso *pendant* con i documenti e le linee-guida diffuse dalla NATO, da ultimo il manuale *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency* del 2022, a testimoniare il già accennato processo di convergenza concettuale tra *cybersecurity* e *cyberwarfare*.

Alla luce di quanto detto potrebbe quasi inferirsi che la sicurezza digitale non sia altro che il complesso, tanto infrastrutturale quanto normativo, di garanzia di sicurezza nel dominio cibernetico, al fine di contrastare minacce e vulnerabilità.

In realtà, è necessario andare oltre il significato classico di sicurezza digitale e sicurezza informatica, sovente peraltro utilizzati in modo sinonimico e interscambiabile.

Se per sicurezza digitale si intende di solito la protezione tecnica dei sistemi informativi e digitali, avendo riguardo a un dato quantitativo e di impatto esteso della minaccia potenziale, e per sicurezza informatica la protezione anche del singolo *hardware/software* da una minaccia, è necessario trascendere questa apparente limitazione e individuare un significato più elevato e complessivamente soddisfacente.

Questo perché non è possibile, non nel dominio digitale, iper-parcellizzare e settorializzare un ambito tanto essenziale.

È pertanto condizione fondamentale identificare nella sicurezza digitale il livello di tutela tecnico-concettuale dell'ordinamento digitale nel suo complesso, il quale opera in maniera multilivello, europeo, nazionale, regionale, comunale, incardinando funzionalmente anche i soggetti privati, al pari della sicurezza integrata, espressione necessitata questa di sussidiarietà e di solidarietà digitale.

In concreto ciò significa ricondurre al significato esteso di sicurezza digitale qui proposto tutti quegli elementi cardine di difesa, sicurezza e preservazione della sovranità nazionale[40] e digitale: dalle recenti evoluzioni normative che hanno esteso la disciplina '*golden power*' anche al 5G e al *cloud*[41], passando per la regolazione

---

[40] T. F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, p. 277, per la questione della cybersicurezza come costola della sicurezza nazionale.

[41] Come noto, il decreto-legge 21 marzo 2022, n. 21 ha integralmente riscritto l'art. 1-bis del decreto-legge 15 marzo 2012, n. 21, inserendo nel perimetro di estensione del '*golden power*' anche il *cloud* e il 5G.

Sul punto, L. FIORENTINO, *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I 'poteri speciali' del Governo nei settori strategici*, ESI, Napoli, 2020, pp. 39 e ss.

dei mercati digitali, come avvenuto con il *DSA* e con il *DMA*, o delle intelligenze artificiali.

Sicurezza digitale sono anche la cyber-diplomazia e la cyber-resilienza, producendo una piena inversione rispetto al rapporto storicamente intercorrente tra sicurezza digitale e sicurezza informatica; sicurezza digitale come attrazione nell'alveo del riferimento costituzionale alla sicurezza e alla difesa, operando un fattore ricombinante[42] della sovranità, sia nella sua dimensione nazionale quanto in quella euro-unitaria.

Questo perché, l'aumento della "superficie di attacco", non più solo fisica e geografica, che uno Stato deve sorvegliare e proteggere, rende gli stessi diritti più esposti agli attacchi del nemico[43] su un raggio di azione assai più esteso del mero perimetro nazionale.

### *2.2 La cybersecurity*

Nel 2003, l'Unione Europea ha predisposto la propria *Strategia in materia di sicurezza informatica* nel cui ambito, pur non essendo utilizzato il termine "*cybersecurity*", viene per la prima volta fatto esplicito riferimento ad una "*dipendenza europea da un'infrastruttura interconnessa nel settore dei trasporti, dell'energia, dell'informazione ed altri, e la conseguente vulnerabilità dell'Europa sotto questo profilo*".

L'espressione *cybersecurity* comparirà per la prima volta nella *Relazione* del 2008 sull'attuazione della *Strategia europea in materia di sicurezza informatica* del 2003, in cui la sicurezza informatica viene presentata come uno degli aspetti critici per combattere il terrorismo e la criminalità organizzata.

---

Anche, B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità*, *competitività e diritti individuali*, in *Federalismi.it*, 14, 2020, specie pp. 38 e ss.

[42] O. POLLICINO, *Potere digitale*, cit., p. 414, parla di una morfologia quadrangolare del potere digitale ripartito in dimensione spaziale, valoriale, soggettiva e rimediale.

Nell'ottica della sovranità digitale, lo Stato vive al contrario di una forma di adattamento ricombinante tra sovranità singolo-nazionale e affermazione sovrana mediante integrazione europea nelle maglie del dominio digitale, propiziata da *GDPR*, *DSA* e *DMA*, *Artificial Intelligence Act*, normativa in tema di *cybersecurity*.

[43] A. LAURO, *Vulnerabilità e tutela dei diritti fondamentali alla prova della guerra cibernetica*, in *DPCE online*, Sp/1, 2024, p. 486.

Definire in cosa materialmente consista la *cybersecurity*, individuarne e delinearne una tassonomia, le caratteristiche costitutive e quelle funzionali è attività di estrema complessità[44], ma del pari di grande utilità.

La complessità deriva dall'accelerato mutamento di contesto e di strumentario tecnologico determinato dalla costante rimodellazione dell'eco-sistema digitale e dall'utilizzo che le compagini statali ne fanno: è stato sottolineato con grande chiarezza come non possa darsi una granitica definizione di *cybersecurity* destinata a rimanere immutata[45] nel tempo.

La grande utilità di procedere ad una definizione di *cybersecurity* si ricava dalla necessità non solo e non tanto di poter procedere a una perimetrazione della materia, quanto da quella di inserire la *cybersecurity* in un più articolato e organico dispositivo funzionale di protezione di beni primari e di diritti fondamentali.

Non vi è dubbio alcuno che un approccio funzionale sia preferibile a uno meramente catalogatorio delle caratteristiche ricorrenti.

Questo perché la *cybersecurity* può essere molte cose diverse e soprattutto può essere chiamata ad operare su molti livelli distinti, da quello dell'organizzazione amministrativa transnazionale alla protezione di diritti fondamentali, ascendendo in questo caso nell'alveo della sovranità digitale e della sicurezza digitale.

I classici scopi sottesi alla sicurezza in un eco-sistema informativo risultano dalla nozione di minaccia *cyber*[46].

Tradizionalmente si registrano tre scopi devoluti al contrasto alle minacce; confidenzialità, integrità, utilizzabilità[47], conosciuti come triade CIA[48].

---

[44] G. BORRIELLO, G. FRISTACHI, *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in *Rivista di digital politics*, 1-2, 2022, p. 160, per la definizione problematica del termine cybersicurezza.

[45] G. ZICCARDI, *La cybersecurity nel quadro tecnologico (e politico) attuale*, in G. ZICCARDI, P. PERRI (a cura di), *Tecnologia e diritto*, III, Giuffrè Francis Lefebvre, Milano, 2019, p. 207.

[46] G. D'ANGELO, G. GIACOMELLO, *Cybersicurezza,* Il Mulino, Bologna, 2023, p. 246, la minaccia è descritta come probabilità che un'entità esterna rappresenti un rischio per la sicurezza o la stabilità di un'organizzazione e di un sistema informatico.

[47] P.W. SINGER, A. FRIEDMAN, *Cybersecurity & Cyberwar*, Oxford University Press, Oxford, 2018, p. 35.

[48] Ampiamente sugli elementi costitutivi della triade CIA, G. D'ANGELO, G. GIACOMELLO, *Cybersicurezza,* cit., pp. 73 e ss.

Si veda anche Com. Comm., JOIN(2013)1) del 7 febbraio 2013, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, *cybersecurity*, che ricomprende l'insieme delle precauzioni e degli interventi che, al fine di preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni ivi contenute, "*… si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei*

A questa triade, la direttiva NIS ha aggiunto i concetti di resilienza e di autenticità[49].

La *cybersecurity* quindi consiste in un approccio finalizzato al collegamento funzionale di prevenzione dei rischi, per come seguito da organizzazioni e Stati per proteggere la triade CIA riferita ai dati e agli *asset* usati nel cyberspazio.

Il concetto include[50] linee guida, *soft law*, tecnologia, strumenti tecnici e addestramento al fine di determinare un efficace livello di protezione[51].

Come si capisce agevolmente, si tratta di un livello definitorio tecnico-funzionale, confermato ad esempio dal CEN/CENELEC[52] .

Lo stesso organismo ha rilevato la necessità di un approccio definitorio di contesto; il termine è polisenso, ma dal punto di vista funzionale mostra un nocciolo comune che è importante delineare ai fini della individuazione di concrete linee di intervento[53].

Approccio questo sposato dall'ENISA nel suo report '*Definition of Cybersecurity*', del dicembre 2015, e dall' *EU Cybersecurity Act*, che all' art 2.1 definisce la *cybersecurity* come quello strumento che consiste nelle attività per proteggere *network* e sistemi informativi, gli utilizzatori di questi sistemi e le altre persone danneggiate da minacce digitali.

Approccio fatto proprio dal legislatore italiano, laddove il decreto legge 14 giugno 2021, n. 82, così come convertito dalla l. 4 agosto 2021, n. 109, stabilisce che per cybersicurezza deve intendersi "*l'insieme delle attività (...) necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e*

---

*confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti".*

[49] J. MICHELS, I. WALDEN, *Complacency and Panic: Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?,* in *European Law Review*, vol. 45, 1, 2020, p. 28.

[50] Una definizione quantitativa di *cybersecurity* è stata proposta da J. KULESZA, *Defining Cybersecurity*, in J. KULESZA, R. BALLESTE (a cura di) *Cybersecurity and Human Rights in the Age of Cyberveillance*, Rowman & Littlefield, Lanham, 2016, p. 31, secondo il quale può considerarsi *cybersecurity* quell'insieme di misure tecniche e normative modellate per proteggere *computer network* e i dati dalle minacce digitali, *ivi* inclusi crimini digitali e altre attività dannose, laddove però dette minacce, attualmente o potenzialmente, rischino di arrecare danno a un numero esteso di persone.

[51] D. SCHATZ, R. BASHROUSH, J. WALL, *Towards a more representative Definition of Cybersecurity*, in *Journal of Digital Forensics, Security and Law*, vol. 12, 2, 2017, p. 66.

[52] *Recommendation #2: Definition of Cybersecurity*, 2016, p. 12, lascia emergere un concetto eminentemente tecnico di sicurezza digitale.

[53] *Recommendation #2: Definition of Cybersecurity*, cit. p. 38.

*l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico*", così all'art. 1, c. 1, lett. a).

In questa definizione emerge un dato significativo: il *range* di copertura e di operatività del termine non è riferito solo ai sistemi ma anche alle persone, determinando una connessione tra la sicurezza dell'ecosistema e quella degli individui e dei loro diritti.

*Cybersecurity* è quindi il livello tecnico-parziale e strumentale di implementazione della sicurezza digitale: in questo livello è accettabile la *actio finium regundorum* delle specifiche competenze nel sistema di *governance* e di una sotto-divisione per temi ed elementi, quali *hardware*, *software*, *digital awareness*, *cloud*.

## 3. L'ordine costituzionale della *cybersecurity*

Seguendo la tassonomia tripartita sin qui illustrata, può ora darsi un inquadramento costituzionale della *cybersecurity*.

Il primo livello è quello della sovranità digitale, ovvero del permanere delle garanzie costituzionali che operano su due piani: uno di sovranità interna, al fine tanto di resistere alle logiche tecniche private del digitale quanto di preservare l'ordine costituzionale interno da minacce e rischi palesati per via digitale, e un altro di sovranità esterna come resistenza ad assalti *cyber* da parte di attori ostili, privati o pubblici.

In questo senso, un ruolo cardinale lo riveste l'articolo 11 della Costituzione che determina la soglia di legittimazione di interventi regolatori e di coordinamento funzionale dell'Unione Europea.

Si tratta di una norma che impone il ragionare di limitazioni di sovranità funzionali al processo di integrazione sovranazionale individuando come soggetto che si autolimita per detti fini lo Stato italiano.

Ovviamente, l'articolo 11, proprio per la potenza intrinseca connaturata alla sovranità e alla contestualizzazione adeguata nella scelta politica dei Costituenti, pone una serie di stringenti problemi che testimoniano la delicatezza di qualunque declinazione del concetto di sovranità: la legittimazione sovrana nei processi di integrazione[54], la scelta internazionalista al fine di non parcellizzare e limitare in

---

[54] M. CARTABIA, L. CHIEFFI, *Art. 11*, in R. BIFULCO, A. CELOTTO, M. OLIVETTI (a cura di), *Commentario alla Costituzione*, I, Utet, Torino, 2006, p. 283. Si è sottolineato in dottrina come la formulazione limitazioni di sovranità in luogo di cessioni possa essere declinato in una duplice modalità: o come modalità di vigilanza integrativa con un nocciolo duro di legittimazione incardinato nel popolo dei singoli Stati e nei suoi mezzi

chiave regionale lo sviluppo della integrazione dell'Italia[55], la funzione dell'articolo 11 come norma di produzione di altre norme[56], la sovranazionalità con il passaggio da un modello basato sulla competenza al modo di riconoscimento di una propria sovranità intangibile, una sovranità costituzionale sotto forma di contro-limiti.

Nello spazio digitale le limitazioni di sovranità per consistere di una sovranità più estesa, integrata in organismi sovra-nazionali, operano in funzione ricombinante[57]; non come cessione o sdilinquimento della propria sovranità, ma come strumento potenziato di mantenimento delle garanzie costituzionali in un mondo nuovo[58].

---

rappresentativi, per arrivare comunque a un processo di federalizzazione democraticamente governata, oppure come paletti e barriere che non consentono di intaccare il nucleo profondo della sovranità statale.

[55] M. CARTABIA, L. CHIEFFI, *Art. 11,* cit., p. 267, sottolineano la scelta dei Costituenti di rifuggire dalle sirene del regionalismo, evitando di menzionare espressamente l'integrazione europea e preferendo mantenersi sul versante largo della integrazione internazionale.

Questo aspetto diviene particolarmente apprezzabile nelle dinamiche della globalizzazione e del digitale, laddove la necessitata integrazione nel percorso euro-unitario e la condivisione assiologica di principi e di norme di diritto internazionale rafforzano la sovranità nazionale, rendendo il Paese più competitivo e sicuro proprio perché integrato in un reticolo espansivo di altri Stati che ne condividono l'*humus* valoriale e di civiltà giuridica.

Un aspetto da sottolineare, quello della sovranità ricombinante, soprattutto in prospettiva di fonti del diritto e di base giuridica della normativa euro-unitaria in tema *cybersecurity*, alla luce del dibattito dottrinale, su cui torneremo, a proposito dell'articolo 114 TFUE come base della normativa in chiave di *cybersecurity*.

[56] Corte Cost., sentenze nn. 348 e 349/2007.

[57] R. URSI, *La sicurezza cibernetica come funzione pubblica*, cit. p. 15, delinea la forma cangiante e complessa della sicurezza cibernetica che sintetizza in maniera sostanziale e procedurale la c*ybersecurity* e la *cyber-defense*, dimostrando la interdipendenza scalare tra sovranità digitale, sicurezza digitale e *cybersecurity*.

[58] Ricorda giustamente F. SERINI, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in *Medialaws*, 3, 3023, p. 171, come la funzione della direttiva NIS 2, esplicitata dall'articolo 1, sia quella di garantire un livello elevato di cybersicurezza europea in modo da migliorare il funzionamento del mercato comune, ma a livello nazionale, in tema di Perimetro di sicurezza nazionale cibernetica, previsto dall'art. 1, c. 1, l. a) del d.l. 21 settembre 2019, n. 105, le norme dettate a livello interno preservano e tutelano sicurezza nazionale e interesse nazionale.

È chiaramente, può aggiungersi, difficoltoso ormai scindere in prospettiva funzionale i due ambiti, che se permangono distinti dal punto di vista del quadro normativo e

Proprio per questo, un secondo aspetto è quello della connessione tra sovranità ricombinante[59] nel cyberspazio, dettata dalla integrazione euro-unitaria, e sovranità interna garantita, anche, dalla sicurezza nazionale.

È naturalmente noto come i Costituenti abbiano voluto attribuire in via esclusiva allo Stato il compito di garantire la sicurezza[60] della Repubblica[61].

A tale ultimo proposito, l'art. 117, c. 2, lett. d), Cost., con riferimento alla sicurezza esterna, ovvero nei confronti di altri Stati, e definendo il perimetro dell'intervento esclusivo dello Stato, in questo caso riferito alla potestà legislativa

---

regolatorio convergono invece lungo la dorsale del mantenimento della sovranità digitale e della sicurezza digitale, proprio a indicare la complessità del mondo nuovo digitale.

[59] "*La sovranità oggi non ha più caratteri necessariamente privati o pubblici, personali o collettivi, ma essenzialmente tecnici*", scrive A. SIMONCINI, *Sovranità e potere nell'era digitale*, cit., p. 20.

Abbiamo visto come e quanto nello spazio digitale tendano a riprodursi le grandi questioni sulle sovranità asimmetriche e disomogenee che già teologi, filosofi e giuristi post-medievali ebbero a porsi davanti l'apertura delle rotte coloniali.

Proprio per questo la sicurezza intesa come riaffermazione dei diritti passa attraverso la regolazione assiologicamente orientata dei paradigmi tecnici, non meramente controllando e ossificando l'opera dei privati ma responsabilizzandoli in maniera proattiva.

Sicurezza e sicurezza digitale operano come scudo dell'ordinamento e dei diritti e delle libertà che questo garantisce. Non essendo ipotizzabile un governo mondiale del digitale che si coaguli in una improbabile sovranità unica, la sicurezza digitale di spazi tra loro connessi dal riconoscimento di un nucleo assiologico comune si atteggia come forma di protezione e di sopravvivenza di questi stessi spazi.

La sovranità va intesa come ricombinante, e avremo modo di tornarci, proprio perché nel digitale queste sovranità parziali, asimmetriche, appartenenti a Stati diversi e a grandi poteri privati si ricombinano funzionalmente.

[60] Definita dalla Corte cost., n. 77/1987, quale "*funzione inerente alla prevenzione dei reati o al mantenimento dell'ordine pubblico*".

[61] L. MORONI, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 14, 2024, pp. 179 e ss.

Ampiamente, G. PISTORIO, *La sicurezza giuridica*, cit. pp. 34 e ss., T.F. GIUPPONI, *La sicurezza e le sue 'dimensioni' costituzionali*, in *Forum di Quaderni Costituzionali*, 2008, pp. 2 e ss.

Si vedano anche V. BALDINI, *Sicurezza e libertà nello Stato di diritto in trasformazione*, Giappichelli, Torino, 2005, A. STERPA, *La libertà dalla paura. Una lettura costituzionale della sicurezza*, Editoriale Scientifica, Napoli, 2019.

dello Stato[62] , dispone la potestà legislativa esclusiva dello Stato in materia di "*difesa e Forze armate; sicurezza dello Stato*".

Mentre, con riferimento alla sicurezza interna al territorio, l'art. 117, c. 2, lett. h), Cost., sancisce la potestà esclusiva dello Stato in materia di "*ordine pubblico e sicurezza*[63]".

La competenza dello Stato in materia di sicurezza esterna e interna, inoltre, è confermata a livello europeo dall'art. 4, par. 2, del Trattato dell'Unione Europea, il quale stabilisce che l'Unione "*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*".

In questo senso, non c'è alcun dubbio che nonostante il processo di integrazione euro-unitaria tanto il livello nazionale quanto quello europeo conservino la sfera di sicurezza nazionale come prerogativa degli Stati membri. Ma ciò avviene sotto una luce nuova e più complessa, di attrazione ascendente verso la UE[64].

---

[62] Ad esempio, Corte Cost. n. 167/2010 che in tema di armi e munizioni attrae la materia esclusivamente allo Stato, sottraendo quindi alle Regioni la possibilità di dettagliare una disciplina per le armi in utilizzo alla polizia locale.

[63] In questo caso, la Corte cost., n. 218/1988, chiamata ad esprimersi sulla distinzione tra polizia amministrativa e polizia di pubblica sicurezza, ha offerto una distinzione molto nitida, sancendo che la prima consiste in 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, senza che ne risultino lesi o messi in pericolo i beni o gli interessi tutelati in nome dell'ordine pubblico e la seconda come l'insieme delle misure preventive e repressive dirette al mantenimento dell'ordine pubblico. Un indirizzo che ha poi trovato conferma con le sentenze n. 740/1988 e n. 162/1990.

Successivamente, pur non scalfendo la sostanza della distinzione, la Corte ha assunto un approccio evolutivo che ha meglio chiarito e definito gli aspetti salienti, si veda ad esempio Corte cost., n. 115/1995.

[64] A. IANNUZZI, *Le fonti del diritto dell'Unione Europea per la disciplina della società digitale*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 13, delinea la attrazione della produzione legislativa e del momento regolatorio verso la UE.

A ben vedere, quando la radice degli interventi euro-unitari in tema *cyber* trova fondamento nell'articolo 114 TFUE[65], proprio perché l'Unione basa la

---

[65] La scelta ha sollevato notevoli perplessità e critiche in dottrina, lo ricorda molto chiaramente E. LONGO, *La disciplina del rischio digitale*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 216.

Sul rapporto tra articolo 114 TFUE ed evoluzione del *framework* normativo in termini di cybersicurezza, alla luce della proposta di nuovo Regolamento sulla cyber-resilienza, P.G. DI CHIARA, *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*, 1, 2023, p. 144.

L'articolo 114 TFUE costituisce, come è stato sottolineato, uno strumento potentissimo e formidabile per ampliare in maniera significativa la competenza legislativa dell'Unione in materie ritenute particolarmente sensibili per la tenuta dell'ordine euro-unitario, così B. DE WITTE, *Exclusive Member States competences: is there such a thing?*, in I. GOVAERE, S. GARBEN (a cura di) *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford University Press, Oxford, 2017, p. 59.

La lettura evolutiva della norma è stata sottoposta a penetranti critiche, ad esempio si vedano M. VARJU, *5G networks, (cyber)security harmonisation and the internal market:the limits of Article 114 TFEU*, in *European Law Review*, 2020, pp. 471 e ss., specificamente per una critica legata all'espansione in ambito *cybersecurity*, 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*, Elgar, Cheltenham, 2015, pp. 403 e ss..

La stessa Commissione, nella sua *Raccomandazione* del 2019 sulla cybersicurezza, Preambolo n. 25, racc. n. 2019/534, aveva demandato ai singoli Stati membri la disciplina di esclusione di servizi digitali dai loro mercati per motivi di sicurezza nazionale.

Una lettura evolutiva dell'articolo 114 TFUE naturalmente non significa legittimare eventuali travalicamenti delle competenze statali da parte dell'Unione, ma alcuni elementi sembrano confermare che una lettura evolutiva dell'articolo 114 TFUE letto nel prisma della sovranità digitale per come sin qui illustrata sia possibile.

Innanzitutto, l'articolo 114 TFUE è e continua a essere il pilastro normativo dell'intero *framework* in tema *cybersecurity.*

L'UE ha istituito una nuova agenzia, l'ENISA, facendo perno sull'articolo 114 TFUE; una modalità che già la Corte di Giustizia aveva fatto salva, si veda Corte di giustizia del 22 gennaio 2014, causa C-270/12, *Regno Unito c. Parlamento e Consiglio*, punto 108.

Nel 2006 la Corte di giustizia aveva già avuto occasione di stabilire che l'art. 95 del TCE, oggi l'art. 114 TFUE, era una base giuridica adeguata alla creazione della Agenzia europea per la sicurezza delle reti e dell'informazione, si veda la sentenza del 2 maggio 2006, causa C-217/04, *Regno Unito c. Parlamento/Consiglio*.

In secondo luogo, l'idea della Commissione nel perseverare a utilizzare l'articolo 114 TFUE come fondamento giuridico fa leva su un *reasoning* già emerso in sede di giustizia

sopravvivenza del proprio sistema digitale mediante la tutela del mercato, dei consumatori e dei prodotti digitali, elevando però in chiave assiologica quella che *prima facie* poteva sembrare disciplina *pro*-mercatoria in scudo di protezione dei diritti fondamentali, appare sempre più difficile poter sostenere che un perimetro nazionale di difesa cibernetica sia e possa essere solo nazionale.

In questo caso, attraverso un processo a geometria aperta[66], facendo leva sull'articolo 11 della Costituzione, l'Italia come Stato membro garantisce diritti e libertà dei propri cittadini, la loro sicurezza, sia mediante l'implementazione della normativa europea direttamente applicabile[67] o da recepirsi, sia mettendo a sistema

---

euro-unitaria, sentenza CGUE, 8 giugno 2010 relativa alla causa C-58/08, *Vodafone* nella quale si legge "*il ricorso all'articolo 114 TFUE è giustificato in caso di divergenze tra le normative nazionali qualora queste incidano direttamente sul funzionamento del mercato interno*".

Ovviamente può eccepirsi che la dimensione della sicurezza vada ben oltre la morfologia del mercato interno. Su questo nessun dubbio.

Del pari però si deve tenere conto del fatto che la tendenziale matrice privatistica, in senso concettuale, degli strumenti di alta tecnologia e delle loro logiche tecniche ripropone il paradigma che abbiamo già incontrato, parlando delle analogie tra pensiero giusnaturalista post-medievale e spazi digitali, di una nuova funzione degli strumenti privati e mercatori, ormai introiettati in dispositivi funzionali anche alla protezione dei diritti e delle libertà di ordine costituzionale.

Esattamente come l'Unione Europea si è evoluta coagulando gli ordinamenti degli Stati membri attraverso la integrazione principalmente economica e attraverso questa integrazione affermando e riconoscendo e potenziando diritti e libertà, così del pari la protezione del mercato interno non è solo difesa degli scambi commerciali e delle libertà meramente economiche.

Un assunto non revocabile in dubbio sol che si consideri la preoccupazione di tutela, anche, di diritti costituzionali che punteggia l'intera costellazione normativa euro-unitaria in tema di digitale, dal *GDPR* al *DSA*, dal *DSM* all'*AI Act*.

Un altro elemento nodale è di matrice politico-istituzionale; sulla sovranità digitale, letta quindi come sicurezza tecnologica e indipendenza digitale dell'Unione, sembra registrarsi una convergenza salda tra Parlamento, Consiglio e Commissione.

La tendenziale acquiescenza poi dei Paesi membri a un utilizzo a maglie larghe dell'articolo 114 TFUE sembra confermare questa lettura.

[66] Non c'è dubbio sul fatto che la normativa di sicurezza digitale stia producendo una duplice integrazione; quella tra gli attori euro-unitari e nazionali della *governance* del digitale, che finisce per determinare un effetto leva sull'integrazione anche in chiave di sicurezza e difesa, e poi una integrazione pubblico-privato similare alla sicurezza integrata.

[67] A. IANNUZZI, *Le fonti del diritto dell'Unione Europea per la disciplina della società digitale*, cit., p. 19, nota la centralità del Regolamento europeo ma anche problemi di potenziale sovrabbondanza normativa.

vari rami di disciplina del digitale, dalla protezione dei dati al contrasto alle *fake news*[68] fino alla *cybersecurity stricto sensu*, sia adottando le proprie misure di sicurezza digitale connesse ai servizi di sicurezza nazionale e di *intelligence*.

In questo senso, l'Italia si trova a dover far fronte ai rischi importati dal digitale e proprio grazie all'Unione riesce a potenziare lo spettro della propria difesa.

Il rischio è parte essenziale del progresso umano e nel digitale esso acquisisce connotazioni nuove. Non deve essere nullificato ma governato razionalmente, nonostante la tendenziale avversione della società al correre rischi, una avversione che ingenera reazioni auto-conservative da parte della società stessa[69].

Il rischio, come l'emergenza, è il grande convitato di pietra del costituzionalismo[70] alla prova della emergente complessità socio-tecnologica la cui portata è eminentemente globale[71].

E questo aspetto si coglie in maniera cristallina quando connettendo[72] tra loro i vari moduli normativi di regolazione del digitale, si vede come e quanto il rischio sia presente; nel *GDPR*[73], nel *Digital Services Act* (*DSA*)[74] e nel *Digital Markets Act*

---

[68] Sul nesso stringente tra lotta alle *fake news* e *cybersecurity*, in prospettiva di tutela dei diritti fondamentali, A. DI CORINTO, *Data commons: privacy e cybersecurity sono diritti umani fondamentali,* in *Rivista italiana di informatica e diritto*, 1, 2022, specie pp. 34 e ss.

[69] Elemento brillantemente colto da E. LONGO, *La disciplina del rischio digitale*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 55.

[70] V. CORNELI, *Sovranità tecnologica: intelligenza artificiale e valori costituzionali*, in *Forum di Quaderni Costituzionali*, 2, 2023, p. 43, scrive "*tutti siamo esposti al rischio, esserne consapevoli comporta un vantaggio strategico in quanto la capacità di anticipare un rischio consente di non trasformare le emergenze in panico sociale, le paure in catastrofi. In particolare, è compito del giurista, oggi più che mai, fornire strumenti per governare questi rischi*".

[71] D. CRISCI, *Cybersecurity e tutela dei cittadini*, in *Dirittifondamentali.it*, 31 marzo 2019, p. 2, sottolinea il rischio non come percezione soggettiva ma come dato globale.

[72] E. LONGO, A. PIN, *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *DPCE*, 1, 2023, pp. 112 e sss, delineano la interconnessione sostanziale tra giustizia dei dati, trasparenza algoritmica, controllo umano.

[73] D. MULA, *Protezione dei dati personali e cybersecurity*, in A. CONTALDO, D. MULA (a cura di), *Cybersecurity Law*, Pacini giuridica, Pisa, 2020, p. 154, sul raccordo, nel contenimento del rischio, tra disciplina di protezione dei dati personali e disciplina *cybersecurity*.

[74] E. LONGO, *La disciplina del rischio digitale*, cit., p. 75.

Cui *adde*, A. MICHINELLI, *La gestione dei contenuti: illegali e non, la loro moderazione*, in L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Digital services Act e Digital Markets Act*, Giuffrè, Milano, 2024, p. 134, per i rischi nel *DSA*.

(*DMA*), *nell'Artificial Intelligence Act* (*AI Act*)[75] e nella normativa di riferimento *cyber*[76].

Un rischio inteso come veicolo di emersione del pericolo e del danno e che deve essere prevenuto e, appunto, governato, onde evitare che esso si traduca in dimensione patologica.

Volendo quindi sintetizzare, il nucleo assiologico della sovranità digitale inerisce i diritti fondamentali e le libertà dei cittadini.

La sicurezza digitale implica invece una *relatio* concettuale diretta tra la fruizione dei servizi pubblici, le libertà e la costruzione di un dispositivo che garantisca tutto ciò bilanciando libertà e sicurezza.

La connessione tra sicurezza digitale e sicurezza nazionale, la costruzione di una cybersicurezza integrata, è invece il livello della *cybersecurity*.

## 4. Dal governo alla *governance* della sicurezza digitale: verso uno Stato 'catalitico'?

La capillare e sovente sovrabbondante espansione degli strumenti, degli istituti e degli organismi organizzativi preposti alla sicurezza digitale, nel quadro di una elevata complessità tecnologica e di percorsi decisionali accelerati, pone la grande questione, già emersa nel cuore della globalizzazione, di un potenziale slittamento da un sistema di governo alla *governance*[77].

---

[75] E. LONGO, *La disciplina del rischio digitale*, cit., p. 72. Sul rapporto specifico tra *AI Act* e *cybersecurity*, estesamente H. JUNKLEWITZ, R. HAMON, A. ANDRÉ, T. EVAS, J. SOLER GARRIDO, J. I. SANCHEZ MARTIN, *Cybersecurity of Artificial Intelligence in the AI Act*, Publications Office of the European Union, Luxembourg, 2023.

Naturalmente il rapporto tra sicurezza e Intelligenza Artificiale può essere declinato anche ai massimi livelli, ovvero nella sfera della sovranità digitale, quando dalla I.A. possano occorrere rischi sistemici per la tenuta di un dato ordinamento, come quello euro-unitario, e dei suoi principi fondanti, si veda O. POLLICINO, P. DUNN, *Intelligenza artificiale e democrazia*, Bocconi University Press, Milano, 2024, pp. 75 e ss.

In questo senso, come non ha mancato di sottolineare A. PATRONI GRIFFI, *Bioetica, diritti e intelligenza artificiale: una relazione da costruire*, in ID. (a cura di), *Bioetica, diritti e intelligenza artificiale*, Mimesis, Milano, 2023, p. 18, '*il costituzionalismo è chiamato oggi a ridefinire i limiti dell'avanzamento tecnologico e, allo stesso tempo, creare un quadro normativo che sia premessa per uno 'sviluppo tecnologico responsabile' e 'sostenibile', fondato su trasparenza, giustizia, responsabilità, sicurezza, privacy*".

[76] E. LONGO, *La disciplina del rischio digitale*, cit., p. 77.

[77] M.R. FERRARESE, *La governance tra politica e diritto*, Il Mulino, Bologna, 2010, pp. 118-119, avverte come l'aspirazione del diritto della globalizzazione, scardinato

Da un lato, quindi, si registra un enorme tema di legittimazione politica e sovrana[78] degli organi che nel loro insieme compongono il *framework* della *cybersecurity*.

E dall'altro lato, la potenziale fisionomia di una nuova forma di governo; quella dello Stato 'catalitico'.

Formula didascalica e descrittiva[79] emersa nel 1992, ad opera di Michael Lind[80], inserita nello sgretolamento del blocco socialista, nella ridefinizione degli assetti economici internazionali, delle logiche mercatorie globali e della stessa trasformazione della CEE, il quale individuava nel processo chimico di catalisi[81] una risposta alla complessità dei tempi e alla presenza di nuovi rischi.

La formula 'catalitica' non per caso venne utilizzata in primo luogo per illustrare quegli ambiti in cui già era emerso il principio di precauzione[82], contraddistinti dalla presenza cospirante di difficoltà regolatorie, evanescenza dell'oggetto

---

l'accoppiamento strutturale legge-sovranità, sia quella di disporre in maniera ordinale delle cose.

[78] Un tema che in realtà riguarda anche a monte il tentativo di giuridificare la sovranità statale, come rileva A. SPADARO, *Dalla 'sovranità' monistica all''equilibrio' pluralistico di legittimazioni del potere nello Stato costituzionale*, in *Rivista AIC*, 3, 2017, p. 3.

Opportunatamente, nel *framework* normativo, emerge un collegamento politico-istituzionale tra gli organismi della sicurezza digitale e il vertice politico, nel caso italiano la Presidenza del Consiglio, tra *cybersecurity*, suoi organismi e recupero del momento parlamentare sotto forma di connessione con il COPASIR. A ciò si aggiunga l'interconnessione tra autorità, in funzione di collaborazione e di tutela intrecciata dei diritti, su cui si tornerà *infra*.

[79] Chi scrive condivide i rilievi critici, in prospettiva deontica, mossi a riguardo delle varie aggettivazioni emerse nel corso degli ultimi anni per descrivere l'attitudine specificamente devoluta alla regolazione, alla promozione, alla avversione ai rischi, da parte dello Stato, si veda ad esempio A. RIVIEZZO, *Lo 'Stato regolatore' come fattispecie a 'legittimazione differenziata'*, in *Forum di Quaderni Costituzionali*, 23 febbraio 2013, specie pp. 4 e ss. sulla ambiguità della espressione 'Stato regolatore'.

È indubbio però che non solo didascalicamente la formula 'catalitico' possa presentare una sua specifica utilità, a patto di mantenerla solo sul versante della forma di governo e di utilizzarla al fine di calibrare le soglie di legittimazione degli organismi e le modalità di tutela dei diritti.

[80] M. LIND, *The Catalytic State*, in *The National Interest*, 27, 1992, pp. 3 e ss.

[81] "*Fenomeno per cui alcune reazioni vengono accelerate (o ritardate) dalla presenza di sostanze (catalizzatori) che prendono parte agli stadî più importanti della reazione e vengono poi rigenerate, ritrovandosi così inalterate alla fine del processo*", in *Enciclopedia Treccani*, disponibile all'indirizzo https://www.treccani.it/vocabolario/catalisi/.

[82] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw Journal – Rivista di biodiritto*, 1, 2019, pp. 86 e ss.

regolando, complessità socio-tecnica e rischi. Venne quindi *in primis* riferita alle politiche ambientali dell'UE[83].

La formula sembra quindi perfettamente attagliarsi anche al *framework* e alle funzioni sottese alla regolazione dell'alta tecnologia e alla *cybersecurity*[84], contraddistinte da tutte quelle difficoltà proprie anche delle politiche ambientali.

Ma in cosa consiste concretamente questa formula e in cosa si differenzia rispetto, ad esempio, allo Stato regolatore o allo Stato promotore?

Innanzitutto, in questa dinamica la sovranità si rende pulviscolare e ricombinante[85]; il proliferare di organismi non opera più solo in chiave regolatoria ma anche come intreccio proattivo di cooperazione e di collaborazione con i privati[86], il cui ruolo è in questo ambito più che essenziale[87].

In questa prospettiva, è quindi essenziale il recupero della legittimazione democratica e soprattutto la modulazione di formula di garanzia dei diritti dei

---

[83] A. PRONTERA, R. QUITZNOW, *The EU as catalytic state? Rethinking European climate and energy governance*, in *New Political Economy*, 3, 2022, pp. 517 e ss.

[84] M. SGUAZZINI, M. DI GIULIO, *Toward a Catalytic State? The Evolution of EU Cybersecurity Policy in Turbulent Times,* in *Rivista italiana di politiche pubbliche*, 1, 2024, p. 68, scrivono come gli ambiti europei in cui emerge una attitudine catalitica siano ad esempio la cyber-diplomazia e la cyber-resilienza.

[85] R. URSI, *La sicurezza cibernetica come funzione pubblica*, cit., p. 8, per la definizione dello spazio digitale come ecosistema complesso originante dal reticolo di mezzi tecnici e interazioni umane. In questa complessità, la sovranità nazionale deve necessariamente ricombinarsi per adattarsi funzionalmente all'ambiente virtuale.

[86] L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi.it*, 25, 2022, pp. 81 e ss., per la collaborazione pubblico-privato nel campo della sicurezza *cyber*.

[87] Uno dei tratti comuni del complesso *framework* della *cybersecurity* europea e di diritto interno è esattamente la costruzione di un processo di cooperazione e di controllo dei privati, i quali molto spesso sono introiettati nei dispositivi di gestione pubblica della sicurezza digitale.

In termini di essenzialità di questa cooperazione, M. SANTANIELLO, *Monocratic cybersecurity*, in *Rivista di Digital Politics*, 3, 2022, p. 317.

Vero è che solo una cooperazione leale con i privati può consentire un governo di un fattore tanto complesso e difficilmente giuridificabile come quello del dominio digitale, L. TORCHIA, *Poteri pubblici e poteri privati nel mondo digitale*, in *Il Mulino*, 1, 2024, p. 17.

Questo aspetto, già evidentissimo nelle maglie del *GDPR*, ha portato le autorità a divenire valutatrici della valutazione effettuata dai privati responsabilizzati, così G. CERRINA FERONI, *Le stagioni del Garante. La privacy e il cambiamento del Paese*, in G. CERRINA FERONI (a cura di), *Il ruolo del Garante per la protezione dei dati personali*, Il Mulino, Bologna, 2023, specie pp. 72 e ss.

cittadini, alla luce della presenza costante e organica di soggetti privati[88] introiettati nelle maglie dei dispositivi pubblici di *cybersecurity*, al fine di determinare la presenza ricombinata ma inalterata dell'ordinamento nel digitale.

Esattamente come nel processo chimico di catalisi si assiste alla immissione di una sostanza che propizia l'accelerazione di una reazione a fronte dell'invarianza della sostanza immessa, in questo contesto per 'catalisi' si deve intendere l'immissione del ruolo pubblico all'interno di logiche tecniche e private, quali quelle della innovazione digitale e della sicurezza digitale, mantenendo inalterati i profili essenziali della sfera pubblica e del suo ruolo di garanzia ordinamentale, a partire dalla tutela dei diritti fondamentali e della sovranità.

Non c'è dubbio che la perdurante centralità della Presidenza del Consiglio[89], sia per quanto attiene la modulazione della *Strategia nazionale di cybersicurezza* e della normativa via via approvata, sia per la procedura di nomina, e di eventuale revoca, del Direttore generale di ACN, si muova esattamente lungo la direttrice di un recupero, nel cuore della articolata e laocoontica *governance* della *cybersecurity*, della legittimazione sovrana[90].

La valenza squisitamente strategica della sicurezza digitale, nella sua connessione con la sicurezza nazionale e con la tutela di diritti fondamentali e dei servizi essenziali, impone poi all'attenzione dell'interprete il potere di direttiva su detto tema che residua in capo al Presidente del Consiglio.

In questa misura, è possibile dire che nella frastagliata e stellare modulazione della sicurezza digitale, la Presidenza del Consiglio è ancora, indubbiamente, il canone di ancoraggio e di definizione della, sia pur indiretta[91], legittimazione sovrana da cui, a cascata, viene irradiato il sistema tecnico preposto funzionalmente alla *governance*.

---

[88] A. SIMONCINI, E. LONGO, *Fundamental Rights and the Rule of Law in the Algorithmic Society*, p. 33, per il ruolo pubblico esercitato fattualmente dai grandi soggetti privati.

[89] Propiziata anche dal verticismo funzionale connaturato allo sviluppo e alla attuazione del PNRR, il quale come noto è anche devoluto alla digitalizzazione del Paese, così S. CALZOLAIO, *Autorità indipendenti e di governo della società digitale*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 102.

[90] T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, cit., p. 288.

[91] È noto come l'indirizzo politico non sia esclusiva del Presidente del Consiglio, pertenendo anche al Parlamento, organo naturale di estrinsecazione della rappresentanza dell'esercizio sovrano da parte del popolo, mediante il voto. Ma al Presidente del Consiglio spetta una delicatissima operazione dinamica di mantenimento dell'equilibrio e dell'unità dell'indirizzo politico, mediando egli tra distinte sensibilità che compongono il Governo e sovente raccordandosi con le forze politico-partitiche presenti in Parlamento, così I. CIOLLI, *La questione del vertice di Palazzo Chigi. Il Presidente del Consiglio nella Costituzione repubblicana*, Jovene editore, Napoli, 2018, p. 127.

In secondo luogo, la formula 'catalitica' si caratterizza per la commistione di elementi propriamente regolatori e giuridici con altri afferenti altre dinamiche e discipline: casi paradigmatici, quelli della cyber-resilienza e della cyber-diplomazia[92].

Entrambi si presentano come marcatamente contraddistinti dalla presenza di soggetti privati, i quali vengono responsabilizzati e 'governati' non in chiave meramente regolatoria e dirigistica in ogni singolo passo decisionale ma tendenzialmente lasciandoli liberi di produrre la loro rete di sicurezza e i loro prodotti, nel quadro generale dato dal potere pubblico[93]: un potere pubblico che rimarrà puntellato dai propri sistemi di *compliance* e di legittimazione, senza però entrare nel merito delle scelte di difesa digitale adottate dai vari soggetti privati, le quali dovranno rispondere a una funzione e a un risultato, come indicato dai paradigmi di '*cybersecurity by design*'.

Sarebbe d'altronde impossibile, e impensabile, una modellazione infrastrutturale ossificata *ex lege*, dovendosi al contrario operare caso per caso, segmento aziendale per segmento aziendale, struttura amministrativa per struttura amministrativa.

Ed è proprio in questo ambito che la presenza del potere pubblico esplica due funzioni essenziali. La permanenza inalterata degli schemi garantistici ordinamentali, da un lato, e dall'altro lato la modellazione della fisionomia del sistema di *governance*.

La *governance* della *cybersecurity* diviene un elemento fondamentale, per due motivi.

La sua estensione è devoluta a evitare che vulnerabilità nel sistema si possano estendere fino al punto di non ritorno.

E in secondo luogo ad una quasi geologica stratificazione normativa[94], consegue la problematicità dei meccanismi di controllo, di garanzia e di tutela dei diritti dei

---

[92] M. SGUAZZINI, M. DI GIULIO, *Toward a Catalytic State?,* cit., p. 60, focalizzano l'attenzione sul *Cyber Diplomacy Toolbox* approvato dal Consiglio UE nel 2017 e che consiste nella legittimazione alla risposta diplomatica e di sanzioni internazionali contro cyber-attacchi.

[93] Auspica giustamente un approccio co-regolatorio, scolpito dagli indirizzi offerti da ACN, G. G. CUSENZA, *I poteri dell'Agenzia per la cybersicurezza nazionale: una nuova regolazione del mercato cibernetico*, in R. URSI (a cura di) *La sicurezza nel cyberspazio*, FrancoAngeli, Milano, 2023, p. 130.

[94] Limitandosi al solo caso italiano, si pensi all'adozione del decreto-legge n. 105/2019.

Detto d.l. e i successivi decreti attuativi, DPCM n. 131/2020, DPCM n. 81/2021, DPCM n. 198/2021, DPCM n. 4/2022, hanno istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC).

Il PSNC elenca tutti gli attori pubblici e privati coinvolti nella protezione del Paese.

cittadini: qui si esalta e apprezza ancora di più la necessità che le varie autorità si rendano per cittadini, imprese, amministrazioni, stelle polari[95] nella applicazione e nella gestione concreta delle norme e degli incombenti *cyber*.

Il sistema di orizzontalità direttoriale che dall'ENISA discende attraverso le autorità nazionali, per gli CSIRT[96] e poi ascende di nuovo, come nel caso delle

---

Oltre quelli che operano nel settore governativo, il PSNC include entità pubbliche o private.

Nel 2021 inoltre, con il decreto legge n. 82/2019, è stata istituita l'Agenzia per la Cybersicurezza Nazionale (ACN).

L'ACN ha ridisegnato il quadro istituzionale per la *cybersecurity* e ha assunto la guida nella direzione e nel controllo della politica di *cybersecurity.*

Nel 2022 l'Agenzia ha elaborato la *Strategia nazionale di cybersecurity* 2022-2026 e il relativo *Piano di attuazione* che comprende 82 interventi per il miglioramento della resilienza informatica.

Sui profili di organizzazione di questo stratificato sistema, A. RENZI, *La sicurezza cibernetica: lo stato dell'arte*, in *Giornale di Diritto Amministrativo*, 4, 2021, pp. 538 e ss., B. CAROTTI, *Sicurezza cibernetica e Stato-nazione*, in *Giornale di Diritto Amministrativo*, 5, 2020, pp. 629 e ss.

[95] Non è certo casuale come questi organismi presentino matrice, natura e funzioni diverse.

ACN è autorità di governo, non indipendente, mentre il Garante per la protezione dei dati personali è tipicamente autorità di governo ma indipendente, S. CALZOLAIO, *Autorità indipendenti e di governo della società digitale,* cit., pp. 99 e ss.

La strutturazione in unico dispositivo di istituzioni diverse, sia ontologicamente che funzionalmente, opera come scudo di protezione del sempre più esteso spazio digitale, embricando tra loro logiche e strumenti diversi. In questa prospettiva, la diversità cooperativa assume anche una valenza di controlli incrociati tra autorità stesse, al fine di garantire la piena tutela dei diritti dei consociati.

[96] Il "*Team di risposta agli incidenti di sicurezza informatica*" adempie compiti di prevenzione delle minacce informatiche, ha funzioni di risposta e assistenza in caso di incidenti nonché di coordinamento e cooperazione in risposta a incidenti di sicurezza informatica.

CSIRT, istituito presso l'ACN, è stato arricchito di nuove funzioni, correlate alla vulnerabilità dei sistemi informatici e di rete; in questa prospettiva, l'art. 12, direttiva UE n. 2022/2555 ha introdotto importanti novità in tema di divulgazione coordinata delle vulnerabilità.

Lo stesso articolo ha peraltro istituito in capo ad ENISA una banca dati europea delle vulnerabilità.

notifiche e delle segnalazioni, all'ENISA[97], snuda un meccanismo complesso, che sa di non potersi permettere l'emersione della minima vulnerabilità e di cui sono parte anche altre autorità, a livello europeo e nazionale, come i Garanti *privacy*, al fine di contemperare sicurezza e diritti.

In questo senso può quindi dirsi che lo Stato 'catalitico' della *cybersecurity* si caratterizzi per: una sovranità funzionalmente ricombinante che sintetizza in maniera procedurale sicurezza nazionale e sicurezza nel dominio digitale, adottando due canali normativi tra loro combinati, una collaborazione pubblico-privato e pubblico-pubblico di matrice radicalmente nuova rispetto il passato, con modalità nuove di controllo e soprattutto non più devoluta a un mero quadro regolatorio e mercatorio ma di protezione dei diritti fondamentali rimessi anche all'operato delle autorità garanti e con la permanenza al centro del sistema degli organismi indirettamente e direttamente connessi alla sovranità, come la Presidenza del Consiglio e, sul versante della sicurezza nazionale, il Parlamento, elevatissima *expertise* tecnica dei soggetti chiamati a presidiare lo spazio digitale.

### *4.1 La tutela dei diritti*

Caratteristica essenziale di questa nuova forma di *governance* dello spazio digitale, innervata nella fisionomia funzionalmente catalitica, è quella di ricombinare la sovranità 'analogica', storica e fisica, con quella digitale, creando nei fatti un doppio canale sintetizzato che operi nel mondo degli atomi e in quello dei *bit*, nella dimensione nazionale e in quella euro-unitaria.

Da un lato, il mantenimento stesso dell'ordinamento, la sua sopravvivenza, è garanzia dei consociati.

Ma più nello specifico, si tratta di un modello partecipato e integrato, che vede flussi collaborativi, cooperativi, informativi, tra istituzioni pubbliche del singolo Paese, di Paesi differenti e con soggetti privati, sempre più coinvolti in un sistema che rievoca non banalmente i modelli di sicurezza integrata.

La sicurezza integrata, prevista e disciplinata dal d.l. 20 febbraio 2017, n. 14, convertito con modificazioni in legge 18 aprile 2017, n. 48, indica come cornice di riferimento e come elementi ordinali lo scambio informativo tra autorità, *governance* multilivello, partecipazione di soggetti privati e dell'associazionismo[98].

---

[97] S. CALZOLAIO, *Autorità indipendenti e di governo della società digitale,* cit., p. 90.

[98] Uno degli aspetti salienti della sicurezza integrata è quello della copertura più ampia possibile in chiave di lotta al terrorismo e al crimine del territorio, proprio attraverso una integrazione funzionale dei distinti livelli di governo.

Questo aspetto non si traduce soltanto in cooperazione e coordinamento e in scambio informativo tra livelli diversi di governo e di amministrazione ma anche nella valorizzazione proattiva degli organismi periferici delle amministrazioni centrali, come ad esempio nella

In questo senso, se la sicurezza integrata è declinazione empirica della sussidiarietà, può dirsi che la *cybersecurity* alla luce degli approdi più recenti sia manifestazione della sussidiarietà digitale e del decentramento funzionale tipologicamente connaturato alle reti digitali.

Per sussidiarietà digitale, si intende il processo collaborativo tra dimensione pubblica e soggetti privati i cui impulsi e i cui sforzi hanno modellato, con la loro innovazione, la frontiera digitale, l'elaborazione dei *software* e i codici tecnici del digitale, mantenendo tra loro un necessitato punto di equilibrio[99].

---

stesura dei patti per la sicurezza e nella elaborazione di linee guida di intervento, ampiamente F. PASTORE, *Il coordinamento delle forze di polizia e di sicurezza italiane nella lotta al terrorismo*, in *Dirittifondamentali.it*, 2, 2021, pp. 12 e ss.

[99] M. DURANTE, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Giappichelli, Torino, 2007, diffusamente pp. 112 e ss., rileva come diventi necessario tornare alla dimensione collaborativa della sperimentazione scientifica e tecnica, alla esplorazione non escludente, come era auspicato nella generale ottica del decentramento tecnico dai primissimi programmatori e scienziati che hanno avuto modo di relazionarsi con Internet e con le Intelligenze Artificiali.

L. TOVARLDS, D. DIAMOND, *Rivoluzionario per caso. Linux*, Garzanti, Milano, 2001, hanno evidenziato come uno dei risultati più straordinari del progetto di sviluppo del *software* libero siano stati certamente i *kernel*, frutto di un sistema di produzione orizzontale e tendenzialmente paritaria, sussidiaria appunto, tra apparati pubblici e innovatori privati, fossero società o singoli individui.

Il *kernel* è una chiave di accesso al sistema operativo che permette una maggiore sicurezza e una maggiore adattività del sistema e che finisce con l'integrare gli estremi di piena sussidiarietà digitale e di un'autentica, basilare sicurezza digitale *by design* oggi sussunta, come concetto, in maniera cristallina nei dispositivi normativi dell'UE, nel prisma della cyber-resilienza.

Il *kernel* è una delle principali componenti operative del progetto GNU e è stato cesellato dal lavoro congiunto di vari operatori che non si sono limitati ciascuno a modificare o cambiare una parte del tutto ma a lavorare direttamente sul tutto nella prospettiva di una modifica strutturale del modo di produzione del *software*.

Y. BENKLER, *La ricchezza della rete*, Università Bocconi Edizioni, Milano, 2007, p. 83, ha sottolineato come il sistema di produzione di *software* libero e del *kernel* si basassero su contributi volontari e sulla condivisione ubiquitaria e ricorsiva: dai miglioramenti incrementali apportati a un progetto da persone sparse sul globo, con alcuni che davano sostanziali contributi e altri minori.

In prospettiva di *cybersecurity*, ciò deve tradursi nella valorizzazione proattiva del ruolo dei privati in un generale quadro di *governance* pubblica che mantenga saldo il baricentro della decisione politico-sovrana, aspetto questo che la più recente normativa, a partire da quella sulla cyber-resilienza, sembra cogliere in maniera nitida.

Il decentramento funzionale è al contrario la caratterizzazione della architettura degli snodi comunicativi e connettivi delle reti, una dimensione multidimensionale che interseca tra loro attori pubblici e privati nella prospettiva non della innovazione ma in quella della gestione e del governo del digitale.

Non c'è alcun dubbio che la cyber-resilienza, ovvero un approccio che mescola elementi regolatori con forme privatistiche ed *expertise* tecnica con perdurante presenza garantistica del potere statale, sia esattamente sussidiarietà digitale.

Esemplare il protocollo siglato nel 2022 tra Garante per la protezione dei dati personali e ACN per stabilire una organica cooperazione tra le due istituzioni al fine di un coerente ed efficace esercizio delle proprie competenze.

Un protocollo che oltre a definire una *actio finium regundorum*, onde evitare sovrapposizioni, presenta anche connotazioni spiccatamente proattive, essendo devoluto alla promozione di iniziative congiunte in tema di cybersicurezza nazionale e di protezione dei dati personali.

L'aspetto evidentemente 'integrato' consiste anche nella facilitazione di interlocuzioni e di scambio informativo e di comune opera di definizione di *best practices* sulla sicurezza digitale, non trascurando l'apporto che il mondo accademico potrà fornire.

Come si intuisce agevolmente, si tratta esattamente di uno spazio aperto, collaborativo, dal 'basso[100]', che vede operare in stretta sinergia soggetti pubblici, soggetti privati, società civile, mondo culturale e universitario, esattamente come nella sicurezza pubblica integrata si trovano, fianco a fianco, diversi livelli delle autorità pubbliche, imprese, società civile, singoli cittadini.

Se la sopravvivenza dell'ordinamento a fronte di minacce digitali esterne, portate cioè da attori ostili, si muove lungo il campo duplice già illustrato della sicurezza nazionale e della sicurezza digitale, tra loro embricate, per determinare cataliticamente la sussistenza dei principi costituzionali nel cuore della sovranità digitale, vi è però da illustrare il portato delle garanzie del cittadino a fronte dell'espansione della sfera di sicurezza e di controllo.

In questo senso, in un sistema basato cardinalmente su informazioni e dati la protezione dei dati personali, quando coinvolti nel complesso meccanismo di *cyber information sharing*, assume una coloritura ancora più determinante ed essenziale, come riconosciuto espressamente dal considerando 22 della proposta di Regolamento *EU Cyber Solidarity Act*.

La trasmissione di informazioni per fini di sicurezza ha visto riconoscere come proprio fondamento giuridico l'art. 6, par. 1, lett. f) *GDPR*, dovendosi poi concretamente, di volta in volta, procedere ad un bilanciamento tra diritti in gioco

---

[100] L. PREVITI, *Pubblici poteri e cybersicurezza*, cit., p. 82.

e alla valutazione sulla base dei criteri di necessità, legittimità e bilanciamento tra gli interessi[101].

Dal punto di vista invece del materiale trattamento di dati da parte di autorità, per fini che potrebbero integrare gli estremi della sicurezza digitale, come ha riconosciuto la giurisprudenza della Corte di Giustizia[102], sarà necessario di volta in volta procedere al bilanciamento tra i diritti del singolo e le esigenze statali: infatti, gli articoli 7, 8 e 11 CEDU non scolpiscono diritti assoluti, ma che, di contro, devono essere concretamente calati nel loro contesto, valutati e bilanciati[103].

Appare infatti palese, da una lettura dei considerando 49 e 50 GDPR, come il trattamento dei dati per fini di sicurezza digitale, intendendo qui nel senso più ampio possibile il termine, rientri nell'interesse del titolare del trattamento, proprio perché i dispositivi di sicurezza digitale sono funzionali alla protezione dei diritti e dei dati.

In questa prospettiva si intuisce agevolmente come trovino sintesi i concetti enucleati di sovranità digitale, di sicurezza digitale e di *cybersecurity*, nei vari livelli e significati sin qui espressi.

Tra loro connessi, determinano la legittimazione degli interventi, il loro fine, la tecnica degli interventi, gli elementi sostanziali e giuridici che ne sono alla base, l'organizzazione delle strutture a ciò preposte e i livelli e meccanismi di tutela dei diritti di cui possa fruire il cittadino contro attori ostili pubblici o privati.

In questa chiave di lettura, i diritti sono protetti dal sistema integrato di sicurezza digitale, mediante collaborazione tra utenti, imprese e istituzioni, al fine di bilanciare esigenza di sicurezza, libertà e diritti fondamentali.

---

[101] Altri autori in realtà hanno individuato l'articolo 6 par. 1, lett. c) oppure art. 6 par. 1 lett. e) *GDPR*, distinguendo tra trattamento funzionale a un obbligo legale, nel primo caso, oppure esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, considerando che la circolazione di dati nel settore cyber non necessariamente deve riguardare organismi di polizia, sul punto ampiamente F. SERINI, *Il sistema europeo di cooperazione informativa*, cit., p. 178.

[102] Si veda in particolare la sentenza CGUE *Tele2 Sverige e Watson* del 21 dicembre 2016 (cause riunite C-203/15 e C-698/15).

[103] M. MAURINO, *Cybersecurity, sicurezza nazionale e trattamento dei dati personali*, in R. URSI (a cura di), *La sicurezza nel cyberspazio*, FrancoAngeli, Milano, 2023, specie pp. 183 e ss.

Sottolinea giustamente A. SIMONCINI, *Do ut data: quali limiti costituzionali alla cessione dei dati personali*, in G. CERRINA FERONI (a cura di), *Commercabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Il Mulino, Bologna, 2024, p. 62, come la previsione dell'art. 8 CEDU non sia assoluta e debba di volta in volta essere valutata e bilanciata. Da qui, la necessitata presenza di una autorità indipendente.

Per stabilire cioè, se *an* e *quantum* di tutela offerta, siano ragionevoli, proporzionali e soprattutto conferenti al *framework* normativo.

Ne consegue che nell'intricato reticolo di *governance*, se da un lato si accresce il ruolo di organismi come ACN[104], dall'altro lato funzione di tutela e di presidio, nel senso anche di tutela dei diritti fondamentali e di legittimazione sovrana, ancora più rilevante acquisiscono le autorità di protezione dei dati personali, come il GPDP, e tutti gli attori, dalla Presidenza del Consiglio ad AGID, chiamati a governare l'ecosistema digitale[105].

In questa prospettiva, la tutela dei diritti, al di là degli ovvi aspetti giudiziali che permangono integrali, è garantita da un *framework* complesso che parte dal perdurare della legittimazione sovrana nel cuore dei dispositivi di *governance* della sicurezza digitale, passa per la integrazione collaborativa tra autorità e privati e arriva alla elaborazione di modelli resilienti e capaci, *by design*, di contemperare protezione dei dati e protezione delle reti.

Il quadro che ne risulta è quello di una piena integrazione armonica e collaborativa, devoluta al mantenimento, in delicato equilibrio, della sicurezza e dei diritti dei consociati.

### *4.2 Il recepimento di NIS 2 in Italia e la legge 28 giugno 2024, n. 90*

Il Consiglio dei Ministri, in data 10 giugno 2024, ha approvato lo schema di decreto legislativo relativo al recepimento della direttiva UE n. 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento UE n. 910/2014 e della direttiva UE n. 2018/1972 e che abroga la direttiva UE 2016/1148.

Lo schema è poi divenuto il decreto legislativo 4 settembre 2024, n. 138 pubblicato in Gazzetta Ufficiale il 1° ottobre 2024.

---

[104] S. CALZOLAIO, *Autorità indipendenti e di governo della società digitale*, cit., pp. 99 e ss.

Di 'ruolo strategico', parla I. FORGIONE, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in R. URSI (a cura di), *La sicurezza nel cyberspazio*, FrancoAngeli, Milano, 2023, pp. 95 e ss.

[105] Lo stesso considerando 63 della direttiva NIS, direttiva UE n. 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 nell'Unione, GU L 194/1, osserva la possibile compromissione di dati personali a seguito di evento con un impatto sulla sicurezza della rete e dei sistemi informativi, ragion per cui, poi, nel corpo della Direttiva si delinea, una rete di collaborazione e scambio di informazioni tra autorità.

I principi e i criteri direttivi che il governo era tenuto ad ossequiare sono contenuti nella legge 21 febbraio 2024, n. 15.

Si tratta di cinque macro-gruppi[106], identificabili con:

1) l'orizzonte dei soggetti pubblici tenuti al rispetto delle nuove previsioni normative
2) i soggetti a livello centrale chiamati a occuparsi di cybersicurezza
3) i destinatari delle nuove norme
4) la divulgazione coordinata delle vulnerabilità procedendo ad un adeguamento della normativa anche se del caso con la introduzione di nuove fattispecie di reato
5) il sistema sanzionatorio amministrativo.

Il decreto legislativo, che consta di 44 articoli e di 4 allegati, rafforza ancora di più il ruolo di coordinamento devoluto in capo all'ACN[107], evolve la dimensione di collaborazione e di cooperazione tra autorità[108] e tra soggetti pubblici e privati, al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala e di tutela dei diritti[109], prevede l'ampliamento dell'ambito soggettivo di applicazione della disciplina di *cybersecurity*[110], confermando l'approccio funzionalmente 'catalitico' sin qui delineato.

---

[106] E. LONGO, *La disciplina della cybersicurezza*, cit., pp. 228 e ss.

[107] Art. 1 c. 2, lett. c) e d). Cristallina conferma del modello di *governance* scelto dal legislatore italiano, I. FORGIONE, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del sistema di sicurezza nazionale,* cit., pp. 100-101.

[108] Esemplare in questo senso, l'articolo 14 che detta una disciplina analitica di collaborazione e cooperazione tra ACN e altre autorità, a partire dal GPDP.

[109] Con le previsioni di cui all'art. 14, c. 2, lett. a), b), c), si rafforza il ruolo del Garante per la protezione dei dati personali in tema di vigilanza su eventuali violazioni dei dati personali derivanti da attacco *cyber*, su segnalazione da parte di ACN.

[110] I commi 1 e 2 dell'articolo 3 prevedono che nell'ambito di applicazione del decreto rientrano i soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV i quali sono sottoposti alla giurisdizione nazionale ai sensi dell'articolo 5.

Gli allegati I e II descrivono i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e le tipologie di soggetto.

Gli allegati III e IV includono, rispettivamente, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetto a cui si applica la disciplina contenuta nel decreto.

Detta normativa si applica ai soggetti delle tipologie di cui agli allegati I e II, che superano i massimali per le piccole imprese ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE.

Merita sottolineare in questo senso la distinzione operata tra "*soggetti essenziali*[111]" e "*soggetti importanti*[112]", e l'adozione di un criterio dimensionale per la loro individuazione.

L'articolo 7 del decreto poi stabilisce che i soggetti essenziali e importanti sono tenuti all'obbligo di registrazione, e in seguito di aggiornamento dei dati richiesti, su apposita piattaforma digitale, ai fini di un costante monitoraggio della loro attività e delle loro dimensioni da parte dell'autorità nazionale competente NIS.

Il decreto sancisce, all'articolo 4, in maniera molto netta, "*la responsabilità dello Stato italiano di tutelare la sicurezza nazionale e il suo potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico*", nonostante come appare evidente, per quanto sin qui detto, la sicurezza nazionale in chiave cibernetica sia attratta anche nella sfera euro-unitaria.

Appare infatti impossibile scindere empiricamente e realisticamente, nella prospettiva del mantenimento della sovranità digitale e della sicurezza digitale, un livello del tutto esclusivamente singolo-nazionale da uno europeo.

Le interconnessioni a rete squisitamente multilivello tra infrastrutture digitali e il decentramento funzionale della stessa *governance* della sicurezza digitale rendono evanescente e liminale la distinzione, la quale certo permane lungo la dorsale della normativa applicabile ma che del pari si combina a sintesi sotto la chiave di volta assiologica dei principi da tutelare e da riaffermare nel cuore di silicio del digitale.

A conferma di questa impostazione, la nuova normativa ambisce a determinare la razionalizzazione dei requisiti minimi di sicurezza e delle procedure di notifica obbligatoria, anche grazie all'adozione di un approccio "multirischio", elemento segnaletico perfezionato di un dispositivo complessivamente cyber-resiliente.

---

[111] Si tratta di **quegli** operatori che erogano servizi di importanza fondamentale, tra i quali per fini esemplificativi possono citarsi i settori dell'energia, della sanità, dei trasporti, delle infrastrutture digitali e dei servizi finanziari**.**

Sono quei soggetti del tutto essenziali per la resilienza del Paese e, naturalmente, dell'Unione Europea. Proprio per questo sono destinatari di una disciplina più stringente e rigorosa.

[112] In questo caso pur essendo in presenza di attività potenzialmente delicata, viene convenzionalmente ritenuto che non si sia in presenza di essenzialità. Si pensi ai sistemi informatici di società che si occupano del ciclo dei rifiuti. Attività importanti e delicate ma che non raggiungono quella soglia di essenzialità rivestita dai soggetti essenziali.

La *ratio* di questa distinzione, lo si può intuire agevolmente, è graduare la focalizzazione della disciplina e degli interventi, regolatori e empirici, da parte di tutti gli organismi che compongo la *governance* della *cybersecurity*.

In tema di coordinamento del sistema di risposta alle crisi digitali, si prevede la regolamentazione della divulgazione coordinata delle vulnerabilità e le specifiche funzioni di coordinamento attribuite a CSIRT.

Il tema del coordinamento è strutturalmente essenziale ed esso punteggia alcune delle norme chiave, oltre a costituire elemento nodale della definizione della *Strategia nazionale di cybersicurezza*; l'articolo 9 c. 2 lett. c) del decreto stabilisce infatti che parte essenziale della *Strategia* è costituita anche dalla presenza di "*un quadro di governance che chiarisca i ruoli e le responsabilità dei pertinenti portatori di interessi a livello nazionale, a sostegno della cooperazione e del coordinamento a livello nazionale tra le Autorità di settore NIS, l'Agenzia per la cybersicurezza nazionale, in qualità di Autorità nazionale competente NIS, di Punto di contatto unico NIS e di CSIRT Italia, nonché il coordinamento e la cooperazione tra tali organismi e le altre autorità competenti ai sensi degli atti giuridici settoriali dell'Unione europea*".

Ma ancor più essenziale è la 'collaborazione', lemma che compare ben venti volte nel decreto e che costituisce punto saliente di un approccio squisitamente 'catalitico'; sia essa collaborazione pubblico-privato o collaborazione tra soggetti e autorità pubbliche, di ogni settore e livello, appare evidente come si assista a una piena integrazione in un unico dispositivo preposto alla tenuta del sistema.

Un dispositivo che è territoriale, nel rapporto tra centro e periferia e tra amministrazioni pubbliche di differente livello, in questo senso si veda il *Tavolo per l'attuazione della disciplina NIS* istituito dall'art. 12 del decreto, e al tempo stesso a-territoriale, funzionale e ascendente verso il perimetro digitale euro-unitario, come nel caso della cooperazione tra autorità preposte al governo di specifici ambiti[113] e alla assistenza reciproca disciplinata dall'articolo 39, oppure ancora chiamato a embricare soggetti privati e soggetti pubblici.

La complessa *governance* delineata estende il perimetro governato e sorvegliato da autorità territoriali le quali finiscono per operare come terminali locali di un sistema che ha il proprio fulcro nell'Unione Europea: la reticolare orizzontalità direttoriale, delineata a raggiera con equi-ordinazione dei poteri e delle funzioni ma con caratterizzazione di direttiva e di indirizzo in capo a Commissione ed ENISA, è figlia della preoccupazione di poter vantare, da un lato, un controllo preventivo e gestionale di eventuali vulnerabilità palesate su base locale e dall'altro lato di determinare una omogeneità di disciplina giuridica e applicativa, senza arrivare però a eccessi di ossificazione formale.

---

[113] Art. 14 commi 1 e 2 disciplinano, come abbiamo visto, la collaborazione tra autorità mentre l'art. 18 è chiamato a disciplinare il gruppo di cooperazione di matrice euro-unitaria e internazionale.

Raffigurazione plastica di quanto si sosteneva a proposito della sovranità ricombinante che in questo reticolo trova maggiore forza, ampliando il proprio raggio di visuale e di azione, pur, in apparenza, finendo modellata tra maglie sovranazionali e non più esclusivamente nazionali.

Opportuna, per questo, la perdurante centralità rimasta in capo alla Presidenza del Consiglio, tanto nel sistema di *governance* quanto nella fase, delicata, di attuazione delle previsioni disciplinate dal decreto; si tratta, come abbiamo visto, di una scelta necessitata ai fini della riaffermazione ordinamentale in un intreccio che fonde tra loro distinti livelli di governo, europeo, nazionale, locale, con corpi tecnici, soggetti privati e che nella Presidenza del Consiglio trova ancoraggio al paradigma della decisione politica indirettamente connessa all'esercizio della sovranità.

La Presidenza del Consiglio, oltre a essere designata dall'art. 11 c. 2 lett. a) autorità NIS in settori come quello TIC, quello dello spazio, delle amministrazioni pubbliche e delle società partecipate e *in house,* a ribadire in maniera esplicita la matrice strategica della *cybersecurity* in alcuni ambiti, adotta con propri decreti, su proposta dell'ACN, i vari elementi funzionali, ai sensi dell'articolo 40 del decreto, alla attuazione della disciplina normativa.

Un ruolo di assoluta centralità, e di sinergia collaborativa con la Presidenza del Consiglio, come si accennava, compete ad ACN. Ai sensi dell'articolo 10 del decreto, ACN è autorità nazionale competente NIS ed è, ai sensi del comma 2 del medesimo articolo, *Punto di contatto unico NIS*.

L'articolo 11, disciplinando le varie autorità NIS di settore, attua quel necessitato decentramento funzionale che coadiuva capillarmente ACN, consentendo una mappatura e un presidio costante del manifestarsi di potenziali vulnerabilità in ambito nazionale.

Abbiamo visto *supra* come la Presidenza sia autorità di settore in ambiti del tutto essenziali e oltre a essa vediamo figurare il Ministero dell'economia e delle finanze, il Ministero delle imprese e del *made in Italy*, il Ministero dell'agricoltura, della sovranità alimentare e delle foreste, il Ministero dell'ambiente e della sicurezza energetica, il Ministero delle infrastrutture e dei trasporti, il Ministero dell'università e della ricerca, il Ministero della salute, il Ministero della cultura, per i settori a maggior tasso di esposizione digitale rientranti nell'alveo delle loro competenze istituzionali e funzionali.

Nel giugno scorso è stata poi approvata la legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Il provvedimento, che consta di 24 articoli, oltre a incidere significativamente sull'introduzione di nuove fattispecie incriminatrici, cui è devoluto l'intero capo II, articoli da 16 a 23, delinea un procedimento amministrativo sanzionatorio per

cui è competente ACN[114] e che dovrà in particolare definire "*termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni*".

Il Regolamento di questo procedimento sanzionatorio dovrà essere adottato con Dpcm, anche in deroga all'articolo 17 c. 3 della legge 23 agosto 1988, n. 400, sentito il Comitato interministeriale per la cybersicurezza e acquisito il parere delle competenti Commissioni parlamentari. Provvisoriamente e nelle more della adozione del Regolamento, si applicheranno le norme della legge 24 novembre 1981, n. 689.

Merita menzione l'articolo 14 recante "*disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*": dalla norma emerge in maniera inequivoca la centralità del dispositivo di sicurezza *cyber* in ambito strategico e soprattutto in funzione di sicurezza integrata tra Paesi UE e di area NATO.

Conferma di quanto già rilevato, ovvero della inevitabile convergenza tra *cybersecurity* propriamente intesa e difesa *cyber*. In questo caso, la contrattualistica pubblica funzionalmente devoluta alla acquisizione di beni e di servizi informatici serventi esigenze strategiche nazionali viene rinforzata dalla necessitata elencazione dei requisiti essenziali di cybersicurezza che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, dovranno possedere e dalla previsione di criteri di "*premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO)".*

L'elencazione in parola sarà contenuta in un decreto del Presidente del Consiglio, adottato su proposta di ACN e previo parere del Comitato interministeriale per la sicurezza della Repubblica.

La legge poi ambisce a ampliare significativamente l'andamento modulare della resilienza delle pubbliche amministrazioni[115], prevedendo la nuova figura del *Referente per la cybersicurezza*.

Figura che dovrà possedere specifiche e comprovate professionalità e competenze in materia di cybersicurezza e che svolgerà, tra l'altro, la funzione di

---

[114] Art. 11, "*Procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'Agenzia per la cybersicurezza nazionale".*

[115] Art. 8, significativamente rubricato "*Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza*".

punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale.

Criticabile la previsione di cui all'art. 8 c. 3 che facoltizza le amministrazioni a individuare detto referente nell'ufficio del responsabile per la transizione al digitale, generando una sovrapposizione, potenziale e attuale, tra figure.

Scelta che non appare del tutto perspicua.

Infatti, il responsabile per la transizione al digitale, introdotto dai decreti legislativi 26 agosto 2016, n. 179 e 13 dicembre 2017, n. 217 che hanno novellato il d. lgs. 7 marzo 2005, n. 82, codice dell'amministrazione digitale (CAD), è figura di coordinamento con AGID e ha compiti che ricadono nell'alveo normativo del citato CAD.

In genere in ambito ministeriale questa qualifica è assegnata a direttori generali che non hanno l'esclusiva direzione dell'ufficio in parola ma di intere direzioni generali, con tutte le implicazioni e le complicazioni del caso.

Pensare di insignire queste stesse figure, rendendo le loro strutture anche strutture di supporto del referente per la cybersicurezza, di una ulteriore qualifica, tanto delicata, significa nutrire un approccio puramente formalistico e che mal si sposa con quell'attitudine funzionalmente devoluta alla copertura di qualunque possibile vulnerabilità e che è cifra sostanziale dei dispositivi di sicurezza digitale.

Non sfugge naturalmente la problematica situazione di ordine finanziario in cui versano molte amministrazioni né la scarsità, spesso, di figure munite della necessitata e richiesta alta qualificazione, ma questi aspetti rappresentano sprone sia per l'utilizzo e l'impiego materiale di risorse pubbliche, devolute tanto alla innovazione digitale quanto alla sicurezza cibernetica, sia per una rimodulazione del reperimento del personale nelle pubbliche amministrazioni, superando auspicabilmente un approccio ossificato ed esclusivamente giuridico-formale e soprattutto superando anche la fisionomia delle attuali modalità di reperimento di personale[116].

---

[116] Appare del tutto palese come, se nelle autorità che presiedono e popolano il sistema di *governance* l'*expertise* richiesta è molto alta, non diversamente da quanto avviene nella galassia delle autorità indipendenti e delle agenzie, del pari i soggetti che ne sono referenti, pur incardinati in strutture amministrative diverse, siano essi Ministeri, altre agenzie, Regioni, Comuni, dovranno saper parlare lo stesso linguaggio e essere muniti di elevata qualificazione.

Ciò non può valere solo per la figura del referente, ma è considerazione che deve essere estesa anche alle figure che più strettamente gli sono vicine e lo coadiuvano.

Ne consegue che dovrà mutare la fisiologia e la tenuta dei concorsi pubblici e delle modalità di reclutamento del personale, anche mediante l'istituzione di specifici albi per la collaborazione di esperti, contrattualizzati per un arco temporale determinato.

Peraltro, le perplessità aumentano laddove si consideri l'intreccio tra nuove responsabilità previste dall'articolo 1 c. 6 della legge n. 90/2024, in tema di obbligo di notifica di incidenti informatici, e dall'articolo 38 c. 7 del d.lgs. n. 138/2024, concernente una responsabilità più ampia e generale per il mancato adempimento delle previsioni contenute nel decreto di attuazione di NIS 2.

Nei fatti, siamo in presenza di una responsabilità geometricamente triangolare, amministrativa da un lato, per quanto concerne l'azione di ACN e disciplinare e contabile dall'altro, per i profili di competenza datoriali e poi eventualmente della Corte dei Conti, con la potenziale sanzione irrogata da ACN e quelle che potrebbero invece essere irrogate dall' amministrazione di appartenenza, con procedimenti, provvedimenti e strumenti di tutela del tutto diversi.

Oltre al non del tutto lineare coordinamento tra le varie responsabilità, che appaiono appartenere a *genus* distinti, seguire linee operative altrettanto distinte ma rispondere alla medesima funzione, si può evidenziare come la figura del referente sia investita di una forma talmente avvolgente e cogente di obblighi e doveri, il cui mancato adempimento si può tradurre in conseguenze sanzionatorie pecuniarie gravi e disciplinari non meno gravi, da dover preferire la sua autonomizzazione rispetto pregresse e già esistenti figure nelle maglie delle amministrazioni.

## 5. Una conclusione (necessariamente provvisoria)

Nell'originaria formulazione dell'ordine del giorno del Consiglio dei Ministri n. 109 del 29 ottobre 2024 è apparso in discussione un decreto-legge recante "*misure*

---

I soggetti aventi le caratteristiche e le qualifiche di studio, cultura e esperienza saranno inseriti in questo albo per singoli incarichi ad altissimo contenuto specialistico, secondo un modello che già l'attuazione PNRR ha in certa misura largamente istituzionalizzato.

E potrebbe pensarsi di utilizzare proficuamente la lezione istituzionale del citato PNRR, iniziando a valorizzare in maniera proattiva l'alta formazione universitaria, i corsi di specializzazione, i *master* specificamente legati alla *cybersecurity*, per il personale già assunto e presente tra i ranghi delle amministrazioni, necessitandosi di una formazione continua che potrebbe essere cesellata sul modello di '*Valore P.A.'* dell'INPS e in questo caso gestita da ACN, e soprattutto i dottorati e gli assegni di ricerca conferenti per materie e disciplina laddove vi sia necessità di immissione e di reperimento di figure altamente specializzate.

Per queste due ultime figure, quelle dei dottorati e degli assegni di ricerca, potrebbe pensarsi all'albo di cui si parlava *supra*, stabilendo caratteristiche e qualifiche per la possibilità di iscrizione, tra cui oltre a quei titoli inserire pregresse esperienze lavorative, di ricerca e professionali nell'ambito *cyber*.

*urgenti di ordinamento giudiziario, di personale di magistratura, di incarichi dirigenziali e di competenza investigativa sulla criminalità informatica*".

Successivamente il testo è stato stralciato dalla discussione ma è verosimile pensare torni nelle sedute successive del Consiglio: si tratta di un tentativo di risposta alle varie indagini giudiziarie che stanno scuotendo il Paese, rimandando esse il quadro di inchiesta su plurimi e massivi accessi abusivi alle principali banche dati delle strutture pubbliche italiane, per fini illeciti di dossieraggio anche su alte figure istituzionali.

Si tratterebbe, nel caso della citata bozza di decreto-legge, di un nuovo capitolo normativo in tema *cybersecurity* e di contrasto al *cyber-crime*, decisamente significativo per il suo impatto e per l'ambito di riferimento, quello delle competenze investigative in tema di crimine digitale e di legittimazione per accedere alle banche dati, in un anno, il 2024, già interessato dalla attuazione di NIS2 e dalla approvazione della legge n. 90/2024.

Tutti i provvedimenti legislativi sin qui citati e analizzati avranno lunga e complessa fase di attuazione, scandita per gli attori istituzionali dalla necessitata adozione di atti regolamentari e di indirizzo e per amministrazioni pubbliche e imprese da adempimenti procedurali, ossequio a incombenti amministrativi e di adeguamento della morfologia stessa delle loro strutture per rispondere alla prospettiva multidimensionale e interconnessa dei rischi digitali.

Si tratta di una sfida che senza retorica può essere definita epocale, perché il *framework* complessivo, seguendo la tripartizione tassonomica teorizzata in questo saggio, tra sovranità digitale, sicurezza digitale e *cybersecurity,* si estende al di là della normativa espressamente ed esclusivamente dettata in tema di *cybersecurity*.

Non c'è dubbio alcuno infatti che, riguardando la questione nella angolazione prospettica della sovranità digitale, debbano tra loro essere armonizzate anche le norme dell'*AI Act,* quelle del *DSA* e del *DMA* e sul versante interno quelle concernenti la declinazione digitale del *golden power* e della sicurezza nazionale, al fine di garantire la tenuta dell'ordine costituzionale e le garanzie in tema di diritti e di libertà dei cittadini.

Questo processo finisce inevitabilmente per ancorare in maniera sempre più significativa la sovranità nazionale a quella euro-unitaria, generando un nesso di interdipendenza funzionale per cui, nella dimensione digitale, l'una finirà per essere sempre più strettamente connessa all'altra e viceversa.

In questo senso, le limitazioni della sovranità nazionale finiscono per determinare un rafforzamento della stessa, presidiando a livello di spazio europeo una sovranità ricombinata e potenziata dalla sintesi delle singole sovranità nazionali coagulate attorno la normativa europea e le istituzioni europee.

Proprio le istituzioni europee, la Commissione in primo luogo, assumono un ruolo centrale di raccordo e di armonico coordinamento del *framework* di governo

della società digitale[117], considerata lungo l'orizzonte della sovranità: è la Commissione infatti a sovrintendere, in questo caso con ENISA, i dispositivi di *cybersecurity*, ma è sempre la Commissione a vigilare sul mercato unico digitale e sulla intelligenza artificiale, operando come necessitato snodo connettivo di tutti i frammenti regolatori concernenti il digitale, nelle varie sfumature e articolazioni.

Questo aspetto determina, inevitabilmente, una spinta sempre più potente e accelerata verso l'integrazione normativa di regolazione del digitale tra Stati e dimensione euro-unitaria, producendo la fisionomia di una già richiamata *cybersecurity* integrata.

Del pari, la spinta pone in maniera sempre più evidente la forma nuova delle dinamiche di collaborazione tra attori pubblici e soprattutto tra sfera statale e soggetti privati, verso quella prospettiva 'catalitica' sin qui discussa.

Proprio per questo, il sistema di *governance* della *cybersecurity* assume connotazioni sempre più delicate proprio sul versante di garanzia e di tutela dei diritti dei cittadini, assistendosi a una tendenziale integrazione tra autorità politiche e autorità di regolazione e di governo.

Da un lato, sul versante nazionale, si rafforza la esigenza della centralità del momento politico-decisionale nel governo della *cybersecurity*, declinabile nella presenza, come fulcro di rappresentanza indiretta del circuito di esercizio della sovranità, della Presidenza del Consiglio, e dall'altro nella integrazione collaborativa tra autorità, da ACN al GPDP.

La prospettiva finale è quella di determinare la costituzione di un sistema a rete in cui i terminali della azione pratica del digitale, amministrazioni e imprese, si trovino in posizione di modellare *by design*, su spinta della normativa via via approvata, i loro processi operativi e le loro architetture organizzative ossequiando la sicurezza digitale, avendo nelle citate autorità dei preziosi alleati e non solo dei meri controllori.

Per accompagnare questo assai complesso percorso, è altresì necessario sviluppare una organica e coerente cultura della sicurezza digitale, mediante opera di disseminazione reticolare di matrice tanto teorico-generale quanto operativa, coinvolgendo ad ogni livello esperti, pratici e accademia, secondo la preziosa lezione già snudata in tema di digitale dal PNRR.

Il governo costituzionalmente orientato della sicurezza digitale, un autentico ordine costituzionale della *cybersecurity* nel senso esteso che nel presente lavoro si è voluto illustrare, deve tradursi, in considerazione della sempre più spinta tecnologizzazione dei dispositivi di protezione informatica, anche nella tutela egualitaria dei diritti e delle libertà dei cittadini avendo sempre come stella polare

---

[117] F. PIZZETTI, *Introduzione alla regolazione europea della società digitale*, cit. p. 4.

un nuovo umanesimo digitale[118] che sappia coniugare sovranità italiana e sovranità euro-unitaria, sicurezza e libertà, umanità e automazione digitale, innovazione e diritti costituzionalmente tutelati.

Per approdare a questo ambizioso e impegnativo traguardo, si deve guardare ai distinti piani, quello della sovranità digitale, quello della sicurezza digitale e quello della *cybersecurity*, connettendoli tra loro in un dispositivo unico.

Strada che la normativa europea e quella italiana stanno, indubbiamente, percorrendo con consapevolezza, al fine di vincere una sfida tanto delicata.

Una sfida necessariamente *in fieri*[119] e le cui soluzioni e i cui effetti potranno e dovranno essere apprezzati e valutati lungo il cammino, ma del pari essenziale

---

[118] Per umanesimo digitale può intendersi una '*filosofia dell'esistenza per la quale la tecnica deve essere sempre e comunque subalterna alla persona*', così L. VIOLANTE, *Introduzione*, in A. PAJNO, L. VIOLANTE, *Biopolitica, pandemia e democrazia. Rule of Law nella società digitale*, I, Il Mulino, Bologna, 2021, p. 14.

Si veda ampiamente poi, nel generale quadro di un potere pubblico algoritmico e dei suoi rapporti con i cittadini, la declinazione della formula offerta da G. GALLONE, *Riserva di umanità e funzioni amministrative*, Wolters Kluwer, Milano, 2023, pp. 32 e ss., come riaffermazione del fattore antropocentrico nei meccanismi di digitalizzazione dei processi giuridici.

Per le implicazioni etiche della macchinizzazione delle decisioni, giuridiche e politiche, J. NIDA-RÜMELIN, N. WEIDENFELD, *L'umanesimo digitale. Un'etica per l'epoca dell'Intelligenza Artificiale*, FrancoAngeli, Milano, 2019.

Non c'è dubbio che la persistenza dell'essere umano, con i suoi principi, rappresenti essa stessa garanzia e fattore di sicurezza.

In secondo luogo, in chiave prettamente *cybersecurity*, ciò deve tradursi nella necessitata presenza dell'uomo, e delle libertà e dei diritti a questi ricollegabili, nei percorsi di strutturazione dei dispositivi di protezione e di difesa digitale, bilanciando tra loro 'esternalizzazione' di funzioni e di processi alle macchine intelligenti e ineludibile riserva di umanità.

[119] Il *framework* normativo prevede una lunga e articolata serie di scadenze per i soggetti tenuti ad adempiere, rimodellando le loro strutture organizzative e ossequiando una serie di incombenti, oltre che la adozione da parte di ACN e della Presidenza del Consiglio degli atti esecutivi e applicativi sequenziali.

La fase di prima applicazione, disciplinata dall'articolo 42, del d. lgs. n. 138/2024, ad esempio, stabilisce una prima scadenza fissata al 17 gennaio 2025 per la iscrizione sulla piattaforma prevista dall'articolo 7 del medesimo decreto, a carico di fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di *cloud computing*, fornitori di servizi di *data center*, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di

perché, come ha affermato lo scrittore William Gibson, padre nobile del cyberspazio, "*il futuro è già arrivato, solo che non è stato ancora equamente distribuito*[120]".

---

mercati *online*, di motori di ricerca *online* e di piattaforme di servizi di *social network* rientranti nei profili soggettivi e oggettivi di applicazione della normativa *de qua*.

Sino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS dovrà riunirsi almeno una volta, e sempre il 31 dicembre 2025 è considerato come data limite per l'adempimento entro nove mesi, computando come *dies a quo* quello della ricezione della comunicazione *ex* articolo 7 c. 3 lettere a) e b), degli obblighi previsti in tema di obbligo di notifica di incidente *ex* articolo 25, mentre in diciotto mesi è fissato il termine per l'adempimento previsto dagli articoli 23, 24 e 29, sempre decorrenti dalla citata comunicazione.

[120] W. GIBSON, citato in A. KEEN, *Internet non è la risposta*, Egea, Milano, 2015, p. xvi.