Paolo Heritier

Il dilemma della Cybersicurezza, tra reale e virtuale: uno sguardo prospettico. Una postfazione[*]

In questa breve conclusione, rinviando a un'ideale sequenza tra la prefazione e l'introduzione del primo e di questo volume, si intende in particolare dar conto della collocazione dei volumi in una rivista a titolo *Teoria e critica della regolazione sociale* che, aperta a contributi di giuristi, economisti, politologi e pur facendo del contesto della società complessa il suo ambito di riferimento, è frequentata in particolare da filosofi del diritto.

L'ipotesi che si propone come prospettiva per l'evoluzione del tema della cybersicurezza intende allora fornire linee di un possibile significato ampio e generale, in cui, da problema specifico e tecnologico, il dibattito tende a sollevare questioni concernenti la stessa configurazione della società contemporanea legate a essa.

La riflessione sulla cybersicurezza, all'interno della riflessione filosofico giuridica, tende spesso a essere letta come ambito proprio dell'informatica giuridica, nel tentativo di indicare come le tecnologie informatiche e il loro sviluppo, da un lato, le rilevanti questioni giuridiche di disciplina del settore, dall'altro, e l'esigenza di tenere insieme i due profili, richiedesse la competenza in entrambe i saperi, da parte dello studioso che se ne occupava.

La visione da cui qui si muove è in parte differente, provando a far interagire esperti di campi disciplinari anche molto lontani tra loro, con tutte le difficoltà che ciò implica, ma anche con l'interesse che tali incroci di sapere implicano. Come ricordato nella prefazione al primo volume, il convegno da cui i volumi traggono origine ha mirato proprio a questo obiettivo e la duplice pubblicazione, sia pure in modo più circoscritto e più limitato a scrittori prevalentemente di ambito giuridico, ne è testimonianza. Tale premessa spiega la metodologia proposta, e giustifica anche la conclusione, volta a indicare alcuni possibili ulteriori direzioni della ricerca da approfondire.

Il tentativo interdisciplinare che i due volumi provano infatti a percorrere – nell'alternanza di piccoli passi avanti conseguiti e di inevitabili stalli che devono essere messi in conto nel procedere, con risultati complessivi che il lettore dovrà giudicare – è una metodologia in cui il confronto fra le discipline diverse coinvolte, tecnologico-informatica, economico-organizzativa, giuridico-positiva, giungono a far intravedere la necessità di un dialogo fecondo intorno al nuovo contesto in cui i saperi chiamati in causa sono, per così dire, immersi.

* Scritto non sottoposto alla procedura di referaggio doppio cieco.

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: 10.7413/197054760168

L'impressione che si ricava da uno sguardo olistico ai due volumi è che la questione della cybersicurezza tenda sempre più a legarsi al, e in qualche modo a sciogliersi nel, classico problema sociale politico e giuridico della sicurezza, in un duplice movimento, per così dire a doppia elica, in cui la società entra in un quadro il cui significato dell'aggettivo 'cyber' e il termine cyberspazio la caratterizzano in modo crescente. Secondo la logica del principio di coproduzione tra tecnica, diritto e scienze sociali, e al seguito dell'apporto dei *Science and Technology Studies*[1], potremmo ripensare al termine cybersicurezza notando proprio due fenomeni da raccordare: il progressivo divenire del cyberspazio, inteso in senso comprendente, come l'ambiente posto tra reale e virtuale, che configura l'esperienza umana nella società contemporanea in quanto tale e l'esigenza speculare di ripensamento della nozione moderna di sicurezza come fondamento stesso delle forme di interazione sociale. 'Cyber' e 'sicurezza', in altre parole, nel loro reciproco avvicinarsi, mediato dalla nozione di 'spazio', si trasformano, divengono altro, configurando un nuovo ambito necessario di saperi che si intrecciano comunicando. Se questa esigenza di allargamento della platea di chi assiste al dibattito in tema è stata recentemente evocata, qui si intende estendere ancora di più questa prospettiva di ricerca, in primo luogo ai giuristi di diversi ambiti disciplinari, ma facendone una questione generale e dunque di interesse filosofico e metodologico. Rileva infatti efficacemente Di Resta, in relazione alla definizione in evoluzione del concetto di cybersicurezza, come corra l'obbligo di rilevare che il *Cyberspazio* sia un concetto più ampio di *internet*, condividendo forti elementi comuni con la nuova strategia europea volta a proteggere il diritto della protezione dei dati e i diritti fondamentali, considerati veri e propri pilastri del futuro mercato digitale che si prevede. In questo senso "il tema della *Cybersecurity* sarebbe una disciplina che non può essere più solo legata ad un dibattito "*militarizzato*" o comunque riservato a pochi esperti del settore"[2]. In quanto disciplina strettamente connessa al fattore umano[3] nell'organizzazione (pubblica o privata), Di Resta auspica che la discussione diventi "più trasparente e multilivello, non solo un dibattito riservato a livello di vertice istituzionale, con un maggior coinvolgimento della società civile, e che sia ispirato a un forte approccio multidisciplinare, poiché la *Cybersecurity* deve includere anche altri esperti – non solo esperti di informatica o di sicurezza informatica – come quelli della protezione dei dati, psicologi o esperti di comunicazione"[4].

Seguendo questa linea, ci chiediamo se il ragionamento dei due autori non sia da spingere addirittura oltre, configurando sullo sfondo la possibilità di un vero e proprio ritorno *filosofico giuridico* dei temi della cybersicurezza, evocando le origini stesse del diritto internazionale (e forse della stessa modernità) fondato nella visione di Grozio, ai tempi incipienti del dibattito sulla regolamentazione (o sull'assenza di essa) dell'*outer space*.

1 Sugli SST ci limitiamo a ricordare Jasanoff 2001.
2 Di Resta, Grassucci in Di Resta 2024: 255.
3 Bossomaier, D'Alessandro, Bradbury 2020.
4 Di Resta, Grassucci in Di Resta 2024: 255-256.

Le questioni che si stagliano sullo sfondo non appaiono solo organizzative, politiche e giuridiche, ma propriamente antropologiche, relative a quale concezione di diritto e di uomo siano implicate nel complesso problema della sicurezza sociale, politica e giuridica, pensata però in un contesto in cui reale e virtuale, umano e artificiale tendono a confondersi e interagire[5].

Si tratta di articolare diversamente, pertanto, la relazione tra ciberspazio e sicurezza nella riflessione filosofico giuridica. Proverò a indicare alcune linee in questa direzione.

La visione reticolare del diritto emersa a inizio millennio[6], successivamente estesa a problematizzare i profili di *governance* inevitabilmente indotti dall'emergere da una profonda trasformazione delle fonti in corso[7], ha condotto in primo luogo i filosofi del diritto a interrogarsi sulla natura estetica[8] e virtuale[9] dell'ordinamento giuridico, legata al modello kelseniano e alla critica della qualificazione giuridica (appunto virtuale) del fatto (reale) accaduto.

La stessa evoluzione del concetto di testo e la dimensione iper-testuale scaturita dalla Rete Internet, rilevante per tutti i giuristi in seguito alle trasformazioni delle banche dati e della conoscenza giuridica disponibili, come seguito *digitale* della tecnica storica della glossa e dal conseguente affermarsi del cyberspazio[10] come luogo sociale di interazione (Second Life, Metaverso), appare la premessa della rivoluzione mediatica digitale. I problemi della sicurezza si rilevano in questo contesto in tutta la loro rilevanza sociogiuridica, prima con l'emergere delle pratiche selvagge di profilazione e di violazione della privacy legati allo strapotere delle *corporation* e all'emergere del capitalismo della sorveglianza[11] e poi in seguito all'onda prepotentemente in corso in corso concessa all'intelligenza artificiale.

Il problema, a un tempo economico, politico e giuridico della sicurezza su cui sorge la stessa concezione del diritto positivo moderno, non può non seguire dunque questo itinerario sul piano *cyber*, configurando un quadro in cui i progetti di meccanizzazione dell'umano, innescati dalla continuità posta tra progetto cibernetico, scienze cognitive[12] e *machine learning*, giungono ad assegnare all'AI un valore salvifico sia dal punto organizzativo ed epistemologico, sia, financo, religioso[13].

La domanda filosofico-giuridica radicale che pone Montanari in un contesto pre-cyber, se la società del benessere intenda oggi barattare la libertà con la sicu-

5 Diversamente sul tema Moallem 2019; Paglia 2024.

6 Due testi quasi contemporanei a inizio millennio, al momento della rivoluzione di Internet, indicavano questa prospettiva rispettivamente dal punto di vista della teoria generale del diritto e della filosofia giuridica: Ost, De Kerchove 2002; Heritier, 2003.

7 Nella sterminata bibliografia mi limito a indicare Lenoble, Maesschalck, 2010; Andronico 2012; Ferrarese 2010.

8 Robilant 1999.

9 Gentile 2005.

10 Tagliagambe 1996.

11 Denunciata dopo un decennio di sostanziale far west nel settore, come è ampiamente noto, sul piano giuridico e politico da Zuboff 2019 e sul piano filosofico da Stiegler 2019.

12 J.P. Dupuy 2015.

13 Pentland, 2015.

rezza[14], e variamente le analisi di Bombelli, Pizzolato e Costa[15], nel porre la tripartizione tra sicurezza attraverso la tecnica (tecnologie securitarie), sicurezza della tecnica (sicurezza dei prodotti tecnici), sicurezza dalla tecnica (rispetto all'uso che altri ne fanno, come la sicurezza del web) precisano un nodo complesso, che chiama in causa una precisa antropologia relazionale moderna necessariamente messa in questione. Il ricorrente ritorno della figura del doppio virtuale della persona e dell'ambiente digitale da abitare, da ultimo nel Metaverso, il gemello digitale[16], sollevano, oltre ai nuovi problemi normativi, un problema antico.

L'individuazione nel fondamento hobbesiano sulla paura della radice della concezione dello stato moderno (il Leviatano), legata anche al principio di precauzione[17], rappresenta una specifica concezione antropologica che mi pare oggi in questione[18]. Specie se analizzata dalla prospettiva che indicava già negli anni Sessanta del secolo scorso Böckenförde, concernente il rilievo secondo il quale lo stato liberale, per amore della libertà, distrugge i presupposti antropologici sui quali pur si fonda. La celebre forma del *dilemma* assume su di sé il paradosso per il quale lo stato si fonda su una dimensione morale condivisa dai cittadini – esattamente quel che giustifica à la Kelsen l'obbedienza dei cittadini alla legge. Tuttavia, la necessità di garantire *per via coercitiva e autoritativa* il fondamento di tale obbedienza implica il paradosso del tornare ad avviarsi verso una via che lo conduce all'implosione della democrazia e del proprio carattere liberale[19]. Ora l'assai noto *dilemma di Böckenförde*, la cui attualità non mi pare possa essere negata oggi, può essere accostato a quello che Buchanan configura come il *paradosso della cybersicurezza*. Una breve analisi dell'argomentazione di Buchanan ci è allora utile a indicare la rilevanza antropologica, e conseguentemente politica e giuridica del problema che affiora dall'incrocio tra i due dilemmi, quello della legittimazione dello stato liberale e della democrazia e quello delle politiche di cybersicurezza investigate in questi volumi. Con una aggiunta, però: inducendoci a interrogaci sull'utilità – seguendo e parafrasando il percorso intellettuale di Jean-Pierre Dupuy[20], applicato però al campo specifico di cui stiamo parlando – di una filosofia della cybersicurezza, da connettere idealmente a una filosofia del diritto, a un'antropologia filosofica e a

14 Montanari 2012: 10.

15 Bombelli 2015; Pizzolato, Costa 2017.

16 Tagliagambe 2022.

17 Dupuy 2011, Sunstein 2010.

18 Mi permetto di rinviare al motto '*homo homini homo*', che intende contrapporsi ai due estremi antropologici dello '*homo homini lupus*' hobbesiano e dello '*homo homini deus*' spinoziano e baconiano (oggi posto alla base della mitizzazione della tecnologia come tecnica di controllo sociale, ben rappresentata dalla proposta di 'fisica sociale' del già citato Pentland). P. Heritier, Homo Homini Homo. *Frammenti di un'antropologia*, 2 voll., in corso di pubblicazione.

19 Böckenförde 2006.

20 L'itinerario del professore di Stanford erede della cattedra di Girard mi pare dunque assai rilevante anche per il tema della cybersicurezza. Se l'applicazione della matrice matematica della teoria del punto fisso endogeno ed esogeno alla filosofica politica e sociale è un tratto costante della produzione dell'epistemologo, è proprio l'analisi del rischio e del principio di precauzione suggerita nella proposta di un "catastrofismo illuminato".

una metodologia delle scienze sociali, come inevitabili esiti della generalizzazione delle problematiche poste.

L'itinerario del professore di Stanford, infatti, erede della cattedra di Girard ma anche allievo di von Foerster e Illich, se realizza già al suo interno una forte interdisciplinarità, mi pare dunque assai rilevante anche per il ripensamento del tema della cybersicurezza. Pur se non appare certo possibile svolgere l'analisi del *catastrofismo illuminato* in questa sede, occorre limitarsi a qualche breve cenno. Se infatti l'applicazione della matrice matematica della teoria del punto fisso endogeno ed esogeno alla filosofica politica e sociale è un tratto costante della produzione dell'epistemologo[21], è proprio l'analisi del rischio e del principio di precauzione suggerita nella proposta di un "catastrofismo illuminato"[22], volto a pensare in un dossier per il governo francese l'utilizzo possibile del principio di precauzione all'inizio del terzo millennio, a costruire la base predittiva per l'analisi della piccola metafisica degli tsunami[23], culminata poi nel saggio di metafisica dedicato recentemente alla guerra nucleare[24].

L'elemento che mi pare interessante da ricercare nella teoria del catastrofismo illuminato dupuiano è proprio la logica di azione predittiva, a un tempo sistemica e antropologica, che egli propone, a fronte dell'uso delle tecnologie e del problema del male nelle relazioni umane[25]. La proposta metodologica si pone infatti precisamente a quel livello fondativo che il dilemma di Böckenförde solleva come problema per le democrazie contemporanee, nell'occuparsi precisamente degli effetti antropologici diffusi della logica della paura e della necessità di un patto sociale, da non condurre più esclusivamente secondo le analisi hobbesiane dello *homo homini lupus*. La presa in conto contemporanea del *dilemma di Böckenförde* e del *paradosso della cybersicurezza* di Buchanan che stiamo per analizzare, mi sembra quindi poter contenere il rinvio a una concezione diversa del diritto e della metodologia dell'interazione sociale regolata. Tale analisi filosofico giuridica, tuttavia, mi pare promettente proprio anche in relazione alla comprensione effettiva delle problematiche complessive che la gestione degli aspetti a un tempo privatistici e pubblicistici, nazionali e internazionali, tecnologici e antropologico-gestionali, che la questione della cybersicurezza fa emergere. La prospettiva che mi pare dischiudersi, e che debba essere portata avanti ben oltre questi due volumi in ottica interdisciplinare, indica che la cybersicurezza non possa affatto essere ridotta a un mero aspetto tecnologico, gestionale, normativo, ma alluda alla necessità di concepire un nuovo paradigma di riflessione politico e fondativo delle democrazie. Tema, questo, che già il conflitto tra prevenzione e precauzione, e l'emergere dell'intelli-

21 Dupuy 2009. Per un'esposizione sintetica del tema e della sua rilevanza giuridica mi permetto di rinviare a Heritier 2012: 125-136.

22 Dupuy 2011. Testo da me tradotto.

23 Dupuy 2006.

24 Dupuy 2022.

25 Dupuy 2015, e 2010, testi tradotti da me, ove l'autore ricostruisce l'ideologia tecnologica cibernetica posta alla base delle scienze cognitive (e, mi permetto di aggiungere, della contemporanea intelligenza artificiale) e della problematica politica del male e della paura.

genza artificiale come tecnologia dall'impatto sociale rilevante, chiede di prendere in conto in termini generali e propriamente filosofici[26].

Limitiamoci dunque a indicare conclusivamente come il problema del dilemma di Böckenförde possa essere duplicato nel paradosso della cybersicurezza, indicato in un recente testo[27].

Muovendo dal presupposto che il tema del cyber hacking rilevi oggi anche della disciplina delle relazioni internazionali, Buchanan precisa il dilemma riferendosi al celebre episodio della Baia dei Porci nel 1962, in cui il mondo si è avvicinato realmente a un conflitto nucleare tra Stati Uniti e Russia.

Il dilemma politico e relazionale già presente in quel potenziale conflitto è costituito dal fatto che quella che i primi ritenevano costituire un'attività difensiva benigna fosse stato interpretato dai sovietici impauriti come una traiettoria di volo, effettuata dal pilota americano apparentemente aggressiva, e dunque da considerare una seria minaccia[28]. L'autore legge la situazione come *paradigmatica della crisi* proprio di un sistema di sicurezza nucleare, oggi ritornato drammaticamente attuale dopo l'invasione dell'Ucraina da parte della Russia e l'evocazione conseguente dello spettro della guerra nucleare, legato appunto al fraintendimento delle reali intenzioni dell'avversario. Buchanan sostiene che la medesima logica può essere vista all'opera nei processi decisionali propri degli Stati relativi alla cybersicurezza, specie in un contesto di riemergere di un mondo a blocchi contrapposti economici e militari, dopo la crisi della globalizzazione[29]. Sinteticamente, i tre pilastri che l'autore propone per l'analisi del paradosso sono rappresentati:

– dal fatto che il desiderio degli Stati per operazioni future di cybersicurezza spinge ad agire in anticipo per rendere tali operazioni possibili[30] e, conseguentemente, di fronte all'azione similare di altri stati, ci si trova di fronte a un dilemma di interpretazione delle intenzioni simile a quello della baia dei Porci (preparazione di un attacco o semplice misura "preventiva" priva di attuali intenzioni malevoli?);

– dal fatto che gli stati hanno ragioni che sono realmente difensive per lanciare intrusioni informatiche nelle reti di altri stati, al fine di migliorare i propri sistemi raccogliendo informazioni utili e scoprendo futuri rischi tramite attività che possono rimanere del tutto nascoste[31];

– infine dalla tendenza, in tale situazione di ambiguità delle intenzioni, a sbagliare sul lato della cautela, pensando al peggio[32].

Sulla base di tali pilastri analitici, la conclusione di Buchanan è che il paradosso della cybersicurezza, legato all'ambiguità di interpretazione del comportamento

26 Galletti, Zipoli Caiani 2024.
27 Buchanan 2016.
28 Buchanan 2016: 15-16.
29 "Ognuno degli elementi che hanno governato il caso della Guerra Fredda ed altri ancora, come la natura anarchica del sistema internazionale, la necessità per gli Stati di predisporre le proprie abilità e i sistemi di *intelligence*, e il rischio sempre presente di un'interpretazione errata e di un'escalation, ha un'enorme rilevanza nella cybersecurity". Buchanan 2016: 17.
30 Buchanan 2016: 48.
31 Buchanan 2016: 72.
32 Buchanan 2016: 96.

dell'avversario, tenderà a aumentare di rilevanza, nella dinamica delle relazioni internazionali[33]: non solo in caso di crisi, ma anche nella mera previsione di una crisi possibile, implicando investimenti in strategie aggressive, formazione del personale, unità militari di cibersicurezza, e finendo per generare nuova paura[34]. Il paradosso può insomma condurre a risultati che nessuno stato realmente desidera, senza che si intraveda la possibilità di individuare una via di uscita facile[35].

Se l'analisi di Buchanan è verosimile, non è difficile notare come la forma del paradosso raggiunga il dilemma di Böckenförde, indicando una situazione potenzialmente erosiva nella stessa relazione umana: ove il progresso rischia di generare dinamiche in grado di distruggere la società. Ove la distruzione è letterale nel caso di una guerra nucleare, semplicemente metaforica nel caso della crisi dello stato liberale e della democrazia e nella difesa dai cyberattacchi (anche se la vicinanza tra questi ultimi e la guerra nucleare apre scenari certo imprevisti). Entrambe le soluzioni rinviano a una riproposizione del patto sociale, e dunque all'ipotesi che evoluzione della cybersicurezza e crisi dello stato liberale rappresentino due differenti versioni dello stesso problema: la difficile articolazione di libertà e sicurezza. Problemi che domandano di pensare, a parere di chi scrive, a nuove forme di risposte non più riferite allo scenario moderno delineato da Hobbes e relativo alla fondazione della norma sulla paura e sulla sanzione (scenario che sembra l'esito del ritorno al principio di precauzione di fronte alle catastrofi, da quella climatica a quella nucleare).

Così, appare possibile estendere, conclusivamente, la logica del paradosso della cybersicurezza in altre direzioni. Le particolarità della dinamica delle relazioni internazionali indica una logica di fondo che, tenendo conto ovviamente delle differenze di situazioni, di investimenti, di attori protagonisti, di circostanze, può differentemente configurarsi anche nelle relazioni private e pubbliche, proprio a partire dalla sostanziale pervasività che si annuncia dei problemi di cybersicurezza, in una società che si approssima a sciogliere, forse definitivamente, la distinzione tra reale e virtuale in una realtà aumentata, sia essa propria del Metaverso[36] o di altre fattezze oggi ancora ignote, in cui il limite tra presenza fisica e presenza virtuale diventerà sempre più elastico e sfumato.

Se già infatti sono stati resi noti casi di "reati" relativi a offese verso la "persona" (ad es. stupri virtuali) commessi nel Metaverso, il problema stesso della cybersicurezza tende a divenire, per la sua articolata dimensione che si estende dal profilo delle relazioni tra stati a quelle fra privati, una questione di sicurezza trasversale, che dai sistemi di sicurezza informatica si volge fino alla stessa "corporeità virtuale" (qualsiasi cosa possa significare l'ossimoro). In una possibile riproposizione del problema di fondo dell'antropologia moderna da cui scaturiscono i diritti dell'uomo, e che, come ha precisato Böckenförde, è alla base del dilemma dello Stato liberale, nel suo connettere libertà e sicurezza.

33 Buchanan 2016: 155.
34 Buchanan 2016: 188.
35 Buchanan 2016: 194.
36 Tagliagambe 2022.

Se la proposta di una filosofia della cybersicurezza, che mi pare al tempo stesso una filosofia del diritto, mi pare implicita nella proposta di Dupuy di un *catastrofismo illuminato*, molte altre riflessioni si prospettano come necessarie di fronte a un cambio di paradigma radicale nella concezione stessa nel giuridico e nelle relazioni sociali, politiche ed economiche tra uomini, che, intravisto all'orizzonte, si sta avvicinando in modo sempre più veloce. È a tale orizzonte che, mi pare, che la riflessione tecnologica, organizzativa e istituzionale sulla cybersicurezza si debba altrettanto rapidamente confrontare, fornendo nuove soluzioni sociali (e non solo tecnologiche, o normative) innovative a vecchi problemi fondamentali, e non limitandosi a seguire la riproposizione di logiche di potere che appaiono oramai consunte, in primo luogo dal punto di vista delle relazioni umane che presuppongono: configurando un nuovo settore di studi autenticamente interdisciplinari e critici.

Bibliografia

Andronico A. 2012, *Viaggio al termine del diritto*. *Saggio sulla* governance, Torino: Giappichelli.

Böckenförde E.W. 2006, *Stato, costituzione, democrazia. Studi di teoria della costituzione e di diritto costituzionale,* Milano: Giuffrè.

Bossomaier T. D'Alessandro S. Bradbury R. 2020, *Human Dimension of Cybersecurity,* Baca Raton, London, New York: CRC Taylor and Francis.

Bombelli G. 2015, *Circuiti pericolosi. La sicurezza tra potere, mercato, e contesti postmoderni. Annotazioni filosofico-giuridiche* in Pizzolato F. Costa P. (a cura di), *Sicurezza, stato e mercato,* Milano: Giuffrè.

Buchanan B. 2016, *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations,* New York: Oxford University Press.

Dupuy J.-P. 2006, *Piccola metafisica degli tsunami. Male e responsabilità nelle catastrifi del nostro tempo*, Roma: Donzelli.

Dupuy J.-P. 2009, *Dans l'oeil du cyclone. Colloque de Cerisy,* ed. Anspach M., Paris: Carnets Nord.

Dupuy J.-P. 2010, *Avevamo dimenticato il male? Pensare la politica dopo l'11 settembre,* Torino: Giappichelli.

Dupuy J.-P. 2011, *Il catastrofismo illuminato. Quando l'impossibile è certo,* Milano: Medusa.

Dupuy J.-P. 2015, *All'origine delle scienze cognitive. La meccanizzazione della mente,* Milano: Mimesis.

Dupuy J.-P. 2022, *La guerre qui ne peut pas avoir lieu, Essai de métaphysique nucléaire,* Paris: Desclée de Brouwer.

Ferrarese M. R. 2010, *La* Governance *tra politica e diritto*, Bologna: Il Mulino.

Galletti M. Zipoli Caiani S. eds. 2024, *Filosofia dell'Intelligenza Artificiale. Sfide etiche e teoriche,* Bologna: Il Mulino.

Gentile F. 2005, *Ordinamento giuridico, tra reale e virtuale,* Padova: Cedam.

Heritier P. 2003, *La rete figurale del diritto. Materiali per un ipertesto didattico, Urbe Internet, vol. 1*, Torino: Giappichelli (Theleme 2001).

Heritier P. 2012, *Estetica giuridica. Vol. 2. A partire da Legendre. Il fondamento finzionale del diritto positivo,* Torino: Giappichelli.

Jasanoff S. 2001, *La scienza davanti ai giudici. La regolazione giuridica della scienza in America,* Milano: Giuffrè.
Kosseff J. 2020, *Cybersecurity Law,* Hoboken: Wiley.
Lenoble J. Maesschalck M. 2010, *Democracy, Law, Governance,* London: Routledge.
Moallem A. ed. 2019, *Human-computer Interaction and Cybersecurity Handbook,* Boca Raton: Crc Taylor and Francis.
Montanari B. 2012, *Capire l'oggi*, in Montanari B., ed. *Luoghi della filosofia del diritto. Idee strutture mutamenti,* Torino: Giappichelli.
O' Connell M. 2018, *Essere una macchina. Un viaggio attraverso cyborg, utopisti, hacker e futurologi per risolvere il modesto problema della morte,* Milano: Adelphi.
Ost F. De Kerchove M, 2002, *De la pyramide au résau? Pour une théorie dialectique du droit*, Bruxelles: Presses Universitaires de Bruxelles.
Paglia V. 2024, *L'algoritmo della vita. Etica e intelligenza artificiale,* Casale Monferrato: Piemme.
Pentland V. 2015, *Fisica sociale. Come si propagano le buone idee,* Milano: Università Bocconi Editore.
Pizzolato F. Costa P. 2017, *Sicurezza e tecnologia,* Milano: Giuffrè.
Resta F. di 2024, *Privacy, data protection, cybersecurity e artificial intelligence,* Roma: Duepuntozero.
Robilant E. di 1999, *Diritto, società e persona. Appunti per il corso di filosofia del diritto 1998-1999,* Torino: Giappichelli.
Stiegler B. 2019, *La società automatica. Vol 1. L'avvenire del lavoro,* Milano: Meltemi.
Sunstein, C.R. 2010, *Il diritto della paura. Oltre il principio di precauzione,* Bologna: Il Mulino.
Tagliagambe S. 1996, *Epistemologia del cyberspazio*, Cagliari: Demos.
Tagliagambe S. 2022, *Metaverso e gemelli digitali. La nuova alleanza tra reti naturali e artificiali* Mondadori: Milano.
Tikk E. Kertunen M. 2020, *Routledge Handbook of International Cybersecurity,* Abingdon, New York: Routledge.
Zuboff S. 2019, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma: LUISS.