Giovanni Bombelli

Dogmatica, certezza e (in)calcolabilità. Note su profili di "anticipazione cognitiva" in tema di legal design *e* decision-making

Abstract: Partendo dal rapporto tra sicurezza e modernità, il saggio si concentra su alcuni aspetti riguardanti la nozione di "cybersecurity" e, in particolare, il legame tra cybersecurity-intelligenza artificiale-dogmatica giuridica. Alla luce di questo quadro, viene discussa la possibilità e la plausibilità di un "approccio cognitivo" (cioè di anticipazione cognitiva) al diritto, con particolare attenzione ai concetti di "legal design" e "decision-making" anche considerando i molteplici riflessi provocati dalle mutazioni tecnologiche sulla dogmatica giuridica. Più in generale, la questione coinvolge la natura del rapporto sfera giuridica-universo digitale e l'inevitabile connessione tra il diritto e le altre scienze

Keywords: Dogmatica giuridica, Certezza, Anticipazione cognitiva, Legal design, Decision-making.

1. Premessa

Nelle pagine seguenti si proporranno alcune riflessioni, da intendersi come mere linee di osservazione, situate a cavallo di fenomenologia sociale attenta alle dinamiche socio-tecnologiche e teoria del diritto.

Senza ambire all'elaborazione di "quadri" o "soluzioni" definitivi, a partire da una prospettiva filosofico-giuridica l'obiettivo è offrire una serie di impressioni che attengono all'universo complesso e inevitabilmente cangiante delle mutazioni tecnologiche in atto e della relativa disciplina normativa.

In questa direzione, si proverà ad articolare un quadro critico strutturato secondo cerchi concentrici. Dopo alcune note introduttive relative al nesso che intercorre tra (cyber)sicurezza e modernità, ci si soffermerà su qualche profilo di carattere generale che attiene alla "cybersicurezza". Ciò consentirà di appuntare meglio l'attenzione sul circuito che intercorre tra quest'ultima, l'intelligenza artificiale e la dogmatica giuridica, con particolare riguardo alla plausibilità del configurarsi di un modello di "anticipazione cognitiva" (o cognitivo-normativa) in tema di *decision-making* e *legal design*.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760157

Per questa via si addiverrà ad alcune notazioni conclusive, con particolare riguardo alla progressiva compromissione della grammatica concettuale e categoriale di matrice moderna determinata dalle mutazioni tecnologiche in atto e dal connesso *framework* normativo vieppiù connotato da forme di *multilevel regulation*: ciò aprirà ad un interrogativo finale relativo al nesso che intercorre tra sfera giuridica e universo digitale, che convoca orizzonti concettuali in qualche misura interdisciplinari.

2. (Cyber)Sicurezza e modernità

Il tema della cybersicurezza chiama in causa il rapporto con le coordinate teoriche che informano la modernità giuridica e la relativa dogmatica.

Più precisamente, viene a tema il nesso concettuale che si istituisce tra la dimensione sicuritaria[1], come luogo teorico classicamente filosofico-giuridico di cui la dizione "cybersicurezza" costituisce una sorta di proiezione contemporanea, l'apparato teorico-concettuale sotteso all'elaborazione del giuridico e il modello di Stato. Un trinomio che informa le grammatiche moderne della sicurezza e da riprendere, in conclusione, con riguardo al grado di funzionalità e legittimità degli odierni assetti democratici.

In questa direzione, il paradigma o termine di confronto critico non può che essere rappresentato dalla prospettiva di Thomas Hobbes. Di essa si richiamano solo due versanti tra loro connessi in quanto appaiono particolarmente funzionali alla riflessione qui proposta: a) la struttura del dispositivo statuale e b) il binomio *safety-security*. Esaminiamoli distintamente.

a) Con buona approssimazione, si può affermare che lo Stato moderno nasca per garantire "sicurezza". Essa, infatti, ne rappresenta una sorta di costante individuando, per molti versi, la cifra essenziale del nuovo soggetto politico-istituzionale inauguratosi al tramonto dell'epoca medievale.

Una dimensione, quella della sicurezza, che appare giocata su due livelli del perimetro statuale: interno e esterno.

Essa viene intesa sin da subito come "sicurezza interna" allo Stato, radicata nella coppia pubblico-privato. Come concettualizzato originariamente da Hobbes, l'edificazione del potere statuale in termini di *pacta* a base territoriale, coincidente con la sfera "pubblica" e fondato sul riconoscimento reciproco dei soggetti in quanto contraenti, appare funzionale sia a predisporre forme di controllo sociale sia, al contempo, a tutelare la sfera individuale o "privata" colta come piano simmetrico allo spazio pubblico[2].

1 In merito, per un quadro generale, *ex multis* Pizzolato, Costa 2015; Cocco 2012; Greco 2009. Per un *focus* sulla realtà della "città" Buzzacchi, Costa, Pizzolato 2019.

2 Per un'articolazione più distesa di questi passaggi concettuali si consenta rinviare a Bombelli 2015a: 53-54 in particolare. Ivi il rinvio a Hobbes 2001 [1651], Parte I, XIV, 9-11; nel testo appena citato si veda anche la nota 19 riguardo al binomio *fear-trust/faith* operante nella riflessione del filosofo inglese (il riferimento è alla edizione italiana del 2001: 218-220).

Tale plesso tematico riposa, a sua volta, su un modello di calcolabilità strutturalmente connesso alla certezza del diritto. in altre parole, il paradigma teorico vive sulla possibilità di "calcolare", nel senso di pianificare o prevedere-anticipare a livello cognitivo, le dinamiche sociali interne allo Stato, mentre l'orizzonte della certezza verte sulla particolare configurazione in termini di certezza conferita (*rectius*: che si pretende di conferire) al diritto. Storicamente ciò si rende possibile in ragione dell'unificazione delle fonti allestita in capo al sovrano e conseguente al processo di affermazione dell'impianto statuale: in altre parole, lo Stato moderno nasce "sicuro" in quanto reso "calcolabile" attraverso il ricorso all'unificazione del diritto inteso come strumento di certezza.

Diverso il quadro "esterno" all'area statuale che, in qualche misura, permane impregiudicato. Alla reale (o, quantomeno, auspicata) sicurezza intra-statuale fa infatti da contraltare lo scenario dei rapporti inter-statuali, ove l'orizzonte del perimetro territoriale funge da mero discrimine tra i nuovi attori interessati (gli Stati).

Se la pace di Vesfalia segna notoriamente un passaggio decisivo nell'istituire le regole che disciplinano tale scenario, al contempo essa non appare in grado di ergersi a regola invalicabile. In tal senso, il principio del *pacta sunt servanda*, in cui si sintetizza l'esito nucleare del trattato del 1648 e il contenuto essenziale del nascendo diritto internazionale, rappresenta un riferimento normativo sempre suscettibile di una ridiscussione radicale. In altre parole, sottraendosi alle forme di controllo giuridico predisposte dalla modernità per il contesto statuale a base territoriale[3], la sicurezza inter-(extra)statuale si configura in termini strutturalmente "in-calcolabili".

b) Come segnalato, nella riflessione hobbesiana il tema della sicurezza, nella sua duplice declinazione intra-statuale e extra-statuale, si intreccia con il binomio *security* e *safety*. Un binomio che il teorico inglese sviluppa segnatamente con riguardo all'orizzonte intrastuale secondo tonalità invero un poco ambigue.

Per un verso, infatti, la sicurezza va intesa come "preservazione" delle condizioni esterne di convivenza e, quindi, in funzione del controllo della sfera individuale: in altre parole, come modello di *security* nel quadro dell'architettura concettuale richiamata al punto precedente.

Al contempo, il tema sicuritario rinvia ad altra area semantica. Da questa prospettiva, esso emerge in termini di *safety* (quasi come forma di sicurezza "interna" o intraindividuale): la funzione di controllo politico attribuita al Leviatano comporta, infatti, che su quest'ultimo gravi altresì l'onere di provvedere al "bene" dei consociati (secondo la dizione *Good-Safety* nella versione inglese del testo hobbesiano, *salus* nella versione latina)[4]. Esso potrebbe intendersi come "sviluppo delle potenzialità" dei singoli consociati: in altre parole, un modello orientato al *flourishing* individuale e collettivo che, in modo solo apparentemente paradossale nel

3 Sul punto ineludibile la menzione di Schmitt 1991 [1974], su cui ancora Bombelli 2015a: 60. Per una contestualizzazione più ampia si consenta, altresì, rinviare a Bombelli 2018: 5-65.

4 Sul punto Bombelli 2015a: 70 (in particolare la nota 56).

quadro della prospettiva del filosofo di Malmesbury, inaugura una sorta di forma embrionale di *Welfare State*[5].

Di là dalle possibili letture che si possono offrire dell'impostazione hobbesiana[6], su cui in questa sede non interessa soffermarsi, si possono trarre almeno tre corollari.

In primo luogo, la polarità sicurezza interna/esterna originatasi a partire dal filosofo inglese permane sino allo scenario contemporaneo. A ben vedere, essa in qualche modo viene progressivamente potenziata in rapporto al processo di edificazione dell'impalcatura statuale trasfondendosi in una vera e propria dogmatica giuridica ad impronta sicuritaria.

Tale dogmatica, in secondo luogo, mira all'ideale rappresentato dalla certezza del diritto o, per dirla con Natalino Irti, della sua calcolabilità[7]. Per questa via, si istituisce la corrispondenza biunivoca tra "norma certa" e "norma calcolabile": più precisamente, la norma è pensabile come "certa" *in quanto* "norma calcolabile". Ciò, si badi, sul presupposto che si dia uno spazio sociale o pubblico, quindi giuridico-normativo rappresentato dallo Stato a base territoriale, controllabile e "dominabile".

Occorre, infine, sin da ora rimarcare come il gioco del binomio *safety-security* si riproponga sul terreno specifico della tutela della sfera individuale: un versante su cui si tornerà variamente nelle pagine seguenti e in conclusione, con riguardo ai contesti odierni pervasivamente connotati da forme di cybersicurezza.

In sintesi. Il trinomio modernità-dogmatica giuridica-certezza/calcolabilità si costruisce e si dispone *en masse*, proprio a partire dal tema della sicurezza (e, con lessico odierno, cybersicurezza), plasmandosi come una sorta di apparato concettuale che, più ampiamente, può fungere da griglia di lettura del contesto moderno e contemporaneo.

3. Cybersicurezza: alcuni profili

Alla luce del quadro storico-concettuale proposto, si orienta ora l'attenzione sul tema specifico della cybersicurezza.

Nel quadro di uno scenario complesso e strutturalmente mutevole, in merito come noto è andato fiorendo un dibattito articolato e arricchito da un'ampia bibliografia[8] a partire dalla definizione stessa della nozione di "cybersicurezza (nella dizione anglosassone ormai invalsa: cybersecurity)"[9].

5 Questo profilo è stato messo particolarmente in luce da uno storico delle dottrine politiche: Galli 1989: 105-106. Tra l'altro, Galli osserva che Hobbes propone "uno Stato che sembra precorrere le leggi antitrust e il Welfare State propugnati dalle correnti progressiste del XX secolo" (inoltre Galli 1995, cap. 2: 42, con riferimento a Carl Schmitt).

6 Per un quadro generale ancora utile Pacchi 2004.

7 Con ovvio rinvio a Irti 2016.

8 A mero titolo di esempio si segnalano Cortesi 2019; Casadei, Pietropaoli 2021; Faini, Pietropaoli 2021, in particolare cap. 5 *Società tecnologica e istituzioni pubbliche. L'amministrazione digitale e aperta*; Ziccardi 2022 (segnatamente il cap. XIV).

9 Si è così passati dalla "sicurezza informatica intesa come Computer Security [n.d.r. protezione del sistema informatico]" ad una "visione della sicurezza maggiormente orientata

In tal senso, muovendo da una prospettiva filosofico-giuridica si proverà solo a stagliare alcuni aspetti di tale groviglio all'incrocio di prassi e teoria e che, richiamandosi circolarmente, appaiono maggiormente conferenti con quanto si va ragionando.

Più precisamente, si orienterà l'attenzione sul nesso tra "sicurezza" e configurazione dei modelli sociali, sul tema dell'autonomia individuale e, infine, sul reticolo normativo[10] originatosi intorno alla cybersicurezza.

L'orizzonte della "sicurezza" rappresenta un nodo centrale nello strutturarsi dei modelli sociali. Esso, però, va valutato alla luce del rimescolamento in essere delle categorie giuridiche maturate, come appena richiamato, nella modernità, segnatamente con riguardo al cruciale binomio "pubblico"-"privato".

Si pensi, a titolo paradigmatico, alle "cyberwars"[11]. Esse rappresentano una delle proiezioni maggiormente rilevanti dei temi di cui si va dicendo, soprattutto alla luce dell'odierno scenario europeo e mondiale: sotto questo profilo, ciò che connota i conflitti "virtuali" (*rectius* combattuti per via tecnologica) è proprio una sorta di compromissione *in progress* della linea di distinzione elaborata agli albori della modernità tra ambito "privato" e sfera "pubblica". Detto in altri termini: tra individuo e Stato, inteso quest'ultimo *à la* Weber come depositario dell'esercizio della forza tradizionalmente legato al ricorso a strumenti formalizzati e riconoscibili (ad esempio gli eserciti) [12].

alla protezione delle informazioni e dei dati, la c.d. Information Security", sino a introdurre (sotto l'impulso della c.d. Cybersecurity Strategy propugnata dall'Unione europea a partire dal 2013 con il documento "Strategia dell'unione europea per cybersecurity: un ciberspazio aperto e sicuro") la nozione di Cybersecurity funzionale "a denotare che gli interessi da proteggere riguardano oggi le infrastrutture di uno Stato, lo sviluppo delle reti e, più in generale, la sicurezza nel ciberspazio inteso come ambiente complesso di interazione tra persone, software e servizi": Brighi 2021: 135-147, in particolare 135-136 (neretti e corsivi nel testo; a tale contributo si rinvia anche per un quadro sintetico relativo alla disciplina della sicurezza informatica nell'ordinamento giuridico comunitario: 144-147).

10 Sul delinearsi di un reticolo normativo insiste, ad esempio, Golisano 2022: 824-834, circa l'accelerazione nelle politiche di innovazione digitale derivante dal PNNR (Piano Nazionale di Ripresa e Resilienza) e la riallocazione delle competenze amministrative in materia di transizione digitale con la loro concentrazione in capo alla Presidenza del Consiglio dei ministri.

11 In merito, ad esempio, Giannuli, Curioni 2019. Il punto si può correlare ad un orizzonte socio-culturale più ampio e dominato da una sequenza temporale di *shocks*: Giaccardi, Magatti 2022 particolare Parte prima, cap. 2 *Entropia, antropia, shock*.

12 Si pensi, per stare ad alcune vicende recenti, all'intersecarsi di soggetti privati e pubblici (o meglio politici). Un profilo riemerso, proprio con riguardo al ricorso a strumenti tecnologici in contesti bellici, in rapporto a figure come quella di Elon Musk e alla relazione tra alcune sue iniziative imprenditoriali (la cosiddetta "Starlink") e alcuni assetti governativi nel quadro del conflitto Russia-Ucraina. A ciò si può aggiungere la questione recentissima legata alla *startup* cinese "Deepseek" con i relativi precipitati in ordine alle forme di controllo sociale e, più ampiamente, in prospettiva geopolitica. In merito vale la pena soffermarsi, in particolare, sulla "teoria delle due piscine" e sul suo progressivo superamento come ben sintetizzato in Macrì 2024: 17-22, segnatamente 17-18: "Nel periodo 2012-2014, quando si prepara la prima direttiva NIS, era accettata la «teoria delle due piscine». La metafora, definita «tanto semplice quanto arrogante», si riferisce alle strutture che mettono a disposizione dei loro clienti due differenti piscine: una di profondità, dove nuotano gli adulti, e un'altra, bassa, per i bambini. Mentre i Paesi come

In questa direzione viene allora a tema la sfera dell'autonomia individuale, come luogo teorico strutturalmente appartenente alla riflessione moderna e che, da Hobbes e Locke, arriva sino ai giorni nostri.

Si tratta di un profilo decisivo. Intorno a tale coordinata, infatti, viene a tracciarsi il perimetro dell'intervento normativo che, lungo la linea del binomio *safety-security*, si sviluppa secondo un delicato equilibrio tra tutela dell'individuo e l'intervento di poteri (pubblici e/o privati) con una potenziale compressione delle libertà costituzionalmente garantite. Il recente fiorire dell'attenzione intorno al "costituzionalismo digitale" [13], una locuzione discussa e discutibile ma ormai invalsa nell'odierno dibattito, va inteso anche in questa direzione alla luce degli evidenti corollari in ordine al tema della cybersicurezza.

Di qui il terzo profilo poc'anzi segnalato: il reticolo normativo connesso alla cybersicurezza.

Non è luogo qui per ricordare tutto il complesso, nonché ancora in via di definizione, percorso di regolazione. Come noto, esso ha interessato sia la produzione normativa nazionale sia il livello sovranazionale laddove, almeno per ora e forse non a caso, minore è stata l'attenzione destatasi a livello di diritto internazionale. Senza ambire ad una rassegna esaustiva, occorre ricordare almeno il D.P.C.M 2013, la Direttiva europea 2016 NIS, il perimetro di sicurezza nazionale predisposto nel 2019 così come l'istituzione di una *authority* europea e nazionale nel 2021 (quest'ultime dotate di uno *status* giuridico un poco peculiare rispetto alle altre *authorities*)[14].

Sul punto ci si limita a formulare due rilievi tra loro connessi.

In primo luogo, occorre rimarcare la complessità di tale scenario.

Canada, Stati Uniti, Regno Unito (che all'epoca era ancora all'interno dell'Unione europea), Australia, Nuova Zelanda, Francia e Germania sono in grado di nuotare nella piscina dedicata agli adulti, gli altri Paesi devono accontentarsi della piscina dei bambini. La crisi ucraina ha messo in evidenza quanto la «teoria delle due piscine» fosse errata, perché mentre nel caso di una guerra tradizionale un'alleanza è forte quanto il suo membro più forte, in una guerra cibernetica un'alleanza è debole quanto il suo membro più debole. Ben presto l'Occidente ha compreso che per difendersi ha bisogno che tutti i sui membri siano affidabili e sappiano «nuotare» nelle piscine per adulti. Cosicché l'Europa per superare questa «teoria delle due piscine» ha puntato sulla conoscenza collaborativa, che è diventata la priorità fondamentale della cybersicurezza: tutti i soggetti che lavorano alla cybersicurezza di ciascuno Stato membro devono collaborare per condividere le informazioni. Si trattava di un passaggio delicato perché nei diversi stati la cybersicurezza è appannaggio di soggetti differenti, non sempre fra loro omogenei e compatibili, come ad esempio i servizi segreti, aggregazioni pubblico-privati, ecc.".

13 In merito ad esempio, da prospettive diverse, Dimasi 2023; Frosini 2021; Iannotti Della Valle 2023.

14 Oltre ai riferimenti contenuti nei testi citati nelle note precedenti e a quelli che verranno menzionati successivamente, su questi temi si rinvia innanzitutto, in modo un poco rapsodico, ad alcuni contributi di Indra Macrì (consigliere dell'area informatica della Corte Costituzionale): Macrì 2024, 2023, 2022a, 2022b, 2021. Inoltre, da una prospettiva essenzialmente amministrativistica, Golisano 2022; Parona 2021: 709-719; Renzi 2021: 538-548. In tema anche "Igiene e sicurezza del lavoro", 2, 2024, inserto dal titolo *Dalla direttiva ala regolamento sulle macchine; che cosa cambia? (Parte II)*, pp. III-XXIII.

Come già sottolineato, esso appare particolarmente intricato nonché, in qualche misura, contraddittorio e talora ridondante. Al suo interno si può intravedere la conferma di un profilo che, per vie diverse, la teoria del diritto va segnalando da tempo[15]: la crescente difficoltà di mantenersi entro i confini di una concettualizzazione assiomatica del normativo, quale quella originatasi in alcuni passaggi del Novecento e, a sua volta, radicata in un modello epistemologico di matrice ottocentesca a lungo reputato scientificamente saldo e operativamente fruibile[16]. Per questa via, si aprono gli spazi teorici per cogliere la rilevanza assunta progressivamente dai modelli giusreticolari[17], di cui la normativa concernente la cybersicurezza sembra costituire un ottimo esempio e sui quali si tornerà più avanti.

Ma l'ambiente normativo di cui si va ragionando contribuisce, altresì, alla ridiscussione dell'apparato dogmatico nel suo complesso. Più precisamente, in gioco sono le condizioni stesse alle quali la modernità giuridica (quantomeno a partire da Hobbes) era andata strutturandosi, anche in ordine alla configurazione del nesso certezza-sicurezza: profilo su cui ora occorre soffermarsi più compiutamente volgendo lo sguardo ai contesti contemporanei.

4. Cybersicurezza, AI e dogmatica giuridica

Su questo sfondo si può situare utilmente un carotaggio intorno al nesso tra cybersicurezza e intelligenza artificiale. In merito, si è giustamente osservato come si debba parlare di "rapporto di presupposizione tra i due plessi normativi, atteso che la cybersicurezza rappresenta una premessa indefettibile per un impegno sicuro dell'intelligenza artificiale", nel senso che "la prima [costituisce], dal punto di vista del diritto positivo, una componente necessaria del quadro normativo in cui la seconda possa essere sviluppata e utilizzata"[18].

Ad uno sguardo più ravvicinato, il tema cruciale è rappresentato dal posizionamento dell'intervento normativo qui inteso in termini articolati e, cioè, inclusivo del profilo cognitivo che accompagna strutturalmente il momento giuridico.

Un buon *test* per sviluppare, in controluce, tale riflessione è rappresentato dal regolamento europeo sull'intelligenza artificiale (d'ora in poi AI Act) che, come noto, va collocato nell'ottica di transizione digitale da tempo predisposta dall'Unione Europea e a sua volta da intendersi *pour cause* nel quadro di un forte nesso con la dimensione della sicurezza.

15 Mi permetto di rinviare a Bombelli 2017, in particolare capp. 3-4.

16 Si pensi, in modo paradigmatico, al nitore che connota una certa stagione del pensiero di Kelsen legata alla prima metà del secolo scorso e, in particolare, alla parabola teorica che, dalla sua *Reine Rechtslehre. Einleitung in die rechtswissenschaftliche Problematik.* Franz Deuticke, Wien, 1934, arriva sino alla nota riedizione di tale opera nel 1960.

17 Bombelli 2017, cap. 3.

18 Parona 2021: 711. Nell'ormai estesissima bibliografia dedicata all'intelligenza artificiale segnalo, per la ricchezza e varietà di spunti ivi proposti, D'Aloia 2020.

Senza ambire ad un'analisi esaustiva della normativa europea, a mo' di *focus* si propongono solo alcune notazioni con riguardo a taluni suoi aspetti o criticità.

Da una prospettiva di carattere generale, un primo profilo attiene alla novità, di portata non assoluta ma certamente rilevante, che connota lo strumento normativo di derivazione sovranazionale. Come noto, esso rappresenta a livello mondiale una delle prime forme di regolazione del fenomeno dell'intelligenza artificiale: più precisamente, l'AI Act può leggersi come l'esito di un bilanciamento tra scelte politiche, operate appunto a livello sovranazionale, e diritto. Un versante, quello del rapporto tra politica e diritto, che in proiezione appare decisivo anche in ordine al problema della sicurezza in chiave di cybersicurezza[19].

In secondo luogo, sempre ad un livello generale, nel documento europeo si staglia con chiarezza la problematicità del nesso tra tecnica e diritto. *Sub specie* della disciplina concernente l'intelligenza artificiale, si delinea la questione del rapporto tra mutamenti sociali e intervento normativo: più precisamente, lo scarto che intercorre tra la rapidità che vieppiù connota i primi e il "ritardo" nella plasmazione delle categorie giuridiche, con riflessi rilevanti sul piano della metodologia giuridica (sul punto si tornerà meglio più avanti).

Entrando più direttamente nella previsione normativa confezionata dal legislatore europeo, è possibile rimarcare alcuni aspetti specifici.

Innanzitutto, l'AI Act non intende regolamentare i "prodotti" legati all'intelligenza artificiale, bensì i suoi modelli o tipologie (i "processi") di natura "generativa". L'obiettivo è disciplinare le forme di intelligenza artificiale a *general purpose* che, come tali, si ritiene possano comportare un rischio sistemico[20].

Di qui l'impianto tecnico-normativo articolato e complesso[21].

Tra i molti aspetti che lo connotano, sempre con riguardo all'intelligenza generativa, in particolare vale la pena mettere in luce come nel documento europeo si individuino livelli differenti di rischio.

Da un lato, infatti, emerge il modello generativo ad alto rischio (o rischio sistemico). Esso richiede un aggiornamento *in progress* dei coefficienti, con i relativi oneri o adempimenti di carattere formale (avviso alle autorità competenti, trasparenza dei processi adottati, ecc. con i relativi dubbi concernenti la moltiplicazione dei soggetti predisposti alla regolazione).

Dall'altro, si pone l'intelligenza artificiale generale o "di base", comunque ritenuta non ad alto rischio. Riguardo ad essa, permane l'obbligo di trasparenza

19 Si veda *supra* nota 12.

20 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio (13 giugno 2024), nn. 84-85 (testo disponibile al https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689).

21 Si segnalano qui solo alcuni tratti che connotano il testo europeo: il lungo elenco iniziale di "considerando"; l'adozione di una certa forma linguistica o lessico; il rinvio a *authorities*; la presenza di norme programmatiche; l'apparato sanzionatorio (analogamente a quanto avviene nel GDPR); la definizione di IA proposta all'art. 3 (e allegato 1); l'esclusione dell'ambito militare; il *risk-based approach* su cui si tornerà poco più avanti.

circa il suo funzionamento, le modalità della sua creazione e la precisazione delle relative caratteristiche tecniche[22].

Tale modello complessivo presenta alcune criticità rilevanti anche in tema di *cybersecurity*.

La prima attiene alle tipologie di intelligenza artificiale. La distinzione tra intelligenza "generativa" e non "generativa" muove dal presupposto che essa permanga nel tempo: ciò a fronte di un processo di innovazione tecnologica sempre più rapido, che rischia di rendere tale distinzione rapidamente obsoleta.

Una seconda criticità attiene al concetto di "rischio". Il documento europeo propone la scansione tra rischio "inaccettabile" (con conseguente divieto), "alto"[23] e "basso" (o minimo). Si tratta di un *risk-based approach* già adottato in altre sedi che, tuttavia, forse omette di ragionare più a fondo sulla distinzione (giuridica) tra "rischio" e "pericolo": se il primo, in un'accezione per così dire tradizionale, appare sempre giuridicamente "calcolabile" o dominabile[24], va osservato che la graduazione della nozione di rischio risente delle incertezze epistemico-cognitive relative al fenomeno *de quo* e alla sua eventuale evoluzione di cui si è detto poc'anzi[25].

Anche le finalità che animano l'AI Act appaiono discutibili. A ben vedere, come peraltro accade di frequente in tema di normativa europea, sembra darsi una tensione tra due dimensioni. Da un lato si staglia la tutela dei diritti fondamentali richiamata nel preambolo e, al contempo, emerge l'attenzione rivolta al mercato: un profilo decisivo, ove si consideri il massiccio (e crescente) volume economico connesso al fenomeno dell'intelligenza artificiale e, conseguentemente, della cybersicurezza come dimensione ad essa connessa[26].

Di qui il tratto oscillante della disciplina in oggetto, con riguardo sia alla sua natura giuridica sia alla struttura complessiva. Si spiegano, così, alcune letture che di essa sono state offerte in termini di normativa "evolutiva" o, al contrario, "regressiva"[27], così come l'equilibrio problematico ivi disegnato tra "innovazione" e "diritti". Un profilo, quest'ultimo, che a ben vedere sembra connotare il quadro complessivo degli obiettivi generali perseguiti dall'Unione Europea, ad esempio a

22 Per i modelli di intelligenza artificiale di uso generale, o comunque non generativa (al *considerando* n. 97), valgono invece altre condizioni: la figura della "licenza", la presenza dell'*open source*, il ricorso a modelli e parametri resi pubblici.

23 Allegato 3 del regolamento europeo di cui si va ragionando.

24 Su questi temi si consenta rinviare a Bombelli 2022a: 177-230, in particolare 200 e ss.

25 Da questa prospettiva riemergono, in altro contesto, alcune istanze sottese all'ormai classico Beck 1986.

26 Nel capo I del Regolamento (UE) 2024/1689, dedicato alle *Disposizioni generali*, l'art. 1, comma 1 recita: "Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione".

27 Oscillazioni che si possono leggere anche in rapporto al contenuto e alle letture offerte di un documento normativo, come il regolamento Digital Markets Act (DMA) approvato dal Parlamento europeo del 5 luglio 2022, per molti versi connesso ai temi di cui si va ragionando.

partire dalla problematica tenuta (sul piano logico e operativo) del nesso operante tra transizione digitale e *green transition*: obiettivo, come noto, al cuore degli obiettivi del programma *Next Generation*[28] e presente anche nella disciplina relativa all'intelligenza artificiale.

Questi rilievi sembrano trovare conferma anche ad un altro livello e, cioè, con riguardo al *range* della normativa europea, la quale per definizione attiene all'ambito dell'Unione (a prescindere da alcuni casi delimitati[29]).

Il punto-chiave è rappresentato dalla natura trasversale dell'intelligenza artificiale: più estesamente, esso rinvia alla capacità strutturale dei mutamenti tecnologici di travalicare gli steccati statuali e sovranazionali. Detto in altri termini: viene qui a tema il problema del nesso tra spazio (o spazialità) e normatività, con evidenti riflessi in tema di cybersicurezza, come luogo classico di definizione del *nomos* e che, almeno a partire da Hobbes, non a caso rimonta alle origini della modernità dispiegandosi sino al dibattito contemporaneo (ad esempio in Carl Schmitt[30]) e alla problematicità della nozione stessa di "cyberspazio"[31].

Riguardato da una prospettiva più generale, il *case study* relativo all'intelligenza artificiale (e, per contiguità logica e tecnologica, alla cybersicurezza) consente di mettere in luce un preciso profilo teorico-giuridico.

Esso attiene alla natura, per così dire, reattiva assunta progressivamente dal diritto (a ben vedere anche in termini di *active defence*[32]): in altre parole, l'intervento

28 Nel senso che un profilo talora può configgere con l'altro: come noto, ove realmente e globalmente perseguita la transizione digitale presenta una serie di costi (economici, sociali e soprattutto ambientali) tale da rendere altamente problematico ambire al contempo, in modo praticabile e realistico, ad una *green transition*.

29 Ça va sans dire si versa in tema di disciplina direttamente applicabile negli Stati membri dell'Unione europea. Per le ipotesi di estensione della normativa al di fuori di tale orizzonte e, più ingenerale, per il rapporto tra quadro comunitario e spazio giuridico ad esso esterno, rinvio a quanto espressamente contemplato nel regolamento europeo relativo all'intelligenza artificiale (ad esempio il *considerando* 46).

30 Si rinvia *supra* n. 3.

31 Nel Regolamento europeo relativo all'intelligenza artificiale la nozione di "spazio", in particolare secondo la dizione "spazio normativo", ricorre frequentemente nei *Considerando* e in altri luoghi: tuttavia, come segnalato *supra* alla n. 9, a livello di strategia europea la saldatura tra il tema della *cybersecurity* e la concettualizzazione della categoria di *cyberspazio* in termini di dimensione "aperta e sicura" risale al 2013. Più in generale, circa il nesso spazio-normatività nell'orizzonte tecnologico si consenta rinviare Bombelli 2010, in particolare cap. 5: 483 e ss.

32 Con riguardo specifico alla cybersicurezza, ciò si evince dal problema della proprietà dei modelli e dei sistemi, ove la regolazione giuridica avviene "a valle", senza intaccare l'originaria disponibilità del "bene" e della sua strutturazione a livello tecnologico in capo al produttore inteso come soggetto privato. Per spunti in tal senso Renzi 2021: 538-539: "La consapevolezza dei pericoli connessi a [fenomeni di attacco cibernetico] ha portato il legislatore a sostituire un approccio di mero contrasto occasionale e la repressione criminale dei comportamenti, con una strategia normativa in grado di assicurare la sicurezza cibernetica preventiva, limitando le possibilità di attacco e riducendo gli eventuali danni che possono essere subiti. L'assunto risulta ancor più vero nel settore che per eccellenza richiede interventi preventivi, quale appunto quello della sicurezza nazionale. Basti pensare, sul punto, a come gli approfondimenti del *World Economic Forum* equiparino gli attacchi informatici alle grandi crisi economico-finanziarie in termini di capacità di influenza sulla stabilità e sulla sicurezza internazionale" (p. 538). Ivi si veda inoltre

normativo sembra situarsi sempre più "a valle" del mutamento tecnologico, assumendo in tal senso una sorta di ruolo ancillare[33]. Ne discende un fenomeno per molti versi nuovo che interessa la relazione tra due dimensioni: l'edificazione della dogmatica giuridica e l'emergere del "fatto sociale (*rectius* tecnologico)".

Se il diritto moderno, con il relativo corredo storico-categoriale, era andato caratterizzandosi per la capacità in qualche modo di pianificare *ex ante* (se non "guidare") il *novum* sociale garantendo la certezza dell'intervento normativo e l'ideale della sicurezza, ciò cui si assiste è una sorta di rovesciamento delle parti.

Ne consegue che la costruzione delle categorie giuridiche, intese propriamente come griglie di lettura dei fenomeni sociali, sembra plasmarsi esclusivamente in funzione di processi in qualche modo *già* compiuti e definiti, nonché alla luce di dimensioni (come in particolare la tecnologia e l'economia) in grado di elaborare autonomamente modelli "interni" di razionalità e che la sfera giuridica si limita a mutuare[34]. Un quadro problematico e categoriale che, nel suo insieme, sembra attestare la transizione progressiva da un repertorio teorico di derivazione moderna a un orizzonte vieppiù abitato da contesti e categorie ad essa eterogenee: riprenderemo il punto in conclusione.

Occorre allora rimeditare il circuito concettuale imperniato sul binomio dogmatica giuridica-certezza del diritto, una sorta di roccaforte teorica della modernità, ove soprattutto si intenda il secondo termine del binomio in termini di calcolabilità (e progressiva in-calcolabilità delle dinamiche *in fieri*) nell'accezione precisata precedentemente, anche alla luce dei profili cognitivi sottesi a tali nuclei concettuali: su questo si concentrerà l'attenzione nelle seguenti pagine conclusive.

5. Per concludere: "anticipazione cognitiva", *legal design* e *decision-making*

La riflessione proposta nelle pagine precedenti apre ad una serie di proiezioni che investono sia il tema della sicurezza (anche nella prospettiva specifica della *cybersicurezza*) sia, in chiave più generale, l'orizzonte teorico e socio-giuridico entro il quale essa sin da ora va modulandosi.

(pp. 546-547) la comparazione con altri assetti normativi (in particolare USA, Grecia, Francia), con la seguente conclusione: "Le vere sfide che caratterizzeranno il prossimo futuro […] saranno connesse […] alla capacità del *framework* [normativo] di assicurare un ampio livello di collaborazione europea, ma anche interistituzionale e con gli operatori privati. Questi ultimi, infatti, oltre a poter fornire un ampio *know know* e a configurarsi come i principali innovatori nel settore, richiedono una costante attività di supporto da parte delle istituzioni. Proprio l'Agenzia nazionale, nonostante il suo non chiaro posizionamento nel contesto del Sistema di informazione nazionale, può porsi come l'interlocutore privilegiato per il superamento di un'ottica di mera vigilanza e controllo, verso una dimensione più partecipata e collaborativa. Questo sulla base proprio della costante interconnessione tra reti ed infrastrutture digitali, che molto speso provoca una sostanziale riduzione delle differenze tra pubblico e privato".

33 Per un quadro più ampio Bombelli, Montanari 2015.

34 In merito mi permetto di rinviare a Bombelli 2015b: 321-358. Profili problematici sono variamente presenti anche in Bombelli 2015a e in Bombelli, Lavazza 2019: 3-34.

Uno scenario, va da sé, articolato e complesso di cui in questa sede si è provato a segnalare almeno alcuni tratti distintivi. Muovendo dal quadro proposto, a mo' di conclusione di seguito si ritagliano tre rilievi che, da un orizzonte generale di natura teorico-giuridica, investono le nozioni di *legal design* e *decision-making* e la cui sequenzialità concettuale apre ad un interrogativo finale.

Il primo versante attiene alle proiezioni in tema di teoria del diritto.

L'esigenza poc'anzi rimarcata di ripensare il nesso tra dogmatica e certezza postula simmetricamente, in chiave più ampia, l'esigenza di rivedere i momenti strutturali che connotano l'intervento normativo, nonché gli schemi concettuali attraverso i quali il diritto legge la realtà sociale e, a sua volta, si autocomprende. L'analisi proposta mostra come appaia ormai quantomeno tortuoso il ricorso a modelli di *geometria juris* di ascendenza moderna o, analogamente, il rinvio a paradigmi *lato sensu* logico-assiomatici di "scienza del diritto" **à la** Kelsen maturati tra fine Ottocento e prima metà del secolo scorso.

Beninteso, ciò non significa abdicare alle istanze sottese alla modernità giuridica. Al contrario: l'esigenza di preservare il "cuore" del moderno giuridico, assiso sul binomio più volte evocato di dogmatica e certezza come sicurezza "calcolabile" con le correlate tutele della sfera soggettiva, richiede di misurarsi apertamente con paradigmi teorico-giuridici inediti.

Ed è qui che si stagliano i modelli reticolari cui si è accennato in precedenza. Prodottisi a seguito di una sorta di circolare rispecchiamento tra prassi e teoria, essi risultano funzionali a comprendere le dinamiche di cui si va ragionando costituendone, in parte, l'esito a livello teorico[35].

Un buon esempio è rappresentato proprio dall'assetto normativo concernente la cybersicurezza e, in combinato disposto, almeno in parte anche dalla disciplina relativa all'intelligenza artificiale. Il crescente articolarsi di disposizioni, così come il fiorire di *authorities* nazionali e sovranazionali dallo *status* ibrido[36], comporta un intersecarsi e parziale sovrapporsi di modelli di regolazione ad andamento reticolare: riflessivamente ne consegue il radicarsi di una autolettura "a rete" della sfera giuridica, con il conseguente incrinarsi del binomio moderno rappresentato dalla dimensione dogmatica e dal binomio certezza-sicurezza.

Di qui l'esigenza di rimarcare il ruolo della dimensione cognitiva sottesa ai nodi problematici sin qui segnalati. Intesa come dotazione epistemica[37], *ça va sans dire*

35 Bombelli 2017, in particolare cap. 3 circa il significativo fenomeno di rispecchiamento tra teoria e prassi e l'originarsi di un modello teorico inedito.

36 Parona 2021: rimarcando la molteplicità di ambiti investiti dalla *cybersecurity* e l'intersecarsi del livello privato e pubblico, l'Autore enfatizza la natura composita e in divenire della relativa disciplina (europea e nazionale). Si vedano, in particolare, le pp. 714-719 circa l'ambiguità e ibridità dell'*authority* nazionale, nonché la sua collocazione (in quanto disciplina *ad hoc*) nel quadro dell'articolazione dei poteri, con rilievi in ordine alla natura *command and control* di tali enti regolativi anche in relazione al crescente nesso tra *cybersecurity* e intelligenza artificiale.

37 La categoria o nozione di "cognitivo" è strutturalmente complessa: per un possibile sondaggio teorico Bombelli 2022b: 71-97. Le matrici originarie di tale prospettiva sono già presenti in Bombelli 2017, in particolare l'Introduzione e i capp. 1-2 con riguardo alla crucialità rivestita dall'orizzonte del "senso comune" (*common sense*) nel costituirsi dell'esperienza giuridica.

essa rappresenta da sempre una *conditio sine qua non* del diritto: da questa prospettiva, i temi di cui si va ragionando costituiscono una sorta di laboratorio del tutto peculiare. A ben vedere, la natura per molti versi "in-calcolabile" dei processi ascrivibili alla cybersicurezza richiede un *surplus* di dotazione cognitiva sia sul piano teorico, sia nella prassi di tutti gli operatori giuridici.

In tal senso appare allora plausibile parlare di "anticipazione cognitiva".

Più precisamente, con essa si fa riferimento all'esigenza di (ri)anteporre l'intervento normativo, colto appunto nella sua dimensione anche cognitiva, al *datum* sociologico (*rectius*: al fenomeno tecnologico) intervenendo "a monte" del medesimo. Per questa via, si tratta di ripristinare lo schema teorico maturato nella modernità e in cui, come osservato, al diritto si attribuiva propriamente il ruolo di griglia concettuale in grado di articolare, mediante le sue categorie, i fenomeni sociali.

Le proiezioni di tale prospettiva si possono cogliere distintamente in ordine a due figure tra loro connesse: il *legal design* e i processi di *decision-making*.

L'espressione *legal design*[38] viene qui utilizzata in termini semanticamente estesi.

Con essa si fa riferimento non solo al significato ordinario che, come noto, attiene alle modalità di redazione della disciplina giuridica tese a garantirne chiarezza, trasparenza e fruibilità, ma anche alla capacità della previsione normativa di cogliere il *proprium* del fenomeno regolato (in tal caso di natura tecnologica).

In altre parole, il *focus* va sull'insieme dei processi sottesi alla plasmazione quanto più pertinente dell'intervento giuridico. Si pensi, ad esempio, alla struttura degli algoritmi: il punto è diradarne l'intrinseca opacità, soprattutto a livello di valutazione giuridica, creando le condizioni affinché il diritto possa entrare "a monte" nei meccanismi cognitivi e *quindi* normativi che presiedono alla loro elaborazione.

Un versante, del resto, ben noto al diritto come avviene in ordine alla concettualizzazione di alcune nozioni, quali quelle già evocate, di "rischio" o di "principio di precauzione".

In esse la disciplina giuridica si configura necessariamente alla luce di una valutazione anche e soprattutto di tipo cognitivo, con riguardo alla specifica struttura delle materie regolate[39]. Da questa prospettiva, è il grado di *cognitum* a determinare l'*an* e il *quomodo* dell'intervento normativo: uno schema concettuale che, ad esempio, dal *climate change* si può estendere all'orizzonte della cybersicurezza, ove soprattutto ove si consideri quest'ultima in continuità logica con l'intelligenza artificiale.

Profili che si riflettono inevitabilmente a livello di configurazione del *decision-making*.

Analogamente a quanto poc'anzi osservato con riguardo alla nozione di *legal design*, anche in tal caso tale espressione va colta nella sua più ampia estensione. Con tutta evidenza essa investe immediatamente le forme del binomio sfera privata-sfera pubblica, ove in ultima istanza quest'ultima coincide con la dimensione politico-istituzionale *tout court*: ciò che rinvia al *continuum* 'sicurezza-funzionalità della democrazia'.

38 Per una presentazione agile e sintetica De Muro, Imperiale 2021.

39 Su queste nozioni rinvio a Bombelli 2022a (vedi anche *supra*).

Di qui, in termini più generali, l'esigenza di ripensare radicalmente il nesso tra meccanismi di produzione del sapere, diffusione della conoscenza e forme di regolazione del vivere associato.

Sotto questo profilo, come qualcuno suggerisce da tempo, acquista allora maggiore plausibilità l'apertura ad una sorta di "coproduzione" tra sapere scientifico (inclusivo delle sue più recenti proiezioni tecnologiche) e diritto[40]. A ben vedere, nell'idea di "co-produzione" si sintetizzano i profili epistemico-cognitivi e regolativi più volte evocati e che, come osservato, l'orizzonte della sicurezza (*sub specie* della cybersicurezza colta come spazio e luogo di esercizio di un potere di natura pubblica) enfatizza in modo peculiare. In definitiva, si tratta di creare le condizioni funzionali a un modello di intervento normativo "cognitivamente maturo" così da attingere, al contempo, a un gradiente di maggiore "democraticità" del sapere.

Ne discende un circuito logico. L'eventuale rimeditazione delle dinamiche di *decision-making* e delle relative *policies* rifluisce sulla configurazione del binomio pubblico-privato, nel quadro di uno scenario fortemente cangiante e in cui il tema della cybersicurezza riveste un ruolo potenzialmente decisivo[41].

Con uno sguardo d'insieme, si tratta di uno scenario connotato da prospettive problematiche e internamente complesse. Esso sembra confermare, come inizialmente accennato, la transizione progressiva dal paradigma moderno ad una grammatica concettuale differente, in grado di mettere in discussione i luoghi teorici decisivi intorno ai quali il primo era andato strutturandosi.

Ciò emerge con particolare riguardo alla sequenza, che di seguito si può solo sinteticamente tratteggiare, disegnata dalle nozioni di "spazio", "soggetti istituzionali", "fonti giuridiche", "norma" e, infine, dalla polarità "pubblico-privato" con la conseguente proiezione sui modelli statuali.

L'intrinseca problematicità del profilo regolativo (nazionale, sovranazionale e, ove presente, internazionale) quale emerge paradigmaticamente in tema di *cybersecurity* attesta, più in generale, la pervasività della tecnologia compromettendo la coppia concettuale di matrice moderna e statuale legata al nesso spazio-norma a base territoriale.

A cascata, muta anche il repertorio dei soggetti istituzionali. La rassicurante individuazione delle competenze risalente alle origini della modernità appare progressivamente inidonea a governare fenomeni strutturalmente refrattari a delimitazioni normative troppo nette, in tal modo originando una moltiplicazione degli attori normativi (come avviene paradigmaticamente con le *authorities*).

Ciò si riverbera sulla galleria delle "fonti" e, più estesamente, sull'idea di "ordinamento".

40 Intorno alla tesi della coproduzione tra conoscenza scientifica e diritto ragiona da tempo Mariachiara Tallacchini: una sintesi preziosa in Tallacchini 2012: 313-336.

41 Si fa qui riferimento a fenomeni molteplici ed eterogenei, come l'emergere di sistemi privati di cybersicurezza o a forme di partenariato pubblico-privato connesso all'istituzione di un polo strategico nazionale. In merito, ad esempio, Renzi 2021: 44.

L'implementarsi di normative a struttura reticolare, attraverso il crescente ricorso ad una disciplina dei fenomeni secondo uno schema a "cloud"[42], non solo revoca in dubbio la categoria stessa di "fonte" ma compromette, altresì, i modelli teorico-giuridici di natura sistematico-ordinamentale variamente elaborati nella tradizione precedente.

Simmetricamente cambiano gli schemi di lettura della "norma" giuridica. Sotto questo profilo, anche il binomio ormai risalente *hard law-soft law* appare in qualche modo logoro e insoddisfacente: a ben vedere, l'intero plesso regolativo dell'universo digitale, a partire dalle norme europee, si connota per una strutturale fluidità tipologica e concettuale.

Per questa via, infine, in prospettiva la riconfigurazione del binomio privato-pubblico[43] più volte rimarcata sembra postulare uno spazio *lato sensu* "pubblico" sinergicamente regolato da attori molteplici (al contempo "privati" e "pubblici" nell'accezione tradizionale). In tale riconfigurazione, inoltre, si intravede *in nuce* la trasformazione progressiva (reale o potenziale) del senso e del ruolo rivestito dalla "sicurezza" come orizzonte della narrazione giuridica moderna.

All'interno del modello delle fonti, definibile a "geometria varabile" e strutturalmente *in progress*, i fenomeni legati al tema della cybersicurezza mostrano, infatti, come l'obiettivo tuzioristico perseguito dal moderno possa realmente trasformarsi nel suo opposto interessando il complessivo assetto statuale. Più precisamente, ciò che viene a tema è la relazione tra Stato (come luogo "classico" del potere) e tecnologia (configurata come *cybersecurity*), con la sua eventuale declinazione in chiave tecnocratica.

Si tratta, allora, di ragionare non solo in termini di "sicurezza *del* potere" ma anche in chiave di "sicurezza *dal* potere"[44]: con lessico hobbesiano, il punto è la prevalenza progressiva della *security* sulla *safety*. La questione della trasparenza della *cybersecurity*, strumento di tutela della sfera individuale e al contempo potenziale forma controllo della medesima, si salda così all'ormai noto problema dei *Big data* in vista della plasmazione di una *governance* complessiva dei processi di cui si va ragionando. Sullo sfondo si intravede il possibile stagliarsi, forse in modo non troppo paradossale, della (cybers)sicurezza come una sorta di panottico digitale, originando una silente microfisica del potere[45] segnata dalla latente torsione del modello liberale in chiave di paternalismo democratico-tecnologico.

42 Ove la nozione di "cloud" non rinvia solo all'oggetto regolato, riferendosi essa anche ad alcuni profili della relativa tecnica regolativa. In merito, ad esempio, Macrì 2023 (con riguardo alle modifiche intervenute nel luglio 2023) e Macrì 2024; inoltre Macrì 2022b.

43 In merito si veda anche la recente presa di posizione di Unione Europea e dei suoi Stati membri in ordine alla nozione di "cyberspazio" finalizzata all'implementazione di modelli di cybersecurity: https://www.cybersecurity360.it/news/diritto-internazionale-nel-cyberspazio-ecco-le-regole-ue-per-la-corretta-applicazione/.

44 Sul punto si consenta rinviare nuovamente a Bombelli 2015a, in particolare: 70 e ss. (in particolare: 75-86, con riguardo sia ai riflessi giuridici in chiave teorica e operativa, sia al nesso tra antropologia e modello liberale).

45 Con ovvio riferimento al classico Foucault 1977.

Sono queste le ragioni che spingono a rimarcare il ruolo decisivo rivestito dalla dotazione cognitiva quando si ragiona del "diritto dell'era digitale"[46]. A ben vedere, il riferimento al momento cognitivo rileva non solo sul piano dell'ideazione del *framework* regolativo dei fenomeni tecnologici ma, in senso più ampio, come *conditio sine qua non* del corretto funzionamento degli apparati democratici (come ribadito espressamente, ad esempio, anche all'art. 1 del Regolamento sull'intelligenza artificiale evocato nelle pagine precedenti)[47].

Questioni e istanze che, come segnalato, aprono a un interrogativo conclusivo nel quale si può condensare l'itinerario teorico sin qui proposto dischiudendo orizzonti da decifrare.

Ove si intenda la sicurezza come un tratto (se non la *cifra*) della modernità giuridica, al contempo enfatizzando il nesso politica-diritto sotteso alla declinazione specifica del tema sicuritario moderno rappresentata dalla cybersicurezza, l'eventuale sottovalutazione dei profili cognitivi può comportare la delegittimazione dei sistemi democratici?

Un plesso tematico da dissodare e in attesa di risposte teoriche e operative.

Bibliografia

Beck U. 1986, *Risikogesellschaft Auf dem Weg in eine andere Moderne*, Frankfrut am Main: Suhrkamp.

Bombelli G. 2022a, "Causalità e diritto: paradigmi e alcune questioni teoriche, in *Jus*, 1-2: 177-230.

Bombelli G. 2022b, "Cognitive Turn? Tra giuspositivismo e giuscognitivismo. Alcuni riflessi socio-giuridici", in *Sociologia del diritto*, 1: 71-97.

Bombelli G. 2018, "Segno, simbolo, diritto: tra semiotica e semantica. Argomenti per un'ipotesi di lavoro", in Manzin M., Puppo F., Tomasi S. (a cura di), *Studies on Argumentation & Legal Philosophy / 3Multimodal Argumentation, Pluralism and Images in Law*, Trento: Università degli Studi di Trento: 5 ss.

Bombelli G. 2017, *Diritto, comportamenti e forme di "credenza"*, Torino: Giappichelli.

Bombelli G. 2015a, "Circuiti pericolosi: la sicurezza tra potere, mercato e contesti postmoderni", in F. Pizzolato-P. Costa (a cura di), *Sicurezza, Stato e mercato*, Milano: Giuffré: 47 ss.

Bombelli G. 2015b, "Diritto, decisione e paradigmi di "razionalità", in Bombelli G., Montanari B. (a cura di), *Ragionare per decidere*, Torino: Giappichelli: 321-358.

Bombelli G. 2010, *Occidente e 'figure' comunitarie. Volume introduttivo: "Comunitarismo" e "comunità". Un percorso critico-esplorativo tra filosofia e diritto*, Napoli: Jovene.

Bombelli G., Lavazza A. (a cura di) 2021, *Diritto e neuroscienze. Nuove prospettive*, Milano: Mimesis.

46 Mutuo l'espressione da Pascuzzi 2025: ivi si veda in particolare, per i temi discussi nel presente contributo, il cap. 26 *Cybersicurezza e rischio digitale*.

47 Ciò, soprattutto, ove si ponga mente al rapporto vieppiù ineludibile che il diritto intratterrà con altri saperi come, ad esempio, con l'ambito delle neuroscienze: in merito Bombelli, Lavazza 2019 e, più ampiamente, i saggi proposti in Bombelli, Lavazza 2021.

Bombelli G., Lavazza A. 2019, "Tecnologia, processi decisionali, sfera pubblica e diritto. Esplorazioni", in Buzzacchi C., Costa P., Pizzolato F. (a cura di), *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, Milano: Giuffré Francis Lefebvre: 3-34.
Bombelli G., Montanari B. (a cura di) 2015, *Ragionare per decidere*, Torino: Giappichelli.
Brighi R. 2021, "Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati", in Casadei T., Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano: Cedam: 135-147.
Buzzacchi C., Costa P., Pizzolato F. (a cura di) 2019, *Technopolis. La città sicura tra mediazione giuridica e profezia tecnologica*, Milano: Giuffré Francis Lefebvre.
Casadei T., Pietropaoli S. (a cura di) 2021, *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano: Cedam.
Cocco G. (a cura di) 2012, *I diversi volti della sicurezza*, Milano: Giuffré.
Cortesi A.D. (a cura di) 2019, *ICT e diritto nella società dell'informazione*, Torino: Giappichelli.
D'Aloia A. (a cura di) 2020, *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano: Franco Angeli.
De Muro B., Imperiale M. 2021, *Legal design*, Milano: Giuffrè, Milano.
Dimasi L. 2023, *I diritti ipermoderni: sfide e cambiamenti nell'era del costituzionalismo digitale*, Bologna: Bologna University Press.
Faini F., Pietropaoli S. 2021, *Scienza giuridica e tecnologie informatiche. Temi e problemi*, Torino: Giappichelli.
Foucault M. 1977, *Microfisica del potere*, Torino: Einaudi.
Frosini T.E. 2021, *Apocalittici e integrati. La dimensione costituzionale della società digitale*, Modena: Mucchi.
Galli G. 1995, *La politica e i maghi. Da Richelieu a Clinton*, Milano: Rizzoli.
Galli G. 1989, *Storia delle dottrine politiche*, Milano: Il Saggiatore.
Giaccardi C., Magatti C. 2022, *Supersocietà. Ha ancora senso scommettere sulla libertà?*, Bologna: il Mulino.
Giannuli A., Curioni A. 2019, *Cyberwar. La guerra prossima ventura,* Milano-Udine: Mimesis.
Golisano L. 2022, "Il governo del digitale: strutture di governo e innovazione digitale", in *Giornale di diritto amministrativo*, 6: 824-834.
Greco T. (a cura di) 2009, *Dimensioni della sicurezza*, Torino: Giappichelli.
Hobbes T. 2001 [1651], *Leviatano*, Parte I, XIV, 9-11, Milano: Bompiani.
Iannotti Della Valle A. 2023, *Le regole di Internet tra poteri pubblici e privati. Tutela dei diritti e ruolo dell'antitrust in una prospettiva costituzionale*, Napoli: Editoriale Scientifica.
Irti N. 2016, *Un diritto incalcolabile*, Torino: Giappichelli.
Macrì I. 2024, "Cybersicurezza, le novità per il 2024", in *Azienditalia*, 1: 17-22.
Macrì I. 2023, "Regolamentazione cloud: le novità per la PA", in *Azienditalia*, 11: 1334-1339.
Macrì I. 2022a, "Il PNNR italiano per la digitalizzazione della Pubblica Amministrazione", in *Azienditalia*, 1: 38-56.
Macrì I. 2022b, "Dalle infrastrutture digitali delle Amministrazioni al cloud, il nuovo regolamento per la sicurezza dei dati e dei servizi pubblici", in *Azienditalia*, 3: 488-504.
Macrì I. 2021, "Cybersicurezza per la Pubblica Amministrazione", in *Azienditalia*, 12: 1996-2006.
Pacchi A. 2004, *Introduzione a Hobbes*, Bari: Laterza.
Parona L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale di diritto amministrativo*", 6: 709-719.

Pascuzzi G. 2025, *Il diritto dell'era digitale*, Bologna: il Mulino.
Pizzolato F., Costa P. (a cura di) 2015, *Sicurezza, Stato e mercato*, Milano: Giuffré.
Renzi A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giornale di diritto amministrativo*, 4: 538-548.
Schmitt C. 1991 [1974], *Il Nomos della terra nel diritto internazionale dello 'jus publicum Europaeum'*, Milano: Adelphi.
Tallacchini M. 2012, "Scienza e diritto. Prospettive di co-produzione", in *Rivista di Filosofia del diritto*, 1 (2). 313-336.
Ziccardi G. 2022, *Diritti digitali. Informatica giuridica per le nuove professioni*, Milano: Cortina.