TCRS 2/2024

Teoria e Critica della Regolazione Sociale

MIMESIS

CYBERSECURITY
E ISTITUZIONI DEMOCRATICHE
UN'INDAGINE INTERDISCIPLINARE: DIRITTO, INFORMATICA E ORGANIZZAZIONE AZIENDALE

Fascicolo I

A cura di/Edited by
Giovanni Bombelli e Stefano Rossa

Introduzione di Alberto Oddenino

La presente pubblicazione è finanziata dal Bando Ricerca UPO 2022 a valere su risorse Next Generation EU e Compagnia di San Paolo, in quanto realizzata nell'ambito del progetto "Cybersecurity Risk Governance in Public Administration – CybeR-GoPA" (ID: 1083758, CUP: C15F21001720001), componenti Prof. Roberto Candiotto, Prof.ssa Lavinia Egidi, Prof.ssa Bianca Gardella Tedeschi, Prof. Paolo Heritier, Dott. Stefano Rossa (responsabile scientifico). Si precisa che il Dott. Stefano Rossa è ricercatore t.d. con contratto finanziato da Commissione Europea – FSE REACT-EU, PON Ricerca e Innovazione 2014-2020 – CUP C65F21001410001. Volume pubblicato con il contributo dell'Università del Piemonte Orientale, Dipartimento per lo Sviluppo Sostenibile e la Transizione Ecologica.

Tutti i contributi del presente volume, ove non diversamente esplicitato in nota, sono stati sottoposti a procedura di doppio referaggio cieco.

Mimesis Edizioni (Milano – Udine)
www.mimesisedizioni.it
mimesis@mimesisedizioni.it

Issn: 1970-5476
Isbn: 9791222320786

Piazza Don Enrico Mapelli, 75
20099 Sesto San Giovanni (MI)
Phone: +39 02 24861657 / 21100089

Registrazione presso il Tribunale di Milano n. 299 del 23-10-15

Indice

Stefano Rossa*

*La necessità dell'indagine scientifica nel contesto del 'rischio da ignoto tecnologico': il caso della cybersecurity, fra multidisciplinarietà e approcci sinergici. Prefazione***

Uno dei fini dello Stato – se non *il* fine ultimo – è garantire la protezione dei propri cittadini, salvaguardandone le situazioni giuridiche soggettive, *anche* tramite il "monopolio dell'uso legittimo della forza fisica"[1]. Circostanza nota e messa in luce da grandi filosofi quali Popper[2] e, prima ancora, pur con l'intento di legittimare l'esistenza di differenti forme di Stato, da Hobbes[3], Locke[4] e Rousseau[5].

Nel corso della Storia gli Stati hanno perseguito tale obiettivo, molto spesso, con sforzi e difficoltà. Oggi, tuttavia, tale compito appare ancora più arduo.

Come ha teorizzato Ulrich Beck, la c.d. società classista (o industriale), che in conseguenza della scarsità delle risorse cercava di risolvere la questione "di come la ricchezza prodotta nella società potesse essere distribuita in maniera socialmente diseguale ma *nel contempo* legittima"[6], è stata soppiantata dalla c.d. società del rischio. Una società post-moderna[7], liquida[8], nella quale il pericolo non deriva più unicamente da fattori esterni[9], come accadeva in precedenza[10], ma esso è la diretta conseguenza del progresso tecnologico a cui la società stessa ricorre per evolvere e progredire[11]. Venendo dunque meno la sua funzione cata-

* Si precisa che l'autore è ricercatore t.d. tipo A) con contratto finanziato da Commissione Europea – FSE REACT-EU, PON Ricerca e Innovazione 2014-2020 – CUP C65F21001410001.

** Contributo non sottoposto alla procedura di referaggio doppio cieco.

1 Così come emerge dalla definizione di Stato elaborata da Weber 2006 [1919]: 5.

2 Popper 1962: 109-110: "*What do we demand from a state? […] I demand protection for my own freedom and for other people's*".

3 Cfr. Hobbes 1642 e, soprattutto, *Id.* 1651.

4 Cfr. Locke 1689.

5 Cfr. Rousseau 1755 e, in particolare, *Id.* 1762.

6 Beck 2000 [1986]: 25.

7 Beck 2000 [1986] si veda anche Luhmann 1991 e Giddens 1990.

8 Il riferimento è chiaramente a Bauman 2000.

9 In tal senso Giddens 1990: 110: "*[i]n conditions of modernity, the dangers we face no longer derive primarily from the world of nature*".

10 Così Beck 2000 [198]: 219 "Se in passato ci trovavamo esposti a pericoli provenienti *dall'esterno* (dagli dèi o dalla natura), la qualità storicamente nuova dei rischi del giorno d'oggi deriva una *decisione interna*. Ciò dipende da una *costruzione* allo stesso tempo *scientifica e sociale*".

11 Cfr. Beck 2000 [1986]: 25: "Nella modernità avanzata la produzione sociale di *ricchezza* va sistematicamente di pari passo con la produzione sociale di *rischi*. Analogamente, ai problemi ed ai conflitti distributivi della società basata sulla penuria si sovrappongono problemi

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760143

lizzatrice di benessere sociale, ma anzi risultando la principale fonte di pericolo, la tecnologia pone un interrogativo allarmante: "[c]om'è possibile impedire, minimizzare, drammatizzare, canalizzare i rischi e i pericoli prodotti sistematicamente come parte del processo di modernizzazione? E quando si presentano sotto forma di 'effetti latenti collaterali', come limitarli, diluirli distribuendoli in modo che non ostacolino il processo di modernizzazione né travalichino i confini di ciò che è considerato 'tollerabile' dal punto di vista ecologico, medico, psicologico e sociale?"[12].

Come intuibile, rispondere a tale domanda non è affatto semplice, a maggior ragione per due motivi: in tale contesto di "rischio da ignoto tecnologico"[13] (o da "incertezza scientifica"[14]), da un lato, le situazioni che si palesano assumono valenza sovranazionale e intertemporale, travalicando globalmente i confini degli Stati[15] e spingendo i decisori pubblici all'ardua composizione di contrapposte posizioni politiche – si pensi, ad esempio, al rapporto fra economia e tutela dell'ambiente nella prospettiva intergenerazionale dello sviluppo sostenibile[16]. Dall'altro lato, la scienza tende a sovrapporsi alla tecnica, riflesso della persistente centralità dei processi produttivi[17], facendo in tal modo venir meno la funzione di indagine e di elaborazione di risposte ai problemi della società[18].

e conflitti che scaturiscono dalla produzione, definizione e distribuzione di rischi prodotti dalla scienza e dalla tecnica".

12 Beck 2000 [1986]: 25-26.

13 Chiaro in proposito Stella 2002: 3: "[t]utti sanno che lo sviluppo della tecnologia degli ultimi decenni ha determinato cambiamento radicali del sistema produttivo, con accelerazioni esponenziali ampie, improvvise e sempre più numerose; e queste accelerazioni hanno costituito la fonte di nuovi pericoli che impongono un ripensamento degli schemi tradizionali, nell'ambito di una nuova concezione del diritto civile e del diritto amministrativo, che mette in discussione la vecchia razionalità e il vecchio modo di calcolare le conseguenze delle nostre azioni". Come spiega Lombardi 2008: 5, tale rischio appare *ignoto* in conseguenza della "sua derivazione da complessi processi tecnologici per i quali mancano punti di raffronto e di riferimento con le esperienze del passato".

14 In tal senso Barone 2006: 16.

15 Sulla relazione fra globalizzazione e diritto pubblico la dottrina è immensa, ragion per cui *ex multis* si vedano Ferrarese 2000 e 2002; Cassese 2003 e 2009; Marino 2005: 25 ss.; Ferrara 2005: 201 ss. e da ultimo *Id.* 2023a: 28 ss. Globalizzazione la quale, tuttavia, pare doversi confrontare con il 'rispolvero' della sovranità nazionale, come rilevato da Ferrarese 2022: 153 ss. e da Casini 2022.

16 In argomento Fracchia 2010; Crosetti, Ferrara, Fracchia e Olivetti Rason 2018; Fracchia e Vernile 2022: 15 ss.; De Leonardis 2023. In relazione al tema dell'intergenerazionalità si veda anche Pantalone 2023.

17 Cfr. sul punto Ferrara 2023b: 789 ss.: "La scienza sembra diventare, sotto questo riguardo, un mero accumulatore e propulsore della tecnologia, e cioè scienza applicata in funzione degli impieghi pratici che dalle sue scoperte possono essere fatti discendere, in un crogiolo di saperi esperti che enfatizzano il ruolo giocato, nella società civile, dagli scienziati e forse ancor più dai tecnici che operano nella concretezza dei processi produttivi".

18 Così Barone 2006: 16: "[l]a scienza perde la sua autonomia, confondendosi con la tecnica, e al contempo fallisce nel fornire 'certezze' sul modo di affrontare e neutralizzare i rischi da essa stessa (più o meno direttamente) generati".

La scienza risulta dunque essere la causa del rischio da ignoto tecnologico. Come messo in luce da Beck, però, essa appare esserne anche il rimedio[19]. Tuttavia, proprio in conseguenza di tale contraddittorietà, è più che mai necessario l'intervento positivo delle Istituzioni Pubbliche[20], tramite la predisposizione di strumenti giuridici e amministrativi volti a gestire tale complessità. Intervento non certamente mirato a eliminare l'eventualità di un rischio ineliminabile, bensì a redistribuirlo nella società[21], nel migliore dei modi possibili, giungendo a soluzioni quanto più ottimali in una logica di giustizia sociale.

Un simile intervento pubblico si è concretizzato, come noto, in strumenti di gestione e valutazione del rischio basati su principi giuridici, in particolare su quello di precauzione[22], anziché su regole prescrittive[23].

Se tale disciplina giuridica ha interessato inizialmente l'ambiente e la salute[24], negli ultimi anni è stata applicata anche al digitale.

Questo aspetto emerge innanzitutto dal Regolamento europeo sull'Intelligenza Artificiale (c.d. EU AI Act)[25], nel quale il legislatore europeo ha tripartito i sistemi di AI in "classi di rischio" (rischio inaccettabile, rischio alto e rischio basso o minimo) in relazione all'impatto di tali strumenti d'automazione sui diritti fondamentali degli individui, sulla salute e sulla sicurezza, prevedendo – in base al concetto *the higher the risk, the stricter the rules*[26] – regole più rigide all'aumento della classe di

19 Cfr. Beck 2000 [1986]: 219: "La scienza è una delle cause, il medium della definizione e la fonte delle soluzioni dei rischi".

20 In tal senso *ex multis* Laus 2023: 12.

21 Lo stesso Beck 2000 [1986]: 35, infatti sottolinea che "[c]ome le ricchezze, i rischi sono oggetto di distribuzioni e sia le une che gli altri creano situazioni: situazioni di *classe* (*Klassenlagen*), o situazioni di *rischio* (*Risikolagen*). Tuttavia, in questi due casi si ha a che fare con un bene diverso e con un diverso tipo di conflitto relativo alla sua distribuzione. Nel caso delle ricchezze della società si ha a che fare con beni […] scarsi e desiderabili. Al contrario, i rischi sono un prodotto secondario della modernizzazione in *indesiderabile abbondanza*, che va o eliminata, o negata, o reinterpretata. Alla *logica positiva dell'appropriazione* si contrappone quindi una *logica negativa dello smaltimento*, dell'evitare, del negare, del reinterpretare".

22 Fra i numerosi contributi si vedano De Leonardis 2005 e 2012: 413 ss.; Marino 2011: 2177 ss.; Cognetti 2014: 127 ss.; Laus 2023: 99 ss.

23 Come sottolineato da Lombardi 2008: 12, risulta chiaro come "l''amministrazione di rischio', in quanto potere flessibile chiamato a fronteggiare le esigenze (di emergenza) del momento concreto, abbia la necessità di muoversi secondo le linee di un diritto che non imbrigli l'azione degli apparati pubblici al rispetto di rigide norme intrinseche di esercizio della funzione, ma costituisca la legittimità dell'azione amministrativa attraverso un sistema normativo basato sull'affermazione di principi piuttosto che sull'osservanza di regole prescrittive".

24 Il riferimento è chiaramente agli strumenti di valutazione e di tutela ambientale e sanitaria, in relazione a cui si vedano, rispettivamente, Dell'Anno 2022: 21 ss.; Gragnani 2003: 10; Ferrara 2020: 23 ss.; Stanzione 2016: 1 ss.

25 Regolamento UE 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 ('Regolamento sull'intelligenza artificiale').

26 Cfr. Council of European Union 2023.

rischio[27]. Ma questa tendenza affiora altresì nella disciplina giuridica della cybersicurezza (o *cybersecurity*) pubblica, come testimoniato dal c.d. Cybersecurity Act[28], dalla c.d. Direttiva NIS2[29] e dal d.lgs. n. 138/2024 di recepimento[30], nonché dal c.d. Cyber Resilience Act[31].

La nuova e recentissima normativa sulla cybersicurezza pubblica testimonia lo sforzo verso il "bisogno di regolazione" che il processo digitale richiede[32]. Ma poiché tale azione si intreccia con il rischio da ignoto tecnologico, è più che mai auspicabile che la dottrina indaghi a fondo i risultati e gli effetti che il legislatore si propone di conseguire e quelli che effettivamente consegue[33].

Proprio con l'intento di approfondire l'analisi della cybersicurezza pubblica, nel gennaio 2023 all'Università degli Studi del Piemonte Orientale si è formato un piccolo gruppo di ricerca, composto da studiosi di distinte discipline afferenti a diversi Dipartimenti: Roberto Candiotto[34], Lavinia Egidi[35], Bianca Gardella Tedeschi[36], Paolo Heritier[37], oltre al sottoscritto[38].

Fin da subito l'idea è stata quella di affrontare questo campo d'indagine da una prospettiva multidisciplinare, in grado di coniugare il diritto (amministrativo, privato e comparato), la filosofia del diritto, l'informatica giuridica, l'informatica e l'organizzazione aziendale, potendo così giungere a una visione integrata di saperi

27 Cfr. artt. 6 ss. Regolamento UE 2024/1689. A riguardo si veda Barone 2020: 63 ss.

28 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ('Regolamento sulla cibersicurezza').

29 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 ('Direttiva NIS 2').

30 Decreto Legislativo 4 settembre 2024, n. 138.

31 Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 ('Regolamento sulla ciberresilienza').

32 Come del resto invocato da Tropea 2023: 189, nel contesto più ampio della regolazione della digitalizzazione pubblica: "visto che la tecnica corre veloce, una prima generale e profonda riflessione va fatta con riferimento a un sistema di fonti efficace, che sappia coniugare il presidio democratico con le esigenze di risposte veloci e calibrate".

33 Fra gli studi di carattere monografico più recenti, relativi al rapporto fra diritto amministrativo e pubblico e cybersicurezza, è possibile citare Ursi 2023 e Buoso 2023; sia consentito il richiamo a Rossa 2023.

34 Professore associato di Organizzazione aziendale, Dipartimento di Studi per l'Economia e l'Impresa (DISEI).

35 Professoressa associata di Informatica, Dipartimento di Scienze e Innovazione Tecnologica (DISIT).

36 Professoressa associata di Diritto privato comparato, DISEI.

37 Professore ordinario di Filosofia del Diritto e Informatica giuridica, Dipartimento di Giurisprudenza e Scienze Economiche, Politiche e Sociali (DIGSPES).

38 Ricercatore a t.d. tipo A) di Diritto amministrativo, Dipartimento per lo Sviluppo Sostenibile e la Transizione Ecologica (DISSTE).

complementari. Il gruppo di ricerca ha deciso di formalizzare la propria attività partecipando e vincendo il Bando Ricerca UPO 2022, finanziato con risorse Next Generation EU e Compagnia di San Paolo, grazie alla presentazione del progetto di ricerca "*Cybersecurity Risk Governance in Public Administration* – CybeR-Go-PA" (ID: 1083758, CUP: C15F21001720001) con responsabile scientifico (*Principal Investigator – PI*) il sottoscritto.

Fra le diverse attività previste dal progetto ha spiccato (*recte*: spicca, essendo il progetto ancora in corso), in particolare, l'organizzazione di un convegno interdisciplinare di carattere internazionale intitolato "Cybersecurity e Istituzioni Pubbliche Rischi e opportunità della regolamentazione informatico-giuridica di un fenomeno trasversale". Esso si è svolto il 23 e 24 maggio 2024 a Novara, presso il Dipartimento di Studi per l'Economia e l'Impresa dell'Università degli Studi del Piemonte Orientale, con il patrocinio del Centro di Ricerca Interdipartimentale sull'Intelligenza Artificiale dell'Università del Piemonte Orientale (AI@UPO), di ItAIS (sezione italiana di AIS – *Association for Information Systems*) e del Centro di Ricerca Interdisciplinare sul Diritto delle Amministrazioni Pubbliche dell'Università degli Studi di Milano (CERIDAP). Il convegno ha visto la partecipazione di più di quaranta fra relatori, alcuni dei quali selezionati tramite una *Call for paper* dedicata agli studiosi più giovani.

Molte fra le relazioni esposte in tale occasione hanno rappresentato la base teorica degli scritti di seguito raccolti: per ragione di sistematica editoriale essi sono raggruppati in due fascicoli, i quali devono pertanto essere letti congiuntamente e considerati una cosa sola. Il primo fascicolo è impreziosito da una introduzione di Alberto Oddenino. Il secondo, invece, è arricchito da una parte introduttiva redatta da Riccardo Ursi. Proprio a voler sottolineare la continuità logica fra i due fascicoli, l'opera si apre con la presente prefazione (fascicolo I) e si chiude con la postfazione di Paolo Heritier (fascicolo II).

La speranza è quella di poter contribuire, seppur in minima parte, al dibattito accademico multi e interdisciplinare su un tema di estrema attualità, viste le recenti notizie di cyber-attacchi alle Istituzioni pubbliche italiane, e di assoluta centralità proprio in relazione al "rischio da ignoto tecnologico".

Torino, 27 gennaio 2025

Bibliografia

Barone A. 2020, "Amministrazione del rischio e intelligenza artificiale", in *Eur. Rev. Dig. Admin. Law (ERDAL)*, n. 1: 63 ss.

Barone A. 2006, *Il diritto del rischio*, Milano: Giuffrè.

Bauman Z. 2000, *Liquid Modernity*, Cambridge: Polity.

Beck U. 2000, *La società del rischio. Verso una seconda modernità*, Roma: Carocci (edizione originale in lingua tedesca: Beck U. 1986, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt am Main: Suhrkamp Verlag).

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Casini L. 2022, *Lo Stato (im)mortale*, Milano: Mondadori.

Cassese S. 2009, *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino: Einaudi.
Cassese S. 2003, *Lo spazio giuridico globale*, Roma-Bari: Laterza.
Cognetti S. 2014, "Potere amministrativo e principio di precauzione fra discrezionalità tecnica e discrezionalità pura", in Cognetti S., Contieri A., Licciardello S., Manganaro F., Perongini S., Saitta F. (a cura di), *Percorsi di diritto amministrativo*, Torino: Giappichelli: 127 ss.
Council of European Union, *Press Release – Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*, 9 December 2023, in https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/pdf/.
Crosetti A., Ferrara R., Fracchia F., Olivetti Rason N. 2018, *Introduzione al diritto dell'ambiente*, Roma-Bari: Laterza.
De Leonardis F. 2023, *Lo Stato ecologico. Approccio sistemico, economia, poteri pubblici e mercato*, Torino: Giappichelli.
De Leonardis F. 2012, "Il principio di precauzione", in Renna M., Saitta F. (a cura di), *Studi sui principi del diritto amministrativo*, Milano: Giuffrè: 413 ss.
De Leonardis F. 2005, *Il principio di precauzione nell'amministrazione di rischio*, Milano: Giuffrè.
Dell'Anno p. 2022, *Diritto dell'ambiente*, Milano: Wolters Kluwer.
Ferrara R. 2023a, "La globalizzazione e il diritto pubblico", in *federalismi.it*, n. 19: 28 ss.
Ferrara R. 2023b, "Scienza e diritto nella società del rischio: il ruolo della scienza e della tecnica", in *Scritti scelti*, a cura di Cimini S., Lombardi p. , Lombardi R., Molaschi V., Porporato A.M., Napoli: Editoriale Scientifica: 789 ss. (originariamente pubblicato in *Dir. e proc. amm.*, n. 1/2021: 63 ss.).
Ferrara R. 2020, *L'ordinamento della sanità*, Torino: Giappichelli.
Ferrara R. 2005, *Introduzione al diritto amministrativo. Le pubbliche amministrazioni nell'era della globalizzazione*, Roma-Bari: Laterza.
Ferrarese M.R. 2022, *Poteri nuovi*, Bologna: Il Mulino.
Ferrarese M.R. 2002, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, Bologna: Il Mulino.
Ferrarese M. R. 2000, *Le istituzioni della globalizzazione*, Bologna: Il Mulino.
Fracchia F., Vernile S. 2022, "Lo sviluppo sostenibile oltre il diritto ambientale", in *Le Regioni*, n. 1-2: 15 ss.
Fracchia F. 2010, *Lo sviluppo sostenibile. La voce flebile dell'altro tra protezione dell'ambiente e tutela della specie umana*, Napoli: Editoriale Scientifica.
Giddens A. 1990, *The Consequences of Modernity*, Cambridge: Polity.
Gragnani A. 2003, "Il principio di precauzione come modello di tutela dell'ambiente, dell'uomo, delle generazioni future", in *Riv. dir. civ.*: 10 ss.
Hobbes T. 1651, *Leviathan*.
Hobbes T. 1642, *De Cive*.
Laus F. 2023, *L'amministrazione del rischio. Tra regole e procedimento, principio di precauzione e approccio multidimensionale*, Milano: CEDAM-Wolters Kluwer.
Locke J. 1689, *Two Treatises of Government*.
Lombardi R. 2008, *La tutela delle posizioni giuridiche meta-individuali nel processo amministrativo*, Torino: Giappichelli.
Luhmann N. 1991, *Soziologie des Risikos*, Berlin: de Gruyter.
Marino I.M. 2011, "Aspetti propedeutici del principio giuridico di precauzione", in *Studi in onore di Alberto Romano*, III, Napoli: Editoriale Scientifica: 2177 ss.
Marino I.M. 2005, "Diritto, amministrazione e globalizzazione", in *Dir. econ.*, n. 1: 25 ss.

Pantalone p. 2023, *La crisi pandemica dal punto di vista dei doveri. Diagnosi, prognosi e terapia dei problemi intergenerazionali secondo il diritto amministrativo*, Napoli: Editoriale Scientifica.
Popper K. 1962, *The Open Society and its Enemies*, I, London: Routledge.
Rossa S. 2023, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale Scientifica.
Rousseau J.-J. 1762, *Du contrat social: ou principes du droit politique*.
Rousseau J.-J. 1755, *Discours sur l'origine et les fondements de l'inégalité parmi les hommes*.
Stanzione M.G. 2016, "Principio di precauzione, tutela della salute e responsabilità della p. A. Profili di diritto comparato", in *Comparazione e Diritto civile*: 1 ss.
Stella F. 2022, "Il rischio da ignoto tecnologico e il mito delle discipline", in AA.VV., *Il rischio da ignoto tecnologico*, in *Quaderni della Rivista trimestrale di Diritto e procedura civile*, Milano: Giuffrè: 3 ss.
Tropea G. 2023, *Biopolitica e diritto amministrativo del tempo pandemico*, Napoli: Editoriale Scientifica.
Ursi R. (a cura di) 2023, *La sicurezza nel Cyberspazio*, Milano: Franco Angeli.
Weber M. 2006, *La politica come professione*, Milano: Mondadori (edizione originale: Weber M. 1919, *Politik als Beruf*, München und Leipzig: Verlag von Duncker & Humblot)

Alberto Oddenino

Pervasività, centralità geopolitica e molteplicità delle istanze di tutela della cybersicurezza: elementi introduttivi[*]

*Abstract***:** Comprendere la cybersicurezza nella moderna società tecnologica e digitalizzata e le istanze di tutela che essa solleva richiede alcune chiavi di lettura preliminari. Il contributo si propone di offrirne tre: esso muove dalla forza espansiva e dalla pervasività della nozione, per evidenziare poi la centralità geopolitica che hanno assunto le sue istanze di tutela, e concludendo con la molteplicità delle dimensioni rilevanti nella considerazione del fenomeno.

Keywords: cybersecurity, globalization, international law, sovereignty, national security

1. La pervasività e la forza espansiva della cybersicurezza nella società contemporanea

Il tema della tutela della cybersicurezza ha assunto una portata sempre più pervasiva nella società contemporanea, in cui la presenza tecnologica è resa essa stessa sempre più capillare e in certo senso ubiqua.

Il progresso tecnologico accompagna da sempre l'evoluzione della società, modificandone radicalmente i valori oltre che abitudini e stili di vita. L'avvento dell'era digitale – caratterizzata da una sempre più vasta interconnessione e da una massiccia elaborazione algoritmica di dati – ha segnato una netta accelerazione di tale processo trasformativo. Ogni attività possiede oggi una propria dimensione digitale, nella quale la tecnologia è divenuta sostrato e strumento spesso imprescindibile. Al contempo, le implicazioni del progresso tecnologico non si limitano alla sfera sociale, poiché lo sviluppo di nuove tecnologie assume un'innegabile rilevanza geopolitica e strategica. Si tratta di un aspetto non nuovo nel panorama internazionale, se è vero che la tecnologia costituisce da sempre

* Contributo non sottoposto alla procedura di referaggio doppio cieco.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760144

terreno di competizione e ambito di elezione per il perseguimento degli interessi strategici, anche in una logica di fusione o almeno di parziale allineamento di interesse fra pubblico e privato[1].

Ciò è tanto più vero nella misura in cui dimensione di collegamento tecnologico è sostrato irrinunciabile per il supporto e lo sviluppo dell'intelligenza artificiale, che nelle sue frontiere più attuali appare portatrice di uno slancio trasformativo senza precedenti per le nostre società, il nostro modello economico e in ultima analisi per lo stesso futuro dell'umanità[2].

Su un piano ancora preliminare si deve ricordare come Internet stessa, la Rete delle reti, risulti "territorio" fortemente conteso: ben lontano da una concezione originaria come spazio di libertà tendenzialmente assoluta, che trovava nell'autoregolamentazione tecnica il solo modello normativo accettabile, la Rete, in ragione delle sue grandi potenzialità strategiche, sociali e commerciali, è oggetto di ambizioni di controllo tecnico ancor prima che di regolazione strutturale e contenutistica[3].

A tali riflessioni ci si riferisce quando si menziona una specifica dimensione geopolitica relativa alla cybersicurezza, ricordando che quella che si gioca sulla Rete non è solo una partita per affermare una prevalenza economica, ma una vera contesa di potere, nella sua accezione più ampia e totalizzante, che coinvolge in modo frontale il tema della sovranità[4].

Peraltro il tema supera di molto la sola dimensione interstatuale o quella riconducibile ad organizzazioni internazionali o organismi sovranazionali, per raggiungere il cuore della *data economy* contemporanea, ponendosi in collegamento con il settore privato, in cui accanto alla dominanza ormai incontrovertibile dei cd. *Big Tech*, fiorisce una ampia congerie di soggetti privati portatori di rilevanti interessi economici legati al commercio e alla circolazione dei dati.

Non deve pertanto sorprendere se la nozione di cybersicurezza, proprio in ragione di questa sua capacità espansiva, abbia assunto crescente centralità nelle valutazioni del potere, tanto pubblico quanto privato.

In piena coerenza con l'evoluzione della società verso la cd. *Risiko Gesellschaft* teorizzata da Ulrich Beck, oggi la valutazione e la gestione dei rischi cibernetici occupa l'agenda tecnologica e regolatoria della più parte degli stati contemporanei.

In prospettiva regolatoria ciò ha condotto a rafforzare un approccio cd. *risk based*, che ha trovato nell'ordinamento della UE un terreno fertile di sviluppo, e che assume oggi una portata sempre più ampia e in certo senso esorbitante, perva-

1 Si tratta di un tema complesso e potenzialmente vastissimo, su cui può bastare in questa sede richiamare la brillante teorizzazione di un nuovo contratto sociale contenuta in Shadmy 2019.

2 In tema si veda da ultimo, fra la ormai vasta letteratura, Aresu 2024.

3 In tema si veda, fra l'ampia letteratura, Muller 2010. Sia consentito rinviare anche a Oddenino 2012.

4 È evidente infatti come la contesa per il controllo della struttura sia propedeutica al controllo dei contenuti. In tema si veda De Nardis 2014, ove si evidenzia come la possibilità di realizzare una penetrante sorveglianza e una raccolta sistematica di informazioni strategiche, anche e soprattutto in dimensione internazionale, sia espressione qualificata di un tale disegno.

dendo di sé, come è noto, non solo l'ambito della *data protection* ma anche il plesso di regolazione oggi dedicato all'intelligenza artificiale.

In definitiva, la cybersicurezza esprime oggi essa stessa una netta attitudine alla esorbitanza, e travalica di molto la tradizionale sua ricostruzione delle origini, che recava un collegamento biunivoco con gli ambiti della Cyber-guerra e del Cyber-terrorismo, per esplicare una capacità di penetrazione di molti altri ambiti collegati con l'ampio concetto strategico di sicurezza nazionale[5].

2. Alla ricerca di una definizione e di una tassonomia per la cybersicurezza

Alla luce di quanto precede si comprende come già la semplice perimetrazione del campo di indagine, e con essa l'individuazione di una nozione univoca di cybersicurezza, non sia agevole. Essa può oggi essere vista come una declinazione della più ampia nozione di sicurezza nazionale, della quale in certo senso rappresenta anche una forma di evoluzione, dotata di notevole potenziale pervasivo.

Per certo, in questo senso, il concetto di cybersicurezza è influenzato dalle esigenze politiche, sociali e culturali di ciascun Paese e, per altro verso, richiede l'adattamento della nozione di sicurezza nazionale ad un sempre mutevole settore digitale. Si ritiene che sempre per questa ragione non è presente, a livello multilaterale, una concettualizzazione univoca della cybersicurezza.

Una certa autorevolezza ha assunto la nozione di cybersicurezza resa dal *U.S. National Institute of Standards and Technology* (NIST), in termini di: "prevenzione del danneggiamento, dell'uso non autorizzato, dello sfruttamento e, se necessario, ripristino dei sistemi elettronici di informazione e comunicazione delle informazioni in essi contenute, al fine di rafforzare la riservatezza, l'integrità e la disponibilità di tali sistemi". Si tratta di una definizione più ampiamente condivisibile in ragione della sua scelta di non distinguere il settore pubblico dal settore privato, né con riferimento agli attori di un possibile attacco, né con riferimento ai potenziali obiettivi. Essa, focalizzandosi esclusivamente sugli eventuali danni all'integrità delle informazioni e dei sistemi informativi, non lascia volutamente emergere altri e più ampi obiettivi, quali ad esempio lo sviluppo delle imprese nel settore digitale, il libero accesso degli individui a Internet, la regolamentazione dei contenuti caricati online, i controlli sul traffico dati anche attraverso *Big Data* e intelligenza artificiale, tutte dimensioni riconducibili alla cybersicurezza, che ne rivelano la multidimensionalità, aspetto su cui si tornerà a breve.

Non deve stupire pertanto se a questa prima definizione di cybersicurezza se ne è affiancata un'altra, più ampia, sviluppata dall'*International Telecommunication Union* (ITU), secondo cui la cybersicurezza è "la raccolta di strumenti, politiche, concetti di sicurezza, garanzie di sicurezza, linee guida, approcci di gestione del rischio, azioni, formazione, migliori pratiche, garanzie e tecnologie che possono essere utilizzate per proteggere l'ambiente informatico, l'organiz-

5 In tema cfr. la ricostruzione tradizionale espressa in Bosco 2013.

zazione e le risorse degli utenti", nella quale rientrano anche "i beni dell'organizzazione e degli utenti" che "comprendono i dispositivi informatici connessi, il personale, l'infrastruttura, le applicazioni, i servizi, i sistemi di telecomunicazione e la totalità delle informazioni trasmesse e/o archiviate nell'ambiente informatico" e, ancora, che "la sicurezza informatica si impegna a garantire il raggiungimento e il mantenimento delle proprietà di sicurezza dell'organizzazione e delle risorse degli utenti contro i rischi per la sicurezza rilevanti nell'ambiente informatico" [6].

Una definizione davvero ampia da cui si deduce come ITU, nella sua qualità di organizzazione internazionale di vertice per il settore delle telecomunicazioni, riconosca l'estrema ampiezza dell'ambito di cybersicurezza nonché la varietà degli approcci e dei possibili rischi per la sicurezza nazionale: di qui la connotazione del tema della tutela della cybersicurezza non solo come semplice insieme di regole, ma come vera e propria strategia *risk based* che pervade l'adozione di atti di *soft* o *hard law* in materia digitale[7].

Alla luce delle incertezze definitorie, può essere meritevole uno sforzo di minima tassonomia. In questa prospettiva le minacce *cyber* possono innanzitutto distinguersi in attive o passive, accidentali o intenzionali.

Le prime nascono da comportamenti che implicano un'alterazione del funzionamento di un bene o di un servizio originariamente previsto, mentre nelle seconde il comportamento non determina alcuna alterazione del funzionamento, ma tende a sfruttare un malfunzionamento o una lacuna nel sistema al fine di operare in maniera illecita.

Accidentali sono invece le minacce determinate da malfunzionamenti o bug dei software o della rete che possono esporre i dati o altri elementi sensibili a rischi, mentre intenzionali sono le minacce rappresentate da comportamenti studiati appositamente per perseguire uno scopo illecito attraverso il cyberspazio.

Quanto ai settori materiali possono essere individuati almeno cinque aree chiave.

Una prima area-chiave per la cybersicurezza, direttamente legata al concetto di sicurezza nazionale inteso in senso tradizionale, è quella della difesa nazionale, che comprende tutto ciò che è legato agli ambiti militare e di intelligence, nella quale

6 Cfr. International Telecommunication Union, "*Overview of Cybersecurity*", Recommendation ITU-T X.1205, aprile 2008, p. 2 par. 3.2.5. Giova sottolineare come le stesse tipologie di attacchi, nel corso degli anni, si siano ampliate parallelamente allo sviluppo tecnologico, ricomprendendo nuovi settori quali i dati sensibili degli utenti o le piattaforme digitali. Resta ferma e fondamentale la distinzione, elaborata dall'ITU stesso, tra attacchi digitali – ad esempio nel caso di *malware* – e attacchi fisici – ad esempio nel caso di danneggiamento di infrastrutture digitali che causi disservizi in un territorio.

7 L'adozione da parte di ITU del *risk based approach* ha condotto ad individuare tre categorie di possibili rischi per la sicurezza nazionale, derivanti da beni e da servizi digitali, e in particolare: i "*service interruption attacks*", che disabilitano, in maniera temporanea o permanente, l'accesso a piattaforme di servizi; gli "*assets compromise*", che danneggiano le infrastrutture e possono cagionare danni su larga scala; i "*component hijacking*", che mirano a prendere il controllo di altri dispositivi da utilizzare per lanciare ulteriori attacchi nel cyberspazio.

sono incluse le infrastrutture utili alla difesa stessa, ai network e ai software collegati e ai loro contenuti quali, ad esempio, le informazioni classificate[8].

La seconda area-chiave nella quale sono possibili cyber attacchi su larga scala, idonei a causare blocchi di funzionamento dalla durata variabile, con conseguenze gravi per i servizi essenziali, è quella legata alle infrastrutture critiche, cioè a quelle infrastrutture utili al soddisfacimento dei bisogni primari della popolazione, quali la fornitura di energia elettrica o le reti 5G, necessarie per la gestione della salute, dell'energia e dei trasporti. L'attacco alle infrastrutture critiche può avvenire in maniera diretta, tramite il tentativo di penetrare al loro interno violando i protocolli di sicurezza, oppure attraverso l'istallazione di *backdoors*, che possono avere natura *hardware* (chip occultati) o *software* (programmi non previsti o creazione di meccanismi che evitano i protocolli di identificazione e di accesso) che rendono possibile l'accesso per soggetti non autorizzati, senza lasciare alcuna traccia di forzatura del sistema[9].

Terza area è quella che attiene allo spionaggio economico che determina l'appropriazione di segreti industriali o la violazione della proprietà intellettuale soprattutto in ambito software. Anche in questo caso, l'accesso fraudolento può avvenire tramite attacchi diretti o, nell'ambito delle catene di fornitura, attraverso l'installazione di *backdoors* nel corso di produzione della componentistica hardware o software utilizzata dall'impresa cui l'attacco è destinato[10].

La quarta area-chiave attiene al settore della *digital information*. Qui gli attacchi informatici possono essere diretti all'acquisizione di dati, come accade quando uno Stato utilizza big data per acquisire informazioni sulle abitudini o preferenze degli utenti di un determinato Paese, oppure diretti alla manipolazione o falsificazione delle informazioni per creare confusione e sfiducia nella popolazione. In questa area si collocano, in particolar modo, le minacce ibride, intese come un tipo di attacco volto a destabilizzare un Paese attraverso meccanismi non convenzionali, quali, ad esempio, la disinformazione o l'acquisizione illecita di dati volti a ottenere informazioni di sicurezza nazionale, utili a facilitare un eventuale attacco di natura convenzionale, quale ad esempio un attacco armato[11].

8 Sui rischi per la sicurezza nazionale derivanti dai tentativi degli hacker di penetrare nei sistemi di difesa per acquisire informazioni relative anche allo sviluppo della componentistica software e hardware nelle apparecchiature militari cfr. si veda ad esempio, *Joint Statement for the Record to the Senate Armed Services Committee – Foreign Cyber Threats to the United States*, 5 gennaio 2017, disponibile a https://www.armedservices.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

9 Una definizione precisa di infrastrutture critiche è data dall'US Patriot Act, secondo cui "le infrastrutture critiche sono quei sistemi o beni, fisici o virtuali, così vitali per gli Stati Uniti che il loro malfunzionamento o distruzione avrebbe un impatto debilitante sulla sicurezza, sulla sicurezza economica nazionale, sulla salute pubblica nazionale o su qualsiasi combinazione di tali questioni" (USA PATRIOT ACT, 2001, 42 U.S.C. §5195c(e)).

10 In tema cfr. National Counterintelligence and Security Center: "Foreign Economic Espionage in Cyberspace", 26 luglio 2018, p. 12. Reperibile in https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

11 Per un'analisi approfondita dell'utilizzo della disinformazione come minaccia ibrida e strumento volto alla destabilizzazione di un Paese si vedano Singer, Brooking 2018.

La quinta e ultima area di operatività dei rischi per la sicurezza informatica riguarda sia l'accesso da parte degli utenti ad internet, quale espressione del diritto alla libertà di informazione ed espressione, sia l'accesso reciproco tra Paesi a informazioni, alla luce del principio di leale cooperazione nei rapporti internazionali. In questi casi, si possono verificare cyber attacchi del tipo *Distributed Denial of Services* (DDOS), che impediscono agli utenti di raggiungere determinati siti o, in generale, di accedere ad internet, causando disservizi o, in alcune occasioni, disinformazione. Si pensi al caso in cui, a ridosso di elezioni politiche, vengano artatamente e illegittimamente oscurati siti di informazione. In alcuni casi può succedere che l'accesso avvenga, in maniera diretta o per il tramite di intermediari privati, da parte di governi stranieri per acquisire informazioni o creare disservizi. Non è infrequente, allora, che vengano poste restrizioni sia in maniera diretta, impedendo l'accesso, oltre i confini nazionali, a siti contenenti informazioni ritenute sensibili, sia in maniera indiretta, impedendo a soggetti stranieri di fare investimenti che, per essere realizzati, richiedono l'accesso a informazioni sensibili[12].

3. La centralità della nozione di sicurezza nazionale, e la tendenza a una determinazione unilaterale delle misure di tutela della cybersicurezza

A fronte di un panorama tanto ricco e complesso, resta evidente che la dimensione del fenomeno, per certo internazionale in ragione della portata globale del fenomeno, vede le risposte tecniche e regolatorie affidate invece a iniziative e sensibilità prevalentemente nazionali.

In questo senso si staglia come assolutamente centrale il rapporto con la nozione di sicurezza nazionale, quale ambito privilegiato di esercizio della sovranità e quale clausola di salvezza anche rispetto alla eventuale assunzione di obblighi internazionali da parte degli stati[13]. Ciò apre ad una interpretazione fortemente unilaterale della nozione di cybersicurezza e a un suo chiaro orientamento in senso geopoliticamente strategico.

Il piano del diritto internazionale resta esile con svariate iniziative di *soft law* [14], accanto a rare emersioni di strumenti giuridicamente vincolanti che sono però del tutto settoriali, come in particolare la Convenzione di Budapest del 2001 sul *cybercrime* elaborata in senso al Consiglio d'Europa[15].

12 Così Meltzer 2020

13 Cfr. GEE, *Report Group of Governmental Experts on Developments in Field of Information and Telecommunications in the Context of International Security*, 14 luglio 2021, UN Doc. A/76/135, par. 7, 14.

14 Nel primo senso si veda su tutto la Risoluzione dell'Assemblea generale delle Nazioni Unite, Creazione di una cultura globale della sicurezza informatica e della protezione delle infrastrutture informatiche critiche, 23 dicembre 2003, n. 58/199, UN Doc. A/RES/58/199.

15 Su questo tema si veda ex multis Mazza 2004. Le azioni del Consiglio d'Europa nel campo della cybersecurity, che hanno due profili principali: la lotta alla criminalità informatica e la protezione delle persone in materia di trattamento automatizzato dei dati personali. Sotto il primo profilo, l'organizzazione di Strasburgo ha iniziato ad occuparsi di criminalità informatica

Le dinamiche internazionali sono piuttosto paradigmatiche di come il settore della cybersicurezza resti un terreno di aspro confronto fra sovranità nazionali, e si presti a qualche strumentalizzazione unilaterale. Ciò è risultato storicamente con particolare evidenza anche in occasione della disputa relativa alla riforma delle *International Telecommunications Regulations* dell'ITU: essa ha visto, nella Conferenza di Dubai del 2012, lo scontro fra visioni e pretese contrapposte, segnando una profonda lacerazione fra gli Stati solidali con la posizione volta al sostanziale mantenimento dello *status quo*, espressa dagli US, e quelli che, come Cina e Russia in particolare, in una logica geopolitica di contropotere, hanno tentato di affermare una visione alternativa, sulla base di dichiarate esigenze di cybersicurezza. Il che evidenzia una volta di può il portato strategico e geopolitico di una nozione che tende a ricalcarsi su quella dell'interesse nazionale[16].

È chiaro come in un mondo globalizzato, e al fine di favorire le dinamiche dello scambio e del commercio internazionale anche dei beni digitali, sarebbe opportuno porre rimedio a una totale discrezionalità nella identificazione delle misure di cybersicurezza da parte dei singoli stati. La disciplina di queste aree di interesse richiederebbe regole armonizzate tra i diversi Paesi, così da evitare che le valutazioni, invero particolarmente discrezionali in quanto legate a informazioni spesso riservate e quindi non conoscibili dai Paesi terzi o da organi sovranazionali, siano strumentali alla creazione di meccanismi protezionistici e di tutela delle imprese interne con conseguente violazione dei principi di libero scambio e libera concorrenza[17]. Tuttavia la clausola di eccezione costituita dell'interesse nazionale costituisce un facile grimaldello per scardinare ogni sistema armonizzato che potesse prendere corpo a partire dalla condivisione di alcuni standard tecnici. Gli stati restano inclini a valutare l'effettiva sussistenza di un interesse di sicurezza nazionale attraverso un approccio caso per caso. Esso si giustifica perché, per un verso, si verificano minacce ambigue e, quindi, difficilmente qualificabili – si pensi a quelle ibride – e, per altro verso, minacce che coinvolgono interessi esclusivi di un Paese che, se dirette contro un Paese diverso, comporterebbero rischi minori[18].

come questione di diritto penale già negli anni '80, a partire dalla promulgazione di due raccomandazioni, relative alla criminalità informatica e al diritto processuale penale legato alle tecnologie dell'informazione. A metà degli anni Novanta, con il consolidarsi delle nuove tecnologie, che hanno portato anche a un loro uso malevolo, il Comitato dei Ministri ha deciso di istituire il Comitato di esperti sulla criminalità informatica (PC-CY), incaricato di redigere un accordo sulla criminalità informatica. La Convenzione che ne è scaturita, conclusa a Budapest il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004, è supportata da un Comitato specifico (T-CY) volto a garantirne l'attuazione attraverso valutazioni, linee guida e altri mezzi, nonché attraverso i programmi di *capacity building*.

16 Sul punto sia consentito rinviare a Oddenino 2013.

17 In tema si rinvia a Oddenino 2017.

18 La natura ambigua dei cyber attacchi ha indotto talora gli Stati ad agire in via preventiva e non sempre proporzionata, ad esempio impedendo ad altri Paesi di accedere ai propri server o alle proprie infrastrutture di rete, oppure limitando eccessivamente il commercio di prodotti dual use, in quanto potenzialmente utilizzabili per sviluppare tecnologie per i cyber attacchi, di software o di hardware potenzialmente idonei a nascondere *backdoors*.

In merito vi è dunque una forte riemersione di sensibilità nazionali sovrane che non trovano facile allineamento. Ciò non fa che riecheggiare una contrapposizione già emersa fra mondo occidentale a resto della comunità internazionale rispetto al tema della applicazione del diritto internazionale al cyberspazio, che merita una indagine comparatistica che evidenzi le diverse sfumature di sensibilità tecnica e giuridica[19].

In tale già articolato scenario, il crescente ruolo del settore privato costituisce un ulteriore elemento di complessità. La nuova realtà internet-based porta con sé nuovi equilibri fra attori pubblici e privati, in quanto sempre più asset di rilevanza strategica per il Sistema Paese sono oggi oggetto di sviluppo, controllo e immissione nel mercato da parte di attori privati o da parte di sinergie pubblico-private. La potenziale dipendenza da altri attori pubblici o privati relativamente alla fornitura e gestione di tecnologie digitali costituisce un fattore di rischio per gli interessi nazionali, e ciò poiché asset strategici controllati da soggetti operanti nel mercato sono maggiormente esposti ad influenze ed operazioni di acquisizione da parte di soggetti potenzialmente ostili. Per questo gli asset rilevanti per la cybersicurezza, particolarmente in dimensione infrastrutturale, sono spesso oggetto dei cd. poteri speciali dei governi rispetto alla penetrazione di investitori stranieri, settore che esso stesso è lungi dall'essere ricostruibile secondo linee sistematiche e armonizzate[20].

4. La molteplicità di angolazioni e di dimensioni sostanziali rilevanti per la cybersicurezza

Una terza chiave di interpretazione, quella della molteplicità, conduce anche a introdurre brevemente gli scritti compendiati in questo volume. Il variegato contesto della cybersicurezza che si è rapidamente tratteggiato si traduce infatti in una molteplicità non solo di piani normativi, ma anche di dimensioni strutturali e sostanziali, che necessariamente trascendono la dimensione squisitamente giuridica, per abbracciare quella tecnica ed economica. Proliferano pertanto le angolazioni da cui muovono le analisi del fenomeno, delle sue potenzialità e delle sfide che esso determina.

In relazione alla prospettiva di protezione si pone un diretto collegamento con il tema della *data protection*, confermando una saldatura che d'altronde discende dallo stesso impianto normativo del GDPR, in cui la cybersicurezza è declinata come elemento qualificante delle istanze di protezione dei dati. Così il contributo di Corso Tozzi Martelli, che approfondisce il rapporto fra la cybersicurezza e il Codice dei contratti pubblici indagando l'opportunità che la nuova normativa italiana (di cui al D.lgs. n. 36 del 2023) offre per rinforzare la protezione dei dati personali

19 In tema cfr. Gargiulo Giovannelli Sciacovelli 2024

20 Paradigmatico è in proposito l'esercizio del cd. *golden power* previsto, con maglie di ampia discrezionalità politica, nell'ordinamento italiano

e la cybersicurezza nel contesto degli appalti; o, ancora, quello che indaga privacy e cybersecurity nel caso delle smart cities, richiedendo la messa a punto di *best practices* adeguate (Maria Notaristefano, Fabio Angeletti, Esli Spahiu).

Una prospettiva in chiave economica è offerta da Alessandra Galassi sui rischi di cybersicurezza in relazione a modelli di sviluppo urbano basati sui c.d. GIS (*Geographical Information Systems*) mentre sempre nella prospettiva di applicazioni materiali si colloca l'analisi di Melissa Capelli su oneri di adempimento e vantaggi competitivi connessi all'applicazione della cybersecurity alla filiera dei servizi nell'ambito turistico.

Prospettive sistemiche legate all'impatto sui modelli di organizzazione e amministrazione sono offerte nel contributo di ampio respiro di Bruno Carotti, nonché da Francesca Castaldo e Federico Serini che approfondiscono l'interazione fra pubblico e privato, proiettando detto rapporto sulla dimensione europea della cybersicurezza, coinvolgendo forme di coregolazione, standardizzazione e certificazione che paiono ormai centrali. Sempre su una prospettiva sistemica policentrica indugia Filippo Galli, che dedica il suo contributo all'organizzazione amministrativa della cybersicurezza nell'ordinamento multilivello.

Una importante dimensione di sicurezza strategica settoriale è al centro del contributo di Matteo Pignatti, dedicato al quadro multilivello della cybersicurezza della infrastruttura ICT in relazione al settore finanziario, ove si evidenziano rischi per la stabilità finanziaria in relazione a cripto-attività, tecnologie a registro distribuito e resilienza delle infrastrutture.

Nella prospettiva della sicurezza nazionale dell'ordinamento italiano si colloca poi Massimiliano Malvicini, che indaga l'evoluzione dell'architettura strategica nazionale in materia di sicurezza cibernetica.

Vi sono infine interessanti prospettive di collegamento fra l'ambito della cybersicurezza e quello della tutela dell'ambiente. Così Teresa Monaco apre una finestra di attenzione sul rapporto fra ambiente naturale e ambiente digitale proponendo una nuova dimensione applicativa del principio di precauzione che dialoga assai bene coi temi della gestione del rischio cibernetico, mentre Maura Mattalia muove dal tema del cambiamento climatico e della governance di Internet per trarre elementi di riflessione sulle potenzialità della governance policentrica anche in relazione alle istanze di cybersicurezza.

In conclusione, una ampia disamina di prospettive che rivela, una volta di più, come il tema della sicurezza cibernetica sia fluido, vario e fortemente evolutivo. I tratti sono labili, i confini mutevoli: forse il tempo consoliderà assetti più certi e prevedibili ma oggi le prospettive e le potenzialità dischiuse dalla tecnologia che pervade il nostro mondo recano inestricabilmente con sé, quasi fosse una faccia nascosta della luna, l'elemento della vulnerabilità: del nostro modello, delle nostre società e, forse ormai, dell'umanità stessa. La spasmodica ricerca di risposte alle istanze di cybersicurezza non è altro che un tentativo del potere di consolidarsi nell'intento di sottrarsi, e sottrarci, almeno un po', a questa vulnerabilità.

Bibliografia

Aresu A. 2024, *Geopolitica dell'intelligenza artificiale*, Milano: Feltrinelli.

Bosco F. 2013, "Cyberterrorismo e Cyberwarfare: profili giuridici e analisi della casistica a livello internazionale, in G. Cassano, G. Scorza e G. Vaciago (a cura di), *Diritto dell'Internet, Manuale operativo*, Milano: CEDAM-Wolters Kluwer, p. 657 ss.

Carotti B. 2020, "Sicurezza cibernetica e Stato-Nazione", in *Giornale di diritto amministrativo*, 5, p. 629 ss.

Cerra R., Crespi F. 2021, *Sovranità tecnologica*, Roma: Centro per l'economia digitale (CED).

De Nardis L. 2014, *The Global war for Internet Governance*, New Haven: Yale University Press.

Egloff F.J. 2022, *Semi-State Actors in Cybersecurity,* New York: Oxford University Press.

Gargiulo p. , Giovannelli D., Sciacovelli A.L. 2024, *Governance e quadri normativi della cybersecurity: Prospettive dei paesi non occidentali e delle organizzazioni internazionali*, Rivista La Comunità internazionale, Quaderno n. 29, Napoli: Editoriale Scientifica.

Ishikawa T., Yarik K. (eds.) 2023, *Public and Private Governance of Cybersecurity: Challenges and Potential*, Cambridge: Cambridge University Press.

Manjikian M. 2023, *Cybersecurity Ethics: An Introduction*, London: Routeldge, Taylor & Francis Group.

Mazza R. 2004, "Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001", in *La Comunità Internazionale*, p. 91 ss.

Meltzer J.P. 2020, "Cybersecurity, digital trade and data flows – Re-thinking a role for international trade rules" in *Global Economy and Development*, Working Paper n. 132, Brookings, p. 7 ss.

Mueller M. 2010, *Network and States. The Global Politics of Internet Governance*, Cambridge, Mass.: MIT Press.

Oddenino A. 2012, "Il problema della governance internazionale della rete" in M. Durante, U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino: UTET, p. 45 ss.

Oddenino A. 2013, "Diritti individuali, sicurezza informatica e accesso della conoscenza in Rete: la revisione delle International Telecommunication Regulations dell'ITU", in *Diritti umani e diritto internazionale*, p. 525 ss.

Oddenino A. 2017, "La violazione dei sistemi informatici contenenti informazioni riservate come illecito internazionale: tra dimensione interstatuale e tutela dei diritti umani" in M. Distefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli: Editoriale Scientifica, p. 13 ss.

Oddenino A. 2018, "Digital standardization, cybersecurity issues and international trade law" in *Questions of International Law*, vol. 51, p. 31 ss.

Pelroth N. 2021, *This Is How They Tell Me The World Ends. The Cyber Weapons Amrs Race*, New York: Bloomsbury Publishing**.**

Rossa S. 2023, *Cybersecurity e pubblica amministrazione*, Napoli: Editoriale Scientifica.

Shadmy T. 2019, "The New Social Contract: Facebook's Community and our Rights" in *Boston University International Law Journal*, vol. 37, p. 307 ss.

Singer p. W. Brooking E.T. 2018, *Like War: The Weaponization of Social Media*, Houghton Mifflin Harcourt: Eamon Dolan.

Melissa Capelli

I diversi volti della cybersecurity: da adempimento a vantaggio competitivo. Cenni al settore turistico

Abstract: Oggi viviamo costantemente "connessi". La tecnologia presenta molte opportunità, ma anche alcuni rischi. Di recente, infatti, gli attacchi informatici sono aumentati quantitativamente, in termini di impatto e di sofisticazione, costituendo un rischio per ogni settore economico. Il legislatore europeo è quindi intervenuto sul piano normativo per rispondere alle sfide odierne. L'aumento della digitalizzazione e della connettività, infatti, rischia di compromettere la tutela dei diritti e delle libertà fondamentali. Lo scopo di questo contributo è quello di rivedere e analizzare la legislazione in materia per verificare se può essere efficace nel proteggere i diritti fondamentali e promuovere la competitività all'interno dei mercati. Per rispondere, viene proposto un breve studio sull'applicazione della cybersecurity nel settore del turismo. In questo settore, lo sviluppo delle TIC non ha avuto un impatto solo sui consumatori e sugli operatori, ma anche sulle destinazioni. L'innovazione tecnologica diventa un driver fondamentale per la crescita dei territori: la cybersecurity diventa quindi non solo una condizione necessaria per garantire i diritti dei turisti, ma soprattutto un vantaggio competitivo.

Keywords: Cybersecurity, Turismo, Diritti, Competitività, Smart Destinations.

Sommario: 1. Luci ed ombre dell'*IoT* – 2. Le principali soluzioni normative europee ed italiane: un breve *excursus* – 3. Gli effetti dello sviluppo delle tecnologie sul settore turistico – 4. Conclusioni e sfide future.

1. Luci ed ombre dell'*IoT*

La società moderna è caratterizzata da elevati ritmi di vita, contraddistinti da cambiamenti rapidi da un tempo cronometrico, lineare, parcellizzato e non qualitativo. Si vive costantemente ´connessí e la tecnologia permea ogni aspetto della vita quotidiana. Oggigiorno, grazie al proprio *smartphone* è possibile, non solo effettuare telefonate e inviare messaggi, ma ricevere e inviare email, partecipare a videochiamate, effettuare operazioni finanziarie tramite *homebanking*, godersi un film collegandosi alle *smart tv* e perfino controllare alcuni elettrodomestici. Tutto ciò è reso possibile dallo sviluppo del settore *ICT*. "Negli ultimi venti anni, la diffusione delle nuove tecnologie dell'informazione e delle comunicazioni ha progressivamente focalizzato il centro delle attività umane di carattere sociale, politico ed econo-

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760145

mico all'interno di una nuova dimensione, denominata cibernetica"[1]. Ecco che, nel tempo, si è creata quella che viene definita *Internet of Things* (*IoT*), ossia una

> rete di oggetti dotati di tecnologie di identificazione, collegati fra di loro, in grado di comunicare sia reciprocamente sia verso punti nodali del sistema, ma soprattutto in grado di costituire un enorme *network* di cose dove ognuna di esse è rintracciabile per nome e in riferimento alla posizione.[2]

Alla luce di tale definizione, l'*IoT* offre nuove opportunità per l'automazione e l'efficienza: i diversi dispositivi, infatti, raccolgono, elaborano e trasmettono dati utili per automatizzare processi, migliorare la sicurezza, ottimizzare le prestazioni e fornire servizi personalizzati. Attraverso i progressi tecnologici, l'*IoT* è in continua espansione, permettendo di spalancare un intero universo di nuove opportunità ed innovazioni in diversi settori: dalla sanità all'agricoltura, dalla produzione industriale alla gestione delle città intelligenti[3].

Con l'incremento delle innovazioni, tuttavia, non crescono unicamente le opportunità, ma anche la dipendenza tecnologica e soprattutto, il rischio di essere vittime di *cyber* attacchi. I crimini informatici crescono nel tempo sia numericamente che qualitativamente, diventando sempre più sofisticati (alcuni attacchi sfruttano perfino l'*AI*)[4]. Per quantificare tale fenomeno, basti pensare che, nel primo semestre del 2023, il numero di nuovi *malware* si avvicina ai 2 milioni e mezzo. Sia l'*ENISA Threat Landscape* (ETL), che la relazione dell'ACN testimoniano come il 2023 sia stato un anno particolarmente prolifico per i *cyber* attacchi: nel dettaglio, l'ETL rileva che, tra luglio 2022 e giugno 2023 vi sia stata una crescita esponenziale degli attacchi rispetto all'anno precedente, con circa 2580 incidenti, cui ne vanno sommati altri 220 che hanno colpito due o più Stati membri dell'UE[5]; mentre la relazione annuale dell'ACN conta 1.411 attacchi *cyber* trattati dalla stessa (+29% rispetto al 2022)[6]. Se tali dati non fossero sufficienti a testimoniare la gravità della

1 Cencetti 2014: 11.

2 Cfr. Treccani.

In realtà tale locuzione non è affatto recente: essa è stata coniata nel 1999 dall'ingegnere inglese Kevin Ahston.

3 "Lo spazio cibernetico ha permesso immense opportunità di sviluppo economico, grazie alle quali le economie dei paesi più avanzati hanno subito una forte accelerazione".

Cencetti 2014.

4 "I sistemi digitali sono divenuti così complessi che è impossibile impedire tutti gli attacchi. Per rispondere a questa sfida occorre una rapida azione di rilevazione e risposta".

Corte dei conti europea 2019: 5.

5 A titolo meramente esemplificativo, l'ETL rileva un aumento sostanziale degli incidenti legati al *ransomware*, soprattutto a partire dal mese di marzo 2023 (+ 91% rispetto al mese precedente e + 62% rispetto a marzo 2022); nonché un incremento del 135% degli attacchi che sfruttano le tecnologie dell'*AI* nel mese di febbraio 2023 rispetto al mese precedente. Per approfondimenti si veda ENISA 2023.

6 Nel dettaglio, l'ACN sottolinea che il numero dei soggetti colpiti è triplicato (da 1.150 a 3.302), rilevando un forte aumento anche degli incidenti (da 126 a 303) e delle segnalazioni (da 81 a 349). Per approfondimenti, ACN 2024.

situazione, Assintel ha rilevato un incremento del 184% di *cyber* attacchi nel mondo (con un totale di 7.068), dei quali il 61% proveniente dal *Dark Web*[7]. Dietro a ciò, naturalmente, si nasconde anche un danno economico[8].

Ecco quindi che, in una società nella quale si parla di rete 5g, di servizi *multicloud* e di digitalizzazione delle informazioni, la *cybersecurity* diventa essenziale. Non esiste una definizione univoca di *cybersecurity*, ma a livello europeo, essa può essere definita come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[9]. È quindi chiaro come vi rientrino sia le attività di prevenzione che quelle relative all'individuazione degli incidenti informatici[10], nonché le risposte agli stessi ed il successivo recupero.

2. Le principali soluzioni normative europee ed italiane: un breve *excursus*

Alla luce di quanto illustrato, non deve stupire il fatto che il Legislatore europeo abbia inserito la *cybersecurity* tra le proprie priorità fondamentali, intervenendo sul lato normativo al fine di rispondere alle sfide odierne. L'incremento della digitalizzazione[11] e della connettività, infatti, rischia di minare la tutela di diritti e di libertà fondamentali, quali la protezione della vita privata e dei dati personali, la libertà d'impresa e la protezione della proprietà o la dignità e l'integrità della persona.

La prima criticità inerente tale intervento è costituita dalla mancanza di una definizione di sicurezza informatica tra gli atti legislativi vincolanti. Il primo approc-

7 Assintel 2024, *Cyber Report 2023*.

8 Uno studio del 2020 del Joint Research Centre ha stimato che il costo globale della criminalità informatica raggiungerà i 5,5 trilioni di euro entro la fine del 2020, rispetto ai 2,7 trilioni di euro del 2015. Le stime per il 2025 arrivano a 10,5 trilioni di dollari. Il costo medio globale di una violazione dei dati nel 2022 è stato stimato in 4,35 milioni di dollari. Tali importi vanno parametrati e cambiano in relazione al settore (le violazioni dei dati sanitari ammontano in media a 10,10 milioni di dollari), al tipo di attacco (gli attacchi distruttivi ammontano in media a 5,12 milioni di dollari) ed alla regione interessata (le violazioni dei dati negli Stati Uniti ammontano in media a 9,44 milioni di dollari). Oltre a ciò, si ricorda che il danno del *cybercrime* non è limitato solo alle entità colpite: oltre il 45% delle violazioni, infatti, riguarda dati personali, esponendo così i cittadini di tutto il mondo a vari rischi, come il furto di identità e la frode finanziaria.

Cfr. Vandezande 2024: 2.

9 https://www.consilium.europa.eu/it/policies/cybersecurity/.

"In termini ampi, essa designa il complesso di tutele e misure adottate per difendere i sistemi informativi e i relativi utenti da accessi non autorizzati, attacchi e danni al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati".

Corte dei conti europea 2019: 7.

10 Tra gli incidenti informatici si possono annoverare: attacchi a imprese ed infrastrutture critiche, furto di dati, frodi, divulgazione accidentale di dati. Indipendentemente dalla fattispecie, tuttavia, tutti possono avere potenzialmente effetti dannosi di ampia portata su persone fisiche, organizzazioni e comunità. A mero titolo esemplificativo, il *ransomware Wannacry* e il *wiper NotPetya* hanno colpito, nel 2017, in totale oltre 320.000 soggetti in circa 150 Paesi. Per approfondimenti si veda Greenberg 2017.

11 Per eventuali approfondimenti, Golisano 2022.

cio alla materia si ha nel 2013 tramite la Comunicazione "Strategia dell'Unione europea per la cybersicurezza: un cyberspazio aperto e sicuro", che ha fornito una descrizione completa di cosa s'intenda per cybersicurezza ed ha accompagnato la strategia dell'UE sulla *cybersecurity* del 2013 (EUCSS 2013). Essa, per la prima volta, ha fissato l'obiettivo di sviluppare una linea a livello comunitario in tale ambito. In tale pacchetto, rientra la direttiva UE 2016/1148 (c.d direttiva NIS). Tale strumento giuridico è molto importante perché, non solo costituisce la prima iniziativa legislativa orizzontale vincolante dell'UE su questa tematica, ma rappresenta una sintesi della maggior parte delle indicazioni incluse nelle precedenti comunicazioni della Commissione. Alla direttiva soggiacciono due obiettivi complementari: la protezione delle infrastrutture critiche e la promozione e potenziamento del mercato interno dell'UE.

Nonostante l'importanza di tale strumento, lo stesso è stato criticato[12], in quanto la NIS si occupa di sicurezza, un'area in cui UE e Stati membri condividono le competenze legislative. Tali critiche sono cessate in seguito ad una lettura attenta del considerando 5, il quale afferma che, in assenza di standard di protezione condivisi, non si avrebbe un'adeguata protezione dei consumatori e delle imprese. Nonostante l'evidente importanza della direttiva NIS, essa non può essere considerata un traguardo, in quanto si concentra maggiormente sull'armonizzazione degli aspetti procedurali per gestire i rischi piuttosto che fornire sostanziali chiarimenti in merito a quali siano i rischi e le minacce per cui tali procedure devono essere adottate. Tale strumento normativo, inoltre, è risultato di difficile attuazione[13], quindi, la direttiva NIS è stata novellata dalla direttiva UE 2022/2555 (c.d. NIS2) ed abrogata a decorrere dal 18 ottobre 2024. La *ratio* è quella di affrontare un panorama di minacce mutato radicalmente e ovviare, al tempo stesso, le problematiche che hanno impedito alla direttiva NIS di ottenere i risultati sperati[14]. Uno dei punti cardine della NIS2 è quello di affrontare esplicitamente la protezione della *supply chain*[15].

12 La stessa Commissione ha effettuato una valutazione sulla direttiva, evidenziando che la stessa non copre tutti i settori che forniscono servizi chiave all'economia e alla società, ma che soprattutto, la normativa avesse concesso poteri discrezionali troppo ampi agli Stati membri.

13 Gli Stati membri hanno infatti recepito la direttiva in modo difforme, vanificando l'intento della normativa stessa e creando, di fatto, un'insufficiente risposta alle nuove e mutevoli sfide della sicurezza informatica.

14 La NIS2, infatti, amplia la portata della direttiva NIS, aumentandone la copertura dei settori: rispetto alle aziende assoggettate alla NIS che venivano identificate da decisioni delle Autorità nazionali competenti, la nuova normativa introduce un singolo criterio per le aziende nei settori elencati, in base al quale devono essere identificate principalmente *ipso iure*, ovvero le dimensioni di un'azienda.

Per approfondire le caratteristiche della Direttiva NIS2 ed apprenderne le principali sfide, si veda Sievers 2021.

15 Per un confronto tra direttiva NIS e NIS2, si consiglia N. Vandezande 2024. Per un approfondimento su NIS2 e *supply chain*, invece, si veda van 't Schip, 2024, nel quale, comunque emergono alcune imperfezioni dell'ultima direttiva.

La strategia europea[16] è stata poi modificata nel 2017 attraverso un pacchetto di norme che comprende misure, vincolanti e non, con le quali la Commissione ha inteso affrontare le nuove sfide in tale ambito. Se la direttiva NIS era il fiore all'occhiello della precedente strategia, questa volta, la punta di diamante è il Regolamento UE 2019/881 (il c.d. *Cybersecurity Act*). Tale regolamento spinge verso un nuovo approccio proattivo, che porti alla costruzione di un sistema condiviso di comprensione dei rischi peculiari della *cybersecurity*.

Rispetto alla presente trattazione, la seconda parte del regolamento, cioè quella relativa alla creazione di un sistema di certificazione della *cybersecurity* dell'UE per prodotti, servizi e processi *ICT*, risulta indubbiamente più interessante. Senza entrare nel dettaglio, il *cybersecurity act* mira a rafforzare il ruolo dell'UE nello scenario globale, migliorando il coordinamento transfrontaliero, dando impulso a misure volte all'armonizzazione sostanziale e procedurale in ambito di cybersicurezza ed infine, promuovendo uno standard europeo in tale ambito. In questa breve disamina non può mancare la proposta di nuovo regolamento, già approvata dal Parlamento europeo: il *Cyber Resilience Act* (CRA)[17], il cui obiettivo è salvaguardare i consumatori e le imprese che acquistano o utilizzano prodotti o *software* con un componente digitale, andando ad integrare la direttiva NIS2[18]. Alla luce di tale carrellata, appare chiaro come,

> nel gergo delle politiche dell'UE, il termine cybersicurezza non è riferito esclusivamente alla sicurezza delle reti e dei sistemi informativi, bensì designa qualsiasi attività illecita che comporti l'impiego di tecnologie digitali nel cyberspazio. Può comprendere quindi reati informatici quali gli attacchi con virus informatici e le frodi perpetrate con mezzi di pagamento diversi dai contanti, travalicando la separazione fra sistemi e contenuti, come nel caso della diffusione online di materiale pedopornografico. Può anche riguardare campagne di disinformazione volte a influenzare il dibattito online e produrre presunte interferenze nelle consultazioni elettorali. In aggiunta, Europol nota una convergenza tra criminalità informatica e terrorismo.[19]

Nonostante le azioni degli anni '90 (l. n. 547 del 23 dicembre 1993 e l. n. 269 del 3 agosto 1998), che hanno definito i reati informatici, apportando importanti modifiche al Codice penale e a quello di procedura penale, dal punto di vista della normativa italiana, gli interventi sono tutti abbastanza recenti. Nel 2002, si è

16 Tale strategia si basa su tre pilastri: resilienza, sovranità tecnologica e *leadership*; capacità operativa per prevenire, scoraggiare e rispondere; ed infine, cooperazione per promuovere un cyberspazio globale e aperto.

17 Per approfondimenti in merito, si veda Chiara 2023.

18 Il *Cyber Resilience Act*, infatti, prevede requisiti di sicurezza informatica per prodotti, *hardware* e *software*, con elementi digitali, anche non coperti da NIS2, con l'obiettivo di affrontare il problema legato al fatto che i dispositivi, come computer e *smartphone*, vengono spesso immessi sul mercato con vulnerabilità di sicurezza e/o una mancanza di aggiornamenti di sicurezza per tutto il loro ciclo di vita. Per approfondimenti, si veda Vandezande 2024

19 Corte dei conti europea 2019: 7.

Per una panoramica più approfondita sulla normativa inerente la sicurezza informatica dell'*IoT*, si veda Chiara 2022.

iniziato ad occuparsi di protezione delle informazioni in formato digitale raccolte dalle PA; mentre, l'anno successivo è stato istituito l'Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni. Da questo momento, diversi interventi si sono susseguiti: il D.Lgs. n. 196 del 30 giugno 2003 (Codice della privacy), il D.Lgs. n. 259 del 1° agosto 2003 (Codice delle comunicazioni elettroniche), il D.Lgs. n. 82 del 7 marzo 2005 (Codice dell'amministrazione digitale), la l. n. 38 del 6 febbraio 2006 (Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet). In questa breve disamina, non possono mancare il D.lgs. 18 maggio 2018 n. 65 (c.d. D.Lgs. NIS) che ha introdotto una serie di obblighi di sicurezza a carico degli operatori e fornitori dei servizi digitali nell'adozione di misure di sicurezza e notifica degli incidenti e ha previsto la creazione del CSIRT; il D.L. n. 105 del 2019, adottato con lo scopo di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati; il D.L. n. 162 del 2019, che ha novellato la normativa precedente; il D.L. 14 giugno 2021, n. 82 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", convertito in legge dalla l. del 04 agosto 2021, n. 109 (si ricorda infatti che la *cybersecurity* è tra gli interventi previsti nel PNRR). Ultimo intervento che si ritiene utile citare è l. n. 90 del 28 giugno 2024 (ex D.D.L. Cybersicurezza) [20], che pone al centro l'importanza della formazione: proprio l'assenza di formazione nei campi *ICT* e sicurezza informatica rappresenta uno dei punti sul quale si tornerà nel proseguo.

"La *ratio* comune alla recente normativa italiana ed alla Strategia Europea risiede nella volontà di fornire strumenti di contrasto più flessibili nel contrasto ad un fenomeno in continua evoluzione capace di adattarsi ai mutamenti sociali ed economici"[21].

3. Gli effetti dello sviluppo delle tecnologie sul settore turistico

Il turismo non poteva certo rimanere immune da digitalizzazione e piattaformizzazione: Internet e le piattaforme *eCommerce* hanno fatto il loro prepotente ingresso in tale ambito, innovandolo profondamente e modificandone le caratteristiche (sia dal lato della domanda che dell'offerta). Fra le innovazioni è possibile citare la nascita delle *Online Travel Agencies* (OTA), lo sviluppo degli *home restaurant* e delle piattaforme di *home exchange* e locazioni brevi, tutte realtà fiorite nell'ambito della *sharing economy*. Nel tempo, infatti, la pratica turistica è mutata e con essa è cambiata la domanda: oggi, il 67% delle persone che progetta un viaggio effettua una ricerca su internet, 2 viaggi su 3 vengono prenotati online, ma non

20 Per maggiori dettagli su interventi normativi e relative evoluzioni, si veda Paganelli 2021.

21 Mattarella 2022: p. 828.

solo, il turista 2.0 resta costantemente connesso anche durante la vacanza ed ama condividere le sue impressioni attraverso *feedback*, commenti e foto[22]. Tutto ciò è esploso in seguito alla pandemia: i dati elaborati dalla Commissione europea, infatti, testimoniano come nel 2019, gli italiani che prenotavano i viaggi online fossero solo il 39%, ma non solo: i servizi internet presso le destinazioni erano di qualità inferiore, così come il ricorso all'*e-commerce* era ben inferiore rispetto alla media europea[23].

> Il processo di digitalizzazione delle destinazioni turistiche richiede un ammodernamento strutturale e globale dell'impianto tecnologico e delle procedure in esso presenti. In particolare, il trattamento e la trasmissione delle informazioni diventano un punto nevralgico del settore dell'ospitalità che rende necessario un nuovo inquadramento concettuale degli spazi interessati all'accoglienza, dei flussi e all'offerta dei prodotti turistici.[24]

L'offerta turistica deve quindi mutare ed adeguarsi alle nuove caratteristiche del turista: nascono le possibilità di ´visitare´ la destinazione attraverso la realtà aumentata, di effettuare il *check-in* online o tramite i dispostivi mobili, nonché la diffusione di app dedicate a hotel.

La crescente proliferazione e diffusione dell'*ICT* nelle infrastrutture delle città ha incrementato l'interesse verso le *Smart Cities*, il cui fine ultimo è quello di migliorare la qualità dei servizi forniti ai cittadini e, di conseguenza, migliorare la loro qualità della vita[25]. Ma l'evoluzione turistica non si è fermata qui: ecco quindi che, dalle *smart cities*, si è giunti alle *smart destinations*, che non solo stanno rivoluzionando il concetto di offerta turistica, ma aprono nuove frontiere di studio e analisi. Alla luce di ciò, le *smart destinations* devono essere intese come un nuovo ecosistema[26], basato

> su uno spazio turistico innovativo e accessibile consolidato su un'infrastruttura tecnologica all'avanguardia che garantisce lo sviluppo sostenibile del territorio, le *smart*

22 Ecco come i consumatori hanno acquisito un ruolo attivo nella co-creazione delle proprie esperienze. In questo contesto, grazie alle tecnologie, si assiste, da un lato alla personalizzazione dei servizi turistici in base alle esigenze e alle preferenze dei singoli turisti e, dall'altro, l'utilizzo di informazioni in tempo reale per migliorare il processo decisionale. Per approfondimenti, Buhalis, Amaranggana, 2015.

23 "Tali considerazioni assumono una valenza assoluta per quanto attiene l'industria turistica in generale, in considerazione delle evoluzioni apportate al comparto dalle recenti dinamiche riconducibili a nuove tipologie di turismo (*smart/digital tourism*). Negli ultimi vent'anni si è assistito a un mutamento radicale nel settore del turismo, sia a livello quantitativo, con una crescita costante del numero di viaggiatori, sia qualitativo: il turista, grazie all'innovazione nel sistema dei trasporti e al consolidamento dei voli *low cost*, è sempre più globale; nella vacanza ricerca l'aspetto locale, la qualità dei servizi e l'autenticità delle esperienze, ma soprattutto è sempre più giovane e digitalmente interconnesso e fa ampio utilizzo delle tecnologie per l'organizzazione delle vacanze".

Cfr. Mariotti, Carrus, Panai, Martinez, Camerada 2018: 65.

24 Mariotti, Carrus, Panai, Martinez, Camerada 2018: 59.

25 Per approfondimenti, si veda Khatoun, Zeadally 2017.

26 Per approfondimenti, si consigliano Boes, Buhalis, Inversini 2016; Gretzel, Werthner, Koo, Lamsfus 2015

> *destination* facilitano l'interazione e l'integrazione dei turisti nell'ambiente e migliorano l'esperienza dei visitatori nonché la qualità della vita dei residenti.[27]

I territori, dunque, non possono trascurare il ruolo degli elementi intangibili che sottendono l'innovazione tecnologica e digitale. Ecco quindi, che le interconnessioni tra i diversi attori all'interno della *smart destination* si moltiplicano e, se questo da un lato provoca una maggiore integrazione del prodotto turistico, dal punto di vista strettamente informatico, ogni attore porta nuove vulnerabilità per l'intera catena e, a sua volta, per il prodotto *ICT* creato dalla catena stessa.

Lo sviluppo della tecnologia, quindi, non ha impattato unicamente su consumatori e operatori turistici, ma persino sulle destinazioni, incrementandone la competitività. L'innovazione tecnologica diviene un *driver* fondamentale della crescita dei territori: la *cybersecurity* diventa, quindi, non solo una condizione necessaria al fine di garantire i diritti dei turisti, ma soprattutto un elemento di distinzione rispetto ai propri *competitors*. Nonostante il turismo sia fortemente radicato sul territorio, molte destinazioni vengono precedentemente ´visitate´ virtualmente: ecco che la competizione è una partita giocata su un terreno non più solo fisico. I *driver* e le dinamiche competitive dei territori sono numerosi ma, per quanto riguarda lo scopo della presente trattazione, si ritiene di concentrarsi principalmente sul legame esistente tra *cybersecurity* e reputazione turistica. Quest'ultima va naturalmente intesa sia come reputazione territoriale, che come reputazione delle aziende che operano nella specifica filiera turistica. Come anticipato, infatti, il turista odierno vive costantemente connesso ed il fatto che le piattaforme digitali siano sempre più interattive, consentendo agli utenti di creare e pubblicare contenuti, permette alle imprese turistiche e alle destinazioni di beneficiare di un'attività di marketing personalizzato[28] rappresentata dall'*electronic word-of-mouth*, cioè una forma di comunicazione online che influisce fortemente sulle dinamiche di scelta e acquisto dei beni e servizi di una destinazione turistica e ne forgia la *web reputation*[29]. Proprio la necessità di tutelare quest'ultima, impone sia alla *governance* aziendale che a quella territoriale, di osservarla, analizzarla, interpretarla e monitorarla, facendo emergere il forte legame che intercorre tra competitività, progettazione della destinazione e *cybersecurity*.

> Tale nesso implica la necessità di contemplare, nel processo di progettazione territoriale turistica, interventi connessi all'implementazione di sistemi informatici sicuri di gestione delle *ICT*, in ogni singola azienda che opera nel comparto. Per poter procedere in tal senso è opportuno diffondere tra gli *stakeholders* un'adeguata cultura in termini di *cyber-igiene*, per permettere al territorio di acquisire un profilo turistico più competitivo.[30]

27 Cfr. Sustacha, Baños-Pino, Del Valle 2023: 1.

28 Per la definizione di marketing personalizzato, si rimanda a R. Moro Visconti 2020: 76.

29 Per approfondimenti, Sweeney, Soutar, Mazzarol 2008: 344-364.
A tal riguardo, appare d'uopo ricordare che la diffusione dei *social network* ha notevolmente potenziato la fruibilità delle informazioni, trasformandosi in uno strumento avanzato di marketing personalizzato e *digital branding*. Si veda Moro Visconti 2020.

30 Mariotti, Carrus, Panai, Martinez, Camerada 2018: 67.

Alla luce di ciò, quindi, domanda ed offerta concorrono alla creazione del valore, arricchendo sempre più l'esperienza turistica[31]: la fruizione della stessa è radicalmente mutata nel tempo, sia dal punto di vista di esperienza in loco sia da quello del prodotto, il cui livello di personalizzazione è in costante crescita[32].

Nonostante quanto sinora sostenuto sull'importanza della *cybersecurity*, il panorama attuale appare alquanto frammentato: sebbene vi sia una maggiore consapevolezza, anche da parte delle imprese, dell'importanza di dotarsi si sistemi di prevenzione, molto spesso tali soluzioni vengono considerate troppo complesse o dispendiose dalle PMI. Alcuni studi, infatti, evidenziano una complessità maggiore nel governo della tutela informatica nelle aziende turistiche di modeste dimensioni, caratterizzate da stagionalità e intermittenti gradi di intensità del lavoro[33].

Si è accennato poco fa, alla *web reputation* ed alla necessità di monitorarla: oltre agli attacchi informatici, infatti, appare d'uopo ricordare altresì un altro grande pericolo della rete, ossia la diffusione delle c.d. *fake news*. Esse possono essere definite come informazioni false, ingannevoli o distorte rese pubbliche, e possono arrivare a minare il corretto svolgimento della concorrenza sul mercato. Possono comportare una distruzione di valore potenzialmente assai rilevante, cui sempre non è facile porre rimedio.

> Ai danneggiati può soccorrere, in talune fattispecie, il diritto all'oblio con la rimozione dei link che rimandano al contenuto online ritenuto lesivo. La portata delle *fake news* è peraltro ben più ampia e spesso travalica la sfera individuale, orientando vaste schiere di cibernauti fino a ingannare l'opinione pubblica una *fake news* contro un concorrente o un prodotto può costituire un atto di concorrenza sleale. Una *fake news* nel sistema della comunicazione pubblicitaria può costituire un atto di pubblicità decettiva e aggressiva o una forma di pubblicità occulta.[34]

4. Conclusioni e sfide future

Nel presente contributo si è analizzato l'impatto delle nuove tecnologie nella vita di tutti i giorni, evidenziandone sia gli aspetti positivi che, soprattutto i pericoli insiti negli stessi. Oltre alle varie risposte tecnologiche, alla necessità di formazione in tali campi e di sensibilizzazione dei cittadini, al fine di ridurre il più possibile i rischi derivanti da tali pericoli, si sono ripercorse le diverse risposte date dal Legislatore europeo e quello italiano nel tempo. Partendo dalla direttiva NIS, vera e propria ´prima pietra´ per una politica di sicurezza informatica all'interno dell'UE, si sono ripercorsi i diversi strumenti normativi adottati, osservando come, negli anni, essi abbiano ampliato sempre più il proprio raggio d'azione. Dalla necessità di fornire un livello comune di sicurezza informatica in tutta Europa, si è passati

31 Si veda Ballina, Vald´es, Del Valle 2019.
32 Sul tema, si consiglia Shoval, Birenboim 2019.
33 Mariotti, Panai, Camerada 2018.
34 Moro Visconti 2020: 82.

alla *cybersecurity* della *supply chain* ed infine ad un atteggiamento proattivo nei confronti del rischio stesso. Da questi primi passi, quindi, la sicurezza informatica è entrata a far parte dell'ordine del giorno dei Legislatori nazionali[35].

Al fine di dare maggiore concretezza a tali osservazioni, si è deciso di tratteggiare gli effetti delle nuove tecnologie su uno dei settori più importanti per l'economia italiana: quello turistico. Senza ripercorrere quanto osservato fin qui, si può affermare che le nuove tecnologie abbiano dunque impattato profondamente su tale settore, migliorandone, da un lato l'esperienza, ma dall'altro lato creando anche dei potenziali effetti negativi (si pensi ad esempio ai rischi legati alla privacy, all'esclusione, al *digital devide* e persino all'alienazione e alla perdita di autenticità)[36]. Considerare entrambe le facce della medaglia è fondamentale per non sopravvalutare gli effetti della tecnologia nel settore turistico. È quindi fondamentale che, all'interno di tale ambito, i diversi attori della filiera comprendano l'effettiva portata dell'*IoT* – nonché i relativi pericoli – al fine di migliorare l'esperienza turistica stessa, aumentando così la soddisfazione dei visitatori e la loro fidelizzazione.

Alla luce di quanto illustrato, emerge come la *cybersecurity* sia un aspetto che riguarda sia il viaggiatore, che le imprese turistiche e i territori: viaggiatori e imprese possono vestire la duplice veste di bersaglio, e di complici involontari degli attacchi informatici. Essi possono infatti essere vettori degli attacchi e della diffusione di disinformazione, in quanto esposti, senza saperlo, a vulnerabilità dei propri dispositivi o vittime di *social engineering*. Ecco quindi spiegata l'importanza della cybersicurezza, ma, nonostante ciò, tale aspetto viene ancora sottovalutato dai principali *stakeholders*. Oggi, infatti, si registra una crescente asimmetria tra le conoscenze possedute dagli *hacker* e quelle necessarie per difendersene: ecco, dunque, che sarebbe fondamentale non solo sensibilizzare sul tema, al fine di costruire un'efficace *cyberresilienza*, ma puntare sulla formazione di esperti in tutti i settori economici. Tale considerazione, che potrebbe apparire scontata, in realtà non è così banale, in quanto, alla luce di un sondaggio mondiale, un terzo delle organizzazioni preferirebbe pagare il riscatto chiesto dagli *hacker*, piuttosto che investire nella sicurezza delle informazioni[37]. Al fine di rendere operativa la sicurezza informatica della *supply chain* (in qualsiasi settore economico) occorrerebbe, quindi, applicare i principi del *Cyber Supply Chain Risk Management*[38], che com-

35 Per ulteriori approfondimenti sul tema delle risposte nazionali, soprattutto in tema di *cybersecurity* nelle *supply chian* si consiglia Ludvigsen, Nagaraja, Daly 2022.

36 L'uso eccessivo della tecnologia potrebbe diminuire la qualità dell'esperienza di viaggio, creando barriere all'evasione, al divertimento e una ´momentanea assenza mentale´ quando i turisti interagiscono online. Oltre a ciò, sembra che l'uso costante dei dispositivi mobili, al fine di preservare i ricordi, possa in realtà impedire ai turisti di ricordare l'esperienza stessa. Ecco, dunque, che oggigiorno si sente parlare anche di *technostress* o stress tecnologico e quindi nasce il bisogno di una disintossicazione e disconnessione digitale. In tema si veda Sustacha, Baños-Pino, Del Valle 2023, ove presenti ulteriori riferimenti bibliografici.

37 NTT Security 2018.

38 Questa disciplina si concentra sui seguenti tre elementi: resilienza informatica; investimenti collaborativi in sicurezza informatica richiesti per raggiungere tale resilienza ed infine, utilizzo di standard riconosciuti. Per approfondimenti: Melnyk *et al.* 2022.

bina aspetti tipici della sicurezza informatica, della gestione dei rischi aziendali e della gestione della *supply chain*. In altre parole, quindi, si dovrebbero mettere in campo una serie di sforzi al fine di accrescere la propria *cyber resilience*: tale risultato è raggiungibile solo attraverso un approccio di *cybersecurity* più ampio, che comprenda una strategia di investimenti collaborativi nonché l'uso di standard armonizzati all'interno della filiera[39].

Si è affermato che, ad oggi, le PMI[40] – soprattutto quelle del comparto turistico con attività stagionali – fatichino ad implementare soluzioni adeguate a garantire la sicurezza delle informazioni: a parere di chi scrive, occorrerebbe riadattare e semplificare la normativa, tenendo conto delle specificità e delle esigenze delle PMI, cercando di fornire loro idonee linee guida sull'applicazione dei requisiti in materia di sicurezza delle informazioni e di privacy e sulla mitigazione dei rischi tecnologici. Non bisogna infatti sottovalutare il fatto che i piccoli potrebbero non avere le necessarie conoscenze o risorse per la sicurezza informatica, quindi, occorrerebbe fornire loro incentivi o comunque sensibilizzarli sull'importanza della *cybersecurity*. Solo attraverso un maggiore coinvolgimento delle PMI e degli strumenti costruiti *ad hoc* per le stesse, tali attori economici potranno finalmente sentirsi parte di una strategia comune e non interpretare la *cybersecurity* come una delle tante obbligazioni alle quali adempiere. Questa, infatti, non può essere una battaglia che i soggetti privati possono vincere da soli: la collaborazione tra pubblico e privato è fondamentale, sia per la condivisione delle informazioni che per lo scambio delle buone pratiche. "Uno scarso coordinamento porta alla frammentazione, alla duplicazione degli sforzi e a una dispersione di competenze. Un efficace coordinamento può avere come risultato successi tangibili, come la chiusura di alcuni mercati del *dark web*"[41].

Si è infine accennato alla diffusione delle *smart cities* ed alla conseguente evoluzione nelle *smart destinations* e, di come, l'irruzione della tecnologia in tali contesti possa comportare diversi problemi di sicurezza e privacy.

> L'evolversi della tecnologia nella gestione delle città e degli enti che le governano aumenta i rischi legati ad intrusioni, usi impropri e attacchi alla sicurezza cibernetica per i quali a livello internazionale e nazionale si sta consolidando una legislazione rivolta alla difesa delle funzioni essenziali dello Stato.[42]

39 Per ulteriori approfondimenti, van 't Schip 2024.

40 Il rapporto dell'Osservatorio *Cybersecurity & Data Protection* della *School of Management* del Politecnico di Milano evidenzia, per l'anno 2023, un incremento della spesa in *cybersecurity* da parte delle grandi organizzazioni, sottolineando che le piccole imprese, invece, non riescano ad effettuare investimenti concreti, a causa di risorse limitate e di difficoltà nel reperire sul mercato, soluzioni che soddisfino le loro specifiche esigenze.

41 Corte dei conti europea 2019: 41-42.

42 Paganelli 2021: 681. L'autore sottolinea come, "la sola esistenza di telecamere che monitorano il territorio richiede una strategia di progettazione che definisca i confini dell'area urbana e ne permetta il presidio. […] questo sistema si è grandemente diffuso ed assicura una copertura abbastanza sistematica dei centri cittadini attraverso il controllo degli accessi, ma origina al contempo una quantità enorme di informazioni da trattare e archiviare. Se a questo aggiungiamo

Anche in questo caso, la normativa dovrebbe essere adattata alle nuove caratteristiche dei territori. Si ricorda infatti che, lo sviluppo delle nuove tecnologie ha determinato una profonda trasformazione nelle modalità di progettazione e governo degli stessi, incrementandone il livello di competizione, rendendo possibili persino le visite virtuali che fino a qualche anno fa erano impensabili.

Alla luce di tale osservazione, in un ambiente sempre più mediato dalla tecnologia, la mancanza di *compliance* nei requisiti di sicurezza e privacy in una destinazione può avere un impatto significativo sulla disponibilità dei turisti[43]: ecco quindi che tale requisito diventa fondamentale per mantenere una reputazione positiva nonché la propria quota di mercato. Non bisogna infatti dimenticare che, grazie alle nuove tecnologie, le *smart destinations* e gli operatori della filiera turistica riescono ad acquisire ed immagazzinare moltissimi dati dei turisti (cosa che, in passato non era neanche immaginabile).

Bibliografia

ACN 2024, *Relazione annuale al Parlamento 2023*.

Assintel 2024, *Cyber Report 2023*.

Ballina F. J., Vald´es L., Del Valle E. 2019, "The Phygital experience in the smart tourism destination", in *International Journal of Tourism Cities,* 5(4).

Boes, K., Buhalis D., Inversini, A. 2015, "Smart tourism destinations: Ecosystems for tourism destination competitiveness" in *International Journal of Tourism Cities,* 2(2).

Buhalis, D., Amaranggana, A. 2015, "Smart tourism destinations enhancing tourism experience through personalisation of services", in Tussyadiah,I., Inversini A. (Eds.), *Information and communication technologies in tourism 2015*, Springer.

Cencetti C. 2014, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Quaderni IAI, Roma: Edizioni Nuova Cultura.

Chiara p. G. 2022, "The IoT and the New EU Cybersecurity Regulatory Landscape", in *International Review of Law, Computers & Technology*, 1.

Chiara p. G. 2023, "Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", in *Rivista Italiana di Informatica e Diritto*, fasc. 1.

Corte dei conti europea 2019, *Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza. Documento di riflessione*.

European Union Agency for Cybersecurity (ENISA) 2023, *ENISA Threat Landscape 2023 (July 2022 to June 2023)*.

Greenberg G. 2017, "Hold North Korea Accountable For Wannacry—and the NSA, too", in *WIRED*.

Gretzel U., Werthner H., Koo C., Lamsfus C. 2015, "Conceptual foundations for understanding smart tourism ecosystems", in *Computers in Human Behavior,* 50.

le telecamere di enti pubblici e privati installate per motivi di sicurezza o funzionali alle attività svolte, allora la copertura è ancora più ampia e nel tempo questo sistema si integrerà in qualche modo, consentendo il passaggio delle informazioni da una rete di sorveglianza all'altra". A ciò si aggiungono altresì le prospettive del c.d. *city sensing*.

43 Per approfondimenti, Jeong, Shin 2020.

Golisano L. 2022, "Il governo del digitale: strutture di governo e innovazione digitale", in *Giornale di diritto amministrativo*, n. 6.
Jeong M., Shin, H. 2020, "Tourists' experiences with smart tourism technology at smart destinations and their behavior intentions", in *Journal of Travel Research, 59*(8).
Khatoun R., Zeadally S. 2017, "Cybersecurity and Privacy Solutions in Smart Cities", in *IEEE Communications Magazine*.
Ludvigsen K. R., Nagaraja S., Daly A. 2022, "Preventing or Mitigating Adversarial Supply Chain Attacks: A Legal Analysis", in *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*.
Mariotti G., Carrus S., Panai E., Martinez V., Camerada M. V. 2018, "Smart destinations e competitività in ambito turistico. Il ruolo della cyber security", in *AGEI – Geotema*, Supplemento.
Mariotti G., Panai E., Camerada M. V. 2018, "Piattaforma per la sicurezza informatica per il comparto turistico: dalla prospettiva nazionale all'azione reale. Focus sulle strutture ricettive", in *AGEI – Geotema*, Supplemento.
Mattarella A. 2022, "Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite", in *Diritto penale e processo*, n. 6.
Melnyk S. A., Schoenherr T., Speier-Pero C., Peters C., Chang J. F., Friday D. 2022, "New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain", in *International Journal of Production Research*, 60(4).
Moro Visconti R. 2020*,* "La valutazione dei social network", in *Il Diritto industriale*, n. 1.
NTT Security 2018, *Risk:Value 2018 Report*.
Paganelli G. 2021, "Perimetri di controllo e sicurezza cibernetica. Una verifica indispensabile", in *Azienditalia*, n. 4.
Shoval N., Birenboim, A. 2019, "Customization and augmentation of experiences through mobile technologies: A paradigm shift in the analysis of destination competitiveness", in *Tourism Economics,* 25(5).
Sievers T. 2021, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations", in *Int. Cybersecur. Law Rev.*, 2.
Sustacha I., Baños-Pino J. F., Del Valle E. 2023, "The role of technology in enhancing the tourism experience in smart destinations: A meta-analysis", in *Journal of Destination Marketing & Management*, 30.
Sweeney J. C., Soutar G. N., Mazzarol T. 2008, "Factors Influencing Word of Mouth Effectiveness: Receiver Perspectives*",* in *European Journal of Marketing*, 42.
van 't Schip M. 2024, "The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things", in *European Journal of Law and Technology*, Vol. 15, No. 1.
Vandezande N. 2024, "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor", in *Computer Law & Security Review*, 52.

Bruno Carotti

Uniformità e autonomia nella sicurezza cibernetica

Abstract: Il settore della sicurezza cibernetica consente prospettive inedite sull'attività amministrativa e sulle formule organizzative. L'analisi qui presentata muove da tre dicotomie che accennano a un movimento tellurico: l'esigenza di assicurare una direzione unitaria preservando l'autonomia dei soggetti coinvolti. Gli spunti presentati inducono a una riflessione su categorie note del diritto amministrativo, quali il coordinamento e l'autonomia nella sua accezione funzionale che, pur conservandosi nella loro essenza, impongono di essere osservate sotto una nuova luce, a testimonianza del modo di costruzione di questa branca del sapere, che deve muovere dal dato reale e non procedere per astrattismi.

Keywords: Cybersecurity, Uniformità, Autonomia, Disciplina istituzionale, Interesse Nazionale.

1. Introduzione

La sicurezza cibernetica contiene una dicotomia: una latente tensione tra uniformità e autonomia. Questa tensione è osservabile in una triplice dimensione: nelle decisioni (centralizzate e singole), nelle funzioni (collaborazione, scambio e unilateralità), nell'organizzazione (centro e periferia). Se ne analizzeranno di seguito tasselli e parti salienti. Questo consentirà di effettuare un primo tentativo ricostruttivo, ricorrendo, in special modo, alle figure del coordinamento e dell'autonomia, nella loro declinazione funzionale e innovativa. Gli equilibri sono altalenanti e mostrano una pittura ancora in corso, in cui alcuni particolari resteranno sfumati, mentre altri saranno definiti con pennellature finali, restituendo un'immagine di competenze e assetti.

Sarà necessaria una premessa, ricordando un interesse che permea l'intera disciplina e l'attività amministrativa che consegue a determinate scelte di politica settoriale.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760146

2. L'elemento unificante: l'interesse nazionale

L'interesse nazionale è centrale nell'ambito della sicurezza cibernetica. Il decreto-legge n. 82 del 2021 – tappa importante di un percorso iniziato, a singhiozzo, circa dieci anni prima – è chiarissimo in tal senso: lo pone alla radice dell'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), ne permea il funzionamento e tinge l'intero settore dei suoi pigmenti. Condiziona l'esercizio delle funzioni e funge da parametro di legittimità.

Questo ritorno all'interesse nazionale stupisce, in un contesto come quello attuale. Allo stesso tempo, non sorprende. Esso, infatti, ritorna con un fine specifico e latente: quello di consolidare gli interessi tutelati, intimi alla dimensione statale, e le istituzioni coinvolte nel settore, secondo un disegno che inquadra l'informatica all'interno dei fattori 'ad alta sensibilità' rispetto a funzioni fondamentali. In un contesto in cui gli attacchi sono aumentati vertiginosamente, e continueranno a farlo alla luce di interessi economici e strategici, crescono le preoccupazioni e i tentativi di risposta da parte dei decisori politici, prima ancora che tecnici[1].

Dietro la natura dell'interesse, dunque, si intravede un sostrato politico, sfociato nel tessuto giuridico, nel quale assume valenza e consistenza operativa. L'interesse nazionale giustifica la presenza di funzioni centrali, di capacità pervasive, di segretezza, di criteri unitari, di poteri di indagine e sanzionatori in capo a un apparato nazionale. Esso si correla, inoltre, all'ormai ben noto concetto di "perimetro", andando a costituire un *unicum* concettuale o, quantomeno, una dimensione simbolica, dove ambiti istituzionali diversi diventano attigui e vengono uniti da un collante omogeneo. La costruzione che ne risulta è lo Stato-Nazione, che torna a parlare e a indicare la necessità di agire in modo granitico.

La natura pregnante di tale interesse, comunque, non esaurisce la dimensione assiologica del settore. In un momento in cui la cessione di sovranità è ancora in essere (11 Cost.) e dove l'Unione europea gioca ancora un ruolo primario, non può non considerarsi la dimensione sovranazionale. L'interesse nazionale si piega solo al suo cospetto: le più scottanti innovazioni in materia, del resto, derivano dall'attuazione di atti normativi sovranazionali, a partire dalla direttiva Nis, per arrivare alla sua revisione (Nis 2), passando per il *Cybersecurity Act* e per il recente *Cyber Resilience Act*[2]. Sono atti normativi che raccordano gli Stati membri in un insieme unitario e, nel rispettarne le unicità, le uniscono in modo indelebile.

1 "*Throughout the latter part of 2023 and the initial half of 2024, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences*": ENISA, *Threat Landscape July 2023-July 2024*, September 2024 (su https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024). L'ENISA ha osservato, in un arco temporale annuale, più di undicimila attacchi riguardanti l'Unione europea, che presenta un tasso di rischio maggiore nel contesto globale: *ivi*, p. 11-12.

2 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022*, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2),* e il Regolamento UE n. 2841/2023, del Parlamento europeo e del Consiglio, del 13 dicembre 2023, *che stabilisce misure per un livello comune elevato di cibersi-*

Dunque, sul versante europeo, diviene – paradossalmente – un altro elemento di integrazione, che spinge verso le sue componenti più dure e legate al concetto di sovranità; sul piano nazionale, legandosi alla sicurezza dello Stato, intende colmare un divario storico che ha caratterizzato l'ordinamento nazionale. In via consequenziale, sia nella disciplina interna, sia nella legislazione europea, si osserva la preoccupazione di unire le forze e far fronte a esigenze di sicurezza cibernetica, sia in difesa che in attacco[3]. Il costrutto richiede unità di intenti e condivisione: se ne osserveranno le forme giuridico-istituzionali[4].

La disciplina vigente si inserisce in questo scenario. Un interesse unitario, dentro e oltre lo Stato, indirizza le forme e i modi dell'attività istituzionale. Un contesto innovativo, come quello informatico, si avvicina all'età adulta senza mostrare, però, segni di maturità: dell'informatica sono ormai note non solo le potenzialità, ma anche i rischi e, in particolar modo, gli usi distorti che possono essere realizzati da singoli, organizzazioni sociali, e persino da istituzioni. I diversi utilizzi della tecnica sono essenziali, anche in questo caso, per comprendere le dinamiche sottostanti.

3. La dicotomia decisoria

Concentrandosi sull'ordinamento nazionale, non vi sono dubbi sulla portata centralizzatrice dell'Agenzia per la cybersicurezza nazionale (ACN) sul piano decisorio. La sua posizione istituzionale, seppur complessa e divisa tra apparati tecnici e di sicurezza (anche in senso tradizionale), è chiarissima[5]. Allo stesso tempo, le competenze non sono interamente attratte presso l'ente: la definizione di alcuni aspetti lascia impregiudicate le attività e le scelte delle singole amministrazioni. Essa svolge una funzione di sostanziale standardizzazione, di definizione di livelli comuni da interpretare quali soglie minime di rispetto. Il quadro d'insieme è com-

curezza nelle istituzioni, negli organi e negli organismi dell'Unione; Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, *relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013* ('regolamento sulla cibersicurezza'); Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, *sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011*.

3 Decreto-legge 14 giugno 2021, n. 82, recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, convertito, con modificazioni, nella legge 4 agosto 2021, n. 109, art. 7.

4 Si veda il *considerando* 3 del citato Regolamento n. 2841/2023: "gli ambienti tecnologici dei soggetti dell'Unione sono interdipendenti, utilizzano flussi di dati integrati e sono caratterizzati da una stretta collaborazione fra i loro utenti. Tale interconnessione significa che qualsiasi perturbazione, anche se inizialmente limitata a un solo soggetto dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata su altri soggetti dell'Unione" (con enfasi sugli aspetti di interconnessione e sulla interdipendenza reciproca, sia in casi fisiologici che patologici).

5 Sul rapporto tra funzione di sicurezza come parte centrale nella costruzione dello Stato e suo sviluppo in ambito informatico, si veda Ursi 2025.

plesso e piuttosto articolato, probabilmente anche a causa della 'giovane età' delle funzioni esercitate dall'agenzia.

Alcuni aspetti consentono di intuire il concreto modo di operare di questo sistema. Il primo è costituito dalle azioni comuni che, per disposizione normativa, sono dirette a realizzare gli ampi obiettivi affidati all'agenzia, in termini di sicurezza e resilienza (ancorate allo sviluppo della digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e, quindi, del "sistema" Paese).

Le azioni comuni integrano linee di indirizzo che dovranno essere seguite da parte di tutti i soggetti che, a vario titolo, partecipano al (e possono causare alterazioni nel) sistema della sicurezza cibernetica[6]. Ciò che desta interesse è che tali linee muovono da una certa altitudine, ma possono scendere di quota e diventare vere e proprie determinazioni concrete. Dallo schema normativo non traspare il punto di caduta: segno dell'ampio raggio che si può percorrere nel momento applicativo. Le azioni comuni, in questo senso, mostrano un assetto particolare all'interno del panorama decisorio settoriale: svelano l'esigenza di agire in modo coerente e non frammentato, richiedono il riconoscimento di un soggetto qualificato che possa contribuire all'unità, impongono il rispetto delle indicazioni (pena la frustrazione degli obiettivi e la comminazione di sanzioni)[7]. Il dato normativo è sintetico, ma dalla sua lettura scaturisce un evidente grado aumentato di articolazione. Il significato complessivo appare quello di conseguire un obiettivo di unità complessiva in modo calibrato, che non tralasci le singole istanze, ma realizzi un dosaggio composto di interventi[8].

Un altro esempio di oscillazioni si rinviene nella prassi amministrativa e nei documenti dell'Agenzia. All'interno dei *Key performance indicators* sono stabiliti gli obiettivi, indicati i metodi di attuazione, illustrati gli incontri istituzionali. Questa breve trilogia rivela una presenza forte dell'ACN dinanzi altre amministrazioni, chiamate a seguire le indicazioni della prima e a conformare – in via tendenziale – la propria attività, al fine di assicurare misure di contrasto ai rischi informatici[9].

In modo più pregnante opera, invece, l'attività di certificazione di componenti e prodotti, che possono entrare a far parte del patrimonio *hardware* delle amministrazioni solo se ritenute privi di pericolo insiti, vale a dire derivanti da modalità di costruzione, *backdoor*, assenza di falle, resistenza a eventuali attacchi malevoli. La certificazione agisce sul sistema degli appalti e consiste, per quanto qui di inte-

6 In altre parole, tutti i soggetti che utilizzano o erogano sistemi informativi e servizi informatici che possono avere un impatto rilevante sull'interesse nazionale.

7 Matassa 2025.

8 Si veda l'art. 7, comma 1, *lett. a)*, del d.l. n. 82 del 2021, in base al quale l'ACN "promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore".

9 Si veda il documento dell'ACN denominato *Manuale operativo. Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026*, del dicembre 2022, disponibile all'indirizzo https://www.acn.gov.it/portale/documents/20119/87708/ACN+Manuale+Operativo+implementazione+misura-82.pdf/ba48be5f-1e69-6b15-8fb9-2d48e52d0d74?t=1704460313679.

resse, nel livellamento delle decisioni su eventuali acquisti, anche in relazione alla possibile inclusione dei prodotti in listini stilati dalle centrali di committenza. In una dichiarazione del G7 le attività di certificazione sono state definite espressamente come uno dei perni del sistema-Paese[10].

Questa funzione, aderente al concetto di perimetro nazionale[11], si pone al confine tra funzione di collaborazione e controllo, tra sostegno e imposizione. La stessa struttura organizzativa, divisa tra centri e laboratori[12], rivela una tendenza all'uniformità, senza che però si comprima del tutto l'autonomia dei singoli centri decisionali. L'interesse nazionale, già richiamato, presidia i rapporti tra differenti strutture e li unisce idealmente.

Non può sottacersi, infine, la strategia nazionale per il *cloud computing*, che ha dato vita al Polo strategico nazionale (PSN), quale infrastruttura tecnologica ormai centrale nel settore pubblico, sulla quale la migrazione dei servizi delle amministrazioni sta crescendo in maniera esponenziale[13]. Una simile strategia mostra, infatti,

10 Il gruppo, si legge nel documento di maggio 2024, "ha discusso di come operare per favorire insieme agli operatori delle infrastrutture critiche la sicurezza dell'intera catena di approvvigionamento, per ridurre fortemente il rischio che componenti tecnologiche possano diventare veicolo per la diffusione di un attacco alle reti infrastrutturali. Un settore in cui è importante applicare il principio di security-by-design attraverso l'acquisizione di componenti che rispondano ad alti standard di sicurezza". Gli stati membri hanno affermato che "[c] oopereremo sempre meglio e ci consulteremo tutte le volte che ne avremo la necessità. Questo è l'impegno che abbiamo assunto insieme. Scambieremo informazioni sulle principali minacce cyber che riguardano le infrastrutture critiche, sugli incidenti, nonché sulle misure di sicurezza che possono essere adottate dagli operatori critici per farvi fronte. Crediamo tutti molto nel coordinamento con il settore privato. In questo senso la nostra Agenzia, forte dell'esperienza della Legge Perimetro ha una naturale propensione a sviluppare l'interazione con il mondo delle imprese e quello della ricerca".

11 Buoso 2025; consentendo il rimando, Carotti 2020.

12 In particolare, il Centro di valutazione e certificazione nazionale (CVCN) è stato istituito dal decreto-legge 21 settembre 2019, n. 105, recante recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, convertito, con modificazioni, nella legge 18 novembre 2019, n. 133. Si veda, in materia, anche il d.P.R. 5 febbraio 2021, n. 54, recante *Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*. Sui poteri dell'Agenzia in materia, si può fare riferimento all'art. 7, comma 1, *lett. e)*, d.l. n. 82 del 2021. Il CVCN, inizialmente istituito presso l'allora Ministero dello Sviluppo economico, è poi transitato nelle strutture dell'ACN; si coordina con i Centri di Valutazione (CV) istituiti presso i Ministeri della Difesa e dell'Interno e può avvalersi del supporto di una rete di Laboratori accreditati di prova (LAP), così realizzando un modello di collaborazione pubblico-privato. Si v. Previti 2024.

13 Come noto, si tratta di una infrastruttura informatica destinata a ospitare sistemi e servizi forniti dalla pubblica amministrazione mediante un *cloud* nazionale e centralizzato, che risponda alle maggiori garanzie di affidabilità, resilienza e indipendenza. Ricompreso tra le missioni del Piano nazionale di ripresa e resilienza (PNRR), quale obiettivo strategico di utilizzo alle tecnologie del *cloud computing*, il PSN ha visto la luce nel 2021, con la definizione del modello e l'affidamento a un partenariato che ne ha consentito la realizzazione effettiva. La vicenda è finita dinanzi agli organi di giustizia amministrativa: Consiglio di Stato, sez. V, 24 ottobre 2023, n. 9219, che ha determinato l'illegittimità della procedura di scelta, senza però poter determinare il subentro nel contratto, in ragione delle disposizioni sugli

una funzione di decisa preminenza dell'ACN, che vincola le scelte delle singole amministrazioni mediante un preventivo controllo. Rileva, da un lato, l'attività di qualificazione di dati e servizi della pubblica amministrazione (necessaria a comprenderne la natura e la portata, per poi poterne definire la destinazione e il livello di sicurezza all'interno del PSN), così come la qualificazione dei servizi in *cloud* offerti alle amministrazioni da parte di terzi (al fine di rivolgersi solo a soggetti qualificati e in grado di offrire idonee garanzie). Queste funzioni sono transitate dall'Agenzia per l'Italia digitale (AGID) all'ACN, ormai *pivot* del processo che, nel quadro della costruzione dell'infrastruttura nazionale, analizza e classifica i sistemi informatici delle singole amministrazioni. L'ACN condiziona amministrazioni e mercato, in quanto la qualificazione dei servizi offerti ha puntuali effetti sulle scelte delle singole istituzioni e sul novero dei soggetti abilitati a offrire determinati servizi in ambito pubblico[14].

L'ambito decisorio, in sintesi, determina effetti innegabili sulla sicurezza cibernetica. I relativi compiti sono diversi e articolati. Alcuni di essi spettano agli apparati centrali, altri sono lasciati alle singole istituzioni[15]. Il loro esercizio denota un assetto complessivo in costante movimento, nella ricerca di una soluzione ottimale, che non è statica e si rivela complessa e difficile da raggiungere.

4. La dicotomia funzionale

Un equilibrio oscillante, ancora incerto, e forse necessariamente destinato a rimanere tale, caratterizza l'esercizio delle funzioni in materia di cibersicurezza.

affidamenti operanti nel quadro del Pnrr (in particolare, l'art. 48, comma 4, del decreto-legge 31 maggio 2021, n. 77, recante *Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*, convertito, con modificazioni, con legge 29 luglio 2021, n. 108, che richiama l'art. 125 del *Codice del processo amministrativo*). Sul piano normativo, si veda, originariamente, l'art. 33-*septies* del decreto-legge 18 ottobre 2012, n. 179, recante *Ulteriori misure urgenti per la crescita del Paese*, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221. A ottobre 2024, la migrazione al PSN è stata effettuata da quattromila amministrazioni (fonte: https://www.polostrategiconazionale.it/media/stampa/comunicato-obiettivi-pnrr-2024-oltre-100-amministrazioni/).

14 Il regime di qualificazione dei servizi offerti alla pubblica amministrazione è ora definitivamente acquisito tra le competenze dell'ACN: da ultimo, si v. il regolamento adottato con decreto direttoriale 27 giugno 2024, n. 21007, in vigore dal 1° agosto 2024.

15 Rilevante, a questo riguardo, la proposta di legge attualmente in discussione presso la Regione Toscana, che nel quadro della ormai consolidata innovazione digitale, si occupa di sicurezza, intelligenza artificiale e tutela dei singoli, ricercando anche una migliore postura dei dispositivi utilizzati. La Regione ha introdotto anche un proprio CSIRT, quale ulteriore nodo di una complessa rete istituzionale. Si tratta della "*Proposta di Legge n. 272 – Modifica della deliberazione di Giunta regionale che ha approvato la proposta di legge n. 1/2024 (Disciplina dell'innovazione digitale nel territorio regionale e tutela dei diritti di cittadinanza digitale. Modifiche alla L.R. 54 del 2009)*", del 29 luglio 2024, approvata il successivo 27 novembre (https://iterlegis.consiglio.regione.toscana.it/#/atto/66b5cb6ad56f26046a7eff9f/).

In merito, rilevano tre aspetti: un primo ambito fa emergere lo scambio di informazioni e la cooperazione (termine conservato volutamente, sebbene l'ambito semantico, come si osserverà in chiusura, rinvia a un orizzonte concettuale noto, ma da tenere sotto osservazione); un secondo concerne la definizione di obiettivi comuni, che orientano l'esplicarsi delle funzioni stesse; un terzo riguarda la presenza e l'esercizio dei poteri unilaterali.

Innanzi tutto, l'impianto normativo, anche nei testi più recenti, conferma il ruolo centrale dello scambio di informazioni, vitale per la sicurezza informatica all'interno dell'Unione e degli Stati membri[16]. Si tratta di un riflesso della polimorfia istituzionale e dell'essere la sicurezza cibernetica una materia 'giovane'. Da un lato, infatti, la presenza di numerosi soggetti istituzionali impone di raccordarne le funzioni per assicurare, mediante l'apporto di ciascuno, un effetto su vasta scala; un metodo che appare preferibile rispetto a un'imposizione centralizzata. Dall'altro lato, poiché si richiedono ancora tempo ed esperienza per irrobustire gli ambienti informatici, appare maggiormente congeniale la condivisione del 'sapere' da parte dei soggetti con maggiori risorse; questo avviene, tipicamente, con il consolidamento di apparati centrali, ma il diffondersi di conoscenza e capacità potrà determinare un riequilibrio, assicurando la compartecipazione dei diversi nodi esistenti, in un complesso sistema reticolare fondato sullo scambio (sia biunivoco, sia multilaterale).

Questo duplice orientamento si nota anche nelle formule normative. La rete chiamata a risolvere gli incidenti informatici (*CSIRT Network*) deve informare le istituzioni preposte, attuare una "risposta coordinata" e assicurare agli Stati membri un'adeguata assistenza, qualora emerga una rilevanza transfrontaliera degli incidenti. Simili funzioni si traducono in forme morbide di coordinamento, in cui si sfrutta la presenza dei nodi della rete – presenti all'interno degli Stati membri – per conseguire una reazione più efficace, basata sull'apporto di ciascuno.

Specifici aspetti, peraltro, meritano attenzione. Ad esempio, sempre in riferimento alla rete degli CSIRT, il *considerando* n. 47 e l'art. 15 della direttiva NIS 2 recano il termine *cooperazione operativa*[17]. L'aggettivo utilizzato sembra far compiere un passo ulteriore rispetto alle attività condotte e sembra indicare l'obiettivo – stabilito in via legislativa – di rendere effettiva l'attività di scambio e collaborazione svolta tra amministrazioni interessate. Un passaggio che denota il superamento del mero aspetto formale o burocratico, per andare a toccare il mondo complesso

16 Si veda, in questo senso, il citato Regolamento n. 2023/2841, il cui *considerando* n. 4 ritiene "necessario che i soggetti dell'Unione raggiungano un livello comune elevato di cibersicurezza attraverso l'attuazione di misure di gestione dei rischi di cibersicurezza commisurate ai rischi per la cibersicurezza individuati, lo scambio di informazioni e la collaborazione". Questo aspetto è in perfetta continuità con il settore delle comunicazioni elettroniche, in cui peraltro affondano le radici dell'ENISA. Sulla collaborazione in questo settore, Carotti 2011.

17 *Considerando* n. 47: "[l]a rete di CSIRT dovrebbe continuare a contribuire al rafforzamento della fiducia e a promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri". La dizione si trova quindi ai paragrafi 1, 2, *lettere j*), *k)* e *p)*, e 4, dell'art. 15 citato nel testo.

dell'effettività[18]. Si è al confine della teoria della norma: non bastano più i caratteri formali, mentre occorre la produzione di effetti nel mondo reale, quasi secondo un avvicinamento alla dimensione extragiuridica. La concretezza dei sistemi informatici, del resto, richiede un approccio realistico.

La cooperazione, confermandosi essenziale, vede allargarsi il suo campo di applicazione, a testimonianza della orizzontalità necessaria in questo ambito e della "convivenza funzionale" tra le istituzioni poste in posizioni centrale e quelle laterali (competenti su ambiti territoriali definiti o su materie più ristrette), che si possono considerare come poste alla 'periferia' del sistema[19]. La necessità di una complessiva convivenza delle funzioni nei vari ambiti, mediante un raccordo, testimonia la tensione tra la ricerca di orientamenti uniformi e la conservazione di margini di apprezzamento da delle singole amministrazioni. Un vero e proprio coacervo, che mostra la difficoltà di ricondurre a sistema un ambito di per sé molto complesso, ancora non idoneo a esprimere una sostanziale unità, nemmeno sotto il profilo funzionale.

Questo assetto risponde, in ogni caso, all'unitarietà di interessi e obiettivi sottesi alla normativa. Un unitario interesse di fondo, collegato a una dimensione non solo nazionale, ma europea permea la cooperazione e lo scambio di informazioni. Emerge, al riguardo, una tenenza ben precisa, che cerca di superare la difficoltà di compiti già affidati a soggetti esistenti e, senza comprimerli o eliminarli, li riconduce a una dimensione unitaria. Ciò avviene – è il secondo aspetto annunciato in apertura – mediante la definizione di obiettivi, livelli e soglie di protezione comuni, la cui assicurazione condiziona le forme di "collegamento" tra istituzioni, centri e relative articolazioni. La dinamica del sistema è instabile e produce formule sperimentali: ad esempio, il gruppo di collaborazione istituito in ambito europeo ha, tra gli altri, l'obiettivo di esaminare le attività dei singoli componenti in ordine alle misure di gestione e di segnalazione dei rischi, secondo un metodo di verifica che si svolge tra pari[20].

Infine, con riferimento ai poteri unilaterali, dalla relazione annuale dell'Agenzia[21] emergono attività diverse, dal supporto nell'esercizio di compiti tecnici all'accesso ai locali, secondo un quadro complessivo di attuazione concentrata nelle

18 Falzea 1965.

19 Si veda l'art. 13, par. 4, della Direttiva NIS 2: "[a]l fine di garantire l'efficace adempimento dei compiti e degli obblighi delle autorità competenti, dei punti di contatto unici e dei CSIRT, gli Stati membri, nella misura del possibile, provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra i suddetti organismi e le autorità di contrasto, le autorità di protezione dei dati, le autorità nazionali ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139, gli organismi di vigilanza a norma del regolamento (UE) n. 910/2014, le autorità competenti a norma del regolamento (UE) 2022/2554, le autorità nazionali di regolamentazione a norma della direttiva (UE) 2018/1972, le autorità competenti a norma della direttiva (UE) 2022/2557, nonché le autorità competenti ai sensi di altri atti giuridici settoriali dell'Unione".

20 Si tratta del "gruppo di cooperazione" di cui all'art. 14 della Direttiva NIS 2, il quale, in base all'art. 19, par. 2, svolge la revisione tra pari del gruppo assicurando, tra le altre cose, "il livello di attuazione delle misure di gestione e delle prescrizioni in materia di segnalazione dei rischi di cibersicurezza […]"; dunque, è in grado di incidere piuttosto a fondo sulle singole istituzioni, raccordandole agli obiettivi unitari e al centro costituito per la loro cura.

21 Relazione annuale per l'anno 2023 presentata dall'ACN, disponibile su https://www.acn.gov.it/portale/documents/20119/446882/ACN_Relazione_2023.pdf.

mani dell'ente centrale, sempre più perno del sistema, ma pronto ad aprirsi alla voce e alla collaborazione di quelli periferici.

5. La dicotomia organizzativa

Esiste un'uniformità organizzativa in materia? Vi è una distinzione tra centro e periferia?

L'impianto organizzativo, che costituisce una ricaduta di quello funzionale[22], testimonia una chiara tendenza alla centralizzazione (come emerge dalla presenza necessaria dell'ACN, dalla sua funzione di raccordo con gli altri soggetti dell'Unione europea, dalla sua preminenza nell'assicurare il più volte richiamato interesse nazionale)[23]. L'innegabile tendenza all'unità non implica una sovra-ordinazione gerarchica, ma un esercizio di funzioni in modo accentrato. È qui che risiede la terza dicotomia che, insieme alle altre due, svela la tensione latente dell'intero impianto.

Secondo il dettato normativo, l'ACN promuove competenze, risponde a crisi, definisce livelli comuni e standard di protezione, creando un minimo comun denominatore che opera anche per i soggetti privati: non si determina, però, un'integrazione strutturale. In ambito organizzativo, infatti, si osservano due fenomeni: la fuga dalla sovra-ordinazione gerarchica e la rispondenza delle strutture a soglie di protezione comuni e ai controlli conseguenti.

Evidente, in merito, quanto avviene all'interno dell'Unione europea. Si prenda il caso del Comitato interistituzionale per la cibersicurezza (*Interinstitutional Cybersecurity Board* – IICB), che attraverso i rappresentanti istituzionali si inscrive all'interno della rete delle agenzie dell'Unione europea (*EU Agencies Network* – EUAN)[24]. Esso assicura l'attuazione delle disposizioni e l'osservanza degli indirizzi impartiti da parte dei "soggetti dell'Unione"[25]; svolge funzioni di monitoraggio e

22 Nigro 1967; Giannini 1993.

23 Si v. l'art. 7, comma 1, *lettera d*), d.l. n. 82 del 2021, ai sensi del quale l'ACN è "l'autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento". La disposizione si può leggere in coordinamento con l'art. 8, par. 4, della direttiva NIS 2, in base al quale "[o]gni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonchéé per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro". Da notare che, ai sensi del successivo art. 9, par. 2, laddove "uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche ai sensi del paragrafo 1, esso indica chiaramente quale di tali autorità deve fungere da coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala".

24 Ai sensi dell'articolo 10, paragrafo 3, del Regolamento, siedono all'interno l'IICB rappresentanti designati da diversi soggetti dell'Unione europea (dal Parlamento alla Corte di giustizia, dal Comitato economico e sociale al Garante europeo per la protezione dei dati, per un totale di diciotto rappresentanti).

25 Art. 12, par. 1, Regolamento n. 2023/1248: "controlla efficacemente che i soggetti dell'Unione attuino il presente regolamento e gli indirizzi, le raccomandazioni e gli inviti a intervenire da loro adottati".

verifica, intervenendo in caso di mancata rispondenza agli atti adottati in base al nuovo quadro normativo, secondo un sistema di risposte 'in progressione' (che possono arrivare al distacco dei sistemi di comunicazione da parte dei soggetti che non mitigano il rischio e mettono in pericolo gli altri, nonché a segnalazioni volte a verificare il corretto uso delle risorse finanziarie messe a disposizione in caso di inosservanza)[26].

L'IICB opera "al fine di contribuire all'instaurarsi di un livello comune elevato di cibersicurezza tra i soggetti dell'Unione". L'espressione "livello comune" suscita interesse: lascia intendere che il comitato fissa condizioni minime di protezione, rimettendo la scelta delle singole misure – e la loro profondità – ai centri decisionali coinvolti. Gli aspetti organizzativi non sono estranei allo svolgimento di tali compiti: sono necessari a perfezionare e a rendere possibile questo *modus operandi*, così come il controllo "tra pari" circa l'adeguatezza delle scelte[27]. Al posto di un'organizzazione uniformata (e uniformante) si perseguono forme più labili e indefinite. Queste ultime consentono di raggiungere un'unità di intenti senza l'irrigidimento di un'organizzazione centrale o relazioni gerarchiche.

Va aggiunto che, mentre in ambito nazionale l'interesse è unidirezionale, in quello europeo si rispetta l'autonomia degli Stati: al fondo, permane l'idea di un rapporto dialettico tra i singoli nodi della rete, dislocati negli ordinamenti nazionali. L'ordinamento europeo raccorda le diverse strutture, senza comprimerle[28]. La tecnica utilizzata è, dunque, quella di 'centralizzare uniformando', con la conseguenza di incidere solo su alcuni aspetti, lasciandone aperti altri: una tendenza calibrata all'unità, 'senza esagerare', che potrebbe definirsi 'centralizzazione gentile'[29].

È qui che, come si vedrà a breve, si innesta l'importanza del coordinamento: una conseguenza logica, che si incastona all'interno del disegno complessivo, e che è destinato a divenire un perno dei rapporti tra strutture (oltre a consentire una prima riconduzione a categorie generali).

26 Art. 12, par. 1, *lett. f)*, Direttiva NIS 2.

27 Ai sensi dell'art. 11, par. 1, *lett. d)*, reg. n. 2023/2847, il comitato "stabilisce la metodologia e gli aspetti organizzativi per lo svolgimento di riesami *inter pares* volontari da parte di soggetti dell'Unione".

28 Questo vale anche sul piano funzionale: si consideri l'art. 9 par. 4, della Direttiva NIS 2, rubricato "*Incidenti e crisi su vasta scala*", in base al quale sono definite dallo Stato "le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale generale di gestione delle crisi e i canali di scambio di informazioni". In una sola disposizione emerge una progressiva integrazione, attraverso le attività delle amministrazioni dei singoli stati che confluiscono in un alveo comune sul piano funzionale, mentre dell'osservanza del tessuto normativo rispondono anche gli Stati, con un gioco di equilibri che spinge al rispetto del quadro adottato.

29 Si veda, da questo punto di vista, l'art. 32 della direttiva NIS 2, rubricato "*Misure di vigilanza e di esecuzione relative a soggetti essenziali*". Gli Stati membri provvedono affinché "le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso" (ai sensi del par. 1) e "le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporrei" i soggetti interessati "come minimo" a ispezioni, *audit*, scansioni, ecc. (in base al par. 2).

In modo connesso, emerge *a latere* il rapporto tra centro e periferia: inteso in modo non formalistico, esso si manifesta *in nuce*, con gradi di intensità non assoluti. Questo aspetto sembra rispondere a una diversa sfida, di natura politica ed economica, più che giuridica: concerne l'assetto generale, per ora incontrastato, dell'oligopolio tecnico operante su scala internazionale, caratterizzato dalla concentrazione in poche mani dell'uniformità delle tecnologie e dei processi di raccolta dei dati[30]. Il rafforzamento delle strutture e l'unione delle loro forze, in un insieme diversificato ma coerente, sono il modo per fronteggiare in modo unitario le capacità di soggetti che hanno acquisito un potere enorme e ancora incontrastato, al fine di mitigare gli effetti sfavorevoli o nocivi dello stato attuale dell'informatica e dei suoi rapporti con il potere. I poteri tecnici si accompagnano necessariamente al potere politico, che li usa a proprio vantaggio a diversi fini: dalla politica interna a quella estera. Un maggiore rafforzamento delle 'periferie' statali in un quadro unitario sembra orientata, dunque, a creare e contrapporre una propria voce a potenze economiche dominanti. Resta aperto il problema di quanto sia possibile fare contro gli stessi poteri pubblici, come i governi che usano gli apparati tecnologici per fini non compatibili con un assetto democratico. Una risposta adeguata ed efficace appare, a oggi, ancora inevasa[31].

6. Possibili ricostruzioni

Dalla pur breve disamina effettuata, in cui si è cercato di cogliere indizi e tratti generali, si affaccia l'accennata tensione tra le esigenze di uniformità e autonomia. La ricerca di soluzioni comuni e unitarie è funzionale a garantire una postura di maggiore sicurezza di fronte a scenari critici; l'ambito riservato all'autonomia è necessario a fronte della impossibilità di esercitare le competenze in modo univoco, per tutti i soggetti coinvolti. Questa tensione non è risolta in modo rigido, ma elastico. Salve future evoluzioni, che dipendono anche dallo scenario internazionale – cui la sicurezza cibernetica è intrinsecamente connessa – questo assetto è destinato a perdurare in un mutevole e delicato equilibrio.

Le dinamiche sottese, pur movimentate, consentono di delineare alcuni aspetti ricostruttivi.

Innanzi tutto, è in corso una ridefinizione dei poteri decisori di maggior impatto sulla sicurezza cibernetica a parziale vantaggio del centro. Questa tendenza è, allo stato, prevalente e la forza centripeta aumenta di intensità: da un lato, gli enti centrali dello Stato (l'ACN) e dell'Unione si stanno consolidando; dall'altro lato, l'elasticità non scompare affatto, e limita l'attrazione della componente decisoria. Quest'ultima non si presenta ancora a tutto tondo, ossia in grado di com-

30 Su tutti, Wu 2020.

31 Il caso della Corte costituzionale romena, che ha annullato le recenti elezioni presidenziali, ne costituisce un esempio lampante. Primi riferimenti possono essere trovati in questo commento di Selejen-Gutan 2024. La sentenza è comunque oggetto di diverse e contrastanti letture.

prendere ogni aspetto connesso alla sicurezza cibernetica: tuttavia alcuni profili, connessi alla definizione di livelli minimi di tutela e degli obiettivi da perseguire, sono attratti al centro (è quanto avviene con la certificazione). Il fine è quello di assicurare una maggiore uniformità, a sua volta funzionale ad aumentare l'efficacia della protezione.

In secondo luogo, il piano funzionale denota un'oscillazione tra uniformità e autonomia più evidente: le funzioni presentano un maggior tasso di distribuzione; il consolidamento avviene senza elidere la componente pluralistica, ma riconoscendo l'apporto di tutti i soggetti competenti. Le istanze unitarie, quindi, sono limitate al raggiungimento di una coerenza complessiva.

In terzo luogo, il piano organizzativo mostra una tendenza biunivoca ancor più bilanciata. La centralizzazione si nota in figure istituzionali di carattere forte, come l'ACN. I centri organizzativi di raccordo, di converso, assumono una forma ibrida, fungendo da snodo per interessi non solo periferici, ma anche centrali, mettendo in comunicazione istanze nazionali e sovranazionali (come avviene con gli apparati preposti alla sicurezza interna ed esterna).

Queste tre dicotomie, che possono orientare la lettura della disciplina della cibersicurezza, spingono a interrogarsi sulle categorie generali: non intravedendosi terre sconosciute – o rare, per restare nel mondo della tecnologia – è comunque possibile ravvivarne l'interpretazione e attualizzarle. Le categorie utilizzabili si stagliano attorno a due picchi: il coordinamento e l'autonomia funzionale.

Il primo, come noto, delinea un *modus agendi* idoneo a collegare soggetti privi di una relazione gerarchica, al fine di assicurare l'uniformità dell'attività. Storicamente, sia nella prassi amministrativa che nella ricostruzione della letteratura, il coordinamento si consolida nel momento in cui viene superato l'assetto monista degli interessi e, dunque, con l'affermarsi dello Stato pluriclasse; mostra, quindi, una sostanziale variazione nell'esercizio delle funzioni, mutando le modalità del momento decisorio[32]. La coesistenza di vari interessi, l'assenza di sovra-ordinazione (quantomeno parziale), la necessità di ascoltare più voci lo hanno reso un cardine nella ricostruzione delle forme di esercizio dell'attività amministrativa; rivela la ricerca di una forma sostanziale di collegamento, che preservi le prerogative dei singoli soggetti istituzionali e apra un metodo aperto, salvaguardando al tempo stesso pluralità, unitarietà e autonomi[33], secondo lo spirito repubblicano che promana dalla Costituzione[34]. Questi caratteri distinguono il coordinamento, pur con sfumature notevoli[35], sia dalla collaborazione, che opera sotto il diverso profilo dell'articolazione gerarchica degli interessi tutelati, sia dalla cooperazione che, invece, agisce a livello europeo.

Il coordinamento, dal solo versante organizzativo, è divenuto uno strumento funzionale. In questa accezione, integra una modalità di raccordo coerente con la realtà in costante evoluzione della sicurezza cibernetica, secondo un orizzonte

32 Bachelet 1957; Orlando 1974; Giannini 1958.
33 In merito alla difficile coesistenza tra autonomia e spinte unitarie, Police 2024: 24.
34 Antonelli, De Martin, Mattarella 2024, D'Angelo 2022.
35 Morana 2024.

concettuale aperto a innovazioni, adattamenti e commistioni. Proprio in quest'ottica non può sottacersi il ruolo dell'interesse nazionale, più volte ricordato, che produce una rottura nella linearità complessiva del coordinamento, riportando in auge elementi che, in precedenza, potevano apparire superati. Ne consegue quella "*sovrana incertezza*"[36] che lo caratterizza e che ne fa ripensare, ancora oggi, la figura: di fronte alla compresenza di più interessi, l'interesse nazionale sembra in grado di spostare l'assetto in essere, modificandone il fuoco e l'ellissi. Non si assiste a un cambio radicale della figura del coordinamento, ma a una sua rilettura, in accordo con la tendenza centralizzatrice di funzioni e strutture.

È di ausilio, a tal fine, considerare sia che il coordinamento esprime una idea di "crisi" (termine tutt'altro che indifferente al settore in esame!)[37], sia che i suoi contorni sono sfumati e privi di coerenza e razionalità granitica. Interstizi e margini di intervento sono utili, del resto, a contrastare eventuali '*moloch*', evitando (o cercando di evitare) contrasti con la protezione di interessi, valori e diritti fondamentali, essenziali alla tenuta di uno stato democratico. Può ricordarsi, in merito, che, "il 'coordinare' è in certo senso manifestazione tipica di una società democratica e pluralistica, che intende ottenere l'armonico orientamento di individui, gruppi, istituzioni verso fini determinati, senza però annullare la libertà o l'iniziativa di tali individui, gruppi o istituzioni"[38].

Dunque, la ricerca di una clausola di salvaguardia, o di una valvola di sfogo, è ancora viva: e questo anche in un contesto, come quello attuale, in cui l'autoritatività sembra prendere il sopravvento, o quantomeno proporsi in modo sbilanciato[39]. È da richiamare, allora, quanto affermato in altri contesti e momenti, ricercando anche nel settore della sicurezza cibernetica un "coordinamento non unilaterale e gerarchico, ma condiviso"[40]; solo esso, infatti, "tende a garantire contemporaneamente la autonomia dei singoli organismi coordinati e insieme la possibilità di un loro indirizzo unitario a determinati fini comuni"[41].

Il ragionamento, probabilmente, va effettuato in termini meno deontici e maggiormente orientato alla sua dimensione effettiva, vale a dire all'effetto che è in grado di produrre[42]. Il cambio del *modus agendi* cerca di orientare l'attività a un determinato obiettivo, forzandola; non devono essere consentiti, però, strappi irreparabili, o stravolgimenti senza rimedio dell'assetto esistente. È l'effetto concreto

36 Cortese 2012.
37 Berti 1982: 31.
38 Bachelet 1962. Sull'incidenza delle attività di cibersicurezza sui diritti, Manjikian 2023.
39 Rossa 2023.
40 Così Merloni 2008: 22. Questo il passo complessivo, analizzato in un contesto istituzionale molto differente, che pur indica somiglianze e punti di continuità: "[u]n definitivo assetto dell'attuale soggetto statale, il CNIPA, potrebbe essere trovato in una amministrazione, con forti tratti di autonomia organizzativa e di indipendenza dei componenti degli organi, largamente partecipata dalle diverse amministrazioni; un'amministrazione di livello nazionale, ma "repubblicana" (rappresentativa dei soggetti costituenti la Repubblica, secondo l'art. 114 Cost.) che contribuisce a un coordinamento non unilaterale e gerarchico, ma condiviso".
41 Bachelet 1962.
42 Cassese 1982: 20.

e la dimensione del reale a contare, e non la ricostruzione idealistica dell'istituto. Una prospettiva che si accorda perfettamente, come anticipato, alla natura decisamente concreta dell'informatica.

Vi è un altro orizzonte concettuale che sembra rispondere alle dinamiche profonde dell'assetto istituzionale di settore: quello dell'autonomia funzionale. L'autonomia deve essere intesa come categoria aperta e, dunque, rispondente a un ordine concettuale magmatico. Non è limitata alla sola capacità di porre regole, ma di decidere e agire secondo criteri non unitari[43], ricercando un equilibrio tra i soggetti che permeano il settore e che già dispongono di competenze consolidate.

Questa forma elastica non consegue allo sfaldamento dello stato unitario, cui l'autonomia è tradizionalmente collegata[44]: il sistema in costruzione, anzi, lo presuppone, per tutelare meglio l'interesse nazionale a esso connaturato (che è l'interesse e da cui si sono prese le mosse in questo scritto). La formula sembra paradossalmente assicurare, dunque, la convivenza di tendenze unitarie e pluralistiche, preservando margini di autonomia. L'autonomia funzionale va ricondotta, in questo senso, al *modus operandi* delle amministrazioni, riconoscendo un *agere* specifico che mira agli obiettivi stabiliti senza implicare un modello organizzativo definito. Si è a metà del guado, con la riva del modello istituzionale ancora da raggiungere.

Nell'insieme, non vi sono risposte certe. Anche il dato normativo non è univoco e sul piano terminologico si nota un utilizzo non sempre coerente, in cui vengono affiancati tecniche e concetti in modo non perfettamente lineare. Soprattutto in ambito dell'Unione europea, i riferimenti a forme di coordinamento, cooperazione e collaborazione non sono ben distinti**.** Il piano semantico non sembra rispondere a un ordine concettuale granitico. Probabilmente anche il tessuto normativo riflette la difficoltà di consolidare uno stato magmatico come quello in cui si trova il settore in esame, dove anche le istituzioni devono ancora assestarsi.

A questo stato si collega un elemento ulteriore di valutazione: un diffuso grado di informalità, che sfrutta le pieghe di una costruzione realizzata per tappe per consentire la convivenza delle istanze autonome con il centro. L'informalità costituisce un collante, in grado di avvicinare i diversi soggetti coinvolti, nel tentativo di ricondurli a unità ed evitare conflitti o contraddizioni. Leggendola a fondo, essa rappresenta un sostrato su cui costruire, in un secondo momento, uno strato più solido di uniformità: i legami teleologici si formano con la prima, proiettandola verso la seconda.

43 Va prestata attenzione poi agli ambiti semantici (che, in tempi di LLM, sono attualissimi): l'autonomia, infatti, è una risposta specifica in ambito internazionale e geopolitico, viene usata e declinata come autonomia tecnologica – in alcuni casi contrapponendosi al concetto di sovranità digitale: Cerra e Crespi 2021. In altri casi richiama il tentativo (per ora ancora tale e piuttosto indefinito) di avvicinarsi a concetti filosofici e ontologici, come avviene con l'uso della dizione "autonomia dell'uomo" contenuta art. 3, par. 2, del disegno di legge governativo in materia di intelligenza artificiale.

44 Merloni 1990.

Non si può prescindere, infine, dalla componente politica. Questo elemento chiude il discorso in modo circolare e ricorsivo. La politica fonda l'ordinamento settoriale della sicurezza cibernetica e appare in costante ascesa: indica la presenza di interessi latenti, primari e coessenziali alla vita stessa dello Stato. Anche limitandosi a osservare la direttiva NIS 2[45], simili interessi si riflettono in modo evidente e convergono verso un punto specifico: la dimensione diplomatica, tipica espressione della compagine statale. Le forme di cooperazione già esistenti vengono qui cristallizzate in uno schema istituzionale dai contorni più precisi, funzionale all'intero disegno della sicurezza cibernetica. È una dimensione che sfugge sia alla tecnica, sia alle funzioni regolatorie e di controllo[46]. La latenza di questo genere di interessi rappresenta una chiave di volta del settore, e ne consente la lettura profonda.

7. Conclusioni

Il settore della sicurezza cibernetica è in costante movimento e in cerca della propria identità. Di questo percorso risentono le istituzioni che lo governano. I tratti sono labili e i confini mutevoli: il tempo consoliderà l'assetto in essere, raffredderà le tensioni e lasciando un precipitato maggiormente visibile. Come si è avuto modo di osservare, è possibile riconoscere qualche carattere generale, ricondursi ad attività storicamente consolidate, tentare un primo approccio di massima. Qualche considerazione generale, in questo senso, può essere tratteggiata, ma non completata.

Nell'insieme, la dimensione normativa e istituzionale cammina di fianco a quella tecnica. Lo si osserva nel caso problematico degli attacchi *zero-days* – ossia di vulnerabilità sconosciute, per le quali non si dispone di un rimedio. Essi costituiscono una base conoscitiva di grande spessore: questi attacchi nascono da vulnerabilità conosciute e taciute per esigenze strategiche. Il problema posto alla loro base, dunque, non concerne tanto la tecnica, ma la loro genesi: un *a priori* composto da esigenze politiche e istituzionali crea una sinergia rischiosa, che può rivelarsi anche controproducente, ritorcendosi contro le esigenze di difesa cui si anela[47].

Svelare e comprendere determinate logiche può contribuire a un rafforzamento complessivo del mondo digitale, ripartendo dalle basi: forse occorre tornare a un 'grado zero della sicurezza' volto al ripensamento delle infrastrutture e alla riscrit-

45 Art. 16, par. 3, *lett. d*), direttiva NIS 2, che prescrive di coordinare la gestione degli incidenti e delle crisi di cibersicurezza su vasta scala e "sostenere il processo decisionale a livello politico" in ordine a questi eventi.

46 Nella direttiva NIS 2, viene affermato al *considerando* n. 71 che "EU-CyCLONe dovrebbe fungere da intermediario tra il livello tecnico e politico durante gli incidenti e le crisi di cibersicurezza su vasta scala e dovrebbe rafforzare la cooperazione a livello operativo e sostenere il processo decisionale a livello politico. In cooperazione con la Commissione, tenuto conto della competenza di quest'ultima nel settore della gestione delle crisi, EU-CyCLONe dovrebbe basarsi sui risultati della rete di CSIRT e utilizzare le proprie capacità per elaborare analisi d'impatto di incidenti e crisi di cibersicurezza su vasta scala".

47 N. Pelroth 2021.

tura delle tecnologie da cui oggi dipendiamo. Si tratta di un tema più generale, a cui si può solo accennarsi: va affrontata in modo sistematico la debolezza di alcuni dei protocolli maggiormente utilizzati, a partire da quelli su cui poggia l'infrastruttura tecnologica dominante, ossia *Internet*. Le vulnerabilità che ne sono alla base indicano momenti primordiali, falle emerse o facilmente prevedibili, cui sarebbe necessario ovviare. La futura sicurezza cibernetica dovrebbe partire da un assunto diverso e ben scandito: la protezione dei singoli individui, e non solo quella degli apparati o dei soggetti con maggiori capacità tecniche e peso economico[48].

È muovendo da queste conoscenze, imprescindibili per capire a fondo il settore, che si potrà rifondare un sostrato giuridico e istituzionale in grado di assolvere al proprio compito: per proteggere la persona e favorirne lo sviluppo, anche in un mondo complesso gli Stati devono dialogare nei consessi internazionali, assolvendo al primario compito di ricercare il bene comune, correggendo le distonie che generano l'attuale situazione di crisi dei diritti e, per quanto di interesse in questo scritto, di 'insicurezza informatica'.

Bibliografia

Antonelli V., De Martin G.C., Mattarella B.G. (a cura di) 2024, *Il coordinamento amministrativo dopo Vittorio Bachelet*, Roma: Luiss University Press.

Bachelet V. 1957, *L'attività di coordinamento nell'amministrazione pubblica dell'economica*, Milano: Giuffrè.

Bachelet V. 1962, "Coordinamento", in *Enciclopedia del diritto*, Milano: Giuffrè, X, *ad vocem*.

Berti G. 1982, "Il coordinamento: parola-simbolo tra gerarchia ed equiordinazione", in Amato G., Marongiu G. (a cura di), *L'amministrazione nella società complessa. In ricordo di Vittorio Bachelet*, Bologna: Il Mulino: 31.

Buoso E., 2025, "Ritorno al futuro: il perimetro di cybersicurezza nazionale", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 33 ss.

Carotti B. 2011, *La collaborazione tra autorità europee delle telecomunicazioni*, London: EPLO.

Carotti B. 2020, "Sicurezza cibernetica e Stato-Nazione", in *Giornale di diritto amministrativo:* 629-641.

Cassese S. 1982, "Il coordinamento prima e dopo Bachelet", in Amato G., Marongiu G. (a cura di), *L'amministrazione nella società complessa. In ricordo di Vittorio Bachelet*, Bologna: Il Mulino: 20.

Cerra R., Crespi F. 2021, *Sovranità tecnologica*, Roma: Centro per l'economia digitale (CED), 50.

Cortese F. 2012, *Il coordinamento amministrativo. Dinamiche e interpretazioni*, Milano: Franco Angeli, 5 ss.

48 Egloff 2022; Ishikawa, Yarik 2023.

D'Alberti, M. 1982, "Coordinamento amministrativo: immagini per la ricerca di un concetto", in Amato G., Marongiu G. (a cura di), *L'amministrazione nella società complessa. In ricordo di Vittorio Bachelet*, Bologna: Il Mulino: 55-64.

D'Angelo F. 2022, *Pluralismo degli enti pubblici e collaborazione procedimentale. Per una rilettura delle relazioni organizzative nell'amministrazione complessa*, Torino: Giappichelli.

Egloff F.J. 2022, *Semi-State Actors in Cybersecurity,* New York: Oxford University Press.

Falzea A. 1965, "Efficacia giuridica", in *Enciclopedia del diritto*, Milano: Giuffrè, Vol. XIV.

Giannini M.S., 1958, "Il decentramento nel sistema amministrativo", in AA. VV., *Problemi della pubblica amministrazione*, Vol. I, Ciclo di conferenze promosso dalla Scuola nell'anno accademico 1956-57, Bologna: Zanichelli.

Giannini M.S. 1993, *Diritto amministrativo*, Milano: Giuffrè, Voll. I-II.

Ishikawa T., Yarik K. (eds.) 2023, *Public and Private Governance of Cybersecurity: Challenges and Potential*, Cambridge: Cambridge University Press.

Orlando L. 1974, *Contributo allo studio del coordinamento amministrativo*, Milano: Giuffrè.

Manjikian M. 2023, *Cybersecurity Ethics: An Introduction*, Abingdon, Oxon: Routeldge, Taylor & Francis Group.

Matassa M. 2025, "Sicurezza cibernetica e nazionale nell'ordinamento multilivello: quale possibile convivenza?", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 75 ss.

Merloni F. 1990, *Autonomie e libertà nel sistema della ricerca scientifica*, Milano: Giuffrè.

Merloni F. 2008, "Coordinamento e governo dei dati nel pluralismo amministrativo", in Ponti B. (a cura di), *Il regime dei dati pubblici*, Rimini: Maggioli: 1-25.

Morana D. 2024, "Il coordinamento nella trama costituzionale: spunti di riflessione", in Antonelli V., De Martin G.C., Mattarella B.G. (a cura di), 2024, *Il coordinamento amministrativo dopo Vittorio Bachelet*, Roma: Luiss University Press.

Nigro M. 1966, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano: Giuffrè.

Pelroth N. 2021, *This Is How They Tell Me the World Ends. The Cyber Weapons Arms Race*, New York: Bloomsbury Publishing**.**

Police A. 2024, "La nozione di coordinamento nell'amministrazione dell'Unione europea e dei suoi Stati membri: una nuova declinazione della lezione di Vittorio Bachelet", in Antonelli V., De Martin G.C., Mattarella B.G. (a cura di), *Il coordinamento amministrativo dopo Vittorio Bachelet*, Roma: Luiss University Press, 24 ss.

Previti L. 2025, "Convergenze e deviazioni in materia di cybersicurezza: implicazioni sistematiche e nuovi interrogativi", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 109 ss.

Rossa S. 2023, *Cybersecurity e pubblica amministrazione*, Napoli: Editoriale Scientifica.

Selejen-Gutan B. 2024, "The Second Round that Wasn't. Why The Romanian Constitutional Court Annulled the Presidential Elections", in *Verfassungsblog*, 7 dicembre (https://verfassungsblog.de/the-second-round-that-wasnt/).

Ursi R. 2025, "Introduzione. La sicurezza cibernetica come funzione pubblica", in Heritier P., Rossa S. (a cura di), *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, II, *Teoria e Critica della Regolazione Sociale*, n. 1/2025, Milano: Mimesis: 7 ss.

Wu T. 2020, *The Curse of Bigness. Antitrust in the New Gilded Age*, New York: Penguin.

Alessandra Galassi

Cybersecurity risks of GIS technology for smart communities. A case study

Abstract: Digital Transformation (DT) is changing the city-citizen relationship, pushing to rethink urban development models to make them consistent with new socio-economic needs, particularly related to land livability and social inclusion. This article aims to provide an overview of digital security issues related to Geographical Information Systems (GIS) useful for rethinking cities in smart terms. In this specific case, a special Public Administration (PA) called the Special Office for the Reconstruction of the Municipalities of the Seismic Crater (USRC) adopts GIS as a tool to support its efforts in post-earthquake reconstruction by creating attractive smart communities. Briefly, the objective is to explore the cybersecurity aspects of GIS and how these should be considered as part of risk management, vulnerabilities of GIS related to information security, and suggest recommendations. The synergy of GIS with other technologies is also discussed, reflecting how technological innovation has pros and cons for an organization.

Keywords: GIS, Cybersecurity, Smart Communities, Information Security, Innovation Technology.

1. Introduction

Putting the welfare of citizens at the forefront by adopting a people-centered approach is a key objective for the European Union and has gained prominence on the social policy agenda over the past decade. It is necessary to rethink cities, including small towns, redesigning services and sub-services with a sustainable approach by combining competitiveness and conservation strategies. Cities-and likewise small towns-can become hubs of resources, investment, and innovation, and from their digitization can pass that of the whole of Italy, which to date does not have an adequate digital culture as mercilessly photographed by the European Commission's Digital Economy and Society Index (DESI)[1].

1 https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760147

Security is the basis for the decisions of any PA, big or small or special as in this case. And Information Security (InfoSec) becomes an essential aspect of any digital initiative. The application of Information and Communication Technologies (ICT) is not accidental but responds to a strategic design that starts from the specific needs of the context.

Here the focus is on the experience of the USRC mission structure of the Presidency of the Council of Ministers, created ad hoc by Law 134/2012[2], established to coordinate the process of reconstruction (of residential/non-residential buildings) and development of the 56 municipalities located in the so-called "seismic crater" hit by the April 6, 2009 earthquake that struck the Abruzzo Region (Italy), and in particular the city of L'Aquila and its province (see Figure 1) (Fico et al., 2017). The reconstruction is scheduled for completion in 2026. The seismic event had devastating consequences (more than 300 people killed), causing widespread damage to infrastructure, displacement of populations and disruption of essential services. Fifteen years later in the aftermath of this natural calamity, trying to look on the bright side, the area has proposed itself as an open space lab and scientific initiatives have blossomed such as INCIPICT project[3], which envisions the implementation of an experimental optical network to build a Metropolitan Area Network consisting in an Optical Ring to connect the main and the most important sites of L'Aquila city; "SICURA – House of Emerging Technologies"[4] as a technology transfer center to support businesses funded by Ministry of Enterprises and Made in Italy; VITALITY Foundation[5], an ecosystem of Innovation, Digitization and Sustainability for the diffuse economy of Central Italy involving universities, research institutions and private entities from Abruzzo, Marche and Umbria Regions.

2 Legge 7 agosto 2012, n. 134, *Conversione in legge, con modificazioni, del decreto legge 22 giugno 2012, n. 83, recante misure urgenti per la crescita del Paese.*

3 http://incipict.univaq.it/.

4 http://www.ctesicuralaquila.it.

5 https://fondazionevitality.it/.

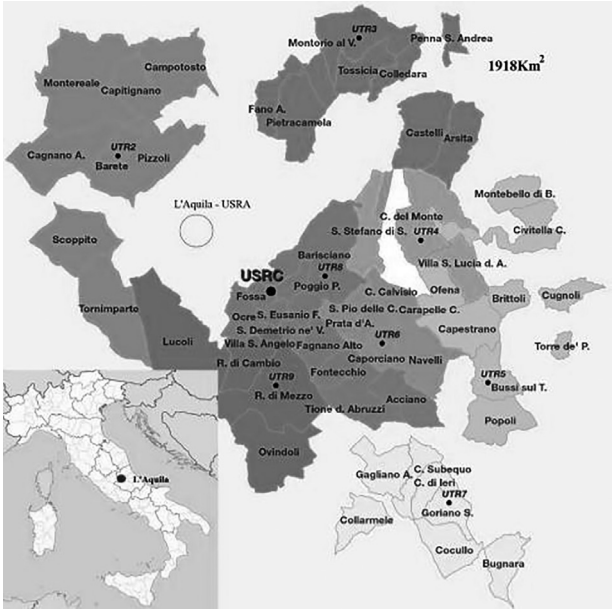

Figure 1: 56 municipalities making up the "seismic crater", divided into 8 homogeneous areas with 8 relevant reconstruction offices, UTRs, dependent on the USRC.

The USRC comprises multidisciplinary teams responsible for different aspects of physical and socioeconomic reconstruction, including engineering, urban planning and community involvement. To restore affected municipalities, the Office undertakes a range of activities, including GIS-based spatial analysis, stakeholder consultations, capacity-building and working groups, and infrastructure investments. The Office also collaborates with several academic institutions to leverage innovative best practices in reconstruction efforts. Hence the partnership with the Department of Telecommunications Engineering at the University of L'Aquila for land development and smart resource management, fostering the DT of these territories, that have characteristics in common, namely low population density, significant historical and environmental heritage. DT can make them attractive, avoid depopulation, promote local economy, counteracting isolation, in line with the National Recovery and Resilience Plan (NRRP)[6] too. From there, the need to develop an ICT platform (which is the core in a smart community) to support the USRC for information management (specifically geodata) useful to re-create more efficient communities.

Thus, GIS technology can play a role in supporting the USRC in both its activities and its DT journey. Whether it is infrastructure planning or resource alloca-

6 https://www.italiadomani.gov.it/content/sogei-ng/it/it/home.html.

tion, by leveraging geodata and analytical capabilities, GIS provides a framework for making informed data-driven decisions, gaining insights, providing innovative services to citizens, and optimizing operations (Fedra & Reitsma, 1990). Through a common platform for mapping and sharing geodata, GIS promotes collaboration and communication within the institution and among stakeholders (Franchi et al., 2024a).

Nevertheless, as institutions embrace DT to optimize operations and enhance services, they face growing cybersecurity risks. Indeed, this introduces potential vulnerabilities and increases the attack surface. Technology is vulnerable to many security issues, such as information theft, communication delays, data manipulation, jamming, remote exploitation, unauthorized access, human factor, etc. According to all 2024 reports released by ACN (National Agency for Cybersecurity)[7], DIS (Department of Information for the Security of the Italian Republic)[8], CLUSIT (Italian Association for Information Security)[9], in 2023 in Italy there was an increase in cyber-attacks against companies, organizations and people, with PA among the main targets of attackers. A successful cyber-attack against PA can lead to disruption of services, financial losses, exposure of private data, erosion of public trust in systems, and even physical damage.

Therefore, cybersecurity has never been more essential than it is now, as organizations have more valuable digital assets than ever before. The increasingly used hybrid cloud architecture and the pervasive use of mobile devices by employees means that enterprise IT must manage the security of many more devices and with a new approach.

2. Geographical Information Systems

Increasingly we hear about the "Science of Where" with geography as a relevant aspect of understanding our world (National Research Council, 2005). And the choice of GIS technology was not accidental but meets the needs of the context and the stakeholder. GIS is an evolving practice that enables organizations to get the most business value by helping multidisciplinary teams work together to make data-driven spending decisions (Chourabi et al., 2012; Franchi et al., 2024a). The literature review suggests that GIS can help understand where, why, and how things happen (Longley et al., 2005; Sui & Elwood, 2015).

Specifically, the USRC has equipped itself with a GIS over these years, but now, given the large volume of data and terminals-so we say big geodata-it needs to move from an on-premises and stand-alone solution to a cloud-edge one, increasing the level of risk of losing security of data. Data not only allow signification, knowledge, or understanding, but they also enable social action. In particular,

7 https://www.acn.gov.it/portale/documents/20119/446882/ACN_Relazione_2023.pdf.

8 https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true.

9 https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2024_web.pdf.

geodata (or geospatial data) are data relating to a location on Earth consisting in information about geographic locations stored in a format (e.g., geodatabase, shapefile, raster image, or even Microsoft Excel spreadsheet) that can be used with a GIS which combines location data (where things are) with descriptive data (how things are like in that location)-this ability distinguishes GIS from other information systems-helping users to discover relationships, enhance situational awareness and understand dynamics to model future scenarios (Worboys & Duckham, 2004).

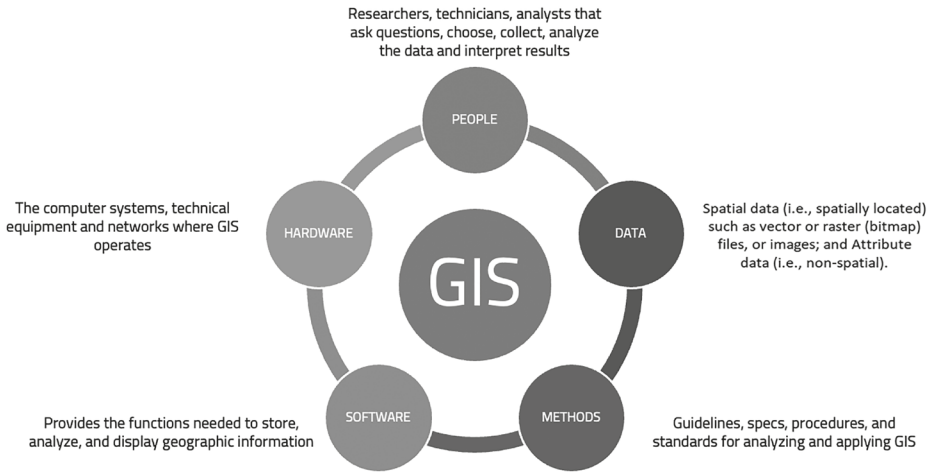

Figure 2: The key components of a GIS.

GIS is an automatic computer-based tool for collecting, analyzing, managing and interactive visualizing geodata, which enables (real-time) spatial analysis, planning strategies and resource management (Costantini et al., 2023). A working GIS integrates five key components: hardware, software, data, people, and methods as shown in Figure 2. Just as it was not exempt from the advent of the world wide web in the 1990s (Dragicevic, 2004), so today GIS establishes a synergy with other new technologies first with the Cloud Computing then with MEC (Multi-Access Edge Computing) and the next frontier is with AI (Artificial Intelligence) toward decentralized intelligence, seizing the opportunities that come with it but at the same time new potential challenges open up (see Figure 3 for the summary of technological evolution). The GIS-Cloud platform offers a dynamic, scalable and cost-effective solution that facilitates real-time data sharing and collaboration, enabling users to make timely decisions (Mell & Grance, 2011). With the GIS-MEC paradigm, cloud capabilities and the IT service environment are enabled at the edge of the network, closer to customers, reducing network congestion, latency, bandwidth requirements, and dependence on centralized IT resources to take advantage of the opportunities offered by next-generation connectivity (e.g., 5G) (ETSI, 2022). All of this is to promote social innovation with the goal of creating

positive societal impact (e.g., smart living and improved quality of life). Finally, Edge-AI enables local data processing on edge devices, reducing the need to transmit sensitive information to centralized servers for analysis, thus improving privacy and security (Wang et al., 2020). AI-powered GIS analysis enables automated data processing, pattern recognition, and predictive modeling of large volumes of geospatial data, enabling organizations to identify trends, detect anomalies, and derive useful information automatically, and users to focus on the most creative-strategic tasks (Ahmad, 2023).

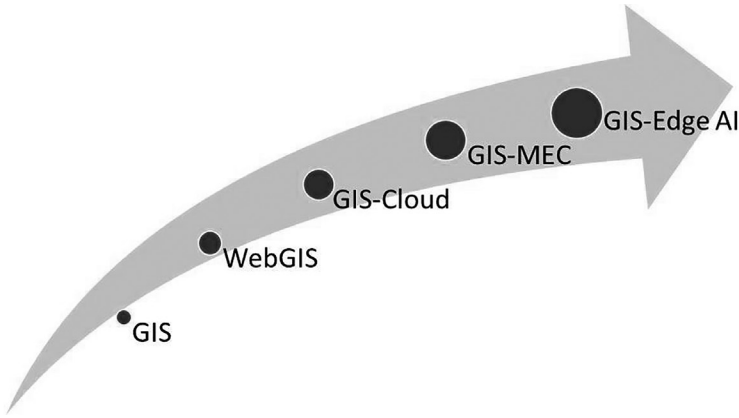

Figure 3: The GIS evolution.

Also, as institutions embrace the Internet of Things (IoT) and sensor technologies, GIS serves as an integration platform (Li et al., 2018).

We can consider GIS a driver of digital innovation, which facilitates spatial analysis, data visualization (including through integration with augmented reality and realistic 3D models), a tool that helps in problem solving (Goodchild & Janelle, 2010). As GIS continues to evolve, public/private organizations should harness the power of geodata and geospatial technologies, and leverage spatial insights to create a more sustainable, resilient and connected society.

2.1. The Role of GIS in Cybersecurity

The synergy of AI with GIS is a promising approach to proactive cybersecurity risk management. GIS can be used to map network infrastructure, visualize threat landscapes, and identify geographic patterns of cyber-attacks (Dash & Sharma, 2022). By integrating GIS with AI, institutions can leverage spatial data to train AI models, enhance predictive analytics, and improve decision making in cybersecurity operations (e.g., identify potential vulnerabilities, mitigate them, and prioritize response efforts) strengthening their posture (Bera et al., 2023; Rathee et al., 2023). Machine learning algorithms can analyze large datasets to identify patterns indicative of cyber threats or anomaly detection, while natural language processing can

analyze unstructured data to gather threat intelligence (Sharma & Dash, 2023; GISGeography, 2024).

Utilities use GIS-AI to analyze spatial data from smart meters and detect anomalies indicative of cyber intrusion or physical tampering; similarly, government agencies use this combination to monitor critical infrastructure, such as transportation and power grids, for cyber threats (Judijanto et al., 2023). These examples highlight the versatility and effectiveness of GIS-AI integration in addressing cybersecurity challenges in various sectors. Future research directions include developing standardized frameworks for GIS-AI integration, solving privacy issues, and exploring new applications of spatial analysis and AI techniques in cybersecurity. Collaboration between academia, industry, and government is essential to advance research in this emerging field and develop practical solutions.

However, challenges such as false positives and adaptability of cyber adversaries require continuous evolution of threat detection mechanisms.

3. An Overview of Cyber for GIS

As GISs continue to evolve, integrate with digital ecosystems, and play an increasingly integral role in the decision-making processes of various sectors (including government, defense, urban planning, environmental management, and others) (Franchi et al., 2024a), it becomes imperative to address the cybersecurity risks to which they are exposed so that data quality is not compromised (ESRI, 2020). By taking proactive measures and remaining vigilant against emerging threats, the USRC can safeguard its GIS infrastructure and preserve the CIA (confidentiality, integrity, availability) Triad for geodata from unauthorized access and exploitation. A balance between reactive and proactive measures should be found (Baskerville et al., 2014).

Among the cybersecurity risks facing GIS are:

1. *Data Breaches*: GIS databases contain a plethora of sensitive information, including geospatial data, demographic details, and infrastructure layouts. Unauthorized access to this data through breaches not only leads to violations of individual privacy, but also compromises national security. For example, exposure of critical infrastructure locations can help adversaries plan targeted attacks.
2. *Ransomware Attacks*: ransomware threats have intensified in recent years and, in a ransomware attack, attackers encrypt GIS data, making it inaccessible until a ransom is paid. These attacks not only disrupt operations, but also result in significant financial losses and erode stakeholder trust.
3. *Insider Threats*: insiders with authorized access to GIS systems, including employees and contractors, present significant risks that can compromise GIS security. Malicious insiders may abuse their access privileges to steal sensitive data, manipulate GIS information, disrupt services, implant malware, sabotage systems, or leak confidential information. In addition, inadvertent actions by well-intentioned insiders can inadvertently expose GIS

systems to vulnerabilities, highlighting the importance of robust access controls and employee training.

4. *Denial of Service (DoS) Attacks*: GIS servers are susceptible to these attacks, in which attackers overwhelm them with an excessive volume of traffic, making them inaccessible to legitimate users and disrupting services. The disruption caused by DoS attacks not only causes downtime and hinders access to critical geospatial information, but also compromises the functionality of GIS applications, potentially affecting emergency response operations and public safety.
5. *Eavesdropping Attacks*: a type of Man-in-the-Middle cyber-attack, which allows hackers to intercept, erase, or modify data transmitted between devices.
6. *Vulnerabilities in GIS Software*: like all software systems, GIS applications and platforms are prone to vulnerabilities that can be exploited by malicious actors both proprietary and open source. From SQL injection and buffer overflows to insecure authentication mechanisms, GIS software vulnerabilities can allow attackers to gain unauthorized access, execute arbitrary code, or compromise GIS data for malicious purposes.

Suggested strategies to mitigate these risks are the following:

1. *Implement Robust Access Controls*: use a defense-in-depth approach to restrict access to GIS systems by implementing access controls based on user roles and responsibilities, least privilege principles, and network segmentation. Use multi-factor authentication, encryption mechanisms, monitoring mechanisms to detect and prevent unauthorized activity, and strong encryption to safeguard data integrity and confidentiality.
2. *Regular Security Audits and Updates*: conduct periodic security audits and vulnerability assessments using scanning tools to identify and correct potential security weaknesses in GIS systems. Apply timely patches and software updates to reduce known security flaws and strengthen the resilience and defenses of the GIS infrastructure. Organizations should deploy intrusion detection systems and traffic filtering mechanisms.
3. *Zero-Trust Architecture (ZTA)*: the underlying concept is "never trust, always verify", meaning that users and devices should not be trusted by default, even if they are connected to an authorized network such as an enterprise LAN (local area network). It describes an approach to designing and deploying IT systems in an enterprise network composed of cloud services, connections to remote and mobile environments, and IoT devices.
4. *Employee Training and Awareness*: educate GIS users on the importance of adhering to cybersecurity best practices, including password hygiene, recognizing social engineering tactics or phishing attempts, and timely reporting of suspicious activity to effectively mitigate insider threats. Promote a cybersecurity culture to reduce insider threats among GIS users through comprehensive training programs and awareness campaigns.
5. *Backup and Disaster Recovery Plans*: implement backup and disaster recovery mechanisms to ensure resilience of the GIS system in the event of an attack such as ransomware or data breach. Maintain regularly updated

backups of GIS data, including off-site copies, and develop comprehensive disaster recovery plans to minimize downtime and facilitate timely restoration of geodata, ensuring business continuity.

6. *Collaborate with Cybersecurity Experts*: collaborate with cybersecurity professionals, practitioners and researchers, industry and government agencies to stay current on emerging threats and best practices in GIS security. Promote collaboration and information sharing initiatives to improve threat intelligence capabilities and strengthen GIS's overall cybersecurity posture. In general, see Information Sharing and Analysis Centers (ISACs), serving the government and national industry, are a resource that enables two-way information exchange between the public and private sectors on cyber causes, incidents and threats (in many cases to critical infrastructure), as well as the sharing of experience, knowledge and analysis.

The human factor seems to be the weakest link in cybersecurity, but organizational posture also matters. PA is trying to increase its cybersecurity by introducing formal policies and training employees, who consequently perceive cybersecurity as important, encouraging them to be aware about. As Alshaikha (2020) suggested, among the ways to improve cybersecurity culture could be the use of incentives, such as "employee of the month"-a reward would ignite a collective call to action, reminding employees that poor cybersecurity practices are not acceptable.

Challenges facing GIS include:

1. *Data Confidentiality*: one of the primary concerns in GIS security is ensuring the confidentiality of sensitive geospatial data. Unauthorized access to GIS databases can lead to data breaches, exposing proprietary information, classified maps, and personal identifiers.
2. *Data Integrity*: maintaining the integrity of GIS data is essential to ensure its accuracy, reliability, and trustworthiness. Malicious actors may attempt to manipulate GIS datasets, altering maps, spatial attributes, or geographic features to mislead decision-makers or disrupt operations.
3. *Service Availability*: for instance, DoS attacks pose a significant threat to GIS service availability, disrupting access to geospatial information and critical applications. Attackers may target GIS servers with overwhelming traffic, rendering them inaccessible to legitimate users.
4. *Over trust in GIS system*: in a fundamental sense, all technology depends on trust, and users need to know how it works. So, it must be trusted without replacing human creativity. Rather, it assists humans as a decision support system to be timely, efficient and predictive.
5. *Ethical issues*: the use of data as a means to exert control over other entities, resulting in an illicit relationship between parent and subsidiary, as also pointed out by Lodi et al. (2014).
6. *Proactive Supply Chain Risk Management*: about the control of data by third parties (Spiekermann et al., 2015). This means that the USRC, like any other PA, must carefully review service contracts and establish clear secu-

rity requirements, including data security, with Managed Service Providers (MSP) and generally with all vendors that support the implementation and operation of smart community technology (e.g., cloud service providers).

The above is summarized schematically in Figure 4.

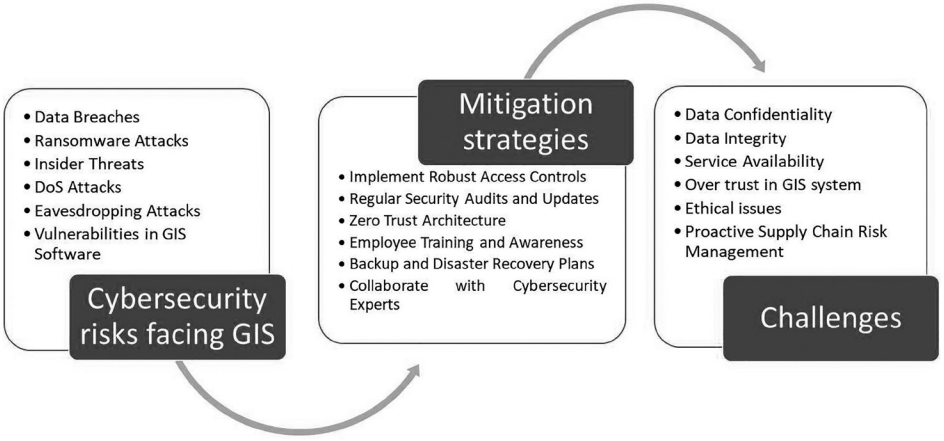

Figure 4: Sum up of Cyber and GIS.

4. The Case Study (hints)

A smart community ecosystem comprises three layers: the edge, which is the frontend (i.e., the devices, such as sensors or smartphones), the core (i.e., the platform, in this case GIS-based in a cloud-edge architecture, which processes the data and generates the business logic to make sense of the data flowing from the edge), and the communication channel (such as Wi-Fi, which establishes a constant two-way data exchange between the core and the edge to integrate the various components of the ecosystem) (Kousis & Tjortjis, 2021).

The development of the GIS platform to support USRC activities is still ongoing and will be completed soon with a kick-off event. The prototype has already been successfully tested (Franchi et al., 2024b). After that, it will be fully adopted by the PA in question. Figure 5 shows a preview of this.

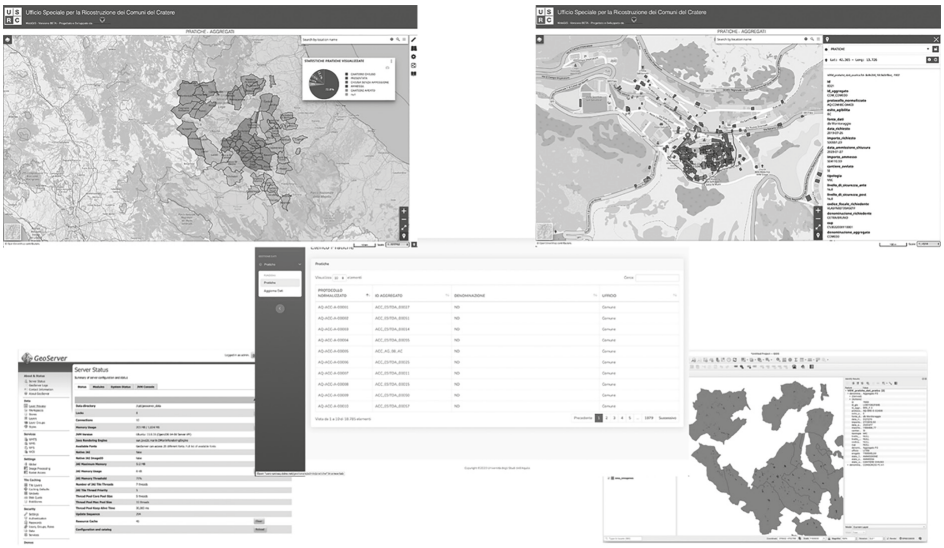

Figure 5: Sneak Peek of the GIS platform under development for the USRC

5. Conclusions

This paper examines cyber risks related to GIS technology supporting the development of smart communities. In the example used is a PA that wants to (re) create smart towns through technological innovation and data-driven decision making, and this introduces potential vulnerabilities and increases the attack surface. Economist J. Schumpeter defines innovation as "creative destruction", two words that seem antithetical but fit well to explain this context and in general that every innovation has costs and benefits, one must be adept at capturing the latter and curbing the former. Thus, the need to address security in data exchange (both processing and storage and transit) perhaps by defining a framework and to take proactive/reactive measures. The pros of this digital strategy, however, include DT and modernization of PA; (re)design of public intervention; efficiency of asset management and infrastructure planning; cost-effectiveness of (public) action; improved quality of city government; and new services provided to the population increase territorial capital. Recommended an interdisciplinary and multistakeholder approach with an ongoing university-institution-industry dialogue to develop solutions and ensure that although innovation runs fast, law is an ally. While the application of increasingly high-performance technologies can certainly improve people's living conditions, it can also, and just as strongly, result in a restriction of their freedom. Hence the decision to identify which public values should be taken

away from the private profit of giant platforms. So much so as stated by the Privacy Guarantor (Jan. 30, 2020), this alliance between technology and law "can be the lintel of a democratic and forward-looking response to the new threats of the digital, inevitably connected to the opposite, extraordinary benefits".

Moreover, the World Economic Forum 2023 reveals a global shortage of cybersecurity talent that needs to be addressed quickly[10]. But as Natasa Perucica says, it is important to remember that "cybersecurity is also the responsibility of all the other employees working for the organization in question. Through their responsible behavior and responsible use of digital technologies, like their devices, they contribute to the security of the overall organization".

Since attacks can have consequences that affect lives, it is imperative that all policymakers prioritize cybersecurity as a strategic necessity when undertaking online and digital initiatives.

In addition, investments by PA are needed to heal the country's structural backwardness, also involving inland and marginal areas. Otherwise, a fragmented system can produce gridlock rather than innovation, leading to what Garret Hardin called the "lifeboat ethic".

It is therefore necessary to be competent digital citizens to consciously navigate our society in the Information Age.

References

Ahmad M. 2023, "AI-Enabled Spatial Intelligence: Revolutionizing Data Management and Decision Making in Geographic Information Systems", in *AI and Its Convergence With Communication Technologies* (pp. 137-166). IGI Global.

Alshaikha M. 2020, "Developing cybersecurity culture to influence employee behaviour: A practice perspective", in *Computers & Security*, 98.

Baskerville R., Spagnoletti p. & Kim J. 2014, "Incident-centered information security: Managing a strategic balance between prevention and response", in *Information & management*, 51(1): 138-151.

Bera S., Glenn L., Raghavan A., Meno E., Cody T. & Beling p. A. 2023, "Deterring Adversarial Learning in Penetration Testing by Exploiting Domain Adaptation Theory", in *2023 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 314-318). IEEE.

Chourabi H., Nam T., Walker S., Gil-Garcia J. R., Mellouli S., Nahon K.,… & Scholl H. J. 2012, "Understanding smart cities: An integrative framework", in *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

Costantini R. A., Thompson C. M. & Delacour H. 2023, "Leveraging geographic information in organization studies: Beginning the conversation", in *M@n@gement,* (1): 35-51.

Dash B. & Sharma p. 2022, "Role of artificial intelligence in smart cities for information gathering and dissemination (a review)", in *Academic Journal of Research and Scientific Publishing,* 4(39).

Dragicevic S. 2004, "The potential of Web-based GIS", in *J. Geograph. Syst.,* 6(2): 79-81.

10 https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

ESRI 2020, "Designing an Enterprise GIS Security Strategy", Available at https://downloads.esri.com/resources/enterprisegis/UC_Web_GIS_Security_Strategy.pdf

ETSI2022, "Multi-Access Edge Computing (MEC); Framework and Reference Architecture", Available at https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_mec003v030101p.pdf

Fedra K. & Reitsma R. F. 1990, "Decision support and geographical information systems", in *Geographical information systems for urban and regional planning* (pp. 177-188). Dordrecht: Springer Netherlands.

Fico R., Gualtieri R., Pecci D., Mannella A., Di Ludovico M., & Prota A. 2017, "Reconstruction model of residential buildings in the historical centers of the crater municipalities after L'Aquila 2009 earthquake", in *16th World Conference on Earthquake Engineering, 16th WCEE.*

Franchi F., Graziosi F., Di Fina E. & Galassi A. 2024a, "A Survey of Cloud-Enabled GIS Solutions Toward Edge Computing: Challenges and Perspectives", in *IEEE Open Journal of the Communications Society*, 5: 312-331.

Franchi F., Graziosi F., Di Fina E. & Galassi A. 2024b, "A Cloud-Edge Architecture to Support Post-Earthquake Reconstruction in Central Italy", in *IEEE Access*, vol. 12, pp. 91823-91831.

GISGeography 2024, "The Rise of Machine Learning and AI in GIS", available at https://gisgeography.com/deep-machine-learning-ml-artificial-intelligence-ai-gis/ (accessed: June 14, 2024).

Goodchild M. F. & Janelle D. G. (editors) 2010, *Spatially integrated social science*, Oxford: Oxford University Press.

Judijanto L., Rahardian R. L., Muthmainah H. N. & Erkamim M. 2023, "Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia", in *West Science Information System and Technology*, 1(2): 90-98.

Kousis A. & Tjortjis C. 2021, "Data mining algorithms for smart cities: A bibliometric analysis", in *Algorithms*, 14(8): 242.

Li S., Da Xu L. & Zhao S. 2018, "5G Internet of Things: A survey", in *Journal of Industrial Information Integration,* 10: 1-9.

Lodi G., Aniello L., Di Luna G. A. & Baldoni, R. 2014, "An event-based platform for collaborative threats detection and monitoring", in *Information Systems*, 39: 175-195.

Longley p. A., Goodchild M. F., Maguire D. J. & Rhind, D. W. 2015, *Geographic Information Science & Systems*, John Wiley & Sons.

Mell p. M. & Grance T. 2011, "The NIST definition of cloud computing".

National Research Council – Division on Earth, Life Studies, Board on Earth Sciences, Geographical Sciences Committee, Committee on Support for Thinking Spatially & The Incorporation of Geographic Information Science Across the K-12 Curriculum 2005, *Learning to think spatially*, National Academies Press.

Rathee A., Malik p. & Parida M. K. 2023, "Network Intrusion Detection System using Deep Learning Techniques", in *2023 International Conference on Communication, Circuits, and Systems (IC3S)* (pp. 1-6). IEEE.

Sharma p. & Dash B. 2023, "Impact of big data analytics and ChatGPT on cybersecurity", in *2023 4th International Conference on Computing and Communication Systems (I3CS)* (pp. 1-6). IEEE.

Spiekermann S., Acquisti A., Böhme R. & Hui K. L. 2015, "The challenges of personal data markets and privacy". *Electronic markets*, 25: 161-167.

Sui D. & Elwood S. (ed.) 2015, *The SAGE Handbook of GIS and Society*, SAGE Publications.

Wang, X., Han, Y., Leung, V. C., Niyato, D., Yan, X., & Chen, X. 2020, *Edge AI: Convergence of edge computing and artificial intelligence* (pp. 3-149), Singapore: Springer.
Worboys M. F. & Duckham M. 2004, *GIS: a computing perspective,* CRC press.

Filippo Galli

L'organizzazione amministrativa della cybersicurezza nell'ordinamento multilivello

Abstract: Lo studio analizza il quadro giuridico multilivello della cybersecurity, con particolare attenzione al profilo dell'organizzazione amministrativa. Prendendo spunto dall'analogia con le Ecatonarchie della mitologia greca, il contributo esplora le intricate strutture che definiscono il panorama operativo della cybersecurity, sottolineando le difficoltà nel concettualizzare la materia come un sistema giuridico coerente senza un'analisi completa della sua natura in evoluzione. Esaminando i modelli organizzativi all'interno dell'UE e delle discipline nazionali e ricostruendone la *ratio*, lo studio evidenzia l'interazione tra gli approcci tradizionali Stato-centrici e i modelli di governance policentrici emergenti. La trattazione sostiene che, in un contesto di assenza di autorità, il concetto di organizzazione emerge come principio relazionale, cruciale per navigare nelle complessità della poliarchia. L'articolo riflette sulle implicazioni per le future discipline giuridiche, sottolineando la necessità di una governance adattiva che possa rispondere alla rapida evoluzione delle minacce nel dominio digitale.

Keywords: Cybersecurity; Organizzazione amministrativa; Digital Governance; Rete; Multistakeholder Approach.

1. 'Catturare l'Ecatonchiro'. Lo studio della cybersicurezza come sistema coerente di diritto

Nei racconti della teogonia greca sull'origine dell'ordine cosmico[1], si narra che dall'unione primordiale tra Cielo (*Urano*) e Terra (*Gea*) nacquero, tra gli altri, gli Ecatonchiri[2]: esseri colossali e dalle fattezze mostruose, erano dotati, ciascuno (da cui il *nomen* collettivo), di cinquanta paia di braccia e altrettante teste, che li ren-

1 Mi rifaccio, in particolare, alla tradizione esiodea (Hes. *Th*. 148 ss.).
2 Dall'unione delle parole *ἑκατόν* ("cento") e *χείρ* ("mano"), latinizzato in *Centimani*.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760148

devano "insuperabili per dimensione e potenza"[3]. Della loro forza Zeus si servì per rovesciare la tirannia del padre Crono, lasciandoli infine a sorvegliare i Titani prigionieri nel Tartaro.

All'osservatore che si accosti al sistema amministrativo della cybersicurezza, la figura dell'Ecatonchiro fornisce una sintetica ma pregnante rappresentazione del 'colpo d'occhio'. Le ragioni dell'analogia sono di natura epistemica, nella misura in cui la comune complessità strutturale dei fenomeni si riflette sulle condizioni di conoscibilità degli stessi: come gli autori classici finiscono per contraddirsi nelle reciproche descrizioni della creatura mitica, faticando persino a immaginarne le fattezze, così lo studio in termini strutturali dell'architettura *cyber* sconta preliminari esigenze di chiarificazione concettuale, nonché di una ricostruzione capace di articolarne in modo significativo le eterogenee componenti e i rispettivi indirizzi operativi.

Si pone, pertanto, un fondamentale problema di definizione dell'oggetto d'indagine e financo di *pensabilità* dello stesso, quanto meno nei termini di un *corpus* unitario e provvisto di pur basilare coerenza. 'Catturando l'Ecatonchiro' nel suo insieme, il giurista può tentare una descrizione della cybersicurezza come sistema di diritto 'in azione', rilevandone, al di là della miriade di norme e apparati, regolarità e matrici funzionali. L'analisi complessiva della materia, oltre a rendere conto della sua categorizzazione, è essenziale per comprenderne il funzionamento globale e individuare le migliori soluzioni *de lege ferenda* nel quadro di una disciplina in rapidissima evoluzione.

In questo senso, il presente lavoro si propone di fornire alcune notazioni di carattere teorico-generale con riferimento alla tipologia organizzativa riscontrabile nell'ordinamento multilivello della cybersicurezza, nonché ai relativi moduli operativi e ai sottesi modelli di regolazione sociale.

2. Organizzazione amministrativa e definizione della funzione: le ragioni di un'inversione di metodo

Questione di rilievo all'apparenza contingente, ma foriera di considerazioni circa lo statuto giuridico della cybersicurezza, è la scelta di partire da uno studio dell'organizzazione, privilegiando un'osservazione del fenomeno amministrativo che ne evidenzi tanto il rilievo istituzionalistico di "grandezza sociale"[4], quanto la natura di "stabile e ordinata struttura politico-sociale in cui coesistono e interagiscono persone con ruoli e responsabilità differenti, utilizzando risorse di vario genere (…) per raggiungere determinati obiettivi"[5] e garanzie.

Si è correttamente osservato, in dottrina, che l'aspetto latamente organizzativo, tradizionale appannaggio di una scienza dell'amministrazione oggi in ripresa[6], è

3 Apollod. *Bibliotheca* 1.1.1.

4 Così Romano 1909: 8, difendendo la "personificazione del potere per mezzo dello Stato" dalla facile critica di costituire nulla più che una "fantasia poetica".

5 Gasparri 2024: 1.

6 Matassa 2022: 627 s., D'Alberti 2013: 65.

costitutivo del concetto stesso di *cybersecurity*, il quale, sul piano etimologico, sta ad indicare un'organizzazione di tipo difensivo[7] e, su quello operativo, ha principalmente ad oggetto la protezione di "infrastrutture informatico-digitali di organizzazioni complesse, pubbliche o private"[8], spesso coinvolte in iniziative di coordinamento difensivo ben al di là delle formali indicazioni normative[9]. Spingendosi oltre tali conclusioni, si può rilevare come, per un settore dominato dalla *disruptive innovation*[10] quale la cybersicurezza, tale profilo strutturale concorra alla stessa definizione della funzione, la quale appare costantemente in via di consolidamento. È del resto opinione diffusa, *a fortiori* in discipline di frontiera, che tracciare un confine netto tra l'ambito dell'organizzazione e quello dell'attività amministrativa sia impresa tutt'altro che agevole (e forse nemmeno auspicabile), modellandosi la prima, anche per un basilare principio di strumentalità, in relazione alle finalità sostanziali che la seconda si propone di perseguire[11].

Se, dunque, secondo l'insegnamento di Giannini, "in principio sono le funzioni"[12] (e quindi i bisogni, cui, solo in un secondo momento, segue l'articolazione amministrativa)[13] – e ciò costituisce un assioma sempre valido – in pochi altri ambiti, nella prassi, la struttura finisce per rivelarsi tanto determinante rispetto ai confini della funzione: in altri termini, tra la cybersicurezza *stricto sensu* (la c.d. cyber-resilienza) e il suo frequente impiego come "*umbrella term*"[14] di più o meno connesse istanze securitarie si riscontra una vasta area di "penombra"[15] semantica, popolata da concetti come guerra cibernetica, cybercrimine e *cyberintelligence* e i cui confini restano segnati, in ultima istanza, dalle scelte discrezionali concernenti l'attribuzione agli apparati delle relative competenze.

7 Rossa 2023a: 9 ss. Rossa 2023b: 162 s. Rossa 2022: 428 s.

8 Rossa 2023b: 163.

9 Odermatt 2018: 354 ss., con riferimento al "*multi stakeholder approach*" tipico dell'Unione europea.

10 L'espressione è resa popolare da Bower e Christensen 1995, che la impiegano per descrivere i processi di innovazione tecnologica capaci di rivoluzionare in maniera 'dirompente' il funzionamento di un determinato mercato, portando in ultima istanza alla sua sostituzione o, quantomeno, a quella delle imprese in esso dominanti: "*The technological changes that damage established companies are usually not radically new or difficult from a technological point of view. They do, however, have two important characteristics: First, they typically present a different package of performance attributes – ones that, at least at the outset, are not valued by existing customers. Second, the performance attributes that existing customers do value improve at such a rapid rate that the new technology can later invade those established markets. Only at this point will mainstream customers want the technology. Unfortunately for the established suppliers, by then it is often too late: the pioneers of the new technology dominate the market*".

11 Franchini e Vesperini 2012: 74. In tema di rilevanza giuridica dell'organizzazione amministrativa, che va ben oltre la mera strumentalità rispetto alla relativa attività, si vedano, *ex multis*, Merloni 2009, Rossi 2005, Nigro 1988, Paleologo 1981, Guarino 1977, Berti 1968, Nigro 1966, Bachelet 1965. Il tema è stato recentemente riproposto da Carbone 2024.

12 Giannini 1957.

13 Gasparri 2024: 2 ss.

14 Odermatt 2018.

15 Hart 1958.

Più in generale, assecondando la comune tendenza degli ordinamenti della sicurezza[16], l'amministrazione *cyber* manifesta, al prezzo di una certa ambiguità categoriale[17], una natura "trasversale"[18], capace di curare molteplici interessi pubblici[19] nelle forme ibride dell'approccio *whole-of-society*[20]. A tale dispiegamento corrisponde, di necessità, l'assestarsi di un'idonea organizzazione pubblica, o piuttosto di quella "miriade di organizzazioni"[21] in cui si esprime ogni ramo di amministrazione, disegnando un "complesso di strutture"[22] e di "modelli differenziati"[23] percorso da relazioni eterogenee: un sistema la cui complessità qualitativa si misura nella coesistenza di figure soggettive (quali 'agenzie', 'comitati' e 'gruppi' di vario tipo) profondamente divergenti per natura, compiti e composizione.

In un settore alimentato dalla digitalizzazione, la quale impone regolarmente il ripensamento degli operatori sul piano organizzativo e financo culturale[24], si fa più stridente che altrove il "paradosso tra l'insufficienza esplicativa del tradizionale modello legalitario-burocratico di amministrazione pubblica e la persistente egemonia del quadro teorico statocentrico"[25], laddove, coinvolgendo ormai in ogni sua componente la vita economica e sociale, l'esigenza di protezione sottesa all'esercizio del potere sembra domandare ad un tempo soluzioni di amministrazione classica e di *governance* globale, generando concorrenza tra i rispettivi modelli.

Per tali ragioni, un metodo d'indagine che, con inversione logica, si appunti prioritariamente all'organizzazione della cybersicurezza consentirà non solo di sondarne la concreta consistenza, ma anche di chiarire le finalità della relativa funzione e, auspicabilmente, la capacità dell'amministrazione di assicurarne gli esiti.

3. In principio è il diritto globale, tra gruppi di intervento e norme tecniche

Peculiarità della cybersicurezza come fenomeno ordinamentale è lo sviluppo originario, e quindi la priorità *in tempore* rispetto al successivo intervento (sovra-)

16 Chiti 2016: 545.

17 La quale finisce per forzare la tradizionale semantica del potere pubblico e della sovranità. Cfr. Slack 2016.

18 Lauro 2021: 532.

19 Sola 2022: 391.

20 Ovvero di un approccio che, oltre alle competenti amministrazioni, "vede coinvolti anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza. Nella presente visione strategica, infatti, quest'ultima è concepita non solamente come un indiretto beneficia rio delle misure contemplate nel Piano di implementazione della strategia, ma anche come parte attiva. L'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale, nessuno escluso" (*Strategia Nazionale di Cybersicurezza 2022-2026*: 8).

21 Guarino 1977: 88.

22 D'Alberti 2013: 73.

23 Guarino 1970: 17.

24 Golisano 2022: 824.

25 Di Gaspare 1995: 513.

statale, di sistemi regolatori globali rientranti a pieno titolo tra le manifestazioni del c.d. *global administrative law*[26].

Benché, infatti, il tema resti perlopiù inesplorato in dottrina, anche perché riconducibile in larga misura a fenomeni di *soft law* posti ai margini della rilevanza giuridica[27], la trentennale[28] esperienza dei gruppi di risposta alle minacce cibernetiche, di eterogenea natura e denominazione (oggi perlopiù *Computer Security Incident Response Team* – CSIRT o *Computer Emergency Response Team* – CERT)[29], ha origine al di fuori di ogni inquadramento normativo o burocratico, esprimendosi nondimeno, fin dal principio, in un sistema deformalizzato di coordinamento globale preposto ad attività di *soft regulation* e scambi informativi.

In linea con la "grande trasformazione"[30] innescatasi a partire dalla seconda metà del XX secolo e la conseguente esplosione della globalizzazione giuridica, le singole cellule operative, talora investite di "mandati pubblici nazionali"[31], hanno progressivamente prodotto aggregazioni complesse di "reti (…) di poteri pubblici neutrali"[32], investite di competenze tecniche dalla portata universale (es. CERT/CC e FIRST) o regionale (es. TF-CSIRT) ma pur sempre estranee al circuito politico-rappresentativo e alle sue istituzioni domestiche o internazionali. Ne è risultato un complesso strutturalmente eterogeneo, orientato alla comunione di funzioni[33] tra soggetti equiordinati[34]; un meccanismo di *governance* informale, animato da relazioni *de iure* paritarie e segnato al più dalla sostanziale primazia di organi particolarmente autorevoli (ad es. il CERT/CC con sede a Pittsburgh).

È solo a ridosso del nuovo millennio che la disciplina della cybersicurezza attira le attenzioni crescenti degli attori politici tradizionali, *in primis* di quello comunitario, i quali non di rado, pur avanzando autentiche pretese conformative e proponendo soluzioni organizzative ad esse adeguate, hanno optato per un innesto dei nuovi sistemi amministrativi sull'intelaiatura preesistente, istituzionalizzando ed arricchendo di funzioni pubbliche la rete 'parallela'[35] costituita dai CSIRT nazionali[36].

26 Sul distinguo v. Battini 2008, Cassese 2005.

27 Laddove "[r]ilevante è, dunque, il fatto che riceve un predicato giuridico; irrilevante, il fatto che non riceve un predicato giuridico", esprimendosi in tal modo non "una nota del fatto, ma la impossibilità del giudizio giuridico" (Irti 1968: 103).

28 A partire dalla diffusione del c.d. Morris Worm, nel 1988, su cui v. Ruohonen – Hyrynsalmi – Leppänen 2016: 748 s.

29 Sulle ragioni della diffusione di una doppia denominazione, v. Serini 2021: 251 e Contaldo – Peluso 2018: 70 ss.

30 Battini 2016: 112 ss.

31 Ruohonen – Hyrynsalmi – Leppänen 2016: 749.

32 Ielo 2003: 374.

33 Su cui Ielo 2003: 384 ss.

34 Sulla *governance* tecnica della cybersicurezza cfr. Mueller, M. – A. Schmidt – B. Kuerbis 2013.

35 Accanto a quella "propriamente amministrativa" (Lauro 2021: 532).

36 La disciplina dei CSIRT e della relativa Rete è, da ultimo, prevista dagli articoli 10-13 e 15 della Direttiva (UE) 2022/2555 (NIS 2).

L'intera vicenda disegna, quindi, un caso singolare di 'glocalizzazione del diritto', il quale, inizialmente etichettabile come 'globale', si fa disciplina comunitaria e poi nazionale, cristallizzando via via in formule normative e istituzionali di maggiore cogenza: un percorso dettato dalla novità della relativa funzione, nata, quantomeno con riferimento al Vecchio continente, in un contesto di forte vitalità oltre i confini (e le categorie) dello Stato[37].

4. Il quadro europeo della cybersicurezza: organizzazioni a rete e integrazione decentrata

Nel senso sopra delineato, l'ordinamento amministrativo dell'Unione è il primo ove sia dato riscontrare un'organizzazione in senso proprio operante, nell'ambito della sicurezza informatica, (anche) entro i confini nazionali, mentre il legislatore italiano esiterà a inaugurare una normativa dedicata per almeno un altro decennio[38]. Il regime comunitario in vigore dai primi anni Duemila[39] viene rimaneggiato a più riprese, specialmente a seguito dell'elaborazione di un'apposita Strategia dell'Unione[40], e si articola oggi in un disegno estremamente complesso.

Prendendo a riferimento i due principali criteri di distribuzione delle funzioni amministrative[41], il sistema, nel suo insieme, può declinarsi *ratione materiae* laddove ogni ripartizione sub-settoriale della cybersicurezza è riconducibile alla competenza di chiare figure istituzionali (ENISA per la cyber-resilienza[42], EC3 per il cybercrimine[43], l'Agenzia europea per la difesa con riferimento alla c.d. guerra cibernetica[44]), ma anche rispetto alla tipologia di attribuzioni: così, attorno al nucleo della regolazione *cyber*, costituito da ENISA con le sue funzioni di assistenza, coordinamento, certificazione e formazione, si sviluppano varie "reti" di carattere tecnico-operativo che coinvolgono agenti e strutture decisionali a diversi livelli di intervento (tra cui la rete dei CSIRT[45], il Gruppo di cooperazione[46] e la nuo-

37 Della Cananea 2009.

38 Con il d.P.C.M. n. 66 del 19 marzo 2013 (decreto Monti).

39 Radoniewicz 2022: 73 ss. Lauro 2021: 531 ss., Ruohonen – Hyrynsalmi – Leppänen 2016: 749 ss.

40 *Strategia dell'Unione europea per la cibersicurezza* (JOIN(2013) 01), già preceduta da una comunicazione sulla *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo* (COM(2001) 298) e da una *Una strategia per una società dell'informazione sicura* (COM(2006) 251), nonché da un piano di azione e una comunicazione *Proteggere le infrastrutture critiche informatizzate* (COM(2009) 149).

41 Franchini e Vesperini 2012: 75 s.

42 L'Agenzia dell'Unione europea per la cibersicurezza, istituita nel 2004 e disciplinata, da ultimo, con Reg. (UE) 2019/881.

43 Il Centro europeo per il cybercrimine, proposto la prima volta con la comunicazione sulla *Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica* (COM(2012) 140).

44 Su cui cfr. *La politica di ciberdifesa dell'UE* (JOIN(2022) 49).

45 Art. 15 Direttiva (UE) 2022/2555 (NIS 2).

46 Art. 14 Direttiva (UE) 2022/2555 (NIS 2).

va rete per le crisi informatiche EU-CyCLONE[47]); con riferimento ai compiti di formazione e scambio di buone prassi, è sorto un vero e proprio ecosistema europeo delle competenze, che vede un Centro europeo di competenza sulla cybersicurezza (ECCC) attorniato da una Rete di centri nazionali di coordinamento e operante nell'ambito della c.d. Comunità europea della cybersicurezza, una sorta di piattaforma di dialogo al servizio dei portatori di interesse[48]; mentre nell'ambito di quest'ultima, rispetto alle specifiche esigenze di rilancio e coordinamento industriale, si è registrato il varo di un vasto programma di partenariato pubblico-privato sotto l'egida di una *European Cyber Security Organization* (ECSO)[49].

L'intreccio di organi e funzioni traccia un regime di *governance* "distribuita"[50] che, partito da basilari compiti di coordinamento dinamico, ha gradualmente accentuato i propri tratti conformativi secondo un processo di stratificazione burocratica (*bureaucratic layering*)[51] lungo le precedenti infrastrutture di cooperazione informale.

In particolare, benché l'impianto complessivo resti chiamato a convogliare nelle sedi decisionali la più vasta platea di soggetti interessati (*multistakeholder approach*), confermando così la propria vocazione partecipativa, emerge il ruolo preminente di ENISA: un'agenzia europea che, inizialmente impegnata in un'ostica "lotta per il riconoscimento"[52] come autorità di settore, si è vista attribuire crescenti competenze operative e promozionali[53], sino a diventare l'*ubi consistam* di un sistema[54] capace di combinare strategie difensive *risk-based* e azioni mirate *threat-based*[55].

Il descritto complesso regolatorio sconta il carattere composito e multipolare proprio delle amministrazioni europee[56], segnate in ogni direzione da rapporti di "interdipendenza strutturale e funzionale"[57]. Ai fini di un inquadramento tipologico, l'esito appare in prevalenza riconducibile a due modelli organizzativi di notevole efficacia descrittiva, ancorché di scarso rigore dogmatico: la figura della rete[58], "contenitore di relazioni"[59] nel quale si realizza una distribuzione di competenze tra nodi e "punti di contatto"[60] orientati alla comune soluzione di problemi

47 Art. 16 Direttiva (UE) 2022/2555 (NIS 2).
48 Reg. (UE) 2021/887.
49 Fondata nel 2016 e il cui statuto è disponibile all'indirizzo www.ecs-org.eu.
50 OECD 2002.
51 Ruohonen – Hyrynsalmi – Leppänen 2016: 753.
52 Honneth 2002.
53 Ulteriormente accresciute con la Direttiva NIS 2 e il Reg. (UE) 2019/881 (*Cybersecurity Act*).
54 Sulle competenze di ENISA, *ex multis*, Rossa 2023b: 166 ss., Forgione 2022, Parona 2021, Pauri 2017, Eckhardt – Kotovskaia 2023.
55 Backman 2023.
56 Franchini e Vesperini 2012: 120, Chiti 2007, Cassese 2002.
57 Franchini – Della Cananea 2010: 143.
58 Frediani 2010: 103 ss. che ne distingue un senso tecnico e uno metaforico o traslato. V. anche Cassese 2001, Lippi 2001.
59 Perulli 1998.
60 Terminologia impiegata dalle stesse Direttive NIS.

tecnici[61], e il concetto, limitrofo, di integrazione decentrata, ove alla contitolarità di una funzione regolatoria tra uffici comunitari e statali corrisponde l'effettiva riconduzione degli stessi ad un'"amministrazione unitaria"[62], principalmente tramite l'istituzione di agenzie europee con compiti di coordinamento.

In questo senso ENISA, centro polifunzionale di un 'sistema a stella'[63] dal quale dipanano diverse reti, ben incarna il fenomeno dell'*agencification* come esercizio congiunto di funzioni europee[64]. Di qui la predilezione, più che per indirizzi atti a vincolare i soggetti statali, per rapporti operativi che concretizzino una "pratica della loro interdipendenza e complementarietà funzionale"[65], ove l'organismo centrale funga da "centro di gestione, elaborazione e condivisione di informazioni a contenuto scientifico particolarmente elevato"[66]. Anche nel settore della cybersicurezza, pertanto, l'integrazione con l'ordinamento europeo supera la vecchia dicotomia (di rilievo meramente funzionale) tra amministrazione diretta e indiretta, confermando il primato dell'organizzazione come principio ordinante per agglomerati di competenze non dipanabili[67] col solo richiamo alle funzioni[68].

5. Il sistema nazionale di cybersicurezza: direzione centrale e operatività diffusa

Anche nel sistema nazionale di cybersicurezza si riconosce un'amministrazione "multiorganizzativa"[69], se non altro per l'evidente condizionamento da parte delle corrispondenti strutture comunitarie, che ad essa delegano compiti e richiedono uffici di collegamento[70]. In "un contesto ispirato al pluralismo istituzionale"[71], la demarcazione delle attribuzioni non ricalca solo la frammentazione concettuale della funzione di sicurezza (anche in questo caso, con cyberdifesa, cybercrimine e *cyberintelligence* distribuiti tra i rispettivi enti)[72], ma attiene al nucleo stesso della resilienza informatica, la cui *governance*, radicalmente rivista su spinta del PNRR[73], ripropone l'"approccio a tre livelli"[74] – tecnico (ACN, CSIRT), operativo (ACN, NCS) e strategico/politico (Presidenza del Consiglio) – dei programmi di coordinamento in sede europea.

61 Cassese 2001.
62 Franchini e Vesperini 2012: 126.
63 Come osserva da ultimo Rossa 2022: 445 s.
64 Chiti 2021.
65 Chiti 2002: 445 ss.
66 Lamberti 2016: 287.
67 Coerentemente alla condizione dello stato contemporaneo, "congiunto organizzato di amministrazioni diverse" per Giannini 1986: 79.
68 Che, nel caso della cybersicurezza, non è espressamente prevista dai Trattati (Chiara 2023 Odermatt 2018, Pauri 2017).
69 Franchini e Vesperini 2012: 86.
70 Franchini – Della Cananea 2010: 163 s.
71 Parona 2021: 6.
72 Si veda la ricostruzione di Serini 2021: 251.
73 Con il d.l. n. 82 del 2021.
74 Raccomandazione (UE) 2017/1584 (c.d. *Blueprint*).

Parimenti valorizzato, pur con le specificità che sempre ne caratterizzano l'impiego all'interno degli ordinamenti statali[75], è il modulo della rete: sia sul piano strettamente operativo, in connessione con l'impianto strategico dell'intero sistema[76] e con l'inedito strumentario collaborativo del 'perimetro nazionale', sia su quello burocratico, da ultimo con l'introduzione di un referente per la cybersicurezza nelle singole amministrazioni[77].

La distanza con gli analoghi sistemi sovranazionali è piuttosto da ricercarsi al cuore degli attributi della sovranità, nella (formale) imputazione e nel (concreto) esercizio dei poteri di decisione politico-amministrativa dello Stato. In questo senso permane, ed è anzi costantemente affinata da un legislatore che persegue la "maggiore concentrazione delle funzioni e delle azioni finalizzate alla prevenzione e al contrasto" delle minacce informatiche[78], la subordinazione dell'intero complesso istituzionale all'"alta direzione" e "responsabilità generale" del Presidente del Consiglio, che la esercita in via diretta o per mezzo di un'agenzia *sui iuris*[79] (ACN) sottoposta a penetranti poteri di controllo[80].

Se alla Presidenza[81], in veste di "super-ministero"[82], sono intestate rilevanti competenze strategiche e un'estesa potestà normativa[83], la cui *ratio* va ricercata nel ruolo di *sedes* istituzionale per l'armonizzazione delle politiche di sicurezza all'indirizzo governativo, l'Agenzia per la cybersicurezza costituisce la vera e propria 'centrale operativa' del sistema, garantendone il quotidiano funzionamento. "Autorità nazionale competente" e "punto di contatto unico" per le finalità di cui alla normativa europea[84], ACN assomma, talora inglobando strutture previgenti[85], le principali funzioni di regolazione, vigilanza, coordinamento operativo e certificazione, beneficiando di un generoso regime di autonomia e di poteri autoritativi corrispondenti a precisi obblighi informativi e di conformazione in capo ai destinatari[86].

L'assetto capillare del sistema viene in tal modo 'ricomposto' e razionalizzato attorno ad un'amministrazione di vertice, la quale unisce ad una costante opera di monitoraggio le concrete capacità per adottare tempestive misure di manutenzione preventiva o risposta difensiva. Ne risulta un'incrementata efficienza decisionale cui, nondimeno, fanno da contraltare criticità di rilievo: da un punto di vista

75 Ielo 2003: 376.
76 Su cui v. Ridolfi 2023.
77 Art. 8 l.n. 90 del 2024 su cui Longo 2024, Pietrangelo 2024.
78 Previti 2022: 92.
79 Ennesimo caso di 'fuga dal modello' normativo di agenzia (Merloni 2005).
80 Art. 2 d.l. n. 82 del 2021.
81 Nonché ai comitati in essa incardinati, ovvero il Comitato interministeriale per la cybersicurezza (CIC) e il Comitato interministeriale per la sicurezza della Repubblica (CISR).
82 Lauro 2021: 545.
83 Su cui Parona 2021.
84 Direttiva (UE) 2022/2555 (NIS 2) e Reg. (UE) 2019/881.
85 È il caso del nucleo per la cybersicurezza (NCS) e del CSIRT Italia, ora ricollocati in seno all'Agenzia.
86 *Ex multis*, Rossa 2023a, Forgione 2022, Golisano 2022, Parona 2021.

operativo, la 'burocratizzazione' dell'impianto sembra progredire a discapito di più agili corpi tecnici[87], mentre la perdurante impostazione securitaria della disciplina solleva questioni di legittimazione democratica ed equilibrio costituzionale. La completa avocazione del settore da parte dell'Esecutivo si risolve nella marginalizzazione *de facto* non solo delle minoranze parlamentari[88], bensì degli stessi operatori, pubblici e privati, che 'collaborano' con l'Agenzia da una posizione di sostanziale (e sanzionata) soggezione[89].

6. Alcune conclusioni. Concorrenza tra modelli, pianificazione strategica e amministrazione integrata

Da una pur sommaria ricostruzione dei suoi assetti strutturali, l'intero processo di emersione dell'ordinamento della cybersicurezza sembra potersi descrivere nei termini di un precario equilibrio tra modelli di regolazione antagonisti, o perlomeno concorrenti, di cui resta traccia nella fondamentale ambiguità delle relative scelte normative[90]: un modello reticolare-cooperativo, facente leva per lo più su soluzioni tecniche e connessioni informali tra strutture prettamente operative, e uno autoritario-accentrato, sulla falsariga degli organi statali investiti di funzioni afferenti alla sicurezza nazionale in senso lato. Le opposte matrici (*rationales*) dei due paradigmi si legano a più radicali concezioni della *governance* digitale, trasponendole nella prassi amministrativa. Si tratta, pertanto, in ultima istanza, di risposte di sistema a fronte delle sfide imposte a caratteri e funzioni della statualità classica[91].

Assodato che "*there is nothing fixed about internet governance arrangements in the same way there is nothing fixed about internet architecture*"[92], e che lo statuto del cyberspazio è ben soggetto ad opzioni ideologiche di fondo[93], il dibattito[94] ha prodotto, da un lato, l'idea di una *governance* distribuita a trazione privata e, dall'altro, la concezione securitaria di una sovranità statale proiettata nel digitale; la prima, fondata su postulati libertari[95], è poi evoluta in un approccio *multi-stakeholder* per la gestione condivisa di problemi globali, mentre la seconda, cercando di circoscrivere uno specifico dominio *cyber* statale e prediligendo il dialogo multilaterale tra i Governi, è parsa contribuire al più complesso fenome-

87 Ruohonen – Hyrynsalmi – Leppänen 2016: 750 ss. Indicativo, in questo senso, è lo *status* dei CSIRT regionali, tuttora di incerta natura e collocazione all'interno dell'architettura nazionale disegnata *ex lege*.

88 Caramaschi 2022, Lauro 2021: *passim.*

89 V. anche i dubbi di Longo 2024, Pietrangelo 2024.

90 Parona 2021: 9.

91 Pohle – Thiel 2020 e Mueller – Schmidt – Kuerbis 2013.

92 Denardis – Goldstein – Gross 2016: 20.

93 Il tema è il qualche misura presente già in Wu 1997.

94 Sul tema v. Natale 2022, Pohle – Thiel 2020, Odermatt 2018, Denardis, – Goldstein – Gross 2016, Liaropoulos 2016.

95 Celeberrima, in tal senso, è la sedicente Dichiarazione di indipendenza del Cyberspazio stesa da Barlow.

no di balcanizzazione della Rete[96]. Posteriore alla prima, la fortuna di quest'ultima prospettiva parte dalla lucida constatazione che "*the necessary authority and relevant resources to manage and regulate a wide range of activities in cyberspace reside largely in certain stakeholders—the states*"[97] e dal concreto assurgere del cyberspazio (comprensivo delle sue fondamentali infrastrutture fisiche) a nuova "dimensione della conflittualità"[98], il cui controllo alimenta tensioni geopolitiche facendone l'ultima frontiera del potere pubblico[99].

È uno sviluppo che ben si comprende alla luce di quel *mix* di conflittualità strategiche, crisi economiche e altri *shock* esogeni che, nell'ultimo quindicennio, ha via via condotto vari settori dell'attività amministrativa a teorizzare, o invocare, il ritorno dello Stato come attore primario della vita economica e sociale: un intervento la cui necessità, nell'ambito della cybersicurezza, non sembra potersi mettere in discussione, rivestendo una vitale funzione di presidio dei diritti dei cittadini-utenti, ma di cui vanno invece discusse le modalità. Si impone infatti l'esigenza irrinunciabile di conciliare con alcune garanzie fondamentali i nuovi paradigmi della sovranità digitale, la cui capacità di condizionare le stesse infrastrutture dell'esistenza sociale li rende potenzialmente più invasivi rispetto alle forme classiche del controllo statale[100]. In questo senso, il (parziale) divorzio della cybersicurezza nazionale dal regime dei servizi d'*intelligence* (che appare non solo incompatibile, ma del tutto antitetico rispetto alle esigenze di pubblicità e diffusione di quella)[101] ha certamente giovato ad una più radicata legittimazione del suo ruolo, ma restano da valutarne la capacità di aggiornamento e di coinvolgimento degli operatori privati[102] che, in un settore ad altissima obsolescenza tecnologica, costituiscono il più sicuro innesto di un'amministrazione efficace.

Traduzione, sul piano operativo, di una connotazione teleologica dell'impianto normativo, che assuma cioè le proprie finalità quale "più intimo significato" delle norme stesse[103], è l'orientamento strategico della conseguente azione amministrativa (come testimoniano i principali documenti d'indirizzo nell'ambito della transizione digitale)[104], fondata, nel caso della cyber-resilienza, sulla difesa dinamica di un ""fortino" degli interessi pubblici rilevanti attraverso un'interrelazione di soggetti preposti"[105] ai diversi livelli di intervento. In questo senso, il ritorno, nel cyberspazio, della politica degli Stati può rendersi un'occasione di sviluppo sinergico per il settore, archiviando il 'falso dilemma' che contrappone

96 Hill 2012.
97 Liaropoulos 2016.
98 Martino 2018.
99 Natale 2022, Denardis – Goldstein – Gross 2016.
100 È l'ammonimento di Pohle – Thiel 2020.
101 Sul tema Previti 2022: 81 ss., Sola 2022: 399 ss., Parona 2021: 8 s.
102 Longo 2024, Poletti 2023, Lauro 2021, Romano 2021.
103 Di Gaspare 1995.
104 Così, tra i molti esempi le citate strategie europee e nazionali per la cybersicurezza, ma anche la recentissima *Strategia italiana per l'intelligenza artificiale 2024-2026*.
105 Forgione 2022.

amministrazione aperta ed efficienza degli apparati[106]; a fronte di un cronico analfabetismo digitale, principale falla di qualsiasi sistema di cybersicurezza[107], la partecipazione amministrativa garantisce la diffusione circolare di cultura informatica a beneficio di tutti i soggetti coinvolti, siano essi funzionari pubblici, operatori economici, o cittadini-utenti.

A tal fine la "poliarchia"[108], che si realizza nella dispersione della funzione tra livelli e settori concorrenti all'interno di ordinamenti plurali, chiama in causa la capacità ordinante dell'organizzazione quale principio relazionale: "*un principe qui maintienne la distinction, mais qui essaie d'établir la relation*"[109], mappando l'attribuzione di un potere diffuso e ricomponendo l'amministrazione in funzione della collettività[110], con la doverosa consapevolezza "*que l'ordre ne signifie pas seulement les lois, mais aussi les stabilités, les régularités, les cycles organisateurs, et que le désordre n'est pas seulement la dispersion, la désintégration, ce peut être aussi le tamponnement, les collisions, les irrégularités*"[111]. Dalla risultante aggregazione dipenderà una più chiara definizione dell'ambito funzionale (nonché della relativa finalità), ma soprattutto l'effettiva possibilità del suo corretto perseguimento, assurgendo il modello organizzativo a componente essenziale dell'azione stessa di cybersicurezza nazionale: una funzione finalizzata al consolidamento della sovranità digitale, che, promuovendo l'adesione di cittadini e imprese agli obiettivi di sicurezza condivisa, ne assicuri al contempo una tutela diffusa.

Bibliografia

Bachelet, V. 1965, *Profili giuridici dell'organizzazione amministrativa*, Milano: Giuffrè.

Backman, S. 2023, "Risk vs. threat-based cybersecurity: the case of the EU", *European Security*, 32 (1): 85-103.

Battini, S. 2008, "Le due anime del diritto amministrativo globale", in AA. VV., *Il diritto amministrativo globale oltre i confini*, Milano: Giuffrè.

Battini S. 2016, "I due grandi dualismi alla prova del diritto (amministrativo) globale", in G. A. Benacchio – M. Graziadei, *Il declino della distinzione tra diritto pubblico e diritto privato*, Napoli: Editoriale Scientifica: 101-131.

Berti, G. 1968, *La pubblica amministrazione come organizzazione*, Padova: CEDAM.

Bower, J. L. – C. M. Christensen 1995 "Disruptive Technologies: Catching the Wave.", *Harvard Business Review*, 73 (1): 43-53.

Caramaschi, O. 2022, "La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari", *Osservatorio costituzionale*, 4: 69 ss.

Carbone, A. 2024, "Considerazioni generali sull'organizzazione amministrativa", *Federalismi.it*, 17: 25-63.

106 Come avviene in altri settori: Galli 2023.
107 Longo 2024, Rossa 2023b, Romano 2021, Montessoro 2019.
108 Dahl 1971.
109 Morin 2005: 4.
110 Franchini e Vesperini 2012.
111 Morin 2005: 4.

Cassese, S. 2001, "Le reti come figura organizzativa della collaborazione", in A. Predieri – M. Morisi (a cura di), *L'Europa delle reti*, Torino: Giappichelli: 43-48.
Cassese, S. 2002, "La signoria comunitaria sul diritto amministrativo", *Rivista italiana di diritto pubblico comunitario*, 2-3: 291-301.
Cassese, S. 2005, "Il diritto amministrativo globale. Una introduzione", *Rivista trimestrale di diritto pubblico*, 2: 331-357.
Chiara, p. G. 2023, "Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali", *Rivista italiana di informatica e diritto*, 1: 143 ss.
Chiti, E. 2002, *Le agenzie europee. Unità e decentramento nelle amministrazioni comunitarie*, Padova: Cedam.
Chiti, E. 2016, "Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia e di difesa", *Diritto amministrativo*: 511 ss.
Chiti, E. 2021, "The Agencification Process and the Evolution of the EU Administrative System", in p. Craig – G. de Búrca (eds.), *The Evolution of EU Law*, Oxford: Oxford University Press: 123-155.
Chiti, M. p. , 2007, "L'organizzazione amministrativa comunitaria", in AA. VV. *Trattato di diritto amministrativo europeo*, Milano: Giuffrè: 415-466.
Contaldo, A. – F. Peluso 2018, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa: Pacini Giuridica.
D'Alberti, M. 2013, *Lezioni di diritto amministrativo*, Torino: Giappichelli.
Dahl, R. 1971, *Polyarchy: participation and opposition*, New Haven: Yale University Press.
Della Cananea, G. 2009, *Al di là dei confini statuali. Principi generali del diritto pubblico globale*, Bologna: Il Mulino.
Denardis, L. – Goldstein, G. – Gross, D. A. 2016, "The Rising Geopolitics of Internet Governance. Cyber Sovereignty V. Distributed Governance", Tech & Policy Initiative, Columbia SIPA.
Di Gaspare, G. 1995, voce "Organizzazione amministrativa", *Dig. disc. Pubbl*, X, Torino: Utet giuridica: 513 ss.
Eckhardt, Ph – Kotovskaia, A. 2023, "The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive", *International Cybersecurity Law Review*, 4: 147 ss.
Forgione, I. 2022, "Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", *Diritto amministrativo*, 4: 1113 ss.
Franchini, C. e Della Cananea, G. 2010, *I principi dell'amministrazione europea*, Torino: Giappichelli.
Franchini, C. e Vesperini, G. 2012, "L'organizzazione", in S. Cassese, (a cura di), *Istituzioni di diritto amministrativo*, Milano: Giuffrè: 73-130.
Frediani, E. 2010*, La produzione normativa nella sovranità "orizzontale"*, Pisa: ETS.
Galli, F. 2023, "Ambiente, amministrazione e democrazia. Sulla nuova relazione pubblico-privato nel sistema di diritto ambientale, tra etica partecipativa ed esercizio di sovranità", *Rivista Quadrimestrale di Diritto dell'Ambiente*, 3: 4-36.
Gasparri, W. 2024, *Lezioni di diritto amministrativo*, II, Torino: Giappichelli.
Giannini, M. S. 1957, "In principio sono le funzioni", *Amministrazione civile*, 1, 11 ss..
Giannini, M. S. 1986, *Il potere pubblico. Stati e amministrazioni pubbliche*, Bologna: Il Mulino.
Golisano, L. 2022, "Il governo del digitale: strutture di governo e innovazione digitale", *Giornale di diritto amministrativo*, 6: 824 ss.

Guarino, G. 1970, "Sulla utilizzazione di modelli differenziati nella organizzazione pubblica", in Id., *Scritti di diritto pubblico dell'economia*, Milano: Giuffrè.
Guarino, G. 1977, *L'organizzazione pubblica*, Milano: Giuffrè.
Hart, H. L. A. 1958, "Positivism and the Separation of Law and Morals", *Harvard Law Review*, 71: 593-629.
Hill, J. F. 2012, "A Balkanized Internet?: The Uncertain Future of Global Internet Standards", *Georgetown Journal of International Affairs*, 49-58.
Honneth, A. 2002 (1992), *La lotta per il riconoscimento*, Milano: Il Saggiatore.

Ielo, D. 2003, "Amministrazioni a rete e reti di amministrazione: nuovi paradigmi della "global governance"", *Amministrare*, 3: 373-403.
Irti, N. 1968, voce "Rilevanza giuridica", *Noviss. Dig. It*, XV, Torino: Utet: 1094 ss.
Lamberti L. – G. A. Primerano, 2016, "Il principio di efficienza ed i modelli organizzativi: le agenzie amministrative" in R. Cavallo Perin – A. Police – F. Saitta, *L'organizzazione delle pubbliche amministrazioni tra Stato nazionale e integrazione europea*, Firenze: University Press: 283 ss.
Lauro, A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", *Rivista Gruppo di Pisa*, 3: 529-545.
Liaropoulos, A. 2016, "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics", *Journal of Information Warfare*, 4: 14 ss.
Lippi, A. 2001, "Il policy making europeo come "rete"", in A. Predieri – M. Morisi (a cura di), *L'Europa delle reti*, Torino: Giappichelli: 1 ss.
Longo, E. 2024, "Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)", *Rivista italiana di informatica e diritto*, 1: 65-70.
Martino, L. 2018, "La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale", *Politica & Società*, 1: 61-76.
Matassa, M. 2022, "Una strategia nazionale a difesa del Cyberspazio", *p. A. Persona e Amministrazione*, 2: 625-653.
Merloni, F. 2005, "Le agenzie a cinque anni dal d.lgs. n. 300: l'abbandono del modello generale?", in G. Vesperini (a cura di), *La riforma dell'amministrazione centrale*, Milano: Giuffrè: 21 ss.
Merloni, F., "Organizzazione amministrativa e garanzie dell'imparzialità", *Diritto Pubblico*, 1: 57-100
Montessoro, p. L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", *Istituzioni del federalismo*, 3: 783 ss.
Morin, E. 2005, "Complexité restreinte, complexité générale", Colloque "Intelligence de la complexité: épistémologie et pragmatique" (Cerisy-La-Salle).
Mueller, M. – A. Schmidt – B. Kuerbis 2013, "Internet security and networked governance in international relations", *International Studies Review*, 15(1): 86-104.
Natale, G. 2022, "La cybersicurezza nazionale: la nuova frontiera della difesa dello Stato", *Rassegna Avvocatura dello Stato*, 1.
Nigro, M. 1966, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano: Giuffrè.
Nigro, M. 1988, voce "Amministrazione pubblica (Organizzazione giuridica dell')", *Enciclopedia Giuridica*, II, Roma: Treccani.

Odermatt, J. 2018, "The European Union as a Cybersecurity Actor", in: S. Blockmans – p. Koutrakos, (eds.), *Research Handbook on EU Common Foreign and Security Policy*, Cheltenham: Edward Elgar: 354-373.
OECD 2002, *Distributed Public Governance: Agencies, Authorities and other Government Bodies*, Paris: OECD Publishing, disponibile a https://doi.org/10.1787/9789264177420-en
Paleologo, G. 1981, voce "Organizzazione amministrativa", *Enciclopedia del diritto*, XXXI, Milano: Giuffrè: 135-151.
Parona, L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", *Giornale di diritto amministrativo*, 6: 709 ss.
Pauri, E. 2017, "Agency Reform in the time of Cybersecurity Governance: ENISA", *Luiss Law Review*, 2: 95 ss.
Perulli, p. 1998, "Forma Stato e forma rete", in Id., *Neoregionalismo. L'economia arcipelago*, Torino: Bollati Boringhieri.
Pietrangelo, M. 2024, "Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa", *Rivista italiana di informatica e diritto*, 1: 25-29.
Pohle, J. – T. Thiel 2020, "Digital sovereignty", *Internet Policy Review*, 9 (4).
Poletti, S. 2023, "La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica", *Media Laws*, 2: 398-410.
Previti, L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *Federalismi.it*: 65 ss.
Radoniewicz, F. 2022, "Cybersecurity in the European Union Law", in K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, (eds) *Cybersecurity in Poland*, Cham: Springer: 73-92.
Ridolfi, M. 2023, "Servizi di informazione e cybersicurezza", *Giornale di diritto amministrativo*, 2: 207 ss.
Romano, B. N., 2021, "Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"", *Amministrativamente*, 3: 545-594.
Romano, S. 1909, *Lo stato moderno e la sua crisi*, Pisa: Vannucchi.
Rossa, S. 2022, "Administrative Law Reflections on Cybersecurity, and on its Institutional Actors, in the European Union and Italy", *Italian Journal of Public Law*, 14 (2): 426-450.
Rossa, S. 2023a, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale Scientifica.
Rossa, S. 2023b, "Cyber attacchi e incidenti nella pubblica amministrazione, fra organizzazione amministrativa e condotta del funzionario", *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio III*, 17: 161-175.
Rossi, G. 2005, *Diritto Amministrativo*, I, Milano: Giuffrè.
Ruohonen, J. – S. Hyrynsalmi – V. Leppänen, 2016, "An outlook on the institutional evolution of the European Union cyber security apparatus", *Government Information Quarterly*, 33 (4): 746-756.
Serini, F. 2021, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", *Federalismi.it*, 12: 241 ss.
Slack, C. 2016, "Wired yet disconnected: the governance of international cyber relations", *Global Policy*, 7 (1): 69-78.
Sola, A. 2022, "Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale", *MediaLaws*, 3: 386 ss.
Wu, T. S. 1997, "Cyberspace Sovereignty? – The Internet and The International System", *Harvard Journal of Law & Technology*, 3: 647 ss.

Massimiliano Malvicini

Appunti sull'evoluzione dell'architettura strategica nazionale in materia di sicurezza cibernetica e sugli spazi di intervento del Parlamento

Abstract: Lo scritto indaga l'evoluzione della governance nazionale della cybersecurity nel contesto giuridico italiano. Nel farlo, il lavoro si concentra sui poteri e le competenze attribuite al Presidente del Consiglio dei Ministri e alle autorità amministrative italiane negli ultimi decenni; successivamente, analizza il controllo parlamentare sui temi della cybersecurity negli anni recenti.

Keywords: Cybersecurity; Presidente del Consiglio dei Ministri; Parlamento; Agenzia per la Cybersicurezza Nazionale; Diritto pubblico italiano.

1. Premessa

La regolamentazione della sicurezza cibernetica è un fenomeno di grande interesse sotto diversi punti di vista[1]. Volendoci limitare all'ambito costituzionalistico, tramite di essa non solo si arricchisce l''intarsio' tra le diverse fonti recanti principi e regole in materia (tra livello nazionale e europeo)[2], ma – inevitabilmente – si altera anche la cornice entro cui si sviluppano i rapporti fra gli organi al vertice dell'ordinamento (la forma di governo) e le relazioni tra questi e i consociati (la forma di Stato, intesa quale declinazione delle interconnessioni tra la sfera dell'autorità e quella della libertà).

Data l'ampiezza del fenomeno in discussione, di seguito si approfondirà, mediante un approccio giuspubblicistico, l'evoluzione dei rapporti fra il nostro Go-

1 Per un inquadramento generale del concetto di cybersecurity ancora molto utile l'analisi di Schatz, Bashroush, Wall 2017. Sulla definizione di sicurezza in prospettiva costituzionalistica v. Giupponi, 2023 e 2022, Ursi, 2022; De Vergottini 2019; Pace, 2014. Sull'inquadramento della cybersecurity nell'ambito delle tradizionali funzioni statali v. Ursi 2023; Vigneri 2023; Scognamillo 2023. In generale, sul rapporto tra cybersecurity e ordinamento giuridico italiano cfr. Rossa 2023: 9-64; Lotta 2024, 173-184; Buoso 2023; Previti 2022; Gaggero, Berruti 2022; Lauro 2021; Renzi 2021; Contaldo, Mula 2020; Montessoro 2019.

2 Su cui, di recente, v. la ricostruzione di Moroni 2024. In generale v. Salvaggio, Gonzales 2023.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760149

verno e il Parlamento in materia di sicurezza cibernetica. In tal senso, il lavoro si soffermerà dapprima sulle coordinate normative che nel nostro ordinamento definiscono poteri, competenze e responsabilità in questa sfera, per poi mettere a fuoco la prassi che negli ultimi anni ha contraddistinto i rapporti fra assise legislativa e organi governativi.

2. Le coordinate istituzionali: l'assetto dei poteri e delle competenze in materia di sicurezza cibernetica

In termini generali, l'attuale quadro ordinamentale in materia di sicurezza cibernetica – ciò a cui ci si riferisce abitualmente come 'l'architettura strategica nazionale' – è il risultato di una stratificazione normativa realizzatasi nel corso di oltre un decennio.

Il primo intervento in materia risale alla legge 7 agosto 2012, n. 133, recante "Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto"[3], la quale intervenne in questo ambito conferendo nuove competenze al Presidente del Consiglio, al Comitato interministeriale per la sicurezza della Repubblica (CISR) e al Dipartimento delle informazioni per la sicurezza (DIS).

In quell'occasione si stabilì che il Presidente del Consiglio dei Ministri[4], sentito il CISR, avrebbe potuto impartire direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale (art. 1). D'altro canto, sulla base delle direttive del Presidente, e in virtù delle informazioni e dei rapporti provenienti dai servizi di intelligence, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati, il DIS avrebbe dovuto coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali (art. 3); infine, il Governo avrebbe avuto l'incarico di allegare alla relazione al Parlamento il "documento di sicurezza nazionale" che avrebbe dovuto contenere non solo un riferimento attività relative alla protezione delle infrastrutture critiche materiali e immateriali ma anche l'indicazione delle azioni volte alla "protezione cibernetica e alla sicurezza informatica" (art. 9).

Di là da questo primo intervento, la definizione delle vere e proprie coordinate istituzionali in materia risale al 24 gennaio 2013, data di approvazione del DPCM recante la direttiva sugli "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" (cd. "decreto Monti").

In termini di politica del diritto, anche allora si scelse di arricchire le competenze del sistema di intelligence, facendo aggio sul compito di salvaguardia del Paese

3 Su cui cfr. Scaccia 2012.

4 Sul ruolo del Presidente del Consiglio dei Ministri nell'ordinamento italiano cfr., da prospettive diverse, Cassese, Melloni, Pajno 2022; Teodoldi 2019; Ciolli 2018.

da pericoli e minacce provenienti sia dall'interno sia dall'esterno, riprendendo il fraseggio della legge 124 del 2007[5].

Così, il DPCM 24 gennaio 2013 individuò nella Presidenza del Consiglio dei Ministri il vertice dell'architettura nazionale in materia di sicurezza cibernetica. Al Presidente del Consiglio fu affidato il potere di adottare: a) il quadro strategico nazionale per la sicurezza dello spazio cibernetico, entro il quale andavano indicati profili e tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, ma anche la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati; b) su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, contenente obiettivi da conseguire e linee di azione da porre in essere per realizzare il quadro strategico nazionale, emana le direttive e gli atti d'indirizzo necessari per la sua attuazione; nella stessa prospettiva, al Presidente era conferito anche il potere di impartire, sentito il CISR, le direttive al DIS e alle Agenzie (*i.e.* l'Agenzia informazioni e sicurezza interna – l'AISI e l'Agenzia informazioni e sicurezza esterna – AISE) ai sensi dell'art. 1, comma 3-bis, della legge n. 124/2007.

Parallelamente, fu potenziato il ruolo del Comitato interministeriale per la sicurezza della Repubblica, affidando a esso alcuni poteri specifici: sorvegliare sull'applicazione del Piano nazionale per la sicurezza dello spazio cibernetico; esprimere pareri sulle direttive del Presidente del Consiglio; approvare specifiche linee d'indirizzo per favorire la collaborazione tra soggetti istituzionali e operatori privati interessati alla sicurezza cibernetica; elaborare indirizzi generali e obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali da perseguire nel quadro della politica dell'informazione per la sicurezza della Repubblica.

Ora, benché, nel disegno di questo DPCM venisse conferita al DIS, all'AISI e all'AISE la funzione di salvaguardare la protezione cibernetica e la sicurezza informatica nazionali tramite l'esercizio di "attività di ricerca e di elaborazione informativa", al cuore del sistema era collocato il Nucleo per la sicurezza cibernetica (NSC), istituito presso il Consigliere militare del Presidente del Consiglio. Presieduto dal Consigliere militare e composto, fra gli altri, dai rappresentanti del DIS, dell'AISE, dell'AISI, del Ministero degli Affari esteri, del Ministero dell'Interno, del Ministero della Difesa, del Ministero dello Sviluppo economico, al Nucleo erano affidate funzioni strumentali a supporto del Presidente del Consiglio in materia di prevenzione e preparazione a situazioni di crisi e per l'attivazione delle procedure di allertamento. Con ciò si costituì altresì il punto di riferimento nazionale per i rapporti con ONU, NATO, UE, altre organizzazioni internazionali e gli altri Stati. Così, al Nucleo fu attribuito il compito di raccordare le varie componenti coinvolte nella salvaguardia della sicurezza cibernetica, ma anche quello di programmare e pianificare le risposte a situazioni di crisi, nonché di promuovere la condivisione di informazioni tra le amministrazioni competenti e tra gli operatori

5 Su cui, cfr. Giupponi 2010; Mosca, Gambacurta, Scandone, Valentini 2008. In prospettiva più ampia si veda altresì Valentini 2017.

privati interessati. Ciò anche al fine della gestione delle crisi e della diffusione di allarmi su eventi cibernetici.

Nel corso degli anni successivi, l'architettura recata dal decreto Monti è stata oggetto di alcuni intenti riformatori. In un primo momento, attraverso l'emanazione del DPCM 1° agosto 2015 (cd. "direttiva Renzi"), venne evidenziata la necessità di consolidare un sistema di reazione efficiente, capace di raccordare le capacità di risposta delle singole Amministrazioni, al fine di assicurare la resilienza dell'infrastruttura informatica nazionale. Per raggiungere questo obiettivo venne indicato come necessario: a) favorire un maggior coordinamento e una più ampia integrazione delle funzioni dei diversi soggetti pubblici, tenendo conto che il quadro di competenze rimane ancora frammentato sotto il profilo legislativo; b) realizzare un maggior sviluppo delle relazioni con il settore privato, mediante un capillare partenariato con tutti gli operatori non pubblici a cui è affidato il controllo di infrastrutture informatiche e telematiche.

Proprio in ottica di coordinamento inter-istituzionale il DPCM evidenziava la necessità che esso si sarebbe dovuto realizzare, a livello centrale, nell'ambito dell'attività degli Organismi di informazione per la sicurezza, ribadendo il ruolo del DIS nell'assicurare la piena unitarietà nella programmazione della ricerca informativa e nel rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Successivamente, la razionalizzazione della governance in materia di cibersicurezza si è perfezionata mediante l'approvazione del Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017 (recante la "Direttiva in materia protezione cibernetica e sicurezza informatica nazionali", il cd. 'Decreto Gentiloni').

In quell'occasione, accanto all'esplicito riconoscimento dell'alta direzione e della responsabilità della politica generale del Governo anche nel campo della cybersecurity, al Presidente del Consiglio vennero attribuite specifiche competenze per far fronte agli scenari di crisi nazionale, sulla scia di quanto disposto dal decreto-legge 30 ottobre 2015, n. 174, in materia di servizi d'intelligence (convertito dalla legge 11 dicembre 2015, n. 198)[6]. Parallelamente, modificando l'impostazione del 'DPCM Monti' accogliendo le linee programmatiche espresse dalla 'direttiva Renzi', si sono potenziate le attribuzioni del DIS, affidando al suo direttore generale il compito di definire le necessarie linee di azione per innalzare i livelli di sicurezza dei sistemi e delle reti (verificandone ed eliminandone le vulnerabilità), ed incardinando al suo interno il Nucleo per la Sicurezza Cibernetica (presieduto da un vicedirettore generale del Dipartimento, su delega del direttore generale) con il compito di elaborare una risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei ministeri competenti in materia.

A un anno di distanza, in attuazione della direttiva (UE) 2016/1148 (c.d. direttiva NIS 1 – Network and Information Security) – il cui obiettivo era stabilire misure per uno standard comune elevato di sicurezza delle reti e dei sistemi informativi

6 Sul punto, volendo, Malvicini 2016.

nell'Unione al fine di aumentare il livello di collaborazione nella prevenzione alle minacce cibernetiche[7] – è intervenuto il decreto legislativo 18 maggio 2018, n. 65 che, fra l'altro, ha attribuito al Presidente del Consiglio la competenza alla definizione della strategia nazionale di sicurezza cibernetica per la tutela delle reti e dei sistemi di interesse nazionale (sentito il CISR).

Un ampliamento delle attribuzioni governative si è inoltre registrato a distanza di qualche mese, a seguito dell'approvazione del decreto-legge 21 settembre 2019, n. 105 (il c.d. 'decreto perimetro')[8]. In particolare, tramite questo atto si è attribuito al Presidente del Consiglio uno specifico potere di ordinanza in materia di cibersicurezza[9]. Nello specifico, in presenza di un "rischio grave e imminente" per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente può disporre, ove indispensabile e per il tempo strettamente necessario all'eliminazione "dello specifico fattore di rischio o alla sua mitigazione", in deroga a ogni disposizione vigente, ma nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, la disattivazione, anche totale, "di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati" (art. 5, c. 1). Entro trenta giorni dall'esercizio di questo potere, il Presidente del Consiglio deve informare il COPASIR delle misure disposte.

Più di recente, anche in attuazione del PNRR[10], l'"architettura italiana" di sicurezza cibernetica è stata oggetto di ulteriori interventi.

In particolare, tramite il d.l. 14 giugno 2021, n. 82 (convertito con modificazioni dalla l. 4 agosto 2021, n. 109)[11] si sono trasposte, coordinandole e razionalizzandole, le innovazioni susseguitesi nel corso dell'ultimo decennio. Nel perfezionare tale passaggio il legislatore ha confermato l'attribuzione al Presidente del Consiglio dei Ministri dell'alta direzione e della responsabilità generale delle politiche di cibersicurezza (art. 2, c. 1), quest'ultima intesa come insieme delle attività "necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico" (art. 1, c. 1). Così, al Presidente spettano l'adozione della strategia nazionale di cibersicurezza e il potere di impartire le direttive per attuarla; nel contempo, egli emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia (art. 2, c. 2). Nell'esercizio delle sue attribuzioni, egli è ora affiancato dal Comitato Interministeriale per la Cybersicurezza (CIC), che presiede, al quale è conferito il compito di proporre gli indirizzi generali da perseguire nel quadro delle politi-

7 Sulle iniziative europee e il loro intreccio con l'ordinamento italiano cfr. Moroni 2024: 185 ss; Matassa 2023; Contaldo, Salandri 2020; Peluso 2020; Salamo 2017.

8 Su cui v. Calandriello 2023.

9 Sul potere di ordinanza v. ex multis Cavino, 2021.

10 Sul Piano Nazionale di Ripresa e Resilienza italiano cfr., da prospettive diverse, e in termini generali: Bartolucci 2024; De Lungo, Marini 2023; Casalone, Sciortino, Massa Pinto 2023.

11 Su cui cfr. Serini 2022.

che di cibersicurezza nazionale, e di realizzare "l'alta sorveglianza" sull'attuazione della strategia nazionale (art. 5, c. 2). Il CIC è composto dall'Autorità delegata (se istituita), dal ministro degli Affari esteri e della Cooperazione internazionale, dal ministro dell'Interno, dal ministro della Giustizia, dal ministro della Difesa, dal ministro dell'Economia e delle Finanze, dal ministro dello Sviluppo economico, dal ministro della Transizione ecologica, dal ministro dell'Università e della Ricerca, dal ministro delegato per l'Innovazione tecnologica e la Transizione digitale e dal ministro delle Infrastrutture e della Mobilità sostenibili (art. 4, c. 3).

Parallelamente, il legislatore ha istituito un apposito ente con specifiche competenze nell'ambito in esame: l'Agenzia per la cybersicurezza nazionale (ACN)[12]. In particolare, l'ACN, il cui direttore generale è nominato dal Presidente del Consiglio, assicura il coordinamento fra i soggetti pubblici coinvolti in materia di cibersicurezza, promuovendo una maggiore tutela e resilienza rispetto alle minacce cibernetiche, spettando a essa ogni competenza in fatto di già attribuita dalle disposizioni vigenti alle strutture preesistenti (i.e. Ministero dello sviluppo economico, Presidenza del Consiglio dei Ministri; DIS, Agenzia per l'Italia Digitale). In tal senso, l'Agenzia ha il compito di predisporre la strategia nazionale di cybersicurezza, oltre che di determinare i livelli minimi di capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione e di definizione dei parametri di qualità, performance, scalabilità, interoperabilità e portabilità dei servizi cloud per la p. A.

Inoltre, all'ACN spettano altri due compiti cruciali: a) sviluppare le capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire attacchi informatici e incidenti di sicurezza informatica, anche promuovendo iniziative di partenariato pubblico-privato, ma coordinando altresì la cooperazione internazionale in tale materia; b) promuovere la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cibersicurezza, tenendo anche conto di orientamenti e sviluppi in ambito internazionale (a tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari in questa materia).

Coerentemente con tale impostazione, è istituito presso l'Agenzia il Nucleo per la Cybersicurezza (NCS), a supporto del Presidente del Consiglio dei ministri in questo ambito (la cui composizione riprende, pur con qualche variazione, quella dell'originario Nucleo per la Sicurezza Cibernetica istituito nel 2013 e, dal 2017, transitato sotto l'egida del DIS).

Nel complesso, dinanzi agli interventi susseguitisi nel corso di un decennio, è possibile affermare che il legislatore ha optato per la definizione di una *governance* nazionale della cibersicurezza contraddistinta dall'attribuzione di ampi compiti di direzione e coordinamento alle amministrazioni nazionali e, rispetto ad esse, soprattutto alle strutture serventi la Presidenza del Consiglio dei Ministri (con ciò, contribuendo ad un rafforzamento delle attribuzioni di

12 Su cui cfr. Forgione 2023; Cusenza 2023; Parona 2021. Sulla specificità dell'ACN cfr. Rossa 2023: 91 ss., spec. 94-95.

programmazione e alta amministrazione del Governo, attribuendo, al più, alle Camere uno spazio di controllo).

A questo esito ha contribuito senz'altro la natura delle problematiche concernenti la cibersicurezza, anche considerando la sua attitudine ad intrecciarsi profondamente (e immediatamente) anzitutto con la sicurezza nazionale[13], la quale ha influito anche sulla scelta di valorizzare, entro l'ambito governativo, la Presidenza del Consiglio dei ministri (in questa sede ritenuta come legittima). Infatti, come afferma Giupponi:

> alla luce della sua natura strategica e trasversale, non stupisce che la responsabilità politica venga affidata alla Presidenza del Consiglio dei ministri, nell'ambito della sua tradizionale funzione di direzione della politica generale del Governo, *ex* art. 95 Cost. Tuttavia, si tratta di un ambito che richiede elevate competenze di natura tecnica, capacità di coordinamento e rapidità di intervento, anche alla luce dell'aumento esponenziale del rischio delle minacce in ambiente cyber cui si è assistito negli ultimi anni, anche attraverso l'utilizzo di veri e propri strumenti di natura ibrida.[14]

Del pari, proprio in virtù del dato normativo, la Presidenza del Consiglio sembra giocare un ruolo mutevole[15], in alcuni casi inserendosi in schemi procedimentali contraddistinti da una collegialità delle scelte di Governo, altri in cui a risultare predominante è l'assunzione di responsabilità del solo Presidente del Consiglio. Ciò vale non solo nell'assunzione delle scelte di carattere organizzativo o strategico in materia di cibersicurezza, ma anche nell'esercizio dei poteri di normativi e/o amministrativi in casi di emergenza. Al fianco della decretazione d'urgenza (la quale, come noto, presuppone un coinvolgimento del Consiglio e implica il necessario coinvolgimento del Parlamento nella fase di conversione), si sommano gli strumenti previsti più di recente, i quali – pur non occultando del tutto il principio collegiale – fanno aggio sulla capacità decisionale del Premier (ciò vale, in parti-

13 A onor del vero, ci si potrebbe chiedere se questa sfera, radicata nell'area ricompresa, quantomeno, tra l'art. 117, c. 2, lettere 'd' Cost. (difesa e sicurezza dello Stato) e lettera 'h' (ordine pubblico e sicurezza), non rappresenti un esempio, paradigmatico, di materia 'trasversale', in quanto suscettibile di riguardare altre materie e interessi pubblici di spettanza dello Stato (*e.g.* si pensi ai politica estera e rapporti internazionali; all'organizzazione amministrativa dello Stato e degli enti pubblici nazionali; alla cittadinanza e le anagrafi) e delle Regioni (per limitarci agli ambiti di competenza concorrente, si pensi alla ricerca scientifica e tecnologica; alla tutela della salute; al governo del territorio; alla gestione di porti e aeroporti civili e delle grandi reti di trasporto e di navigazione, ma anche alla produzione, trasporto e distribuzione nazionale dell'energia) e – alla luce di ciò – quali conseguenze ciò comporti rispetto agli spazi di intervento delle altre amministrazioni e soggetti di cui si compone la Repubblica. Un profilo, questo di indubbio interesse, anche considerando i profili di coordinamento inter-istituzionale ad esso connesso (*in primis*, quello dell'eventuale coinvolgimento degli enti regionali e degli altri enti territoriali considerati non solo quali terminali delle scelte compiute dallo Stato in materia di ordine pubblico e sicurezza, ma anche come portatori di interessi che, ancorché non direttamente afferenti alla materia *de qua,* Cost., siano teleologicamente connessi alla competenza esclusiva dello Stato, senza però dimenticare l'importanza degli operatori privati e le istituzioni sovranazionali).

14 Giupponi 2024: 295.

15 Giupponi 2024.

colar modo, per il potere *ex* art. 5 del d.l. 105/2019, la cui competenza spetta al Presidente del Consiglio, previa deliberazione del Comitato interministeriale per la Sicurezza della Repubblica)[16].

3. (segue) I principali interventi del Parlamento

Ora, premesso che l'attuale assetto della *governance* della cybersecurity si caratterizza per una concentrazione di competenze di indirizzo e programmazione in capo al Presidente del Consiglio e all'ACN, è interessante provare a determinare quali sono le principali coordinate entro cui si può sviluppare l'azione del Parlamento.

Ora, posto che il dato normativo sancisce un assetto di competenze per il quale l'indirizzo sulla materia *de quo* è attribuito al Governo e, nello specifico, al Presidente del Consiglio dei ministri (ad esso spetta l'adozione della strategia nazionale di cibersicurezza e il potere di impartire le direttive per attuarla, art. 2, d.l. 82/2021), lo spazio che, attualmente, sembra residuare alle Camere è quello del controllo politico[17]. Per chiarire meglio questo profilo può essere

16 Un profilo di particolare interesse – al quale in questa sede si può solo accennare – riguarda l'opportunità della previsione di uno specifico potere di ordinanza in materia di cibersicurezza a (parziale) integrazione della generale potestà legislativa nella forma della decretazione d'urgenza. Ora, posto che dinanzi ad un "rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi facenti parte del perimetro di sicurezza nazionale" la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati da parte del Presidente del Consiglio sembra iscriversi all'esercizio di un potere riconducibile più alla cura concreta e attuale degli interessi pubblici (il provvedere) che non alla predisposizione di una disciplina generale (il predisporre), il riconoscimento del potere di ordinanza finalizzato a questo scopo non sembra risultare inopportuno (anche considerando come esso rispetti il principio di legalità sostanziale, data la determinazione del contenuto e delle modalità di esercizio – su questi profili v., *ex multis*, Corte cost. sent. 115/2011).

Ciò posto, anche alla luce di quanto appena affermato, va comunque detto che la risposta (in termini giuridico-costituzionali) all'interrogativo di apertura dipende, da un lato, dal tipo di bene/interesse che si vuole proteggere e, dall'altro, dalla minaccia che incombe (del resto, lo stesso potere di ordinanza incontra dei limiti rispetto alle materie coperte da riserva di legge: nei casi di riserva assoluta esso non è ammesso – lasciando così spazio alla sola decretazione d'urgenza –, mentre nel caso della riserva relativa di legge l'attribuzione del potere di ordinanza è ammissibile purché delimitato nel suo esercizio così da orientare, anche in modo non dettagliato, l'adozione dei provvedimenti urgenti; sul punto v. Corte cost. sent. n. 115 del 2011).

17 Dal punto di vista generale, la valorizzazione dei poteri di indirizzo del Governo nei confronti del Parlamento si colloca in linea di continuità rispetto a quanto avvenuto con riguardo ai servizi di intelligence (ma in linea di discontinuità rispetto ad altri ambiti, come evidenziato in Malvicini 2022, 221-261). A questo esito contribuisce, molto probabilmente, non solo la tecnicità della materia e la capacità del solo Governo a tutelare adeguatamente, nei tempi e nei modi, gli interessi preminenti dell'ordinamento, ma anche la cultura organizzativa (e costituzionale) delle varie componenti dell'assise parlamentare, a partire da quelle maggioritarie, dalla quale potrebbe scaturire una preferenza, in termini di politica del diritto, verso opzioni normative volte a istituzionalizzare un assetto di poteri/competenze

utile individuare quali sono le principali figure tramite cui l'assise rappresentativa può esercitare questa attività, intesa quale "riesame compiut[o] da un soggetto od organo (le Camere) nei confronti di un altro soggetto od organo (il Governo) al fine di verificare e garantire la corrispondenza del comportamento del soggetto od organo controllato ai canoni normativi che tale comportamento disciplinano"[18].

Nel fare ciò, occorre considerare almeno due variabili: da un lato, la presenza, in capo agli organi di indirizzo, di un obbligo di ostensione della loro attività alle Camere (o loro organi, anche ausiliari), valutando come tale eventuale onere possa articolarsi nelle sue varie dimensioni. Considerando questa variabile, possiamo analizzare l'ampia ed eterogenea fenomenologia delle figure di verificazione identificando quelle a maggiore istituzionalizzazione, ossia le ipotesi in cui il Governo è tenuto a sottoporre, spesso periodicamente, la propria attività alle Camere, *ex lege* o perché il Parlamento si è dotato di un organo che può far valere una specifica competenza al riguardo, ma anche le fattispecie in cui è il Governo che si induce sua sponte a 'ostendere' la propria attività, su richiesta meramente eventuale del Parlamento.

La seconda variabile è la presenza, in capo alla Camera e/o al Senato, di un onere (reciproco al primo), circa la necessità (o meno) di procedere effettivamente al riesame dell'attività governativa, vuoi per obblighi disposti dall'ordinamento o per accordo interistituzionale.

L'applicazione di questo schema all'ambito della sicurezza cibernetica ci fornisce qualche indicazione di grande interesse.

Anzitutto, l'attuale quadro normativo fornisce una notevole variabilità di strumenti di controllo a disposizione delle Camere, alcuni dei quali prevedono un riesame periodico, ancorché eventuale, dell'attività del Governo, mentre altri sono improntati a una maggiore istituzionalizzazione.

In secondo luogo, anche in virtù dell'impostazione originaria data dal legislatore nel 2013, il controllo del Parlamento sul Governo in questo ambito specifico è rafforzato dalla presenza del Comitato Parlamentare per la Sicurezza della Repub-

volutamente sbilanciato a favore del governo per quanto riguarda la promozione dell'indirizzo politico. Sul ruolo del Governo e il suo rafforzamento nei confronti del Parlamento si vedano i contributi in Musella 2019.

18 Cfr. Chimenti 1974. Come evidenziato in altra sede (Malvicini, 2022, a cui si rinvia per la letteratura sul tema), nella sua accezione ristretta di attività di riscontro-verificazione, il controllo parlamentare si qualifica per tratti tipici: il carattere relazionale, che si presenta anzitutto come alterità tra il soggetto controllante e quello controllato; il suo profilo logicamente accessorio e strumentale; il parametro sulla base del quale avviene l'attività di riesame, costituito, salvo eccezioni, anzitutto, dal programma di governo ma anche da tutti gli atti e documenti idonei ad integrare quest'ultimo; la natura politica del giudizio in cui si concretizza l'attività di verificazione del Parlamento sul Governo; le figure tipiche in cui si articola. Questo *modus operandi* – che si richiama all'impostazione di matrice amministrativista le cui origini risalgono quantomeno alla riflessione di U. Forti degli inizi del Novecento (1915), poi ripresa da autorevolissima dottrina, a partire da M.S. Giannini (1974) – porta a distinguere l'attività di controllo dal mero esercizio di 'influenza' o 'ingerenza' politica delle Camere nei confronti del Governo. Sui controlli si cfr., di recente, D'Alterio 2019: 681 ss.

blica (COPASIR)[19]. A quest'ultimo si riferiscono le principali figure di verifica sui profili organizzativi e funzionali di poteri e strutture competenti in materia[20].

In particolare, l'art. 2, c. 3, del d.l. 82/2021 prevede che il Presidente del Consiglio debba informare periodicamente il Comitato parlamentare, oltre che le commissioni permanenti competenti, sulle nomine del direttore generale e del vicedirettore generale dell'ACN. In aggiunta, ai sensi dell'art. 5, c. 6, del d.l. 82/2021, lo stesso COPASIR può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza (ex art. 31, c. 3, l. 124/2007).

Inoltre, il Comitato parlamentare esprime un parere, fra l'altro, sul regolamento circa l'ordinamento e il reclutamento del personale dell'Agenzia (art. 12, c. 8) e sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi finalizzate alla tutela della cibersicurezza, art. 11, c. 4).

In aggiunta, l'art. 14, comma 1 del d.l. 82/2021 stabilisce che, entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri debba trasmettere al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente in materia di cibersicurezza nazionale; a tale relazione se ne aggiunge un'altra, che va presentata dal Presidente del Consiglio entro il 30 giugno al COPASIR e che verte sulle attività svolte l'anno precedente dall'Agenzia rispetto alle attività di tutela della sicurezza nazionale nello spazio cibernetico.

Accanto a questi istituti si colloca l'onere che grava sul Presidente del Consiglio di informare il Comitato sull'avvenuta disattivazione, anche totale, "di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati", in caso di rischio grave e imminente» per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici (ai sensi di quanto previsto dall'art. 5, c. 1 del d.l. n. 105/2019).

Chiarite le principali figure di controllo delle Camere nei confronti del Governo in materia di cibersicurezza, è di particolare interesse completare l'analisi considerando anche la prassi attuativa (passando in sostanza dal piano delle regole a quello delle regolarità). In tale direzione, nonostante la particolare riservatezza dei lavori parlamentari, emergono numerosi elementi di grande interesse. Nello specifico, emerge che, analogamente ad altri ambiti riconducibili alla sua sfera di attribuzione, il Comitato è stato non solo un organo *reattivo* ma anche *proattivo* nell'esercizio delle sue attribuzioni[21].

19 Sul ruolo e l'attività del Comitato parlamentare per la sicurezza della Repubblica cfr. Perini 2023; Giuffrè 2021; Perrone 2018; Franchini 2014: Nardone 2008; Campanelli, 2008.

Per un'analisi di tipo comparato cfr. Schirripa, 2023; Piciacchia, 2018 e 2017.

Anche in virtù delle competenze ex art. l. 124/2007 il COPASIR viene identificato come un organo attraverso il quale il Parlamento esercita, accanto alla funzione di controllo, quella di garanzia costituzionale. Sulla funzione di garanzia costituzionale nel nostro ordinamento si vedano, quantomeno, Tarchi, 2021; Silvestri, 2009; Galeotti, 1950; 1969. Sull'attività di salvaguardia costituzionale svolta dalle Camere v. Gianniti, Lupo 2023[4]: 194-196; Manzella, 2003[3] e, soprattutto, 1970.

20 Sul punto v. Caramaschi 2022.

21 Sul punto si vedano gli acuti rilievi di Perrone 2018 secondo cui: "il Comitato, nell'effettivo dipanarsi della sua attività, si è rivelato organo di cerniera e cinghia di trasmissione affin-

In tal senso non si può non richiamare come, sin dalla XVI legislatura, il COPASIR sia stato promotore di iniziative di studio e approfondimento sulla sicurezza cibernetica, sotto molteplici punti di vista. Esito di questa attività è stata anzitutto la "Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico" presentata alle Camere il 7 luglio 2010 (Doc. XXXIV, n. 4). In essa si possono trovare riferimenti all'esigenza di pianificare in modo coordinato la difesa dei sistemi strategici nazionali connessi alla rete informatica, oltre che la raccomandazione al Governo di predisporre soluzioni organizzative presso la Presidenza del Consiglio, capaci di assicurare "leadership adeguata", anche tramite l'elaborazione di adeguate "politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati".

A tale documento ha fatto seguito, nella XVII legislatura, la "Relazione sulle procedure e la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni" (Doc. XXXIV, n. 7), dove si trovano numerosi riferimenti all'esigenza di perfezionare alcuni aspetti della governance predisposta dai primi DPCM. Nella XVIII legislatura, anche in reazione ad alcuni attacchi informatici subiti dal nostro Paese, il Comitato ha approfondito alcuni aspetti trattati incidentalmente nel corso degli anni precedenti. Anche grazie a un ciclo di audizioni articolato, che ha coinvolto sia il direttore del DIS sia una pluralità di rappresentanti e autorità militari e civili, ivi incluse aziende strategiche nazionali, il Comitato ha così potuto concentrarsi su alcuni profili specifici circa la sicurezza cibernetica nel Paese (*e.g.* il livello di sicurezza informatica garantito ai cittadini, alle istituzioni, alle infrastrutture critiche e alle imprese di interesse strategico nazionale; il grado di implementazione degli interventi attuativi delle linee di indirizzo strategiche e operative fissate nei documenti di indirizzo approvati). Con ciò il Comitato ha perfezionato specifiche valutazioni e proposte attuative, contenute nella "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale" presentata al Parlamento il 12 dicembre 2019 (Doc. XXXIV, n. 1).

Più di recente, nell'ambito della Relazione sull'attività svolta nella prima parte della XIX legislatura, presentata alle Camere il 17 aprile 2024 (Doc. XXXIV, n. 1), il Comitato si è occupato di sicurezza cibernetica nell'ambito di varie audizioni, riservando specifica attenzione alla trasformazione delle minacce informatiche di conseguenza, ai meccanismi di tutela necessari per salvaguardare il processo di digitalizzazione della pubblica amministrazione, alla luce della Strategia nazionale di cybersicurezza 2022-2026 e dell'annesso Piano di implementazione.

L'intraprendenza del COPASIR, che conferma l'immagine di un Parlamento che esercita un controllo a 'geometria variabile' (di notevole istituzionalizzazio-

ché potesse realizzarsi – nel metodo e nel merito – la mediazione tra le diverse esigenze richiamate; in tale ottica, il Copasir si è presentato come una sede di dialogo e camera di compensazione e di verifica tra il Parlamento legislatore e le richieste dei diversi attori chiamati ad intervenire sul piano della lotta al terrorismo internazionale".

ne nell'ambito della sicurezza nazionale, di minor proiezione su altri campi)[22], è stata massima nella fase crepuscolare della XVIII legislatura. Da un lato, il Comitato ha interloquito con il Governo al fine di modificare l'allora bozza del decreto-legge 14 giugno 2021, n. 82, prevedendo specifici spazi di controllo a disposizione delle Camere rispetto all'azione dell'ACN inizialmente non facenti parte dell'assetto di governance del sistema. Dall'altro, tra il 2021 e il 2022, il Comitato ha provveduto con sollecitudine all'esame e all'espressione del parere sugli schemi previsti per il funzionamento dell'ACN (*i.e*. il regolamento di organizzazione e funzionamento dell'Agenzia, il regolamento del personale, il regolamento di contabilità e quello recante le procedure per la stipula di contratti di appalti di lavoro, servizi e forniture).

Bibliografia

Bartolucci, L. 2024, *Piano nazionale di ripresa e resilienza e forma di governo tra Italia e Unione Europea*, Torino: Giappichelli.

Bassu, C., Pistorio, G. e Sterpa A. (a cura di) 2023, *Diritto pubblico della sicurezza*, Napoli: Editoriale Scientifica: 89-108.

Buoso, E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Giappichelli, Torino.

Calandriello, L. 2023, "Il perimetro di sicurezza nazionale cibernetica"*,* in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 139-151.

Campanelli, G., 2008, "Il Comitato parlamentare per la sicurezza della Repubblica nella legge 3 agosto 2007 n. 124", in *Quaderni costituzionali*, 2: 372-375.

Caramaschi, O., 2022, "La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari", in *Osservatorio costituzionale AIC*, 4: 69-83.

Cariola, A., Castorina, E. e Ciancio, A. (a cura di) 2010, *Studi in onore di Luigi Arcidiacono*, vol. IV, Torino: Giappichelli.

Casalone, G., Sciortino, A. e Massa Pinto, I. 2023, *Il Piano Nazionale di Ripresa e Resilienza*, Napoli: Editoriale Scientifica.

Cassese, S., Melloni, A. e Pajno A. (a cura di) 2022, *I Presidenti e la Presidenza del Consiglio dei ministri nell'Italia repubblicana: storia, politica, istituzioni*, Bari-Roma: Laterza.

Cavino, M. 2021, *Ordinamento giuridico e sistema delle fonti*, Napoli: Editoriale Scientifica, 361-388.

Chimenti, C. 1974, *Il controllo parlamentare nell'ordinamento italiano*, Milano: Giuffrè.

Ciolli, I. 2018, *La questione del vertice di Palazzo Chigi. Il Presidente del Consiglio nella Costituzione repubblicana,* Napoli: Jovene.

Contaldo, A. e Mula, D. (a cura di) 2020, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche,* Pisa: Pacini Giuridica.

Contaldo, A. e Salandri, L. 2020, "La disciplina della cybersecurity nell'Unione Europea", in A. Contaldo e D. Mula (a cura di) 2020, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: 1-55.

22 Malvicini 2022, 221-261.

Costanzo, p. Magarò, M. e Trucco, L. (a cura di) 2022, *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Atti del Convegno annuale dell'Associazione "Gruppo di Pisa", Genova 18-19 giugno 2021, Napoli: Editoriale Scientifica.
Cusenza, G.G., 2023, "I poteri dell'agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 123-151.
D'Alterio, E. 2019, "La funzione di controllo e l'equilibrio tra i poteri pubblici: 'dove nascono i problemi'", in *Rivista trimestrale di diritto pubblico*, 3: 681 ss.
De Lungo, D. e Marini, F.S. (a cura di) 2023, *Scritti costituzionali sul piano nazionale di ripresa e resilienza*, Torino: Giappichelli.
De Vergottini G. 2019, "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata", in *Rivista AIC*, 4: 65-84.
Dickmann R. e Staiano, S. (a cura di) 2008, *Funzioni parlamentari non legislative e forma di governo. L'esperienza dell'Italia*, Milano: Giuffrè.
Forgione, I. 2023, "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) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 95-121.
Forti, U. 1915, "I controlli nell'amministrazione comunale", in *Trattato di diritto amministrativo* diretto da V.E. Orlando, vol. II, parte II, Milano: Giuffrè.
Franchini, M. 2014, "Alcune considerazioni sulle nuove competenze del Comitato Parlamentare per la Sicurezza della Repubblica", in *Rivista AIC*, 1.
Gaggero, F. e Berruti, M. 2022, "I pilastri normativi della sicurezza cibernetica", in p. Costanzo, M. Magarò e L. Trucco (a cura di) 2022, *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Atti del Convegno annuale dell'Associazione "Gruppo di Pisa", Genova 18-19 giugno 2021, Napoli: Editoriale Scientifica.
Galeotti, S., 1950, *La garanzia costituzionale (presupposti e concetto),* Milano: Giuffrè.
Galeotti, S., 1969, "Garanzia costituzionale", *Enciclopedia del diritto*, vol. XVIII, Milano: Giuffrè, 491-511.
Giannini, M.S. 1974, "Controllo: nozione e problemi", in *Rivista trimestrale di diritto pubblico*, 4: 1263-1283.
Gianniti, L. e Lupo, N. 2023, *Corso di diritto parlamentare*, Bologna: il Mulino.
Giuffrè, F., 2021, "I 'Servizi di informazione e sicurezza' della Repubblica nella dialettica tra Governo e Parlamento", in *Percorsi costituzionali*, 3: 757-776.
Giupponi T.F. 2022, "I rapporti tra sicurezza e difesa. Differenze e profili di convergenza", in *Diritto costituzionale. Rivista quadrimestrale*, 1: 21-48.
Giupponi T.F. 2023, "Sicurezza e potere", in *Enciclopedia del diritto. I tematici, Vol. V, Potere e Costituzione*, Milano: Giuffrè: 1165 ss.
Giupponi T.F. 2024, "Il governo nazionale della cybersicurezza", in *Quaderni costituzionali*, 2: 277-303.
Giupponi, T.F. 2010, "Servizi di informazione e segreto di Stato nella legge n. 124/2007", in A. Cariola, E. Castorina e A. Ciancio (a cura di) 2010, *Studi in onore di Luigi Arcidiacono*, vol. IV, Torino: Giappichelli: 1677-1751.
Lauro, A. 2021, "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", in *La Rivista del Gruppo di Pisa,* fasc. spec. 3: 529-545.
Lotta, C. 2024, *Governance della rete, accesso a internet e cybersicurezza. Profili costituzionali* Napoli, Editoriale Scientifica.
Malvicini, M. 2016, "Sicurezza della Repubblica e forma di governo parlamentare. Il Rapporto tra presidente del Consiglio dei ministri e Copasir alla luce dei più recenti inter-

venti legislativi (legge 11 dicembre 2015, n. 198)", in *Forum Quaderni Costituzionali*, 11 maggio 2016.
Malvicini, M. 2022, *La funzione di controllo del Parlamento nell'ordinamento costituzionale italiano*, Torino: Giappichelli.
Manzella, A. 1970, *I controlli parlamentari*, Milano: Giuffrè.
Manzella, A. 2003, *Il Parlamento*, Bologna: il Mulino.
Manzella, A. 2017, "Il Parlamento come organo costituzionale di controllo", in *Nomos. Le attualità del diritto*, 1.
Matassa, M. 2023, "La regolazione della cybersecurity in Italia", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 21-42.
Montessoro, p. L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Le Istituzioni del Federalismo*, 3.
Moroni, L. 2024, "La governance della cybersicurezza a livello interno ed europeo: un quadro intricato", in *Federalismi.it*, 14: 179-197.
Mosca, C., Gambacurta, S., Scandone, G., e Valentini, M. 2008, *I servizi di informazione e il segreto di stato (Legge 3 agosto 2007, n. 124)*, Milano: Giuffrè.
Musella, F. (a cura di) 2019, *Il governo in Italia. Profili costituzionali e dinamiche politiche*, Bologna: il Mulino.
Nardone, C. 2008, "Il controllo parlamentare sui servizi di informazione", in R. Dickmann e S, Staiano (a cura di) 2008, *Funzioni parlamentari non legislative e forma di governo. L'esperienza dell'Italia*, Milano: Giuffrè: 375-415.
Pace, A. 2014, "La funzione di sicurezza nella legalità costituzionale", *Quaderni costituzionali*, 4: 989-1000.
Peluso, F. 2020, *La disciplina italiana in tema di cybersecurity*, in A. Contaldo e D. Mula (a cura di) 2020, *Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica: 119-144.
Parona, L. 2021, "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale di diritto amministrativo*, 6.
Perini, M. 2023, "Evoluzione della forma di governo alla luce della disciplina e della prassi del COPASIR", in *Rassegna parlamentare*, 1: 19-41.
Perrone, A., 2018, "Le prospettive del controllo parlamentare nella recente attività del Comitato parlamentare per la sicurezza della Repubblica", in *Federalismi.it,* 11: 1-28.
Piciacchia, p. 2017, *Parlamenti e costituzionalismo contemporaneo. Percorsi e sfide della funzione di controllo*, Napoli: Jovene.
Piciacchia, p. 2018, "La dimensione del controllo parlamentare su segreto di Stato e intelligence alla prova delle crescenti esigenze di sicurezza degli Stati tra problemi aperti e prospettive: le esperienze di Italia, Francia e Belgio", in *Democrazia e sicurezza – Democracy and Security Review*, 1: 37-107.
Previti, L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it,* 25.
Renzi, A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giornale di diritto amministrativo,* 4.
Rossa, S. 2023, *Cybersicurezza e Pubblica Amministrazione*, Editoriale Scientifica, Napoli.
Salamo, L.V.M. 2017, "La disciplina del cyberspace alla luce della direttiva europea sulla sicurezza delle reti e dell'informazione", in *Federalismi.it*, 23.
Salvaggio, S.A. e Gonzales, N. 2023, "The European framework for cybersecurity: strong assets, intricate history", in *International Cybersecurity Law Review*, 4.
Scaccia, G. 2012, "Intelligence e segreto di Stato nella legge n. 133 del 2012", in *Diritto e società*, 3.

Schatz D. Bashroush R. e Wall J. 2017, "Towards a More Representative Definition of Cyber Security", in *Journal of Digital Forensics, Security and Law*, 2: 53-74.
Schirripa, M. 2023, *Il controllo parlamentare sulle attività del Sistema di informazione per la sicurezza nazionale: il ruolo del Copasir ed uno sguardo comparato*, in C. Bassu, G. Pistorio, A. Sterpa (a cura di) 2023, *Diritto pubblico della sicurezza*, Napoli: Editoriale Scientifica: 89-108.
Scognamillo, L. 2023, "Cybersicurezza e sicurezza nazionale", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 71-84.
Serini, F., 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", in *Federalismi.it*, 12: 241-272.
Silvestri, G., 2009, *Le garanzie della Repubblica,* Torino: Giappichelli.
Tarchi, R., 2021, *Democrazia e istituzioni di garanzia*, Napoli: Editoriale Scientifica.
Teodoldi L. (a cura di) 2019, *Il presidente del Consiglio dei ministri dallo Stato liberale all'Unione Europea*, Milano: Biblion Edizioni.
Ursi R. 2022, "La difesa: tradizione e innovazione", in *Diritto costituzionale. Rivista quadrimestrale*, 1: 5-20.
Ursi, R. (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli.
Ursi, R. 2023, "La sicurezza cibernetica come funzione pubblica", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 7-20.
Valentini, M. 2017, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionali*, Napoli: Editoriale Scientifica.
Vigneri, A.F. 2023, "I profili giuridici della sicurezza nazionale. Tra collocazione sistematica e problemi definitori: un'introduzione critica", in R. Ursi (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli: 43-69.

Maura Mattalia

L'impatto della cybersecurity nelle politiche digitali delle amministrazioni pubbliche. Una riflessione giuridica sulle sfide globali: dalla sicurezza informatica al cambiamento climatico

Abstract: Sebbene clima e cyberspazio siano ambiti distinti, condividono problematiche simili, di uso eccessivo, difficoltà di regolamentazione, oltre che le sfide associate alla deresponsabilizzazione collettiva, ove si consideri che tanto Internet quanto il clima sono influenzati da milioni di attori. Con il cambiamento dei modelli meteorologici, l'innalzamento del livello globale dei mari e le temperature destinate a superare 1,5 gradi, il cambiamento climatico è un problema che riguarda tutto il mondo, ma i benefici derivanti dalla lotta ad esso sono dispersi, con danni spesso concentrati. Del pari, il costo degli attacchi informatici si concentra in un numero relativamente piccolo di nazioni, e altre stanno diventando paradisi per i criminali informatici. Ciononostante, le azioni intraprese da una molteplicità di attori su piccola scala possono avere un impatto sia sul problema del cambiamento climatico globale sia sulla causa della promozione di una cultura globale della sicurezza informatica. Questo articolo ripercorre l'evoluzione del regime dei cambiamenti climatici, concentrandosi sia sugli sforzi *top-down* della Convenzione quadro delle Nazioni Unite, dell'Accordo di Parigi e dei Regolamenti europei sui cambiamenti climatici, che su quelli *bottom-up* bilaterali e regionali, per poi confrontare e contrapporre quanto emerso con la *governance* di Internet. Viene valutato il potenziale della *governance* policentrica per mitigare i due problemi di azione collettiva globale del cambiamento climatico e degli attacchi informatici.

Keywords: Cybersicurezza; Cambiamento climatico; Climate Change Law; Ambiente.

1. Amministrare le sfide del XXI secolo

Tra le sfide globali del XXI secolo vanno annoverate: la lotta ai cambiamenti climatici[1], la lotta alle pandemie e all'(in)sicurezza informatica[2].

Seppur possano risultare problematiche distinte in realtà si tratta di problematiche complesse, interdipendenti, interconnesse e resistenti alle soluzioni. Per il

1 Lazarus, 2008: 1153.
2 Carr e Lesniewska, 2020: 391-412.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760150

sistema giuridico non sono prescritte norme volte a eliminare i rischi sottesi a tali sfide, ma l'obiettivo che il sistema (internazionale, europeo e nazionale) si è posto è piuttosto quello di mitigarli il più possibile[3].

Quanto prospettato consente di maturare una visione differente riguardo a ciò che, comunemente, viene percepito come 'problema'; al contempo, permette lo sviluppo del pensiero critico, con l'obiettivo di ideare approcci nuovi e utili per affrontarli[4]. Ed infatti, le questioni ora citate rappresentano una sfida senza precedenti, per diversi motivi: trattasi di problematiche intrinsecamente destabilizzanti[5] e, più in genere, sono costituite da diversi 'sotto-problemi' che hanno conseguenze diverse, sia per gli attori che per il contesto, rendendo qualsiasi questione ad essi relativa un problema globale poiché capace di coinvolgere un numero indeterminato di soggetti.

Per due decenni, i governi hanno cercato di creare un sistema normativo integrato e coerente per la gestione dei cambiamenti climatici e per garantire la sicurezza informatica. Tuttavia, queste iniziative hanno prodotto una pluralità di regimi normativi spesso frammentati: in quanto strettamente interconnessi, questi regimi talvolta si pongono in conflitto tra l'oro e, talaltra, si rafforzano a vicenda.

Si consideri ora il cambiamento climatico: le emissioni di CO2 sono continuate a crescere, raggiungendo nel 2022 un totale di 53,8 miliardi di tonnellate, con un incremento dell'1,4% rispetto al 2021. Cina, Stati Uniti, India, Unione europea, Russia, Brasile hanno contribuito per il 61,6% di tali emissioni. Tra queste, dal 1990 al 2021 le emissioni dell'Unione europea si sono ridotte del 27%, quelle della Russia del 15,5% e degli Stati Uniti del 2,4%. Si registra invece, nel medesimo periodo di tempo, un aumento del 285% in Cina e del 170% in India. Evidente è il ruolo delle due grandi potenze emergenti del continente asiatico nell'accelerazione del problema.

Ove però si consideri non solo l'evoluzione passata, ma anche la prevedibile evoluzione futura, la Cina mostra notevoli potenzialità di miglioramento nel settore energetico, pur essendo indicata nel dibattito corrente come la principale responsabile dell'aggravamento della crisi climatica, giocando pertanto un ruolo decisivo per il controllo delle emissioni di CO2. Il World Energy Outlook del 2023, predisposto dall"International Energy Agency (IEA), sottolinea come il governo cinese preveda di arrivare al picco delle emissioni nel 2030, con l'obiettivo intermedio di consumo di energia non fossile pari al 20% del 2025 e l'obiettivo finale di emissioni zero nel 2060. Parallelamente, considerando la collocazione della Repubblica popolare Cinese negli equilibri globali, essa ha istituito un Fondo di Cooperazione Sud-Sud sui cambiamenti climatici, con un investimento di 20 miliardi di yuan (3,1 miliardi di dollari), al fine di sostenere altri paesi in via di sviluppo nell'affrontare il cambiamento climatico e nella transizione verso un'economia verde e a basse emissioni di carbonio.

3 Coen e Pegram, 2019.
4 Shackelford e Fort, 2016.
5 Berman, 2018: 149-82.

In Europa, dopo l'approvazione del Green Deal[6], importanza primaria nella lotta ai cambiamenti climatici è attribuita all'adozione della *Climate Law*, con l'obiettivo intermedio, giuridicamente vincolante, di una riduzione del 55% delle emissioni di CO2 nel 2030, per raggiungere la c.d. *carbon-neutrality* nel 2050[7]. Ancora, il pacchetto "Fit for 55" istituisce un nuovo sistema di scambio dei permessi di emissioni separato per ciascun settore – tra cui quello dell'edilizia, dei trasporti e della piccola industria, tra gli altri, oltre che il settore marittimo con estensione graduale – imponendo l'acquisto di tali permessi a produttori e importatori che forniscono combustibili e progressivamente riducendo la concessione di permessi a titolo gratuito agli operatori del settore aereo. In questo contesto si inserisce altresì il regolamento (UE) 2023/956, che, a partire dal 1° ottobre 2023 ha introdotto il meccanismo di correttivo fiscale alle frontiere dell'Unione[8], con l'obiettivo di far pagare un prezzo per le emissioni durante la produzione di merci a elevata intensità di carbonio importate nell'Unione e di evitare una perdita di competitività della produzione verde europea nei confronti di paesi con politiche ambientali meno ambiziose.

Nonostante questi sforzi, gli obiettivi fissati dagli Accordi di Parigi del 2015 sembrano difficilmente raggiungibili senza un impegno globale, come ben è evidenziato dal Fondo Monetario Internazionale che ha proposto un accordo tra i cosiddetti 'Big Emitters' di CO2 per la fissazione di un prezzo minimo globale per il carbonio. Simile ipotesi potrebbe essere fatta propria dall'Unione, con l'obiettivo di costituire un gruppo ristretto di Paesi impegnati a preparare il terreno per decisioni vincolanti a livello globale, da assumersi quindi nell'ambito delle Conference of Parties (COP) a maggior ragione ove si consideri la difficoltà in tale sede di raggiungere accordo all'unanimità. Ed ancora, ove si consideri l'impatto in termini quantitativi delle emissioni della Cina, come sopra ricordato, l'evoluzione della relativa politica in tema di controllo dei cambiamenti climatici può rappresentare un esempio utile per coinvolgere i paesi del Global South nel raggiungimento dell'obiettivo della decarbonizzazione[9].

Nelle più recenti trasformazioni climatiche, l'azione umana ha fortemente condizionato – sia su scala locale che globale – l'ambiente terrestre nell'insieme delle sue caratteristiche fisiche, chimiche e biologiche, dando origine al riscaldamento globale in corso e all'epoca geologica dell'Antropocene. L'impatto dell'uomo sulla terra è testimoniato da molteplici indicatori, che riguardano sia le attività umane (popolazione, urbanizzazione[10], consumo energetico, utilizzo delle risorse del pianeta[11]) che lo stato dell'ambiente (tra cui biodiversità, deforestazione, presenza di

6 Bevilacqua 2024; Bevilacqua, Chiti 2024.
7 De Bellis 2012: 759; Gratani 2013: 392.
8 Carbon Border Adjustment Mechanism.
9 Majocchi, 2024.
10 Sandulli 2019: 291; Santiello 2022: 105 e s.
11 Giannini 1973:15; Carducci 2021: 1-26; Caputi Jambrenghi 1989: 301; Caputi Jambrenghi 1996: 311; Caputi Jambrenghi 2009: 49.

anidride carbonica, temperature superficiali)[12]. In tale contesto, al fine di adeguatamente affrontare i problemi posti dal cambiamento climatico, si rende necessario un riallineamento delle politiche pubbliche di incentivazione[13], ancor più ove il soggetto agente (ossia 'chi inquina') non abbia interesse immediato a tenere un determinato comportamento positivo o a porre in essere azioni che, di contro, sono a beneficio di altri soggetti o parti sociali[14]. In questi casi, è perlomeno necessaria una compensazione del comportamento che lede l'interesse altrui, tanto che persino i governi più riluttanti ad adottare politiche di lotta al cambiamento climatico richiedono talvolta compensazioni e pagamenti, come incentivo affinché si cooperi in vista degli obiettivi climatici.

Si giunge a conclusioni simili quando si considera un'altra grande sfida per i sistemi giuridici moderni: la sicurezza informatica. Questa, infatti, presenta problematiche e presupposti analoghi a quelli già menzionati per le politiche di risposta al cambiamento climatico, al punto da rendere utile un confronto e una possibile adozione delle stesse soluzioni.

Nell'ultimo quarto di secolo, la *governance* delle tecnologie digitali è emersa come una delle grandi sfide contemporanee, presentando interrogativi, in parte irrisolti, relativi alla misura in cui la *cybersicurezza* impatti sulla stabilità e l'ordine internazionale.

Mentre la cooperazione tecnica globale in materia di *cybersicurezza* ha prodotto risultati positivi, la cooperazione politica[15] è stata lenta, ostacolata da sistemi valoriali differenti e tensioni geopolitiche. Nell'ultimo ventennio i tentativi di affrontare la politica della sicurezza informatica globale sono stati condotti nel rispetto di istituzioni emerse nel secondo dopoguerra al fine di garantire un ordine internazionale pacifico e sono stati caratterizzati dall'istituzione di occasioni di dialogo secondo il modello 'multistakeholder' che caratterizza la governance di Internet.

Nonostante l'incremento delle esigenze, il coordinamento politico internazionale continua a procedere a un ritmo che non risponde adeguatamente alle necessità di gestione di un'economia globale sempre più basata su piattaforme digitali. Questo disallineamento si traduce in un processo decisionale spesso lento e inefficace, incapace di adattarsi in modo tempestivo alle sfide poste dall'evoluzione tecnologica e dall'integrazione economica su scala mondiale.

Nel contesto ora brevemente delineato, l'obiettivo del presente lavoro è quello di classificare strumenti per delineare un quadro giuridico sostenibile ed efficace per la protezione dai rischi informatici, al fine di consentire ai decisori di agire in

12 Sul punto: IPCC Fifth Assessment Report. Ove si evidenzia che l'uomo, a causa dell'utilizzo dei combustibili fossili e della deforestazione, ha contribuito al cambiamento climatico in una misura pari al 95%. The Fifth Assessment Report (AR5) of the Intergovernmental Panel on Climate Change (IPCC) of 2014, http://www.ipcc.ch/

13 Clarich 2007:219.

14 Pernice 2024: 95-98; Meli 2023: 2045-2052; Mauro 2022; Chiti 2022: 680-686.

15 Corvese 2022: 391; Fornasari 2022: 480.

modo preventivo[16], descrivendo e modellando la combinazione di strumenti di regolazione ritenuti più efficaci nella gestione e prevenzione delle minacce informatiche, utilizzando dagli strumenti giuridici già in uso per la lotta al cambiamento climatico e proponendo un'analisi parallela. Individuata la dimensione globale di entrambi i regimi, si procede ad un esame del quadro giuridico internazionale con riferimento ad alcuni degli attori principali della *governance* del cambiamento climatico e della sicurezza cibernetica, infine verificando la possibilità di applicare i principi del diritto ambientale alla dimensione cibernetica.

L'urgenza della questione può facilmente essere compresa ove si osservino le conseguenze per le persone e i costi stimati del mancato intervento contro le minacce ora ricordate, come ricordato già dalla Strategia dell'Unione Europea 2013.

Cambiamento climatico e sicurezza informatica possono essere entrambi considerati come 'problemi collettivi globali', che condividono pratiche e preoccupazioni simili e interessano la sfera privata, con somiglianze che consentono di analizzare le questioni relative al cyberspazio attraverso il prisma del diritto e della politica ambientale. In entrambi i casi, peraltro, possono riscontrarsi problematiche inerenti alla sostenibilità dell'ambiente, alla scarsità di risorse, all'ascesa di una politica multipolare, oltre che alla necessità di un progresso normativo che tenga il passo con il progresso tecnologico, politico ed economico[17].

Ove si considerino gli strumenti politici e legislativi inerenti alla questione ambientale – la cui azione può assumere peraltro varie forme, dalla mobilitazione dei finanziamenti alla sensibilizzazione della società civile – segno distintivo di questi è diventato l'agire per obiettivi, fulcro dei colloqui internazionali sul clima e della copertura mediatica sul cambiamento climatico, tanto da costituire spesso le richieste principali sia delle proteste che delle controversie a favore di un'azione climatica più ambiziosa. Ciononostante, poiché gli obiettivi rappresentano semplicemente il risultato finale[18] che si intende raggiungere, pur ove questi vengano tradotti in impegni giuridici, come è avvenuto nell'ambito europeo, non consentono di individuare con precisione le modalità con cui si intende raggiungerli.

Si consideri che sulla discrezionalità lasciata agli Stati nella scelta dei mezzi migliori per assicurare i risultati richiesti dalle norme si configura oggi il precedente delineato dalla sentenza CEDU del 9 aprile 2024, con la quale la Corte europea dei diritti dell'uomo si è pronunciata su tre casi che hanno sollevato, per la prima volta, la questione della tutela dei diritti umani nel contesto dei danni ambientali causati dal riscaldamento globale[19]. Le soluzioni adottate dai giudici di Strasburgo sono originali e contribuiscono a delineare i contorni del ragionamento europeo su una delle questioni più preoccupanti del nostro tempo[20].

16 McGinnis, 2011.
17 Hardin, 1968: 1243-1248.
18 Barone 2023: 383 s.
19 Si tratta dei casi n. 53600/20, *Verein KlimaSeniorinnen Schweiz e altri c. Svizzera*; n. 7189/21, *Carême c. Francia* e n. 39371/20, *Duarte Agostinho e altri c. Portogallo.*
20 Brillat, 2023.

In particolare, una delle controversie è stata avviata da un'associazione di donne ultrasettantenni, avente ad oggetto la promozione ed attuazione di un'efficace protezione del clima per conto dei suoi membri, lamentando la mancata adozione di misure sufficienti per ridurre le emissioni di gas serra, con conseguenze negative per la vita degli associati della ricorrente. La Corte ha riconosciuto senza ambiguità ed in via generale che si trattava di "questioni nuove" (§ 414), chiaramente indicando la necessità di stabilire un nuovo approccio alla propria giurisprudenza, al fine di soddisfare i requisiti di protezione dei diritti umani nel contesto del riscaldamento globale, le cui fonti sono diverse e gli effetti collettivi. In risposta ai numerosi interrogativi giuridici sollevati, la Corte ha individuato taluni principi che definiscono gli elementi del ragionamento europeo in materia di clima, accertando la violazione della Convenzione da parte della Svizzera, dichiarando irricevibili le altre due domande.

Gli sviluppi sono particolarmente lunghi ed è possibile individuarne gli aspetti principali, pur potendosi rilevare la natura particolare del contenzioso sul clima sia la natura tecnica del diritto europeo dei diritti umani.

In primo luogo, la Corte rifiuta di estendere la sua giurisprudenza sull'effetto extraterritoriale della Convenzione europea, come i ricorrenti l'hanno invitata a fare in altro caso diretto contro il Portogallo ed altri Stati parte della Convenzione europea[21]. I giudici europei hanno respinto la richiesta, anche in ragione delle molteplici fonti territoriali di emissione di gas serra, ricordando che l'applicazione extraterritoriale della Convenzione implica un controllo effettivo da parte dello Stato sulla persona del richiedente che si trova in territorio straniero, senza che sia sufficiente una mera incidenza sui suoi interessi, ancor più ove non siano ancora state esaurite le vie di ricorso interne.

Ciò premesso, il primo – e senza dubbio il principale – ostacolo nelle cause sul clima riguarda la legittimazione dell'attore di presentare alla Corte un ricorso relativo agli effetti negativi del riscaldamento globale: all'impatto sulla generalità dei consociati delle conseguenze del riscaldamento globale fa, infatti, da contraltare l'impossibilità della Corte di decidere in merito ad un *actio popularis*, in ragione di un sistema giuridico basato sul diritto di petizione individuale al fine di affermare l'esistenza di una specifica violazione di un diritto fondamentale. Di contro, il contenzioso sul clima porta alla luce un gran numero di potenziali vittime, con l'ulteriore rischio di minare la separazione dei poteri ove la Corte europea dovesse accettare di trattare qualsiasi domanda in questo settore. In risposta a questa difficoltà, la Corte ha cercato una risposta alle istanze presentante nel personale e diretto coinvolgimento dei soggetti ricorrenti colpiti dalle presunte violazioni. Così, è richiesto che siano soddisfatte due condizioni cumulative: il richiedente deve essere intensamente esposto alle conseguenze negative del riscaldamento globale e deve esistere una necessità impellente di garantire la sua protezione individuale. Condizioni, non facilmente riscontrabili in concreto, come la stessa Corte ha avuto

21 Caso n. 39371/20, *Duarte Agostinho e altri c. Portogallo.*

modo di riconoscere[22] dichiarando l'irricevibilità di uno dei ricorsi proposti[23], in ragione del fatto che il ricorrente non aveva più residenza nello specifico comune interessato da eventi climatici estremi (nella specie, una inondazione), non potendo pertanto egli affermare di essere vittima di un rischio per la sua vita, la sua abitazione o la sua vita privata e familiare.

Di contro, in altro caso[24] la Corte ha accolto la possibilità che un'associazione sia legittimata a rappresentare le vittime del riscaldamento globale davanti a sé, purchè siano soddisfatte determinate condizioni: l'associazione deve essere legalmente costituita nel Paese in cui è stata presentata la domanda e il suo scopo statutario deve essere la difesa dei diritti umani dei suoi membri (o deve essere autorizzata a difendere gli interessi dei suoi membri colpiti dal riscaldamento globale). Non è tuttavia necessario che si dimostri in giudizio che i singoli membri dell'associazione ricorrente siano vittime individuali dell'evento climatico dannoso. La Corte europea ha confermato altresì, nel medesimo caso ora in commento, che il diritto alla vita può essere invocato nelle controversie sul clima se viene dimostrato un rischio reale e imminente per la vita. Anche il diritto alla vita privata e familiare può servire come base per un ricorso purché esista un legame diretto e immediato tra gli effetti del riscaldamento globale e il diritto individuale del richiedente, senza che sia sufficiente il deterioramento generale dell'ambiente per stabilire l'esistenza di un'interferenza.

Superato l'ostacolo processuale, nel merito la Corte si è concentrata sulla modulazione del margine di apprezzamento nazionale in materia climatica, sottolineando che tale margine è limitato quando si tratta di stabilire l'obiettivo da raggiungere, mentre è ampio quando si tratta di valutare le risorse impiegate per raggiungere tale obiettivo. In termini pratici, "l'effettivo rispetto dei diritti tutelati dall'articolo 8 della Convenzione impone a ciascuno Stato contraente di adottare misure per una riduzione significativa e progressiva dei propri livelli di emissioni di gas a effetto serra, al fine di raggiungere la neutralità della rete, in linea di principio entro i prossimi tre decenni"[25]. La Corte ha fornito indicazioni specifiche per valutare queste misure di mitigazione alla luce dei requisiti della Convenzione: le autorità nazionali devono "adottare misure generali che specifichino il calendario da rispettare"; "fissare obiettivi e traiettorie provvisori di riduzione delle emissioni di gas serra (per settore o con altri metodi pertinenti)"; "fornire informazioni che dimostrino se hanno debitamente rispettato i pertinenti obiettivi di riduzione delle emissioni di gas serra o se sono in procinto di farlo"; "aggiornare gli obiettivi di riduzione delle emissioni di gas serra con la dovuta diligenza e sulla base dei migliori dati disponibili"; "agire in modo tempestivo, appropriato e coerente nello

22 "La soglia da rispettare per soddisfare questi criteri è particolarmente alta" e può essere determinata solo da un esame approfondito di ogni singolo caso: Caso n. 7189/21, *Carême c. Francia,* par. 488.

23 Caso n. 7189/21, *Carême c. Francia.*

24 Caso n. 53600/20, *Verein KlimaSeniorinnen Schweiz e altri c. Svizzera.*

25 Caso n. 53600/20, *Verein KlimaSeniorinnen Schweiz e altri c. Svizzera*, par. 548.

sviluppo e nell'attuazione della legislazione e delle misure pertinenti"[26]. Le misure di mitigazione non sono gli unici requisiti convenzionali: lo Stato deve anche mettere in atto misure di adattamento per limitare gli effetti attuali del riscaldamento globale. A causa delle gravi carenze nelle misure adottate dalle autorità svizzere per mitigare gli effetti del riscaldamento globale, la Corte ha riscontrato una violazione della Convenzione europea senza nemmeno esaminare l'esistenza e il contenuto delle misure di adattamento.

L'esame della recente giurisprudenza della Corte in tema di cambiamento climatico e tutela delle parti sociali e degli individui è qui presupposto per alcune considerazioni inerenti alla cybersicurezza, ancor più ove si consideri che nel trattamento dei dati rilevano gli articoli 7 ed 8 della CEDU, ossia i medesimi sinora invocati a protezione da eventi climatici estremi. Nonostante venga generalmente considerato come ricompreso nel diritto al rispetto della vita privata, il diritto dell'Unione europea dedica al diritto alla tutela dei dati personali disposizioni specifiche, segnatamente l'art. 8 della Carta e l'art. 16, TFUE. Tuttavia l'art. 8, per indicazione della stessa Corte di giustizia, non può che leggersi in combinazione con l'art. 7 della Carta. La Corte, nella sentenza Volker und Markus Schecke e Eifert, aveva infatti evidenziato "… da un lato, che il rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta, sia riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile (…) e, dall'altro, che le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondano a quelle tollerate nell'ambito dell'art. 8 della CEDU"[27].

2. Dal cambiamento climatico agli attacchi informatici: un'analogia

Il cambiamento climatico, come noto, e come già più volte ribadito, rappresenta una delle più importanti sfide della nostra epoca e i suoi impatti si ripercuotono in maniera aggravata sulla città e sul benessere e la salute di tutti i cittadini. Eventi climatici sempre più intensi e violenti, quali isole di calore urbane[28], precipitazioni estreme, fenomeni siccitosi e tempeste di vento, insieme ad un tendenziale incremento della popolazione nelle città, definiranno le principali condizioni di vulnerabilità ed esposizione innescando differenti livelli di rischio. Le città rappresentano il luogo fisico di concentrazione di tali impatti e il principale habitat dell'essere umano e, pertanto, richiedono strategie e soluzioni progettuali di adattamento capaci di incidere sulla vivibilità dell'ambiente urbano e l'incremento della resilienza climatica.

Il cambiamento climatico globale e le minacce informatiche sono due importanti sfide globali future in termini di regolamentazione e gestione. Anche se le variabili

26 Caso n. 53600/20, *Verein KlimaSeniorinnen Schweiz e altri c. Svizzera*, par. 550.

27 CGUE, sentenza del 9 novembre 2010, causa C-92/09, Volker und Markus Schecke and Eifert, ECLI:EU:C:2010:662, punto 52.

28 Gherri 2020; Colucci 2020.

che influenzano il cambiamento climatico, il cyberspazio e la cybersecurity sono diverse, presentano caratteristiche simili dal punto di vista normativo e gestionale, in quanto sono associate a rischi di natura antropica che colpiscono i beni critici, compresi i settori chiave delle infrastrutture critiche, come il settore energetico. I punti di contatto tra i due settori – cambiamento climatico globale e minacce informatiche – sono vari e numerosi. Basti pensare, ad esempio, all'origine umana del rischio: in entrambe le ipotesi i rischi sono antropogenici, cioè derivanti dalle attività umane. Pertanto, la gestione degli stessi, in entrambi i contesti, richiede regole e politiche che regolano il comportamento umano. Ancora, e sempre per entrambi i settori, si rileva la necessità di una governance multilivello, che coinvolga governi nazionali, organizzazioni internazionali e settore privato[29]. Siffatta organizzazione presuppone, quindi, un necessario coordinamento tra più livelli istituzionali al fine di garantire un'efficace attuazione delle politiche adottate.

Parimenti, la regolamentazione di entrambi settori non solo deve mantenersi in continua evoluzione, il che richiede una flessibilità normativa con una relativa capacità di aggiornare regole e politiche in modo tempestivo, ma si basa su una logica di prevenzione e mitigazione dei rischi, in cui si promuove un approccio proattivo per prevenire i danni e ridurre al minimo l'impatto delle minacce.

Allo stesso modo, anche l'approccio e le iniziative per contenere i due settori sono ancora guidati 'dal basso verso l'alto', con particolare rilievo del settore privato, nonostante sia la cybersecurity – o, meglio, la 'cyber insicurezza' – sia il cambiamento climatico siamo problemi globali. A tal proposito, infatti, l'Accordo di Parigi[30] firmato nell'ambito della Convenzione delle Nazioni Unite sui Cambiamenti Climatici (UNFCCC) (The United Nations Convention on Climate Change, 1994), delinea, per la prima volta nella *governance* dell'inquinamento atmosferico, un approccio 'integrato' dall'alto verso il basso e dal basso verso l'alto, in contrapposizione al chiaro approccio *top-down* del suo predecessore, il Protocollo di Kyoto (2005).

La *governance* di Internet si sta invece frammentando, il che rende ancora più difficile affrontare le sfide della sicurezza informatica[31]. I primi teorici consideravano il cyberspazio come un "ambiente senza confini e libero dal controllo degli Stati"[32], oppure come uno spazio artificiale in cui è possibile una regolamentazione[33]. Il concetto di cittadinanza digitale è emerso originariamente per descrivere

29 De Nicola, 2023: 37 ss; Neri, Russo, 2018: 43 ss; Giliberto, 2024: 64 ss, Landini, 2014, 14 ss.

30 L'Accordo di Parigi è stato adottato il 12 dicembre 2015 dalla XXI Conferenza delle Parti della Convenzione quadro delle Nazioni Unite sul cambiamento climatico, tenutasi a Parigi dal 30 novembre al 13 dicembre 2015. Aperto alla firma e alla ratifica dal 22 aprile 2016, l'Accordo è entrato in vigore trenta giorni dopo la soddisfazione dei requisiti previsti dall'art. 21. Ai sensi della disposizione l'Accordo sarebbe stato vigente quando fosse stato ratificato da almeno quarantacinque Parti della Convenzione quadro, a condizione che da esse fosse provenuto almeno il cinquantacinque percento delle emissioni globali di gas serra.

31 Force Hill, 2012.

32 Murray, 2006.

33 Lessig,1999: 501,502, 533.

la condizione che caratterizza le società contemporanee in cui l'impegno politico, l'accesso ai servizi e più in generale una parte considerevole delle attività sociali ed economiche passano attraverso le interazioni online. La digitalizzazione di aspetti fondamentali della nostra vita e il ruolo crescente dell'intelligenza artificiale stanno trasformando profondamente i nostri ambienti sociali, politici ed economici. Da una parte, questo cambiamento ha rafforzato la capacità d'azione dei cittadini; dall'altra, ha agevolato la raccolta e l'analisi dei dati personali in modi mai visti prima, consentendo così decisioni automatizzate basate su tecniche di profilazione. Questi sviluppi suscitano importanti preoccupazioni per la salute della cittadinanza democratica, rendendo urgente ripensare la nostra concezione di cittadinanza digitale per affrontare le varie forme di monitoraggio, sorveglianza, categorizzazione e profilazione a cui i cittadini sono sempre più sottoposti. In quest'ottica la cybersicurezza divine presupposto essenziale per la cittadinanza digitale ed essenziale per salvaguardare una parte molto rilevante dei diritti dei cittadini.

Molte autorità nazionali e locali hanno compreso l'importanza delle pratiche di adattamento e mitigazione climatica e hanno iniziato ad agire ma, sia sul piano della pianificazione che su quello della programmazione e realizzazione degli interventi, la transizione climatica per l'adattamento prosegue molto più lentamente rispetto a quella della mitigazione e alla velocità degli impatti provocati dal surriscaldamento globale attualmente in corso. Ad aggravare la situazione inoltre, nel caso della mitigazione, gli obiettivi climatici prefissati non mostrano risultati incoraggianti e, in maniera analoga, per l'adattamento, si stanno riscontrando problematiche sul monitoraggio e sulla valutazione dell'efficacia delle prestazioni delle soluzioni e strategie intraprese. Entrambi sono sfide globali[34].

Il cambiamento climatico è un problema politicamente difficile per tre ragioni fondamentali. In primo luogo, si tratta di un problema globale, la cui soluzione non può essere raggiunta attraverso gli sforzi di un singolo Stato o di un piccolo gruppo di Stati.

In secondo luogo, gli effetti negativi del cambiamento climatico non sono osservabili ora, ma si prevede che si verificheranno solo alcuni anni dopo. Si tratta quindi di un problema intergenerazionale (art. 9 Cost.): si prevede che le generazioni attuali paghino i costi per i benefici dei loro successi due o più generazioni nel futuro. I leader politici che cercano di intervenire efficacemente sul cambiamento climatico devono convincere i loro cittadini sia che le loro azioni possono fare la differenza, in parte incoraggiando altri Paesi ad agire, sia che i costi sostenuti oggi sono nell'interesse delle generazioni successive[35].

In terzo luogo, per modificare le pratiche relative al cambiamento climatico è necessario cambiare le abitudini di miliardi di persone e di organizzazioni come le imprese; ma le politiche pratiche per generare incentivi per questi cambiamenti

34 Faure e Nollkaemper, 2007: 123 ss.; Voigt, 2008: 1 ss.; Klinski, 2009: 377 ss.; Fitzmaurice, 2010:89 ss.; Ferenandez Egea, 2011: 375 ss.; Lefeber 2012: 321 ss.

35 Bartolucci 2024: 39; Gazzolo 2024: 89; De Francesco 2023: 139; Molfetta, 2023: 222; Bifulco 2021; Bin 2021; Carducci 2021; Montaldo 2021; Pignataro 2021; Roerig 2021.

comportamentali richiedono l'azione dei governi che, in molti casi, potrebbero non avere l'interesse o la capacità di esercitare molta influenza sui propri cittadini.

Un'altra questione preliminare risiede nell'individuazione della norma primaria sul cambiamento climatico la cui violazione da parte di uno Stato, attraverso una condotta a esso attribuibile, costituisca un illecito internazionale per il quale lo Stato stesso sia responsabile. Ai fini della presente indagine, interessano gli obblighi non già procedurali, bensì materiali, direttamente disciplinanti la determinazione del fenomeno. È sintomatico che, ancorché si tratti di un numero esiguo di Paesi, alcuni Stati insulari, che sono tra quelli più esposti agli effetti del cambiamento climatico, hanno dichiarato che le rispettive ratifiche dell'emendamento di Doha al Protocollo di Kyoto[36] e dell'Accordo di Parigi non implicano la rinuncia ad alcun diritto al risarcimento dei danni provocati dal cambiamento climatico o, più in generale, ad alcun diritto derivante dal regime di responsabilità internazionale degli Stati[37].

Con riguardo alla cessazione dell'illecito, accompagnata, se del caso, da adeguate garanzie di non ripetizione, deve osservarsi che la riduzione del rilascio di un'eccessiva quantità di emissioni di gas serra, nonché il suo assorbimento, possono realizzarsi solo gradatamente, entro un arco di tempo piuttosto ampio, cosicché lo Stato responsabile non potrebbe rapidamente porre termine all'illecito.

Anche per costituirsi come cittadini (digitali), i rivendicatori di diritti devono non solo essere autenticamente coinvolti nelle loro richieste, ma anche esprimerle nel linguaggio dei diritti. Questo impegno qualifica la dimensione politica della loro azione, poiché comporta l'assunzione di responsabilità verso gli altri, in modo prospettivo e proattivo: "diventare politico è il momento in cui ci si definisce come esseri capaci di giudizio sul giusto e sull'ingiusto, si assume la responsabilità di quel giudizio e si sceglie di unirsi ad altri o di opporsi ad altri per adempiere a tale responsabilità". La necessità di rivendicazioni qualificate richiede, infatti, non solo un autentico impegno verso i diritti invocati, ma anche, più in profondità, il riconoscimento degli altri come soggetti di diritti, pari e uguali[38].

Ciò precisato circa la cessazione dell'illecito, in merito al contenuto della responsabilità occorre soffermarsi maggiormente sull'obbligo di riparazione.

36 Adottato nel 2012 dalla Conferenza delle Parti del Protocollo di Kyoto (par. 1 della decisione 1/CMP.8, in FCCC/KP/CMP/2012/13/Add.1), il c.d. Emendamento di Doha non è mai entrato in vigore a causa del mancato raggiungimento del necessario numero di ratifiche. Esso avrebbe dovuto aggiornare il Protocollo, rinnovando gli impegni di mitigazione del cambiamento climatico per un secondo commitment period, intercorrente tra il 2013 e il 2020

37 Con riguardo all'Emendamento di Doha, la dichiarazione è stata apposta dalle Isole Marshall, dalla Micronesia, da Nauru e dalle Isole Salomone. Rispetto all'Accordo di Parigi, un'analoga dichiarazione è stata apposta da Nauru, Tuvalu, Niue, Vanuatu, dalla Micronesia, dalle Isole Cook e dalle Isole Salomone, mentre le Isole Marshall hanno più genericamente affermato di non rinunciare ad "any rights under any other laws, including international law".

38 Gorgoni 2023: 507.

In primo luogo, la *restitutio in integrum* sarebbe difficilmente applicabile. Consistendo nel ripristino della situazione esistente prima della commissione dell'illecito, la restituzione esigerebbe che lo Stato responsabile realizzasse un abbassamento delle temperature globali. È evidente che siffatto obiettivo è 'materialmente impossibile', solo che si consideri la molteplicità di fattori, antropogenici e non, che incidono sulle temperature terrestri. Lo stesso problema è ravvisabile nelle ipotesi di violazione del cyber spazio – da considerarsi come la continuità dello spazio fisico e non come un'astrazione – gli attacchi informatici infatti rischiano di pregiudicare irrimediabilmente la privacy dei soggetti colpiti e anche in questo caso la *restitutio in integrum* è difficilmente applicabile[39].

In secondo luogo, il surriscaldamento globale, in quanto tale, non rappresenta un danno concreto, quantificabile in termini economici secondo la definizione di danno risarcibile fornita dalla Commissione del diritto internazionale. Proprio in ragione dell'astrattezza del pregiudizio consistente nell'innalzamento delle temperature *ex se*, verrebbero in rilievo le note difficoltà del risarcimento del c.d. 'danno ambientale puro'. Peraltro, sarebbe irragionevole se si pretendesse che gli Stati offensori, che avessero massicciamente contribuito al cambiamento climatico, risarcissero i costi sostenuti dalla generalità degli Stati, tutti egualmente colpiti dall'innalzamento globale delle temperature, per la mitigazione del surriscaldamento, provocato anche da fattori non antropogenici.

Infine, la soddisfazione sembra una forma di riparazione inadeguata, o comunque insufficiente, a causa della portata e della gravità dell'innalzamento delle temperature. Ciò, senza considerare che l'identificazione del pregiudizio nell'innalzamento delle temperature comporterebbe un arduo appuramento del nesso di causalità. Tralasciando la pluralità di fattori che contribuiscono al surriscaldamento globale, la ricostruzione del nesso di causalità sarebbe ostacolata dalla menzionata distanza temporale tra il rilascio di gas serra e l'innalzamento delle temperature, attesa la permanenza di tali gas nell'atmosfera e la gradualità del cambiamento climatico. Quantunque sia pressoché certo, in generale, il contributo delle emissioni di gas al surriscaldamento globale, appare difficilmente accertabile la consequenzialità tra determinate emissioni di gas serra, provenienti da certi Stati in un dato momento storico, e l'aumento delle temperature terrestri in uno specifico periodo successivo, ancorché notevoli progressi scientifici siano stati compiuti in tale direzione.

Tre variabili forniscono un quadro analitico utile per indagare l'evoluzione della *governance* del clima e di Internet. In primo luogo, i progressi tecnologici che hanno dato vita al cyberspazio stanno plasmando sia il ritmo del cambiamento climatico sia le modalità con cui può essere affrontato, come si può vedere nel calo dei prezzi delle energie rinnovabili. In secondo luogo, la crescente scarsità sta influenzando le decisioni di governance in entrambi i settori[40], così come in

39 Bonfanti 2018: 118.

40 Anche se pochi se ne accorgono, vista la velocità con cui Internet è riuscita a scalare insieme al numero e al tipo di domini di primo livello, alcuni aspetti del cyberspazio sono sempre più scarsi, compreso un elemento fondamentale: lo spazio per gli indirizzi IP.

tutti i beni comuni globali. In terzo luogo, la variabile strutturale della politica multipolare, sorta dopo la fine della Guerra Fredda e il 'momento unipolare' degli Stati Uniti, sta frammentando i forum multilaterali, rendendo molto più difficile il raggiungimento del consenso sulle questioni di governance.

3. Il concetto di '*global commons*'

In termini generali e nella terminologia delle scienze sociali, si parla di 'comune' dove un bene non è, o forse non può essere, appropriato da una singola entità, ma serve e deve essere curato dalla collettività di riferimento.

La necessità di organizzare l'uso e la conservazione di un bene comune e i relativi problemi di azione collettiva sono talvolta evidenziati parlando della "tragedia dei beni comuni"[41], ricordandosi che nel 2009 è stato assegnato il Premio Nobel a Elinor Ostrom per le sue innovative ricerche economiche in questo settore[42]. La gestione dei beni comuni richiede – e non è solo una questione semantica – un approccio comune ed è in parte altresì legata all'idea di intendere l'ordinamento giuridico internazionale come una 'comunità'.

È scientificamente provato che il clima ha un ruolo essenziale per il pianeta e per l'umanità e che la sua stabilità può essere messa in discussione dalle emissioni che avvengono in numerosi luoghi del pianeta[43]. Pertanto, non si può dubitare che il clima sia un bene pubblico e che debba essere considerato un bene comune globale.

Per organizzare l'uso e la manutenzione collettiva di un bene comune è necessario che sussista un quadro giuridico chiaro, tanto che la stessa prospettiva giuridica può contribuire alla comprensione del contesto, dei mezzi a disposizione, dei difetti, dei successi e dei fallimenti dell'azione collettiva per la gestione dei beni comuni.

A livello internazionale, le aree che non rientrano nella giurisdizione di un singolo Paese sono definite 'beni comuni internazionali o globali'. La nozione di beni comuni globali presuppone che ci siano limiti alla sovranità nazionale in alcune parti del mondo e che queste aree siano aperte all'uso da parte della comunità internazionale, ma chiuse all'appropriazione esclusiva tramite trattati o consuetudini. Esempi sono l'alto mare, l'Antartide, lo spazio esterno e l'atmosfera, ma anche il cyber-spazio. I beni comuni globali sono spesso regolati da normative a più livelli, come quello internazionale, regionale e nazionale. Non esiste un principio giuridico vincolante per governare i beni comuni globali, ma il più vicino storicamente utilizzato è il concetto di patrimonio comune (CHM). Poiché il cyber-spazio è l'aggiunta più recente alla sfera dei beni comuni globali, vale la pena considerare come il CHM possa essere applicato per migliorare la sicurezza informatica[44].

41 Hardin, 1968: 1243-1248; Fox, 1996: 2499-2542.

42 Sul punto si richiama Ostrom, 1990; Ostrom et al.,1994; Ostrom, 2010.

43 Si rimanda, di nuovo, al V rapporto sul clima: the Fifth Assessment Report (AR5) of the Intergovernmental Panel on Climate Change (IPCC) of 2014, http://www.ipcc.ch/

44 Mulligan, Schneider, 2011: 70.

Non esiste ancora un accordo su una definizione comune e consolidata di CHM, ma il CHM può essere definito da cinque elementi: 1) non ci possono essere appropriazioni private o pubbliche; nessuno possiede legalmente gli spazi del patrimonio comune; 2) i rappresentanti di tutte le nazioni devono lavorare insieme per gestire le risorse del *pool* di beni comuni globali; 3) le nazioni devono condividere attivamente i benefici acquisiti dallo sfruttamento delle risorse della regione del patrimonio comune; 4) non ci possono essere armi o installazioni militari nelle aree del patrimonio comune, perché dovrebbero essere utilizzate per scopi pacifici; 5) i beni comuni devono essere preservati per le generazioni future[45].

Tuttavia, è difficile delimitare il cyberspazio, al pari di quanto può dirsi in relazione ad un controllo dell'uso dell'atmosfera per prevenire il cambiamento climatico. Se non viene controllata, la perpetrazione di minacce cibernetiche può destabilizzare la sicurezza informatica o addirittura la pace del cyberspazio. A questo punto è importante discutere le implicazioni del modo in cui percepiamo il cyberspazio: è un 'bene comune' o è un insieme di infrastrutture fisiche composto da cavi, hardware, fibre ottiche, tubi o Internet? Il fatto che diverse infrastrutture di Internet siano possedute e gestite da aziende private e soggette a una *governance* multilivello presuppone che il cyberspazio sia un bene atipico o 'imperfetto', controllato da entità pubbliche e private e soggetto a una combinazione di diversi strumenti e strategie politiche private e pubbliche.

4. Conclusioni

È chiaro che la *governance* dell'internet non prenderà, anzi, probabilmente non potrà prendere, la stessa traiettoria di quella adottata per affrontare i cambiamenti climatici. La *governance* del cambiamento climatico ha le sue radici fondamentali saldamente collocate all'interno dei sistemi di relazioni internazionali esclusivi e incentrati sullo Stato. Tuttavia, coloro che cercano di domare il "problema malvagio" della cybersicurezza possono trarre spunto dalla manovra ibrida adottata con l'Accordo di Parigi[46] per aggirare l'impasse dei negoziati basati sugli Stati e attingere al potenziale di altri interessi acquisiti, in particolare le imprese, per diventare parte di un approccio di *governance* più diffuso.

Senza il requisito che tutte le regole siano imposte da un'istituzione comune, può essere possibile adattare le regole a condizioni diverse su questioni diverse, o per coalizioni diverse di attori (es. regole per i Paesi in via di sviluppo, regole per membri del G8 ecc.). Diversi Stati potrebbero aderire a diverse serie di accordi, rendendo più probabile il rispetto di alcuni vincoli sulle emissioni di gas serra.

I regimi complessi possono anche avere una maggiore adattabilità nel tempo. Ancor più pare evidente che le nazioni che non sono vincolate perché non hanno aderito agli accordi godono dei benefici dovuti ai sacrifici di altre nazioni senza

45 Frakes, 2003, cit.: 409.
46 Bodansky, 2016: 288 ss.; Gervasi, 2016: 21 ss.

rendersi conto dei costi; le soluzioni "negoziate a livello globale, se non sono sostenute da una serie di sforzi a livello nazionale, regionale e locale,… non sono garantite per funzionare bene"[47].

I cambiamenti nelle diverse aree tematiche, o all'interno della politica interna dei diversi Paesi, possono avvenire a ritmi diversi. A differenza delle regole provenienti dalle istituzioni sovrane gli accordi bilaterali o multilaterali possono essere in grado di adattarsi più prontamente, soprattutto quando l'adattamento richiede cambiamenti complessi nelle norme pregresse e nei comportamenti.

Disporre di un linguaggio condiviso come quello fornito dall'IPCC contribuirebbe a facilitare la collaborazione tra la comunità tecnica, le imprese e i responsabili delle politiche governative. L'organizzazione adatta a ricoprire questo ruolo non è immediatamente evidente, ma forse un consulente delle Nazioni Unite per le tecnologie digitali, come proposto dall'UNHLP sulla cooperazione digitale, potrebbe essere una valida opzione.

È diventato sempre più chiaro che i meccanismi, i forum e gli strumenti sviluppati per affrontare i problemi di sicurezza globale delle tecnologie emergenti non sono in grado di far fronte alle esigenze dell'ultimo decennio di innovazione tecnologica e non sono assolutamente attrezzati per andare avanti nel prossimo decennio. L'Accordo di Parigi ha rotto lo stampo in cui era stato inserito: quello di un trattato *top-down* basato su regole gerarchiche e centrate sullo Stato. In questo modo, sostiene Falkner, ha posto le basi per una "nuova logica della politica climatica internazionale". L'Accordo di Parigi ha creato spazi per rendere visibili le molteplici interconnessioni esistenti a livello globale. Ha modellato un percorso che ha permesso a coloro che sono stati colpiti, non solo dal cambiamento climatico ma anche dalle misure di risposta, di far sentire la propria voce, di iniziare a rivendicare il proprio potere e di definire una politica che rispondesse alle loro priorità – in particolare le donne nei Paesi in via di sviluppo, le popolazioni indigene e i popoli sfollati. È probabile che lo stesso debba accadere nella *governance* globale della tecnologia e che la capacità dei sistemi IoT di provocare danni fisici sia il catalizzatore di questa trasformazione.

La gestione delle sfide alla sicurezza globale che emergono richiederà una rigida regolamentazione a livello statale, un coordinamento internazionale e il coinvolgimento di un'ampia gamma di altri attori pubblici e privati. Per un solido processo decisionale in questo ambito, saranno fondamentali e indispensabili meccanismi molto più efficaci per fornire supporto tecnico alle politiche. Non mancano i precedenti di progressi significativi nella mitigazione dei problemi di sicurezza globale. Ma è chiaramente giunto il momento di smettere di guardare allo stesso terreno all'interno della cybersecurity, degli studi strategici e delle relazioni internazionali per trovare ispirazione per progredire nella *governance* delle tecnologie emergenti. Gli approcci multidisciplinari sono essenziali a livel-

47 Si veda Ostrom 2010, che spiega che c'è "almeno un risultato [che] produce rendimenti più elevati per tutti coloro che sono coinvolti, ma i partecipanti… che massimizzano i benefici a breve termine prendono decisioni indipendenti e non sono predisposti a raggiungere questo risultato".

lo accademico: riunire studiosi di informatica, ingegneria, ecologia, diplomazia e diritto è un elemento integrante per rafforzare le discussioni tecniche e politiche in ambito pratico. Come farlo in modo efficace sarà la sfida del nostro tempo e il suo raggiungimento trasformerà la (in)sicurezza informatica globale in modo più profondo di qualsiasi innovazione tecnica.

Bibliografia

Barone A. 2023, "Il sindacato sugli atti di pianificazione o programmazione, con particolare riferimento al PNRR", in *Il Processo*, 2: 383 s.

Bartolucci L. 2024, "La valutazione di impatto generazionale delle leggi come forma di attuazione degli articoli 9 e 97 della Costituzione", in *federalismi.it*, (4): 39 (in https://federalismi.it/nv14/articolo-documento.cfm?artid=50152).

Berman p. S. 2018, "Global Legal Pluralism as a Normative Project", in *UC Irvine Law Review*, 8(2): 149-82.

Bevilacqua D., Chiti E. 2024, *Green Deal. Come costruire una nuova Europa*, Bologna: Il Mulino.

Bifulco R. 2021, "Perché la storica sentenza tedesca impone una riflessione sulla responsabilità intergenerazionale", in *LuissOpen*.

Bin R. 2021, "La Corte tedesca e il diritto al clima. Una rivoluzione?", in *LaCostituzione.info*. (in https://www.lacostituzione.info/index.php/2021/04/30/la-corte-tedesca-e-il-diritto-al-clima-una-rivoluzione/).

Bodansky D. 2016, "The Paris Climate Change Agreement: A New Hope?", in *AJIL*, 288 ss;

Bonfanti A. 2018, "Attacchi cibernetici e cyber war: considerazioni di diritto internazionale", in *Notizie di Politeia*, n. XXXIV(132): 118.

Brillat M. 2023, "L'urgence climatique devant la Cour européenne des droits de l'homme: enjeux et perspectives à partir des audiences du 29 mars 2023", in *Dalloz actualité*. (in https://www.dalloz-actualite.fr/flash/l-urgence-climatique-enfin-devant-cour-europeenne-des-droits-de-l-homme-enjeux-et-perspectives).

Caputi Jambrenghi V. 1989, "Valutazione d'impatto ambientale e garanzie giustiziali", in *Sanità pubbl.*: 301;

Caputi Jambrenghi V. 1996, "Tutela dell'ambiente e beni pubblici. Provocazioni per uno studio sul dominio ambientale eminente", in *Scritti Predieri*, I.

Caputi Jambrenghi V. 2009, "La fase istruttoria nei procedimenti amministrativi di tutela preventiva dell'ambiente", in Parisio V. (a cura di) *Diritti interni, diritto comunitario e princìpi sovranazionali. Profili amministrativistici*, Milano: Giuffrè, 49.

Carducci M. 2021, "Libertà 'climaticamente' condizionate e governo del tempo nella sentenza del BVerfG del 24 marzo 2021", in *LaCostituzione.info* (in https://www.lacostituzione.info/index.php/2021/05/03/liberta-climaticamente-condizionate-e-governo-del-tempo-nella-sentenza-del-bverfg-del-24-marzo-2021/).

Carducci M. 2021, "Climate Change and Legal Theories", in Pellegrino G. (a cura di), *Handbook of the Philosophy of Climate Change, Climate Change, Social Sciences and Philosophy,* Cham: 1-26;

Carr M. e F. Lesniewska 2020, "Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance", in *International Relations*, 34(3): 391-412 (in https://doi.org/10.1177/0047117820948247).
Cassotta S. e M. Pettersson 2019, "Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example", in *Bejiing Law Review*, 10(03): 616-642.
Clarich M. 2007, "La tutela dell'ambiente attraverso il mercato", in *Dir. pubbl.*: 219.
Chiti L. 2022, "Chi inquina paga. La crisi climatica è (anche) una questione di giustizia", in *Aggiornamenti sociali*, 2022: 680 – 686.
Coen D. e T. Pegram 2015, "Wanted: A Third Generation of Global Governance Research", in *Governance*, 28 (4). (in https://papers.ssrn.com/abstract=2765904).
Colucci C. 2020, *Studio dello scambio radiativo in un canyon urbano: analisi delle riflessioni multiple come una delle cause del fenomeno uhi e di un possibile intervento di mitigazione*. (in https://core.ac.uk/display/288655941).
Corvese C.G. 2022, "La sostenibilità ambientale e sociale delle società nella proposta di 'corporate sustainability due diligence directive' (csddd) (dalla 'insostenibile leggerezza' dello scopo sociale alla 'obbligatoria sostenibilità' della 'due diligence')", in *Banca Impresa Società*: 391.
De Bellis M. 2021, "Certification and climate change. The role of private actors in the clean development mechanism", in *Riv. it. dir. pubbl. comunit*: 759.
De Francesco G. 2023, "Note brevi sulla 'questione ambientale'. Una lettura evolutiva delle esigenze e dei livelli della tutela", in *La Legislazione penale* (4): 139;
De Nicola M., "Difendere e creare valore con la cybersecurity", in *Controllo di gestione*, 1/2023: 37 ss.
Faure M.G e A. Nollkaemper 2007, "International Liability as an Instrument to Prevent and Compensate for Climate Change", in *SELJ*, (26A): 123 (in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1086281).
Fernández Egea R.M. 2011, "State Responsibility for Environmental Harm, 'Revisited"'within the Climate Change Regime", in S. Maljean-Dubois, L. Rajamani (a cura di) 2011, L*a mise en* œuvre *du droit international de l'environnement*, London/Boston: 375 ss.
Fitzmaurice M. 2010, "Responsibility and Climate Change", in *GYIL* (53):89 ss.
Force Hill J. [2012] (2014), "Internet Fragmentation Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers", in *Harvard Belfer Center for Science and International Affairs Working Paper* (in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439486).
Fornasari R. 2022, "Comandare allo stato di agire: 'climate change' e responsabilità civile del potere pubblico", in *Persona e Mercato*, 3: 480.
Fox S.T. (1996), "Responding to Climate Change: The Case for Unilateral Trade Measures to Protect the Global Atmosphere", in *The Georgetown Law Journal* 84(7):2499-2542.
Gazzolo T. 2024, "Da dove vengono le generazioni future? (Commento a: F.G. Menga, 'Etica intergenerazionale', Morcelliana, 2021)", in *Notizie di Politeia*, (153): 89;
Gervasi, M. 2016, "Rilievi critici sull'Accordo di Parigi: le sue potenzialità e il suo ruolo nell'evoluzione dell'azione internazionale di contrasto al cambiamento climatico", in *CI*: 21 ss.
Gherri B. 2012, *Il confort outdoor per gli spazi urbani*, *Ecocities* (in www.researchgate.net/publication/323006526).

Giannini M.S. 1973, "Ambiente: saggio sui diversi suoi aspetti giuridici", in *Riv. trim. dir. pubbl.*:15.
Giliberto C. 2024, "Cambiamenti climatici: impatti sul sistema economico-finanziario e gestione del rischio", in *Amministrazione & Finanza*, 2/2024: 64 ss.
Gorgoni G. 2023, "Being digital citizens by claiming rights on the cyberspace. A ricoeurian reading"*, in Ragion pratica*, *Rivista semestrale* (2): 507.
Gratani A. 2013, Le quote per inquinare: a titolo gratutito o oneroso?, in *Riv. giur. amb.*: 392.
Hardin G. (1968), "The Tragedy of the Commons", in *Science* 162(13): 1243-1248.
Hussein M.T., Trautman L.J., Ngamassi L.; Molesky M.J. 2022, "Climate, Cyber Risk, and the Promise of the Internet of Things (IoT)", in *SSRN Eletronic Journal* (in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3969506).
Kilinski J. 2009, "International Climate Change Liability: A Myth or Reality?", in *JTLP*: 377 ss.
Klein J. e Hossein K. 2020, "Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change", in *Arctic Review on Law and Politics*, 11: 1-18.
Landini S., "Principio di precauzione, responsabilità civile e danni da eventi catastrofali", in *Contratto e impresa/Europa*, 1/2014, 14 ss.
Lazarus R. 2008, "Super Wicked Problems and Climate Change: Restraining the Present to Liberate the Future", in *Cornell Law Review*, 94, 1153.
Lefeber R. 2012, "Climate Change and State Responsibility", in R. Rayfuse, S.V. Scott (a cura di) 2012, *International Law in the Era of Climate Change*, Cheltenham: Northampton: 321 ss.
Lessig L. (1999), "The Law of the Horse: What Cyberlaw Might Teach", in *Harv. L. Rev.* (113): 501, 502, 533.
Majocchi A. 2024, *Il ruolo di Cina ed Europa nella lotta ai cambiamenti climatici* (in www.csfederalismo.it).
Mauro A.*,* Il principio 'chi inquina paga' nelle sfide della 'environmental justice'", in *giustizia civile.com* (in https://giustiziacivile.com/).
McGinnis M.D. 2011, "Costi e sfide della governance policentrica: An Equilibrium Concept and Examples from U.S. Health Care", in *Conference on Self-Governance, Polycentricity, and Development* (Renmin University, Beijing, China) (8 maggio 2011) (in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2206980).
Meli M. 2023, "Ancora sul principio chi inquina paga e sull'obbligo di bonifica del proprietario incolpevole", in *Giurisprudenza italiana*: 2045 – 2052.
Molfetta A. 2023, "L'interesse delle future generazioni oltre la riforma degli articoli 9 e 41 della costituzione (Intervento al Seminario 'Ambiente e salute: le prospettive di tutela alla luce della legge costituzionale n. 1 del 2022', Università degli Studi dell'Insubria, 20 gennaio 2023)", in *Rivista AIC*, (2): 222
Montaldo R. 2021, "La neutralità climatica e la libertà di futuro (BVerfG, 24 marzo 2021)", in *Diritticomparati.it.* (in https://www.diritticomparati.it/la-neutralita-climatica-e-la-liberta-di-futuro-bverfg-24-marzo-2021/).
Mulligan D.K. Schneider E.F.B. 2011*,* "Doctrine for Cybersecurity", in *Daedalus*, n. 140, vol. 4, 70.
Murray A. 2006, *The Regulation of Cyberspace, Control in the Online Environment*, Routledge; Cavendish.
Neri L., Russo A. 2018, "La gestione del cyber risk: riflessioni sul tema, in *Controllo di gestione*, 4/2018, 43 ss.

Ostrom E. 1990, *Governing the Commons: the Evolution of Institutions for Collective Action*, Cambridge: University Press.
Ostrom, E. 2010, *A Polcycentric Approach for Coping with Climate Change*, Policy Research Working Paper 5095, World Bank (in http://www10.iadb.org/intal/intalcdi/pe/2009/04268.pdf).
Ostrom, E. et al. 1994, *Rules, Games and Common-pool Resources*, University of Michigan Press.
Pernice G. 2024, "Gestione d'affari non rappresentativa supera il principio 'chi inquina paga', nota a Consiglio di Stato, Sezione IV, 2 febbraio 2024 n. 1110", in *Guida al Diritto*: 95-98.
Pignataro M. 2021, "Il dovere di protezione del clima e i diritti delle generazioni future in una storica decisione tedesca", in *EuBlog.eu* (in https://eublog.eu/articolo/34751/Il-dovere-di-protezione-del-clima-e-i-diritti-delle-generazioni-future-in-una-storica-decisione-tedesca/Pignataro).
Rakes J. 2003, "The common heritage of mankind principle and the deep seabed, outer space, and Antarctica: will developed and developing nations reach a compromise?", in *Wisconsin International Law Journal*, 21(2): 409-434.
Roerig M.T. 2021, *Tribunale costituzionale federale, ordinanza del 24 marzo 2021 (1 BvR 2656/18, 1 BvR 96/20, 1 BvR 78/20, 1 BvR 288/20, 1 BvR 96/20, 1 BvR 78/20), in merito alla tutela del clima e alla riduzione di emissioni di gas serra anche a garanzia delle libertà delle generazioni future*, Servizio studi della Corte costituzionale.
Sandulli M.A. 2019, "Cambiamenti climatici, tutela del suolo e uso responsabile delle risorse idriche", in *Riv. giur. ed.*, II: 291.
Santiello p. 2022, "Consumo di suolo: la rigenerazione urbana come veicolo di sostenibilità", in *Le Regioni*: 105 s.
Shackelford S. 2016 [2015], "On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems", *Vanderbilt Journal of Entertainment & Technology Law*.
Shackelford S.J. e T. L Fort 2016, "Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks", in *University of Illinois Law Review*, 2016.
Voigt C. 2008, "State Responsibility for Climate Change Damages", in *NJIL* (77): 1 ss.

Teresa Monaco

Ambiente naturale e ambiente digitale: una nuova declinazione del principio di precauzione

Abstract: Nell'ottica di una regolamentazione giuridica dei sistemi di cybersecurity, il presente studio mira a valutare la possibilità dell'applicazione del principio di precauzione anche al cosiddetto "ambiente digitale", cioè allo spazio di interazione e integrazione tra uomo e macchina (nel quale rilievo assumono i sistemi di AI), con particolare attenzione al suo uso da parte delle pubbliche amministrazioni e in particolare delle agenzie pubbliche di cybersecurity. Tale estensione parte dalla tesi secondo la quale l'ambiente digitale ha i medesimi livelli di rischio sulla salute delle persone propri dell'ambiente "naturale". Lo studio, quindi, metterà in evidenza la necessità del giusto bilanciamento tra il bisogno di una crescente sicurezza quale manifestazione di un interesse pubblico e il rischio di una eccessiva compressione dei diritti e delle libertà dei singoli, alla luce dei principi di adeguatezza e proporzionalità ribaditi nel Regolamento Ue/2023/2841. Infine, si procederà ad una analisi dei principi di precauzione e di valutazione del rischio nelle diverse forme di regolamentazione e di autoregolamentazione tipiche della cyber security.

Keywords: Ambiente digitale; Ambiente naturale; Principio di precauzione; Rischio; Valutazione impatto digitale.

1. Introduzione

L'uso delle tecnologie e del digitale ha un peso sempre più forte nell'esistenza di ognuno. Il nesso tra 'ambiente' e 'digitale' e l'accostamento dei due termini per la creazione della nuova locuzione 'ambiente digitale' è determinata dal forte parallelismo che esiste tra l'ambiente naturale e quello digitalizzato, in particolare su almeno tre piani.

In primo luogo, è possibile notare una similitudine innanzitutto temporale: l'Unione Europea e, a cascata, gli Stati nazionali sono alle prese con una doppia transizione, quella ambientale (ed energetica) e quella digitale[1].

1 Per una recente disamina delle cd "transizioni gemelle", si veda Camisa 2024: 55-75.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760151

È possibile riscontrare, poi, una similitudine strutturale: i due ambienti sono caratterizzati da una forte presenza umana e dalla manipolazione da parte dell'essere umano. Inoltre, sono ambienti in cui la presenza del rischio e del pericolo è preponderante.

È possibile, infine, rilevare una similitudine nella risposta che viene data alla presenza dell'incertezza: la gestione del rischio il *trait-d'union* che esiste nella normativa (comunitaria e italiana) su cybersecurity e regolazione dell'intelligenza artificiale.

L'ambiente digitale che, allo stato attuale e per la tecnologia presente sul mercato, risulta essere quello più 'minaccioso' è sicuramente quello legato all'intelligenza artificiale. Gli algoritmi di A.I. sono l'oggetto dell'attenzione sia da parte del mercato privato che da parte delle pubbliche amministrazioni per gli sviluppi e le possibilità che possono fornire. Allo stesso tempo, proprio in virtù dell'attenzione che suscitano, sono anche al centro dell'attuale dibattito dottrinale e dello sforzo regolativo. Inoltre, in virtù della loro concezione e strutturazione, sono gli algoritmi con il più alto tasso di incertezza. L'intelligenza artificiale risponde, quindi, alle tre caratteristiche enucleate in precedenza, diventando l'ambiente digitale per eccellenza.

2. La società dell'incertezza

L'ambiente digitale, così come quello naturale, presenta una serie di caratteristiche strutturali: innanzitutto è un contesto complesso, caratterizzato da un gran numero di variabili – già di per sé generatrici di complessità –, a cui si unisce l'interazione che esse hanno tra loro (ulteriore elemento che aumenta il grado di complessità dell'ambiente).

In una società del rischio[2], nuova tipologia di strutturazione della moderna società[3], il fulcro risiede nella presenza di rischi che valicano i confini nazionali diventando globali, in grando di influenzare la vita sociale, economica e politica[4]. Lo sviluppo tecnologico e l'interazione internazionale hanno ulteriormente ampliato i rischi, aggiungendone di 'nuovi' ed elevando il grado di complessità del contesto, tanto da spingere alcuni autori[5] a definire la moderna società come "dispensatrice di rischi".

In una società del genere, la richiesta avanzata dai cittadini è di governare il rischio[6]. Consci dell'impossibilità di azzerarlo, sono in cerca di una modalità che

2 Beck 2000: 67; si veda anche Iannello 2014: 2.

3 Beck 2000: 14, ricorda che il rischio non è una invenzione della modernità. La differenza sta nel fatto che ciò in passato "si trattava di rischi personali, non di pericoli globali come quelli che incombono sull'umanità" come avviene, invece, nella società moderna.

4 Cibella 2023: 511-536

5 Iannello, già citato.

6 Ragone 2019: 159 sostiene che la gestione del rischio è uno degli attributi che la modernità ha aggiunto agli Stati: "Nella storia del costituzionalismo, lo stato social-democratico si è

consenta di mitigarne gli effetti e di garantire un livello maggiore di sicurezza: i cittadini chiedono ai governi di difenderli da rischi eccessivi ed incerti. E da questa aspirazione nasce l'idea della precauzione, condensata nel motto *Better Safe than Sorry*: un'idea oggi centrale nell'ambito della normativa ambientale, probabilmente il settore del diritto nel quale il ragionamento scientifico ha maggiore importanza[7].

L'aumento dei fattori di rischio nell'attuale strutturazione della società determinerebbe la necessità del ricorso al principio di precauzione[8] in diversi ambiti ulteriori rispetto a quelli all'interno del quale è nato[9], cioè tutela della salute e dell'ambiente. Nel corso tempo, questo superamento dei confini è avvenuto su una serie di materie: il principio è stato impiegato anche per le politiche di bilancio degli stati UE, sottoforma di "principio di precauzione finanziaria"[10]; infine per fenomeni come terrorismo e immigrazione[11].

In questo contesto di espansione del principio di precauzione al di fuori dei tradizionali ambiti di riferimento, sembra possibile allargare lo spettro della riflessione sul rischio pure ai rapporti tra intelligenza artificiale e pubblica amministrazione. Il tutto, per altro, al di là dei pur interessanti profili applicativi già individuati sia in sede dottrinaria che giurisprudenziale, come ad esempio per la regolazione del rischio 'tecnico' in sede di partecipazione alle gare pubbliche[12].

3. Pericolo e rischio

A venire in rilievo, quindi, è la nozione di rischio, da tenere sempre correlata a quella di pericolo (i due elementi sono stati per lungo periodo sovrapposti[13]).

Con "rischio" si intende "la probabilità che un effetto negativo colpisca un essere umano o l'ambiente per effetto dell'esposizione ad un pericolo, che può essere biologico, fisico o chimico" (da non confondersi con la nozione di "incertezza" che è una "situazione di dubbio circa l'affidabilità, l'accuratezza o la rilevanza di una informazione")[14]. Presupposto della definizione del concetto di rischio – e del-

gradualmente incaricato di garantire ai propri cittadini la protezione di una serie di beni ritenuti preminenti (in primis salute e ambiente) attraverso interventi proattivi e preventivi. In questo contesto, il principio di precauzione è divenuto criterio atto ad orientare la decisione politica nell'attuazione di misure volte a fronteggiare una pluralità di fattori di rischio, i quali – in un dato momento storico – sono ritenuti più meritevoli di attenzione di altri".

7 DeSadeleer 2006: 139-172.

8 De Leonardis 2005.

9 Barone 2020: 65

10 Perez 2011: 1043-1055

11 Simoncini 2010.

12 Barone, già citato.

13 A loro volta differenti dalla nozione di azione preventiva e del principio di prevenzione. Gros, Serges 2013: 710, sostiene che il principio di prevenzione "muove dalla pretesa di una 'certezza scientifica' – concetto di per sé piuttosto fumoso […], allorché in realtà può parlarsi, al limite, di una minore incertezza, ma non certo di una certezza – per la quale si possono conoscere quali danni potrebbero prodursi, ma non se effettivamente tali danni si produrranno".

14 Per le definizioni di rischio e incertezza si veda Salter e Howsam 2002: 208-213.

la conseguente invocazione del principio di precauzione – è l'assenza di certezze scientifiche. La necessità di definire ciò che è considerabile rischio è rilevante proprio in virtù del conseguente principio da applicare: in un ambito caratterizzato dal rischio, si agisce escludendo altri principi e orientando il proprio agire in base a quello di precauzione. Ecco perché appare necessario effettuare il discrimine tra pericolo e rischio e, successivamente, dalla possibilità di agire orientati da prevenzione o da precauzione.

Eventi[15] o situazioni strutturali[16] possono stressare gli ordinamenti giuridici, determinando una doppia conseguenza: la necessità di resistere alla situazione in questione e, dall'altro lato, reagire a ciò che mette alla prova l'ordinamento. Questo genere di azioni implica un dialogo serrato tra diritto costituzionale e diritto amministrativo: il primo è chiamato a fornire la cornice entro la quale affrontare i fenomeni; il secondo deve fornire gli strumenti di gestione.

Quando si tratta di emergenza, gli strumenti del diritto amministrativo diventano straordinari per adeguarsi a fenomeni straordinari. Nel caso dell'intelligenza artificiale, i confini tra emergenza e rischio sono molto sfumati: un fenomeno strutturale non può di per sé essere emergenziale[17]. Eppure, un fenomeno sempre diverso da se stesso non può nemmeno essere considerato parte dell'ordinamento *tout-court*. Il fenomeno emergenziale è *extra ordinem* per il diritto amministrativo, tanto che si rende necessario l'inserimento di nuovi strumenti e l'attribuzione di nuovi poteri. L'intelligenza artificiale è nei fatti elemento interno all'ordinamento né, per la sua diffusione stabile, assume carattere momentaneo, come sono temporanee le misure giuridiche adottate[18].

Entra, così, in gioco la teoria della regolazione del rischio che, a differenza del paradigma emergenziale, riconosce i diritti e considera interessi concorrenti: l'obiettivo è quello di gestire i rischi che non sono accettabili per la società. La loro valutazione da un punto di vista scientifico e l'adozione di misure di controllo proporzionate, possono consentire di evitare che la condizione diventi emergenziale.

4. Il principio di precauzione

Per una definizione del principio di precauzione[19], si fa riferimento innanzitutto ad alcune pronunce giurisprudenziali. Come ricorda il Consiglio di Stato (sez. V,

15 Si prenda ad esempio la recente pandemia da Sars-Covid-19.

16 Come, nel caso di specie, è l'utilizzo dell'intelligenza artificiale.

17 Simoncini e Martinico 2022: 77.

18 Per Cerulli Irelli 2008: 155, 176, 189-191 i poteri straordinari non possono essere applicati a disfunzioni dell'amministrazione oppure a fenomeno che mancano dei presupposti di imprevedibilità e contingibilità.

19 Storicamente, la più risalente espressione del principio di precauzione viene generalmente ricondotta allo Environmental Protection Act svedese del 1969 (Trouwborst, 2002: 378). Durante gli anni Settanta, l'espressione Vorsorgeprinzip è stata utilizzata soprattutto in Germania, nell'ambito delle normative e linee guida sull'inquinamento atmosferico (Marr e Schwemer, 2004:127). La consacrazione a principio ispiratore arriva con in occasione della Conferenza

sentenza n. 2495/2015), "il principio di precauzione comporta che, ogni qual volta non siano conosciuti con certezza i rischi indotti da un'attività potenzialmente pericolosa, l'azione dei pubblici poteri debba tradursi in una prevenzione anticipata rispetto al consolidamento delle conoscenze scientifiche, anche quando i danni siano poco conosciuti o solo potenziali".

In una pronuncia più recente, Cons. Stato, sez. III, n. 6655 del 2019 ricorda che "fa obbligo alle Autorità competenti di adottare provvedimenti appropriati al fine di scongiurare i rischi potenziali per la sanità pubblica, per la sicurezza e per l'ambiente, senza dover attendere che siano pienamente dimostrate l'effettiva esistenza e la gravità di tali rischi e prima che subentrino più avanzate e risolutive tecniche di contrasto. L'attuazione del principio di precauzione comporta dunque che, ogni qual volta non siano conosciuti con certezza i rischi indotti da un'attività potenzialmente pericolosa, l'azione dei pubblici poteri debba tradursi in una prevenzione anticipata rispetto al consolidamento delle conoscenze scientifiche".

ONU del 1992 di Rio de Janeiro sull'ambiente e lo sviluppo. Secondo il documento del 1982, "(i) le attività che comportano un elevato grado di rischio per la natura devono essere precedute da un esame approfondito e i loro promotori devono dimostrare che i benefici derivanti dall'attività prevalgono sui danni eventuali alla natura; e (ii) qualora gli effetti nocivi di tali attività siano conosciuti in maniera imperfetta, esse non dovranno essere intraprese (art. 11, b)".Con il nuovo millennio, il principio di precauzione ha costituito uno degli aspetti fondamentali di numerosi Accordi internazionali, fra i quali si segnala in particolare la Convenzione di Stoccolma del 2001 sugli inquinanti organici persistenti (POPs), che individua un numero definito e preciso di sostanze considerate a rischio, la cui produzione deve pertanto cessare (sia pure con limitate deroghe assai ben motivate, come quella relativa al DDT), e che viene generalmente considerato – tanto dai produttori come dagli ambientalisti – una equilibrata espressione del principio di precauzione (Nespor, "Un trattato che è una pietra miliare. Il principio di precauzione applicato ai POP ha messo d'accordo organizzazioni internazionali, ONG e industrie", in Scienza Esperienza, 2003). In ambito europeo, la positivizzazione del principio avviene attraverso il trattato di Maastricht, all'art. 130R ("La politica della Comunità in materia ambientale mira a un elevato livello di tutela, tenendo conto della diversità delle situazioni nelle varie regioni della Comunità. Essa è fondata sui principi della precauzione e dell'azione preventiva, sul principio della correzione, anzitutto alla fonte, dei danni causati all'ambiente, nonché sul principio "chi inquina paga". Le esigenze connesse con la tutela dell'ambiente devono essere integrate nella definizione e nell'attuazione delle altre politiche comunitarie. In questo contesto, le misure di armonizzazione conformi a tali esigenze comportano, nei casi appropriati, una clausola di salvaguardia che autorizza gli Stati membri a prendere, per motivi ambientali di natura non economica, misure provvisorie soggette ad una procedura comunitaria di controllo"); poi art. 174, par. 2, Trattato CE tra quei princìpi sui quali avrebbe dovuto essere fondata l'azione (poi la politica) delle istituzioni comunitarie nel settore della tutela dell'ambiente, ora codificato nell'art. 191 par. 2 del TFUE. Successivamente, attraverso la giurisprudenza comunitaria, quello di precauzione è divenuto principio generale del diritto comunitario, il quale, in situazioni di incertezza scientifica, anche al di fuori della politica ambientale, impone "alle autorità competenti di adottare provvedimenti appropriati al fine di prevenire taluni rischi potenziali per la sanità pubblica, per la sicurezza e per l'ambiente facendo prevalere le esigenze connesse alla protezione di tali interessi sugli interessi economici" (Sentenza del Tribunale CE, sez. II ampliata, 26 novembre 2002, caso Artegodan punto 184; Sentenza del Tribunale CE, II sez., 21 ottobre 2003, caso Solvay). Inoltre, va considerata anche COM/2000/0001, del 2 febbraio del 2000 sul principio di precauzione in sede europea. Sullo sviluppo comunitario del principio si vedano Marini 2004; Sollini 2006; Alemanno 2016; Titomanlio, 2018.

Sempre la medesima sentenza sostiene che il principio di precauzione costituisce "non solo un presupposto di legittimazione ma anche un vero e proprio parametro di validità per tutte le politiche e azioni europee in materia di ambiente, salute e sicurezza e che, pertanto, anche in forza dell'efficacia trasversale del principio di integrazione delle esigenze di tutela dell'ambiente in tutte le politiche e azioni dell'Unione, si configuri ormai come parametro generale di legittimità non solo della funzione normativa esercitata dalle istituzioni dell'Unione ma anche di quella amministrativa"[20].

Al riguardo particolarmente rilevante è la sentenza del Consiglio di Stato, sez. V, sentenza n. 6250/13 che, secondo parte della dottrina, ha definito un vero e proprio "decalogo di regole per una corretta applicazione del principio di precauzione". Facendo propri i dettati elaborati dalla giurisprudenza europea sul punto, secondo i giudici, l'applicazione degli elementi caratterizzanti il principio di precauzione devono rinvenirsi "lungo un percorso esegetico fondato sul binomio analisi dei rischi – carattere necessario delle misure adottate" con la diretta conseguenza che le attività da porre in essere in via precauzionale "presuppongono che la valutazione dei rischi di cui dispongono le autorità riveli indizi specifici i quali, senza escludere l'incertezza scientifica, permettano ragionevolmente di concludere, sulla base dei dati disponibili che risultano maggiormente affidabili e dei risultati più recenti della ricerca internazionale, che l'attribuzione di tali misure è necessaria al fine di evitare pregiudizi all'ambiente o alla salute".

Sulla base di tali considerazioni gli stessi giudici hanno chiarito come una corretta applicazione del principio di precauzione debba necessariamente prevedere l'adozione di misure volte "al preventivo svolgimento di una valutazione quanto più possibile completa dei rischi calata nella concretezza del contesto spazio temporale di riferimento" in modo da individuarne la misura "necessaria".

Alla luce delle sentenze poc'anzi enunciate e della linea stabilita in sede europea, appare evidente come la definizione di "principio di rischio" mette in luce come, in assenza di certezze tecnico-scientifiche, l'obiettivo sia quello di comprendere il livello di rischio accettabile per l'ordinamento.

La portata del principio, quindi, resta il vero nucleo sul quale riflettere. Esiste una interpretazione "massimalista", che tenderebbe a vietare qualunque progetto che presenti anche solo rischi ridotti; come posizione contrapposta esiste quella "minimalista" che, invece, imporrebbe il ricorso a misure di precauzione esclusivamente in presenza di rischi seri più che probabili[21].

20 Cons. Stato, sez. III, n. 6655 del 2019.

21 Ragone 2019: 158, sulla posizione "minimalista", si segnala anche Grassi, Gragnani 2003; De Leonardis 2005: 51 secondo il quale il principio di precauzione è considerato, dalla giurisprudenza europea, "una filiazione del principio di proporzionalità" in considerazione del fatto che "prima che fosse espressamente riconosciuto come tale veniva, nella giurisprudenza incluso in esso". L'Autore evidenzia altresì che "se si definisce, però, il principio di precauzione come il principio in base al quale, anche in caso di incertezza tecnico – scientifica, la decisione amministrativa deve essere supportata da un'adeguata istruttoria volta a far emergere il rischio probabile e deve, in ogni caso, essere proporzionata, non si può non pervenire alla conclusione che si tratti di un principio cogente a tutti i livelli ordinamentali in quanto col-

L'applicazione del principio implica la determinazione di una serie di elementi che sono alla base del procedimento amministrativo successivo: innanzitutto la determinazione del livello di rischio che si intende accettare; successivamente l'individuazione degli organi deputati alla valutazione della sussistenza del rischio e dell'incertezza scientifica; infine, le modalità attraverso le quali giungere ad una valutazione.

Lo schema deisionale[22] che rientra nell'applicazione del principio di precauzione prevede innanzitutto che il decisore politico si confronti con un sapere scientifico che è incontrovertibile. Nel caso dell'ambiente (sia esso naturale che digitale), invece, a dominare il contesto è la grande incertezza, soprattutto quella legata all'*an*. Il suddetto schema presume la successiva analisi su:

1. valutazione del rischio che non deve basarsi solamente su valutazione ipotetiche;
2. sussistenza (almeno) della probabilità del danno reale.

In questa situazione di costante dubbio, si inserisce anche il difficile rapporto tra tecnica e diritto[23], sia nella fase di formazione della norma che in quella di definizione del procedimento e, successivamente, nel sindacato giurisdizionale. Nell'ordinamento, allo stato attuale, non esiste una disciplina generale di formazione della regola tecnica che possa consentire un discrimine tra la formazione della regola tecnica stessa e la decisione politica che la presiede.

Tralasciando l'aspetto normativo, sul fronte amministrativo, l'utilizzo del principio di precauzione coincide con uno spazio discrezionale molto ampio che contempera gli interessi in gioco, valuta l'interesse pubblico e lo tramuta in atti. Anche l'amministrazione[24] si muove in un ambiente estremamente "accidentato", in cui l'incertezza tecnica si riverbera anche sulla valutazione che effettua.

Accanto all'enunciazione del principio di precauzione, quindi, è necessaria anche la sua attuazione, ambito quest'ultimo che spetta all'amministrazione. In un ordinamento fondato sul rigoroso rispetto del principio di legalità[25], non è suffi-

legato direttamente con il principio (istituzionale) di ragionevolezza". *Contra* Cordini 2012: 187, secondo il quale ogni azione preventiva costituisce anche applicazione di un più generale principio di precauzione.

22 Aversante 2020.

23 Barone 2020 sottolinea l'altrettanto difficile rapporto con il principio di legalità (addirittura definendola crisi) in quanto, in un contesto di incertezza scientifica, il tradizionale portato del principio di legalità non è sufficiente come non è possibile che la norma assorba l'enorme spazio che il rischio e la sua gestione acquistano.

24 È una delle manifestazioni della "riserva di amministrazione" (art. 1, co. 1 L. 241/90) visto come spazio democratico all'interno del quale, attraverso il confronto procedimentale fra interessi diversi, l'Amministrazione caratterizza il contenuto giuridico del singolo principio in relazione alle peculiarità del caso concreto.

25 Una parte della dottrina (Follieri, 2016:1495), sottolinea che l'art. 1 L. 241/90 non possa essere invocato per ampliare la portata applicativa del principio di precauzione in ambito nazionale rispetto a quanto previsto dall'ordinamento europeo, trattandosi invero di una norma per effetto della quale viene operato un mero rinvio. Ne discenderebbe che, non essendo la logica precauzionale nell'ordinamento europeo un criterio di attribuzione di poteri amministrativi, anche nel nostro ordinamento non potrebbe derogare al principio di legalità.

ciente assegnare all'amministrazione il potere di intervenire in via precauzionale, essendo pure necessario definire entro quali limiti e con quali modalità tale intervento possa avvenire legittimamente, salvaguardando tanto i diritti e gli interessi dei terzi quanto quelli dei soggetti cui compete l'azione preventiva (i quali potrebbero incorrere in responsabilità, anche penali, in caso di un'inerzia loro imputabile[26]). Sorge, quindi, una tensione tra principio di precauzione e quello di legalità che, inevitabilmente, si riflette anche sull'operato dell'amministrazione. L'azione precauzionale, infatti, è atipica rispetto all'*agere* amministrativo in senso stretto, determinando la necessità di fattispecie sempre aperte[27].

Una volta effettuata la decisione di applicare il principio di precauzione alla fattispecie concreta, il passo successivo è comprendere fino a che punto il rischio possa essere accettato. Risulta, in questo modo, anche uno strumento di bilanciamento degli interessi in gioco, nella maggior parte delle volte confliggenti.

5. L'ambiente digitale e il principio di precauzione

La qualificazione del principio di precauzione a principio generale consente di renderlo applicabile anche ad altri ambiti che siano al di fuori di quelli espressamente richiamati[28]. Nel possibile contesto di espansione del principio di

26 Di conseguenza, va effettuata una distinzione tra le materie di competenza comunitaria e quelle residuali statali: "La precauzione è volta alla tutela della salute e dell'ambiente (nella prospettiva dello sviluppo sostenibile), tanto nell'ordinamento comunitario, quanto in quello interno 50. Dal punto di vista soggettivo, nelle materie di competenza dell'Unione, la precauzione per la salute e l'ambiente è obbligatoria per il legislatore e per la p. A., nell'esercizio delle funzioni previste dall'ordinamento (c.d. soggezione della precauzione al principio di legalità).

Nelle materie di competenza dell'ordinamento interno, invece, la precauzione è concepita dal legislatore, tramite il rinvio ai principi generali dell'ordinamento comunitario ex art. 1, c. 1, l. n. 241/1990, quale criterio volto a orientare l'esercizio delle funzioni autoritative della p. A., unitamente agli altri principi di matrice comunitaria" (Longo, Distefano, 2019:20).

M. Renna 2023: 342

27 Proprio in virtù di questa atipicità, nel "Codice dell'Ambiente" (art. 301) sono stati inseriti una serie di limiti al potere amministrativo, cercando di mitigare l'eccezionalità e l'ampiezza della discrezionalità accordata all'amministrazione stessa. Eppure, il provvedimento amministrativo adottato sulla base del principio di precauzione si caratterizza per un elevato tasso di discrezionalità, posto che la scelta pubblica sul rischio non risulta vincolata ad un dato tecnico-scientifico per definizione incerto.

28 Zuddas 2020: 411, ricorda come questa attitudine ad essere considerato principio generale viene dimostrata anche dall'inserimento del principio in atti normativi, sebbene essenzialmente di soft law come parametro di interpretazione e di legittimazione dell'azione amministrativa, in particolare quelli che disciplinano l'utilizzo dell'intelligenza artificiale. Lo stesso autore traccia un'analogia tra lo spazio normativo scientificamente riservato all'autonomia e alla responsabilità del medico con lo stesso spazio che potrebbe essere accordato all'ingegnere informatico (oppure al programmatore del software) se non fosse che a rilevare sono le regole deontologiche operanti in campo medico non sono ugualmente strutturate per gli operatori tecnici dell'informatica. Inoltre, l'affidamento all'autoregolazione in una fase di sviluppo come quella che sta vivendo l'ambiente digitale rappresenta ancora un'incognita.

precauzione al di fuori dei tradizionali ambiti di riferimento, un ulteriore ambito in cui allargarne l'applicazione è il rapporto tra intelligenza artificiale e pubblica amministrazione[29].

Il fatto che ci sia una grande evoluzione tecnologia attorno ai sistemi di intelligenza artificiale implica anche che risulta difficoltoso prevenire tutte le tipologie di rischio ad essa connesse[30].

Entra in gioco, quindi, il "*risk based approach*" e la "*risk regulation*". Infatti, il punto distintivo del principio di precauzione risulta essere proprio la separazione tra la valutazione scientifica e la gestione del rischio. Inoltre, la valutazione deve essere fatta caso per caso.

Il principio di precauzione applicato all'intelligenza artificiale inizia ad avere alcuni fautori nel dibattito dottrinale che si è sviluppato nel corso del tempo, sottolineando il parallelismo tra natura e mondo digitale[31].

All'interno di questo ambiente digitale così fortemente governato dall'incertezza, uno degli aspetti più rilevanti resta quello della cybersecurity. Con l'avvento dei software di intelligenza artificiale nella pubblica amministrazione, il rischio legato alla tutela dei dati da possibili attacchi e reati informatici ha subito modifiche in termini quantitativi e qualitativi[32].

Il tema della cybersicurezza (inteso come protezione dell'ambiente digitale da un pericolo/rischio[33] di attacchi alla sicurezza dell'ambiente stesso e dei diritti dei cittadini che in questo ambiente vivono e trovano applicazione) è l'ambito che più di tutti mette in luce i parallelismi con l'ambiente naturale[34]. I concetti di incertezza e rischio, quindi, appaiono evidenti.

Cosa avviene, concretamente, da parte dell'amministrazione per gestire questo rischio[35]? La peculiarità del principio di precauzione si riflette concretamente

29 Barone 2020. L'autore profila un'espansione dell'applicazione anche al di là dei profili che sono stati individuati in sede di dottrina e in quella giurisprudenziale, legate essenzialmente al rischio "tecnico" nella partecipazione alle gare pubbliche (Tar Lazio, sez. II, 7 febbraio 2020, n. 1710).

30 Sugli algoritmi, la loro opacità e il loro rapporto con l'amministrazione si vedano, tra gli altri, Simoncini 2019; Cavallo Perin, Alberti 2020; Masucci 1993; Follieri 2017; Avanzini 2019.

31 Sul punto si veda Barone 2006; Cibelli 2023; Zuddas 2020.

32 Sul punto si veda "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations" redatta dal National Institute of Standards and Technology (NIST) e reperibile al sito https://csrc.nist.gov/pubs/ai/100/2/e2023/final.

33 Intenso come certezza che possa avvenire un attacco ma, allo stesso tempo, incertezza delle modalità e del luogo in cui questo attacco può avvenire.

34 Gallone, Orofino 2020:1798; Barone 2006. Gli Autori mettono in risalto come l'intelligenza artificiale sia entrata a far parte di ogni aspetto della vita: "Più in generale, sembra possibile affermare che gli studi giuridici sul rischio debbano oggi ampliare lo spettro di indagine tradizionale per includere l'intelligenza artificiale e le sue applicazioni per la pubblica amministrazione, nella prospettiva di un nuovo umanesimo giuridico "digitale".

35 Cecchietti 2006: 103, sottolinea come l'aspetto amministrativo è rilevante tanto quanto (se non di più) rispetto a quello normativo e giurisprudenziale perché il principio "non fornisce una regola per decidere, quanto piuttosto una regola di procedere" in quanto la ratio ispiratrice non può che rinvenirsi "nell'organizzazione delle procedure, nei cui casi si convogliano le valutazioni scientifiche, economiche e politiche che fondano il ricorso alla misura cautelativa". La decisione di adottare misure precauzionali deve essere quindi considerata la sintesi della volontà

nella decisione amministrativa, sugli effetti della decisione di agire o non agire in presenza del rischio e sulla provvisorietà di questa valutazione[36]. Segue il monitoraggio delle scelte precauzionali assunte in prima battuta (e solo dopo aver deciso se agire o meno): queste scelte sono caratterizzate dall'apposizione di "condizioni" da rispettare, ovvero al riesame del provvedimento precauzionale di fronte all'acquisizione di nuove conoscenze scientifiche[37].

Scelta condizionale[38] e riesame risultano essere elementi strutturali della decisione amministrativa adottata entro il perimetro del principio di precauzione. Si delinea, quindi, un tratto caratteristico di questo genere di decisioni: la provvisorietà. Sono sempre soggette a riesame davanti all'acquisizione di nuovo sapere scientifico, ovvero delle migliori tecnologie disponibili.

L'ulteriore elemento che viene in rilievo sono proprio le BAT[39], cioè le tecniche da adottare in un ciclo di produzione idonee ad assicurare la migliore protezione ambientale (e dell'ambiente digitale?) possibile e che siano, al contempo, disponibili in termini di accessibilità a costi ragionevoli[40]. Le BAT, quindi, servono per definire il limite (o valore-soglia) oltre il quale il rischio non può più essere accettato, ma anche parametri da rispettare nello svolgimento dell'attività. Sono, quindi, il punto di incontro tra diritto, scienza ed economia, il loro contemperamento nonostante gli opposti interessi in gioco.

politica e di valutazioni amministrative avvalorate da fondamenti di natura scientifica e, al tempo stesso, da un bilanciamento tra interesse costituzionalmente garantiti. Inoltre, diventa parametro di legittimità per la valutazione dell'azione amministrativa. Sul punto, si vedano anche Bartolomei 2001:321; Grassi 2001: 53; Vineis, Ghisleni, Ricciardi 2002: 102; Manfredi 2004: 1081; Principalli 2004: 152; Gestri 2006: 477; Antonioli 2007: 85.

36 Stanzione 2016: 16.

37 Barone 2006. L'Autore sottolinea come le scelte di *risk management* rispettose del principio di precauzione tendono ad evitare (ove possibile) l'opzione zero, cioè il diniego secco, e consentono l'avvio dell'attività (e quindi la realizzazione del progetto), che viene però subordinato ad una serie di condizioni a garanzia della tutela della salute e dell'ambiente.

38 Frediani 2017: 447.

39 Per una definizione di BAT (*best available techniques*) fare riferimento all'art. 5 co. 1, l. l.ter del TUA: "la più efficiente e avanzata fase di sviluppo di attività e relativi metodi di esercizio indicanti l'idoneità pratica di determinate tecniche a costituire, in linea di massima, la base dei valori limite di emissione e delle altre condizioni di autorizzazione intesi ad evitare oppure, ove ciò si riveli impossibile, a ridurre in modo generale le emissioni e l'impatto sull'ambiente nel suo complesso. Nel determinare le migliori tecniche disponibili, occorre tenere conto in particolare degli elementi di cui all'allegato XI. Si intende per: 1) tecniche: sia le tecniche impiegate sia le modalità di progettazione, costruzione, manutenzione, esercizio e chiusura dell'impianto; 2) disponibili: le tecniche sviluppate su una scala che ne consenta l'applicazione in condizioni economicamente e tecnicamente idonee nell'ambito del relativo comparto industriale, prendendo in considerazione i costi e i vantaggi, indipendentemente dal fatto che siano o meno applicate o prodotte in ambito nazionale, purché il gestore possa utilizzarle a condizioni ragionevoli; 3) migliori: le tecniche più efficaci per ottenere un elevato livello di protezione dell'ambiente nel suo complesso". Va comunque rilevato che il meccanismo di formazione delle BAT non è rimesso all'auto-normazione dei soggetti privati ma avviene comunque in una sede pubblica e istituzionale.

40 Longo, Distefano 2019: 13.

La procedura che porta all'elaborazione delle *BAT Conclusions* si articola in due fasi: quella del BREF e quella delle vere e proprie *BAT Conclusions*[41].

Le BAT, quindi, concorrono nel definire il parametro di legge (VLE normativamente previsti), ovvero di autorizzazione (le BAT concorrono a stabilire le condizioni per il conseguimento dell'AIA) quando si parla di ambiente.

Dal punto di vista del diritto amministrativo, alla luce del parallelismo tra ambiente naturale e ambiente digitale, quindi, è possibile immaginare uno sviluppo di BAT anche per l'ambiente digitale, così da poter avere un perimetro entro il quale l'amministrazione possa muoversi a livello autorizzatorio. Sebbene lo spazio di discrezionalità amministrativa sia sempre molto ampio quando entra in gioco il principio di precauzione, la definizione di BAT digitali potrebbe supportare sia l'amministrazione che il privato nella gestione dei software di intelligenza artificiale al servizio dei cittadini, della tutela dei diritti all'interno del procedimento (grazie alla costante revisione legata alle tecnologie in evoluzione, ma anche il più ampio tema della cybersecurity).

Associata alle BAT e in chiave preventiva, è immaginabile anche mutuare dall'ambiente naturale la valutazione di impatto che, nello specifico, sarebbe "digitale", cioè valutazione degli effetti di una decisione di agire o non agire assunta in presenza di un rischio meramente ipotizzato e non ancorato a dati connotati da acclarate conoscenze scientifiche. L'intero problema, quindi, ruota attorno a quale grado di rischio sia accettabile, alla soglia di tollerabilità?

Quale grado di compressione delle libertà e di diritti, oppure degli interessi in gioco (spesso confliggenti), è possibile consentire/tollerare per una migliore gestione degli indirizzi di cybersecurity?

Il ruolo dei dati nell'attuale società[42] è in continuo crescendo, così come la necessità di una strategia che sia a supporto della loro protezione[43] da parte di reati

41 Il procedimento BREF prevede la costituzione di un tavolo di esperti con il compito della predisposizione di un documento e di una successiva valutazione attraverso la "procedura di comitato". Alla luce delle *BAT Conclusions* verranno determinati i valori massimi di emissione associati, appunto, alle migliori tecniche disponibili.

42 Si veda D.U. Galetta, 2018, p. 327, ma anche COM(2020) 66 final, 12 febbraio 2020, 2 e il Rapporto OECD, Data-Driven Innovation. Big Data for Growth and Well-Being, in oecd-ilibrary.org, 6 ottobre 2015.

43 Viene garantita attraverso un pacchetto di regole comunitarie: Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati); Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati); Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali); Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

informativi e di attacchi[44]. La strategia europea[45] è caratterizzata da una dimensione verticale e una orizzontale: la prima è legata al rapporto che intercorre tra l'autorità europea e quelle nazionali, attraverso anche il nesso tra Enisa e le agenzie nazionali. La seconda dimensione, invece, nonostante sia formalmente legata alla collaborazione dei vari attori in campo, compresi quelli privati, è caratterizzata dall'approccio autoritativo "obbligo-sanzione"[46]. Il processo di determinazione delle strategie di sicurezza e il successivo approvvigionamento delle stesse, quindi, risulta essere caratterizzato da un'ampia azione amministrativa, esattamente come avviene per la gestione dei rischi ambientali. Le minacce all'ambiente digitale non sono di pertinenza del singolo individuo, ma diventano di interesse globale perché legati a questioni di sicurezza pubblica, ma anche economica oltre che riguardante la tutela dei diritti.

Tracciare il quadro delle minacce risulta essere difficoltoso vista la loro continua evoluzione e imprevedibilità[47]: si tratta in questo caso di un nuovo parallelismo con l'ambiente naturale in grado di condurre verso la possibilità di estendere gli stessi approcci di gestione del rischio anche all'ambiente digitale. Sebbene non se ne faccia mai menzione all'interno dell'AI Act, il principio di precauzione guida le azioni legate alla gestione dell'intelligenza artificiale, fissando il limite di tollerabilità che può essere accettato. Di fatto, si tratta di una BAT non classificata come tale: viene effettuata una preventiva valutazione dell'impatto digitale delle tecnologie, così da poter comprendere se quelle disponibili (e che vengono mano mano implementate grazie all'evoluzione tecnica) possano essere compatibili con il livello di tolleranza che è stato fissato attraverso il regolamento europeo e le successive normazioni statali. L'analisi caso per caso, utilizza le migliori tecnologie disponibili, contemplando un'anticipazione rispetto al possibile danno.

44 Il DDL C 1717 Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici deriva da una serie di interventi regolatori che arrivano dall'UE quali la Direttiva (UE) 2022/2555 del Parla-mento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (cosiddetta "direttiva NIS 2".

45 Il regolamento 526/2013 è il primo passo della strategia europea per la sicurezza informatica. Prevede un rafforzamento dell'Agenzia Ue per la cybersecurity (Enisa). Viene definito un framework politico in materia di protezione informatica, prevedendo cinque aree prioritarie di intervento: 1) rafforzare la capacità di cyberdifesa nei diversi Paesi europei; 2) irrobustire i livelli di protezione delle reti di comunicazione e informazione della politica europea di sicurezza e di difesa comune; 3) promuovere la cooperazione civile e militare con riferimento alle politiche informatiche; 4) garantire maggiori opportunità di istruzione e di formazione digitale; 5) supportare i rapporti con i principali partner internazionali.

46 Rossa 2023: 132.

47 Brighi, Chiara 2021: 21, gli autori sottolineano anche come l'IA offre nuovi modi di condurre attacchi cyber, sempre più efficaci, sfruttando la capacità di tali sistemi di identificare vulnerabilità che possono sfuggire a un esperto umano; di automatizzare attacchi di ingegneria sociale personalizzati mediante informazioni raccolte online; di generare immagini e video non distinguibili dalla realtà (i c.d. deep fake); di realizzare malware autonomi nel mascherarsi e selezionare il proprio target, o ancora di attaccare altri sistemi di IA applicando in modo avverso gli stessi paradigmi del machine learning.

Anche il regolamento sulla Cybersecurity (o *resilience*) è un tentativo di costante adattamento ad un rischio/pericolo in costante evoluzione e abbisognoso di una revisione continua delle scelte amministrative effettuate in precedenza.

Un elemento di forte interesse sono le sandbox, cioè uno spazio, virtuale oppure fisico, all'interno del quale è possibile testare per un periodo di tempo limitato progetti innovativi da un punto di vista tecnologico, con la possibilità di derogare la normativa di settore in modo da consentire ai promotori di svolgere i test nella maniera più esaustiva, completa ed efficiente possibile. Quale luogo di incontro tra pubblico e privato, è anche molto vicino allo spirito partecipativo del procedimento, oltre che strumento di bilanciamento degli interessi in gioco.

6. Conclusioni

L'ambiente digitale è diventato un "terreno virtuale" nel quale l'agente umano è immerso costantemente e dal quale non è possibile prescindere: non è possibile per i singoli cittadini né tantomeno per le amministrazioni pubbliche.

Nell'impossibilità di poter evitare l'ambiente digitale e i suoi rischi, l'approccio che viene utilizzato è quello della gestione[48]. L'amministrazione, quindi, nel perseguire gli interessi generali e nella sua azione orientata alla protezione dei diritti fondamentali, è tenuta ad adottare le misure preventive senza attendere che la gravità dei rischi derivanti da una attività sia scientificamente provata. Una precauzione che spesso, però, incontra confliggenti interessi e che, quindi, risulta non sempre agevole da praticare.

La difficoltà, infatti, risiede anche nell'assenza di principi specifici legati all'ambiente digitale e ad una regolazione che si stacchi dall'essere meramente operativa[49]. Se per l'ambiente naturale la regolamentazione europea (prima) e il montante giurisprudenziale (poi) hanno definito nel corso del tempo quale sia il parametro di legittimazione delle scelte amministrative, per quello digitale ancora si fa fatica a reperire le pietre angolari dell'azione.

Con particolare riferimento alla p. A., il principio di precauzione e l'approccio basato sul rischio (e sulla sua eventuale mitigazione) hanno contribuito a tracciare la strada che l'amministrazione può percorrere quando si trova davanti a scelte altamente discrezionali come quelle legate alla tutela dell'ambiente e della salute. Questo principio, vista la sua duttilità, è stato impiegato anche in altri ambiti, facendone crescere il raggio d'azione.

È possibile immaginare, quindi, che la sua estensione nel corso del tempo investirà anche l'ambiente digitale per una analogia che si basa sul parallelismo che

48 Per una valutazione del "*risk based approach*" nella regolamentazione dell'intelligenza artificiale si veda Cibella 2023.

49 Il riferimento è al Codice dell'Amministrazione digitale che è per lo più concentrato sugli aspetti puramente operativi della digitalizzazione nella p. A., ma non fornisce una base normativa di azione né chiarisce la natura dell'atto amministrativo adottato con l'aiuto di algoritmi di intelligenza artificiale.

esiste tra i due ambiti. A questo punto, una volta scelta l'applicazione del principio di precauzione anche per l'ambiente digitale, è possibile prendere in prestito dalla gestione del rischio ambientale anche gli strumenti amministrativi che vengono utilizzati. Il riferimento è alla valutazione di impatto (ambientale), da estendere anche all'intelligenza artificiale per determinare, di volta in volta, se il rischio è tollerabile oppure no; le BAT con simultanea possibilità di revisione della decisione amministrativa assunta. Sia la valutazione che la possibilità di una decisione amministrativa revisionabile (in virtù delle modifiche tecnologiche che avvengono nel corso del tempo) sono strumenti che danno effettività e applicazione al principio e che, al contempo, sono in grado di orientare l'azione della stessa p. A. senza dover sacrificare i diritti fondamentali.

Bibliografia

Alemanno A. 2016, "The precautionary principle", in C. Baudenbacher (Eds.), *The handbook of EEA law*, New York: Springer.

Antonioli M. 2007, "Precauzionalità, gestione del rischio e azione amministrativa", in *Rivista Italiana di Diritto Pubblico*.

Avanzini G. 2019, *Decisioni algoritmiche e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli: Editoriale Scientifica.

Aversante G. 2020, "Il principio di precauzione: il rapporto problematico tra diritto e incertezza scientifica", in *DPCE*, 3.

Barone A. 2020, "Amministrazione del rischio e intelligenza artificiale", in *European Review of Digital Administration & Law – Erdal*, 1.

Barone A. 2006, *Il diritto del rischio*, Milano: Giuffrè.

Bartolomei S. 2001, "Il principio di precauzione: norma assoluta o regola procedurale? in *Biotetica*.

Beck U. 2000, *La società del rischio. Verso una seconda modernità*, Roma: Carocci.

Camisa F. 2024, "Ambiente e tecnologia, l'interconnessione tra le transizioni gemelle", in *Federalismi*, 14.

Cavallo Perin R., Alberti I. 2020, "Atti e procedimenti amministrativi digitali" in R. Cavallo Perin, D.-U. Galetta (a cura di), *Diritto dell'amministrazione pubblica digitale*, Torino: Giappichelli.

Cecchietti M. 2006, "La disciplina giuridica della tutela ambientale come 'diritto dell'ambiente'", in *Federalismi*, 25.

Cerulli Irelli V. 2008, "Principio di legalità e poteri straordinari dell'amministrazione, in AA.VV., *Il principio di legalità nel diritto amministrativo che cambia*, Milano: Giuffrè.

Cibella E. 2023 "Il principio di precauzione nell'ambiente digitale", in *PA Persona e Amministrazione*, 12.

Cordini G., 2012, *Diritto ambientale comparato*, Padova: Cedam.

De Leonardis F. 2005, *Principio di precauzione e amministrazione di rischio*, Milano: Giuffré.

DeSadeleer N. 2006, "The Precautionary Principle in EC Health and Environmental Law", in *European Law Journal*, vol. 12, n. 2.

Follieri E., 2017, "Decisione amministrativa e atto vincolato", in *Federalismi*.

Follieri E. 2016, "Decisioni precauzionali e stato di diritto. La prospettiva della sicurezza alimentare", in *Rivista Italiana di Diritto Pubblico Comunitario*, 6.

Frediani E. 2017, "Decisione condizionale e tutela integrata di interessi sensibili", in *Diritto amministrativo*.
Galetta D.-U., 2018, "La pubblica amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?", in *Ciberspazio e diritto*, 3.
Gallone G., Orofino A. G. 2020, "L'intelligenza artificiale al servizio delle funzioni amministrative", in *Giurisprudenza Italiana*.
Gestri M. 2006, "La portata normativa del principio di precauzione nel diritto comunitario: gestione politica del rischio e controllo giurisdizionale", in B. Andrea, M. Gesti (a cura di), *Il principio precauzionale nel diritto internazionale e comunitario*, Milano: Giuffrè.
Grassi S., Gragnani A. 2003, "Il principio di precauzione nella giurisprudenza costituzionale", in L. Chieffi (a cura di), *Biotecnologie e tutela del valore ambientale*, Torino: Giappichelli.
Grassi S. 2001, "Prime osservazioni sul principio di precauzione nel diritto positivo", in *Dir. Gest. Amb*.
Gros M., Serges G. 2013, "Il principio di precauzione dinnanzi al giudice amministrativo Francese", in *Diritto e Società*, 4.
Iannello C. 2014 "Note sul principio di precauzione" in L. Chieffi (diretto da), *Frontiere mobili*, Milano: Mimesis Edizioni
Longo A., Distefano F.M. 2019, "Il ruolo del principio di precauzione nella tutela del bene ambientale fra diritto amministrativo e penale", in *Federalismi*, 16.
Manfredi G. 2004, "Note sull'attuazione del principio di precauzione in diritto pubblico", in *Diritto pubblico*, 3.
Marini L. 2004, *Il principio di precauzione nel diritto internazionale e comunitario*, Padova: Cedam.
Marr S., Schwemer A., 2004, "The Precautionary Principle in German Environmental Law", in *The Yearbook of European Environmental Law*, 3.
Masucci A. 1993, *L'Atto amministrativo informatico*, Napoli: Jovene.
Perez R. 2011, "L'azione finanziaria europea al tempo della crisi", in *Rivista italiana di diritto pubblico comparato*.
Principalli A.M. 2004, "Il principio di precauzione: 'danni gravi e irreparabili' e mancanza di certezza scientifica", in *Il diritto dell'agricoltura*.
Ragone G. 2019, "Il principio di precauzione nella prospettiva del giudice costituzionale", in *BioLaw Journal*, 2.
Renna M. 2019, "Il principio di precauzione e la sua attuabilità", in *Forum di Quaderni Costituzionali*, 2.
Rossa S. 2023, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale Scientifica.
Salter J., Howsam p. 2002, *The Precautionary Principle and the law on risk*, I, Manchester: University Press, Manchester.
Simoncini A. 2019, "Amministrazione digitale algoritmica", in *BioLaw Journal*.
Simoncini M. 2010, *La regolazione del rischio e il sistema degli standard. Elementi per una teoria dell'azione amministrativa attraverso i casi del terrorismo e dell'ambiente*, Napoli: Editoriale Scientifica.
Simoncini M., Martinico G. 2022, "Dall'emergenza al rischio nel diritto pubblico comparato: un'introduzione", in *DPCE online*.
Sollini M. 2006, *Il principio di precauzione nella disciplina comunitaria della sicurezza alimentare*, Milano: Giuffré.
Stanzione M.G. 2016, "Principio di precauzione, tutela della salute e responsabilità della p. A. Profili di diritto comparato", in *www.comparazionedirittocivile.it*.

Titomanlio R. 2018, "Il principio di precauzione fra ordinamento europeo e ordinamento italiano", Torino: Giappichelli.
Trouwborst A. 2002 "Evolution and Status of the Precautionary Principle in International Law", in *Kluwer Law International*.
Vineis p. , Ghisleni M., Ricciardi V. 2002, "Sulle giustificazioni scientifiche del principio etico di precauzione", in *Notizie di Politeia*.
Zuddas p. 2020, "Pregiudizi digitali e principio di precauzione", in *Consulta Online*, 2.

Maria Notaristefano, Fabio Angeletti ed Esli Spahiu

*Privacy e cybersecurity nelle Smart City: un caso di studio**

Abstract: Le iniziative di smart city offrono numerosi vantaggi, tra cui lo sviluppo economico e la distribuzione efficiente delle risorse, nonché il miglioramento delle politiche e del benessere sociale. Il fulcro di queste iniziative è la raccolta, l'elaborazione e l'utilizzo dei dati. Tuttavia, la gestione di questi dati in una rete IoT coesa comporta rischi, in particolare per quanto riguarda la sicurezza dei dati e la protezione dei dati personali. Pertanto, un'efficace governance delle smart city deve incorporare solide misure di protezione dei dati per mantenere gli standard di sicurezza e privacy. Tuttavia, le applicazioni pratiche della letteratura accademica a questo proposito sono limitate. La presente ricerca si concentra quindi sull'offrire una panoramica completa delle migliori pratiche normative e tecnologiche che possono migliorare la sicurezza e la privacy dei dati nelle smart cities. Nel far ciò, lo scritto si concentra sulla Roma Data Platform (RDP), un progetto che mira ad accelerare la transizione di Roma verso un modello di smart city in vista del Giubileo del 2025.

Keywords: Smart City; Sicurezza; Privacy, Protezione dei dati; Roma Data Platform.

1. Introduzione

Le smart city rappresentano un tema di grande attualità. Non c'è città che non si metta alla prova nel progettare e realizzare soluzioni "smart" per migliorare i propri servizi e salvaguardare ambiente e condizioni di vita dei cittadini.

* Gli autori ringraziano il Prof. Paolo Spagnoletti dell'Università Luiss per la preziosa guida e il supporto forniti nello sviluppo di questo lavoro. Si ringrazia anche Unindustria per aver facilitato il confronto con gli stakeholder. Lo studio pubblicato è stato finanziato dall'Unione Europea – NextGenerationEU, Missione 4, Componente 2, nell'ambito del progetto GRINS – Growing Resilient, INclusive and Sustainable (GRINS PE00000018 – CUP B43C22000760006). I punti di vista e le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione Europea, nè può l'Unione Europea essere ritenuta responsabile per esse.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760152

In questo contesto, i dati divengono una risorsa necessaria delle moderne aree urbane. Al riguardo, i big data e le nuove opportunità che essi rappresentano hanno senz'altro contribuito in modo determinante alla trasformazione delle smart city (Hashem et al., 2016; Bibri, 2018). Le ricerche dimostrano che un apposito disegno programmatico che riguardi la raccolta, la gestione e l'analisi dei dati nelle smart city è fondamentale per creare città che siano operativamente maggiormente efficienti (Al Nuaimi et al., 2015; Hashem, 2016; Lim et al., 2018). In qualunque smart city, la capacità di gestire questi dati e di facilitarne il trasferimento e lo scambio tra soggetti, sistemi e piattaforma, garantisce la loro interoperabilità e promuove una collaborazione sostenibile (Brutti et al., 2019; Buchinger et al., 2021). Tale interoperabilità consente un flusso efficiente di informazioni e una migliore comunicazione tra amministrazioni, organizzazioni private e cittadini (Koo & Kim, 2021). Inoltre, rendendo le informazioni prontamente disponibili e garantendo un accesso paritario ai dati, le smart city forniscono un approccio più trasparente alla condivisione dei dati e alla cooperazione (Hardy & Maurashat, 2017).

Partendo dalla osservazione che le smart city e le piattaforme che ne supportano il funzionamento si nutrono di dati, grandi masse di dati (big data), risulta cruciale individuare forme di condivisione dei dati che possano migliorare le smart city, utilizzando, ove possibile, anche le nuove risorse previste dal Data Governance Act e dal Data Act (Sánchez-Corcuera et al., 2019; Voorwinden, 2021).

Se si vuole, allora, migliorare i nostri contesti urbani e i servizi che li corredano si devono esplorare idonee forme di condivisione dei dati [1].

Questo articolo esamina, allora, le forme di condivisione dei dati, del tipo Business-to-Government data sharing per il pubblico interesse; Government-to-Business data sharing e Civic data sharing (Mossberger et al., 2023), le leve normative che possono incentivarle, magari, anche sfruttando il potenziale di "monetizzazione" dei dati (Ritala, 2024) e le soluzioni che devono essere implementate per garantire sicurezza e protezione dei dati.

2. Sfide aperte nelle smart city

Le smart city sono costituite da piattaforme interconnesse. Le infrastrutture ICT e digitali costituiscono la sua spina dorsale. Queste tecnologie digitali consentono a diversi dispositivi e reti di scambiare informazioni in tempo reale per migliorare i servizi che la città offre ai suoi cittadini. Le smart city si affidano

1 Come affermato anche dallo studio ENISA, Progettare La Condivisione dei Dati Personali, 2023, "il successo delle forme di condivisione dei dati dipenderà dall'istituzione di una forte governance dei dati e anche di garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. La progettazione della protezione dei dati può essere un fattore chiave per costruire un ambiente di condivisione affidabile, in cui le organizzazioni possono inviare dati senza divulgare dati personali o informazioni aziendali sensibili o divulgare dati personali con un adeguato livello di protezione".

tipicamente a dei "*data centers*" o dei "*data lake*" per ospitare tutte le informazioni digitali ottenute attraverso sensori, dispositivi IoT e reti interconnesse (Sinaeepourfard et al., 2020; Ramos et al., 2023). Tuttavia, senza solide misure di sicurezza, questi repository di dati possono essere soggetti ad attacchi informatici che possono mettere a rischio non solo il funzionamento del sistema, ma anche i dati personali dei cittadini (Elmaghraby & Losavio, 2015; Mehmood et al., 2017; Chan et al., 2018).

Secondo Sookhak et al. (2018), nelle smart city, le minacce alla sicurezza si possono manifestare in quattro modi principali. In primo luogo, gli aggressori possono accedere ai sistemi senza essere autorizzati. In secondo luogo, gli aggressori possono accedere a dati ed informazioni sensibili, violando gli accordi di riservatezza intercorrenti con gli utenti. In terzo luogo, gli aggressori possono rendere la piattaforma o il sistema non disponibile per gli utenti o rendere impossibile il suo funzionamento (ad esempio, con attacchi DoS). Infine, le violazioni della sicurezza possono consistere anche nella violazione dei dispositivi che sono utilizzati per inviare e ricevere false comunicazioni. È, quindi, essenziale sviluppare meccanismi resilienti per proteggere le applicazioni delle smart city. Tuttavia, la ricerca mostra anche che gli attuali modelli di difesa della cybersecurity non sono in grado di tenere il passo dello sviluppo delle smart city, in considerazione della natura scalabile e dinamica di questi nuovi modelli urbani (Cui et al., 2018; Chen et al., 2021). La sicurezza e la privacy sono strettamente dipendenti l'una dall'altra; pertanto, qualsiasi violazione della sicurezza può portare all'accesso abusivo e all'uso improprio di informazioni che dovrebbe rimanere riservate (Belance-Gracia et al., 2015; Khan et al., 2017; Cao et al., 2020). I dati devono essere protetti in tutte le attività di trattamento, che riguardano il loro trasferimento, l'archiviazione e l'elaborazione; mentre, qualsiasi violazione di una piattaforma può mettere a rischio l'integrità dell'intero sistema su cui poggia la smart city. Per questo motivo, è assolutamente indispensabile stabilire misure di sicurezza adeguate che evitino accessi abusivi da parte di soggetti non autorizzati (Propecul & Genete, 2016; Khatoun & Zeadally, 2017). Del resto, proprio per salvaguardare adeguatamente le informazioni sensibili ed evitarne la loro perdita di riservatezza, le smart city dovrebbero porre l'accento anche sulle specifiche misure richieste dai big data (Edwards, 2016; Khatoun & Zeadally. 2017) e investire nella progettazione e nell'implementazione di adeguate tecnologie (Khan et al., 2017; Gharaibeh et al., 2017; Cao et al., 2020).

Al giorno d'oggi, l'assenza di un quadro normativo omogeneo che abbia come oggetto le smart city può essere considerata una barriera per una più ampia adozione dei servizi smart city, poiché non esiste un quadro chiaro che indichi come affrontare e risolvere correttamente le questioni che si pongono nella pratica e come promuovere una cooperazione sicura tra le piattaforme (Lucic, et al., 2018; Weber & Žarko, 2019). Inoltre, è stato dimostrato che affrontare tali questioni è importante per mantenere il sostegno e la partecipazione dei cittadini allo sviluppo delle smart city (Van, 2016). Ciononostante, le amministrazioni locali sono spinte dalle aziende ad implementare le tecnologie per le smart city senza aver preventivamente affrontato le esigenze e le richieste dei

cittadini in merito alle modalità di generazione e utilizzo dei big data (Viitanen & Kingston). (Viitanen & Kingston, 2014). Sebbene diversi studiosi abbiano cercato di offrire una soluzione per tutelare i dati personali e la sicurezza nelle smart city, il compromesso tra il raggiungimento della sicurezza e la creazione di servizi efficienti è comunque estremamente impegnativo (Badii et al., 2020; Al-Turjman et al., 2022). Il motivo potrebbe essere agganciato al fatto che l'Internet delle cose (IoT) presenta molte vulnerabilità e l'eterogeneità e la scalabilità delle smart city oggi richiedono norme più puntali e severe (Qu et al., 2019). Di conseguenza, la costruzione di strategie personalizzate, quadri normativi e soluzioni tecnologiche su misura può essere considerata la chiave del successo delle applicazioni per le smart city.

3. Le smart city e la condivisione dei dati

Le smart city rappresentano al giorno d'oggi sicuramente un nuovo paradigma di condivisione dei dati che vengono raccolti ed elaborati mediante le tecnologie più varie: sensori, applicativi Big Data, IoT, algoritmi di AI (Hashem et al., 2016; Bibri, 2018).

L'inserimento delle tecnologie utilizzate nel sistema delle smart city nella più ampia rete dell'Internet of Things (IoT) amplifica – senz'altro – i rischi per i dati, tra cui anche quelli che dipendono da interconnessioni e scambi massivi (Mehmood et al., 2017; Chan et al., 2018; Colapietro, 2023).

Le smart city hanno bisogno di nutrirsi di dati, essendo la circolazione, la condivisione, la portabilità e l'interoperabilità le sue basi portanti (Paolucci & Pollicino, 2023). Non vi è dubbio, infatti, che più sono i dati raccolti ed elaborati dalle smart city, migliori e più efficienti sono i servizi erogati ai cittadini.

Ma la raccolta di grandi masse di dati, necessarie per l'operatività delle smart city, pone come già indicato significative criticità per quanto riguarda la sicurezza e la protezione dei dati personali.

È allora evidente che, nella fase di progettazione e poi nella concreta implementazione della loro governance, delle loro infrastrutture e delle tecnologie che le supportano e che rendono possibile la condivisione dei dati deve essere considerata anche la protezione dei dati personali (Khan et al., 2017; Cao et al., 2020).

Dopo di che, non c'è protezione dei dati senza adozione di misure di sicurezza adeguate. Sicurezza e protezione dei dati personali sono ambiti tra loro strettamente implicati e solo l'adozione di misure di sicurezza adeguate può realizzare un'efficace protezione dei dati. Nelle smart city, dunque, devono essere considerate, da un lato, le istanze di protezione dei dati personali; dall'altro, le sfide poste dalle moderne e sempre più insidiose minacce cibernetiche, da contrastare con le necessarie misure di prevenzione e reazione (Zhang et al., 2017; Appio et al., 2019; Makedoom et al., 2020).

Nonostante la chiarezza di una simile osservazione, la tutela dei dati personali nelle smart city è scarsamente considerata dalla letteratura e lo è ancora meno nelle sue applicazioni pratiche (Eckhoff, 2017).

Mentre, è stato evidenziato che per realizzare un sistema di condivisione dei dati utile e valido è necessario generare un clima di fiducia digitale nei cittadini[2].

La considerazione delle aspettative di *privacy* e di sicurezza dei dati dei cittadini è la premessa fondamentale – come detto – per qualsiasi attività di progettazione e sviluppo di una qualunque smart city o di sue parti e/o servizi[3].

Diventa, poi, pertinente e rilevante parlare di una "privacy" complessiva della smart city, piuttosto che di "privacy" delle singole tecnologie che la integrano (Paolucci & Pollicino, 2023).

Ma come si concilia la fame di dati delle smart city con le esigenze di protezione dei dati personali? Come si possono al contempo assicurare privacy e sicurezza senza limitare lo sviluppo delle smart city?

4. Metodologia

L'obiettivo che, allora, si pone è quello di affrontare le suddette questioni anche alla luce dei recenti interventi normativi in materia di Strategia Europea dei Dati e delle innovazioni emergenti, che possono rendere queste moderne aree urbane più sicure rispetto al trattamento dei dati e, di conseguenza, migliorarne la funzionalità. A tal fine, questo articolo si basa sulla osservazione della Roma Data Platform (nel seguito, RDP), una piattaforma digitale progettata per integrare informazioni provenienti da fonti diverse in un unico sistema preposto al governo della smart city di Roma. Nonostante il suo potenziale, l'attuale piattaforma ha una portata limitata. Nella configurazione attuale, gli archivi di dati e l'interoperabilità tra sistemi IoT sono efficaci solo per uso interno. Atteso che la RDP intende estendere il suo campo di applicazione a un sistema interconnesso di condivisione dei dati tra varie entità, nel tentativo di migliorare i propri servizi ai cittadini, questo articolo mira a fornire una panoramica delle pratiche che possono supportarla, basandosi su un'ampia revisione della letteratura e sulla stretta collaborazione con le figure chiave coinvolte nella progettazione e nell'amministrazione della RDP.

Per acquisire elementi utili di valutazione sono stati, quindi, raccolti dati primari e secondari. I dati primari sono consistiti in discussioni e incontri con i rappresentanti dello sviluppo della RDP. Ciò ha permesso di entrare in contatto diretto con

2 Documento di lavoro dei servizi della Commissione – Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni 'Verso uno spazio comune europeo dei dati' (COM (2018) 232 final).

3 Come affermato anche dallo studio ENISA, Progettare La Condivisione dei Dati Personali, 2023, "il successo delle forme di condivisione dei dati dipenderà dall'istituzione di una forte governance dei dati e anche di garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. La progettazione della protezione dei dati può essere un fattore chiave per costruire un ambiente di condivisione affidabile, in cui le organizzazioni possono inviare dati senza divulgare dati personali o informazioni aziendali sensibili o divulgare dati personali con un adeguato livello di protezione".

le figure chiave coinvolte nel progetto e di ottenere una comprensione completa dello sviluppo graduale e del suo funzionamento in termini di infrastruttura informativa e governance dei dati. La raccolta di dati primari è stata particolarmente preziosa anche per comprendere le sfide e i limiti attuali del sistema. Quest'ultima aiuterebbe a riconoscere le aree che devono essere affrontate e le attuali barriere che impediscono alla RDP di operare a pieno regime. Inoltre, i dati secondari sono consistiti in un'ampia analisi della letteratura che si è articolata in tre fasi importanti: in primo luogo, è stata effettuata un'analisi desk su come le smart city raccolgono, monitorano e analizzano i dati condivisi tra autorità pubbliche e private. In secondo luogo, l'analisi è consistita nello smontare i progetti di smart city più consolidati dal punto di vista tecnologico, normativo e legale. Si è trattato di un passo fondamentale per capire come le iniziative attualmente più rivoluzionarie e di successo al mondo gestiscano i rischi legati ai temi della sicurezza e della privacy senza compromettere la loro efficienza operativa. Infine, l'analisi si è concentrata sul confronto tra le diverse iniziative nel tentativo di arrivare a delle soluzioni ideali (Baskerville et al., 2013).

5. Roma Data Platform

La Roma Data Platform (RDP nel seguito, per brevità) è una piattaforma digitale. La RDP ha una propria infrastruttura, i propri dataset, le proprie logiche ed anche sensori distribuiti. È in grado di raccogliere ed elaborare dati eterogenei e costituisce uno strumento utile di governance per l'Amministrazione comunale di Roma. La RDP si compone di un "cruscotto" centralizzato per l'osservazione e la gestione delle informazioni relative agli aspetti essenziali della vita urbana quotidiana nella città di Roma (Ariano, 2021).

La Roma Data Platform è stata lanciata nel 2020 dalla Città di Roma proprio con l'ambizioso scopo di diventare il cruscotto della città e di portarla ad essere un modello esemplare di smart city. La RDP mira a valorizzare le enormi quantità di informazioni prodotte dalla Città di Roma e dai cittadini tramite l'utilizzo di dispositivi connessi e intende migliorare la governance della città basata sui dati (data-driven), facendola evolvere a grande velocità.

Essa supporta, di fatto, molteplici forme di condivisione dei dati, non solo tra soggetti pubblici ma anche tra i predetti e le imprese private. La RDP è in continua evoluzione e sviluppo e incorpora ciclicamente nuovi stakeholder, dati, conoscenze, algoritmi e altri strumenti di elaborazione. L'architettura informatica che supporta RDP è in grado di raccogliere, registrare ed integrare molteplici flussi di informazioni provenienti da fonti diverse, riuscendo ad incorporarle in un unico sistema. Tutte queste informazioni vengono elaborate dalla RDP che restituisce dei *"data insights"* utili per la governance cittadina ed anche per gli stessi cittadini. In effetti, l'ulteriore obiettivo della RDP è proprio quello di promuovere la partecipazione attiva dei cittadini alla condivisione dei dati, in modo tale che questa partecipazione possa aggiungere valore per l'intero ecosistema dei dati, supportando ulteriormente una governance intelligente

della città e agevolando anche il processo decisionale-strategico delle imprese che scambiano dati.

Poiché la città di Roma genera un'enorme quantità di dati, il progetto Roma Data Platform offre l'opportunità di creare un ampio repository per l'archiviazione e lo scambio di dati con altri sistemi e vari stakeholder. Tuttavia, nel corso degli anni, il suo utilizzo è stato limitato alla governance della città, mancando l'interoperabilità diretta e le connessioni con attori esterni, nonché non più accessibile dai cittadini. In collaborazione con le figure chiave coinvolte nella creazione e nell'amministrazione della piattaforma, è stata condotta una valutazione strategica delle sue capacità e della possibilità di aprirsi allo scambio di dati con entità esterne come organizzazioni private, imprese e cittadini.

La RDP adotta un approccio federato per la gestione dei dati, allineandosi anche con i principi di Gaia-X[4]. Gaia-X rende disponibile le principali linee guida per realizzare piattaforme e strumenti che coinvolgono dati eterogenei ma non fornisce del software ne degli applicativi pronti all'uso. Al seguito di Gaia-X, per facilitare lo sviluppo ed il fiorire dell'economia dei dati europea, composto da molteplici realtà e stakeholder, nasce FIWARE. Contrariamente a Gaia-X, FIWARE non ha lo scopo di promulgare linee guida ma bensì rende disponibili diverse componenti software pronte all'uso e all'integrazione per realizzare smart city efficienti e soprattutto rispettose delle normative europee (Fiware, 2024). Utilizzando FIWARE come base software, RDP promuove la condivisione e l'interoperabilità dei dati tra i vari ecosistemi urbani. Ogni ecosistema è gestito in maniera quasi indipendente, supportando l'approccio federato nella gestione dei dati che è un pilastro fondante di Gaia-X. Proprio grazie a questo approccio, e con l'ausilio del software reso disponibile da FIWARE, la RDP consente non solo alla città di Roma ma anche a tutti gli altri stakeholder di mantenere la sovranità dei dati, assicurando che le informazioni rimangano sotto il controllo dei rispettivi proprietari e garantendo che siano utilizzati in conformità con le normative europee sulla privacy e la sicurezza. Di fatto, Gaia-X stabilisce un modello e le linee guida generali per la gestione decentralizzata, con lo scopo di evitare il proliferare dei silos di dati, ovvero la centralizzazione delle informazioni dove ogni stakeholder controlla e gestisce singolarmente i propri dati, mentre FIWARE mette a disposizione proprio gli strumenti informatici per poter dare forma a questa visione. In questo modo si

4 Con lo scopo di create un'economia europea dei dati nasce Gaia-X. Si tratta di un'iniziativa tutta europea con l'obiettivo di creare un'infrastruttura federata e sicura per i dati. Diversamente da altre soluzioni, è interamente basata su valori europei, quali controllabilità, trasparenza, interoperabilità e portabilità. Lo scopo principale di Gaia-X è gettare le basi per stabilire un ecosistema fidato di dati dove questi possano essere condivisi e resi disponibili, lasciando agli utenti la sovranità sui propri dati ed il loro controllo. Gaia-X mira quindi a collegare vari fornitori di servizi, anche cloud, ed utenti in un sistema trasparente e federato. È proprio questa federazione che consente la portabilità e l'interoperabilità di dati e servizi attraverso i più diversi settori e piattaforme. Regole comuni permettono ai fornitori ed agli utenti di fidarsi reciprocamente e sono basate su di una tecnologica che facilita lo scambio libero e sicuro tra molteplici stakeholders. Questo specifico punto è fondamentale nel supportare la sovranità digitale in Europa ed al contempo non limitare l'innovazione.

favorisce la collaborazione tra stakeholder eterogenei, inclusi produttori di dati, gli sviluppatori di applicazioni e gli enti sia pubblici che privati. La RDP, quindi, non solo intende garantire la sicurezza e la privacy dei dati, ma vuole anche facilitare l'innovazione e la competitività nell'economia digitale, contribuendo a un ecosistema urbano più intelligente, resiliente, sostenibile e con un valore aggiunto tangibile. Per ricapitolare i principali pilastri di Gaia-X, possiamo sintetizzare cinque i principali obiettivi di Gaia-X orientati su altrettanti cinque temi distinti (Bonfiglo, 2021):

- *Sovranità dei Dati*: Garantire che i proprietari dei dati mantengano il controllo sui loro dati;
- *Ecosistemi Federati*: Creare un'infrastruttura di dati interconnessa e decentralizzata;
- *Prestazioni e Scalabilità*: Costruire servizi cloud e di dati efficienti e scalabili;
- *Conformità e Standard*: Adesione alle normative e stabilimento di standard comuni;
- *Sicurezza e Fiducia*: Migliorare la cybersicurezza e costruire fiducia nei servizi digitali.

A marzo 2024, ha preso avvio il progetto "Evoluzione Roma Data Platform", in cui l'Amministrazione comunale di Roma ha inteso investire le risorse necessarie per potenziare la RDP, per migliorare l'efficienza e l'inclusività della gestione urbana in vista del Giubileo 2025 (Comune di Roma, 2024).

6. Incentivare la condivisione dei dati

Le collaborazioni, la condivisione dei dati e il coordinamento tra il settore pubblico e quello privato è, sicuramente, il "motore principale" di una smart city, nel cui ambito hanno un crescente ruolo attivo anche i cittadini (Voorwinden 2021).

La collaborazione sui dati consente di indirizzare i dati, che sono nel dominio di soggetti privati (imprese, in particolare), verso istanze di interesse collettivo (Spagnoletti et al., 2025; Kazemargi et al. 2023). Ma si tratta ancora di pratiche non sufficientemente sperimentate, atteso che – soprattutto nel settore privato – i dati sono prevalentemente utilizzati all'interno delle organizzazioni.

Si osserva che tradizionalmente lo scambio di dati nel settore privato è ostacolato da due cause principali[5]. Le aziende tendono a trattare i dati per il loro uso esclusivo e per mantenere un vantaggio competitivo rispetto ai loro concorrenti. Dopo di che, i privati mantengono i dati di cui sono titolari all'interno della loro organizzazione e non sono disposti a condividerli, quando i benefici che ne trae il pubblico sono poco chiari o quando il loro utilizzo non è sufficientemente remu-

5 European Commission, 2020. *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

nerativo rispetto alle loro missioni imprenditoriali" (Grimaldi & Fernandez, 2019; Mossberger et al., 2023).

Quindi, per invertire questa tendenza, va fatta pressione:

- da un lato, sulle imprese private, per migliorare lo scambio di dati secondo le formule "Business to Government data sharing" e "Government to Business data sharing";
- dall'altro, sui cittadini, che decidono di condividere i loro dati (c.d. "Civic data sharing"). Questi dati servono alle smart city, in quanto sono ricchi delle informazioni necessarie alla fornitura e al miglioramento dei servizi[6].

Le smart city devono, allora, adoperarsi per attirare il conferimento dei dati da parte degli stakeholder nelle forme del "Business to Government data sharing" e del "Civic data sharing".

Peraltro, assicurandosi che gli incentivi pensati a vantaggio dei partecipanti non costituiscano pratiche vietate proprio sotto il profilo della protezione dei dati personali.

Con provvedimento in data 8 giugno 2022, dal titolo *"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"*, infatti, l'Autorità Garante per la Protezione dei Dati Personali ha comunicato di avere avviato alcune istruttorie su una serie di progetti sperimentali promossi enti pubblici e società private, volti ad attribuire dei premi ai cittadini che avessero scelto di condividere spontaneamente i loro dati nella smart city. L'intervento dell'Autorità Garante per la Protezione dei Dati Personali si è reso necessario, poiché queste pratiche risultavano rischiose per i diritti e le libertà degli interessati, tra i quali, anche soggetti vulnerabili. Tra queste istruttorie spicca quella avviata dall'Autorità Garante per la Protezione dei Dati Personali in merito al "Progetto Pollicino", che ha interessato il Comune di Bologna, la Fondazione per lo Sviluppo Sostenibile, il Ministero della Transizione Ecologica e il Ministero delle Infrastrutture e della Mobilità Sostenibile e alcune società private preposte alla erogazione dei premi ai cittadini (Vigorito 2023).

Nello specifico, il progetto prevedeva di svolgere di indagini statistiche di tipo sperimentale nelle quali i cittadini erano incentivati a conferire i loro dati (apparentemente "in forma anonima"), per consentire analisi utili allo sviluppo dei servizi della smart city. Quale contropartita della condivisione dei propri dati, il cittadino veniva poi ammesso ad usufruire dei premi offerti dai partner privati del progetto.

6 "Il successo delle forme di condivisione dei dati dipenderà anche dall'istituzione di una forte governance dei dati e di garanzie efficaci per i diritti e gli interessi delle persone fisiche che siano pienamente conformi al GDPR. L'ingegneria della protezione dei dati può essere un fattore chiave per costruire un ambiente di condivisione affidabile, in cui le organizzazioni possono inviare dati senza divulgare dati personali o informazioni aziendali sensibili o divulgare dati personali con un adeguato livello di protezione" (ENISA 2023).

7. Data Governance Act e Data Act

Anche i recentissimi interventi normativi relativi alla Strategia Europea per i Dati concretizzano ulteriori opportunità utili a raggiungere gli obbiettivi di smart city di cui sopra e dovranno – senz'altro – essere oggetto di approfondimenti e sviluppi.

Nello specifico, il Data Governance Act (Regolamento europeo 2022/868 del 30 maggio 2022) può essere sfruttato per la condivisione dei dati Government to Business Data Sharing.

Il Data Governance Act si propone di rimuovere gli ostacoli alla condivisione dei dati nel settore pubblico. Seppure la condivisione dei dati in questo settore sia una pratica senz'altro più sperimentata che nel settore privato – come visto sopra – è rimasta comunque sottoutilizzata per i motivi più vari. Tra questi, la scarsa fiducia e il poco interesse nella condivisione come tale (senza un qualche ritorno economico e, più in generale, di utilità), ma anche gli ostacoli normativi al riutilizzo dei dati[7].

Il considerando 5 del Data Governance Act afferma che "è necessaria per aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano e al fine di affrontare altri ostacoli al buon funzionamento di un'economia competitiva basata sui dati".

L'intervento del legislatore europeo mira a "creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche". [8]

Il Data Governance Act sosterrà, inoltre, lo sviluppo di spazi comuni di dati europei in vari settori che interessano anche le smart city (come la sanità, l'ambiente e la mobilità) "per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile. I servizi di intermediazione dei dati potrebbero includere la condivisione bilaterale o multilaterale dei dati o la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati, nonché *l'istituzione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti dei dati*" (considerando 27).

Queste iniziative mirano a facilitare la condivisione dei dati, permettendo ai cittadini e alle imprese di appropriarsi dei relativi vantaggi.

7 European Commission, 2020. *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

8 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

Rientrano nell'ambito di applicazione del Data Governance Act sia i dati personali che quelli non personali, con tutte le complesse implicazioni che ne conseguono circa l'applicabilità – rispetto ai primi – del Regolamento europeo 2016/679.

Date queste premesse, è di immediata evidenza che il Data Governance Act potrebbe essere estremamente utile per incentivare forme di condivisione dei dati all'interno delle smart city. Infatti, i dati potenzialmente oggetto di riuso, detenuti dai soggetti pubblici, potrebbero costituire oggetto di scambio con le imprese private per attirare, nelle smart city in generale e nella Roma Data Platform in particolare, dati, congrui investimenti e nuove tecnologie utili a migliorare le sue infrastrutture e i suoi servizi.

Salva la necessità di approfondire più nel dettaglio le opportunità offerte dal Data Governance Act e le limitazioni che ad esso può porre il Regolamento europeo 2016/679, ai nostri fini sicuramente rileva l'art. 6, paragrafi 1 e 4 del Data Governance Act, alla cui stregua "Gli enti pubblici che consentono il riutilizzo … di dati … possono imporre tariffe per consentire il riutilizzo di tali dati" e che "Qualora gli enti pubblici applichino tariffe, essi adottano misure per incentivare il riutilizzo di dati… a fini non commerciali, quali la ricerca scientifica, e da parte delle PMI e delle start-up in conformità delle norme sugli aiuti di Stato. A tale riguardo, gli enti pubblici possono anche mettere a disposizione i dati a una tariffa ridotta o nulla, in particolare per le PMI e le start-up, la società civile e gli istituti di istruzione. A tal fine, gli enti pubblici possono stilare un elenco di categorie di riutilizzatori a cui i dati per il riutilizzo sono forniti a una tariffa ridotta o a titolo gratuito. Detto elenco è reso pubblico unitamente ai criteri adottati per la sua redazione".

Peraltro, il fatto che sia possibile applicare delle tariffe al riutilizzo dei dati, potrebbe anche aprire ad accordo o ad altre forme di monetizzazione e/o, comunque, di valorizzazione dei dati.

Il Data Act (Regolamento europeo 2023/2854 del 13 dicembre 2023) potrebbe, invece, essere utilmente sfruttato per la condivisione dei dati del tipo Civic Data Sharing, come sarà indicato di seguito.

Per converso, il Data Act non può essere utilizzato per sostenere forme di condivisione dei dati del tipo "Business to Government", di tipo volontario. A ben vedere, infatti, questo atteso intervento normativo non introduce elementi di novità rispetto ad iniziative volontarie di *data sharing* del tipo "Business to Government" (cfr. considerando 65 e 66), che restano escluse dal suo campo di applicazione, focalizzato su obblighi di condivisione dei dati per ragioni di emergenza pubblica (Masnada, 2023).

8. Dati dei Cittadini ("Civic Data Sharing")

Come detto, i cittadini hanno senz'altro un ruolo attivo rispetto agli obbiettivi di smart city che si stanno considerando (Grimaldi e Fernandez, 2019). In definitiva, si tratta di ipotizzare un contesto partecipato da vari stakeholder che mirano ad un obbiettivo comune di interesse pubblico. Segnatamente, gli autori dell'articolo

"*The public good and public attitudes toward data sharing through IoT*" mettono in evidenza che i cittadini sono disposti a conferire i dati a soggetti pubblici e privati se hanno un ritorno in termini di vantaggi personali o di tipo collettivo – una migliore sanità pubblica, minor traffico, ecc. (Mossberger et al., 2023).

In definitiva, i cittadini trasferiscono i loro dati quando hanno fiducia in colui che li riceve e che li tratterà e se ha anche un ritorno personale, che però – come abbiamo visto – non può basarsi su sistemi di scoring e correlati premi, se questo impatta sui loro diritti e libertà personali.

Ora interessanti prospettive di "*Civic Data Sharing*" possono conseguire – come detto – anche dalla applicazione del Data Act, alla cui stregua "su richiesta di un utente, o di una parte che agisce per conto di un utente, il titolare dei dati mette a disposizione di terzi i dati prontamente disponibili, nonché i pertinenti metadati necessari a interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo continuo e in tempo reale" (art. 5, Data Act).

Il diritto dell'utente, di condividere i dati con terzi previsto dal Data Act, costituisce un'estensione del diritto alla portabilità dei dati personali, già previsto all'art. 20, Regolamento europeo 2016/679 e potrebbe avere rilevanti applicazioni nel contesto che ci sta occupando, rafforzando gli strumenti degli individui per trasferire i loro dati da un fornitore ad un altro.

9. Modelli di protezione dei dati personali

Per assicurare il diritto alla protezione dei dati personali trattati nell'ambito delle condivisioni di cui sopra sono tradizionalmente utilizzati due modelli.

Un primo modello che utilizza solo dati anonimizzati e, quindi, applica misure di "privacy", anziché misure di sicurezza. Una soluzione di questo genere elimina – senz'altro – qualsiasi questione in materia di protezione di dati personali, poiché i dati anonimi non sono dati personali e, quindi, non si applica il Regolamento europeo 2016/679.

È stato, però, osservato che – anche rispetto ai dati anonimi – non è sempre risolta ogni questione di protezione dei dati personali, se non sono implementate tecniche di anonimizzazione sufficientemente solide, poiché in questo caso resta alto il rischio di reidentificazione degli interessati. Ad esempio, sono stati reidentificati dati che si credeva fossero stati irreversibilmente anonimizzati, a seguito di incidenti che hanno interessato alcuni database sui dati di navigazione degli utenti (Germania), sui dati relativi alla salute (Italia, Australia), sui dati del trasporto pubblico (Lettonia) (De Cordes, 2019).

È stato, poi, ulteriormente sottolineato che l'anonimizzazione dei dati porta a perdere molte informazioni importanti. In definitiva, i dati anonimizzati diventano meno ricchi di informazioni e, quindi, meno utili agli obbiettivi delle smart city (De Cordes, 2019).

Un altro modello è rappresentato dalla definizione di appositi accordi contrattuali sui dati, che definiscano i soggetti e le responsabilità relative al trattamento dei dati personali. In questo modello, le questioni di "privacy" restano in tutta la loro portata e richiedono che siano definiti i ruoli dei soggetti coinvolti nel trattamento dei dati personali, le informazioni da dare agli interessati, le basi giuridiche necessarie per trattare i dati, le valutazioni d'impatto sulla protezione dei diritti e le libertà fondamentali degli interessati, da effettuare (de Montjoye, 2018).

Rispetto ai due approcci tradizionali visti sopra, si collocano delle soluzioni ulteriori che promuovono lo scambio dei dati sotto il dominio degli utenti, i quali potranno scegliere selettivamente le imprese o i soggetti pubblici che avranno accesso a tutti o parte dei loro dati, nonché la durata del loro utilizzo e tutte le altre condizioni per usufruirne (De Cordes, 2019).

Attraverso, poi, l'esercizio dei diritti degli interessati (artt. 15-2, Regolamento europeo 2016/679) i cittadini potranno, successivamente al loro conferimento, anche controllare come vengono utilizzati i loro dati.

10. Conclusioni e sviluppi futuri

Lo scopo di questo articolo sta nel mettere in evidenza le varie forme di condivisione dei dati tra soggetti pubblici, privati e i cittadini che possono essere utilizzate per migliorare ed accelerare lo sviluppo delle smart city, ponendole nella condizione di rispondere efficacemente ai bisogni di moderne ed affollate aree urbane, come anche la smart city di Roma e la piattaforma che la supporta.

L'attività di analisi di cui sopra è stata condotta andando a vedere se anche i recenti interventi normativi, relativi alla Strategia Europea dei Dati, potessero svolgere un ruolo di impulso e incentivo rispetto a quelle forme di condivisione.

Le smart city hanno, infatti, necessità di raccogliere grandi masse di dati per poter rendere utili ed efficaci servizi ai cittadini.

È, quindi, emerso che in effetti ci sono ulteriori significativi margini di sviluppo nel ricercare quali potrebbero essere le applicazioni concrete di quelle previsioni normative, per incentivare la condivisione dei dati nelle smart city, sfruttando e facendo leva anche sul potenziale di "monetizzazione" dei dati oggetto di scambio, da indirizzare comunque verso l'attuazione di interessi collettivi (mobilità, turismo, sanità).

In questo contesto, non abbiamo potuto prescindere anche dal considerare le problematiche poste dalla necessità di proteggere i dati personali dei cittadini (applicando il Regolamento europeo 2016/679 e la normativa interna in materia di protezione dei dati personali) che, in effetti, sono poco studiate nella letteratura e sono ancora meno considerate nelle loro applicazioni pratiche, delineando quali sono le soluzioni tradizionali proposte ed applicate e quali potrebbero essere le alternative da esplorare.

Nei successivi capitoli di questa ricerca vogliamo allora sviluppare ulteriormente questi temi di indagine, andando anche oltre lo scenario della smart city di Roma

(che è sicuramente riduttivo) per proporre un modello valido e tendenzialmente replicabile per qualunque moderna smart city.

Bibliografia

Abella A., Ortiz-de-Urbina-Criado, M. and De-Pablos-Heredero, C. 2017, "A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems", in *Cities*, *64*, pp.47-53.

Al Nuaimi E., Al Neyadi H., Mohamed N. and Al-Jaroodi, J. 2015, "Applications of big data to smart cities", in *Journal of Internet Services and Applications*, *6*, pp.1-15.

Al-Turjman F., Zahmatkesh H. and Shahroze R. 2022, "An overview of security and privacy in smart cities' IoT communications", in *Transactions on Emerging Telecommunications Technologies*, *33*(3), p. e3677.

Angelidou M. 2015, "Smart cities: A conjuncture of four forces", *Cities*, *47*, 95-106.

Ariano A. 2021, "Il caso della Roma Data Platform", in *Una geografia delle politiche urbane tra possesso e governo. Sfide e opportunità nella transizione*, pp.177-183.

Batty M., Axhausen K.W., Giannotti F., Pozdnoukhov A., Bazzani A., Wachowicz M., Ouzounis G. and Portugali Y. 2012, "Smart cities of the future", in *The European Physical Journal Special Topics*, *214*, pp.481-518.

Baskerville R., de Marco M., & Spagnoletti p. 2013, *Designing Organizational Systems: an interdisciplinary discourse* Cham: Springer. https://doi.org/10.1007/978-3-642-33371-2.

Belanche-Gracia D., Casaló-Ariño L.V. and Pérez-Rueda A. 2015, "Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions", in *Government information quarterly*, *32*(2), pp.154-163.

Bibri S.E. and Krogstie J. 2017, "Smart sustainable cities of the future: An extensive interdisciplinary literature review", in *Sustainable cities and society*, *31*, pp.183-212.

Bokolo A. Jnr. 2022, "Data driven approaches for smart city planning and design: a case scenario on urban data management", in *Digital Policy, Regulation and Governance*, vol. 25, n. 4, pp. 351.

Bolognini L. 2024, *Ammissibilità del modello "pay or consent": tra rivoluzione economica digitale e modernizzazione della protezione dei dati. Un* open access paper *dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati.*

Bonfiglio F. 2021, *Gaia-X Vision and Strategy* (https://gaia-x.eu/wp-content/uploads/2021/12/Vision-Strategy.pdf) (Accessed: May 14, 2024).

Brutti A., De Sabbata p. , Frascella A., Gessa N., Ianniello R., Novelli C., Pizzuti S. and Ponti G., 2019, "Smart city platform specification: A modular approach to achieve interoperability in smart cities", in *The internet of things for smart urban ecosystems*, pp.25-50.

Buchinger M., Kuhn p. , Kalogeropoulos A. and Balta D., 2021, "Towards interoperability of smart city data platforms", in *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Cao Q.H., Giyyarpuram M., Farahbakhsh R. and Crespi N. 2020, "Policy-based usage control for a trustworthy data sharing platform in smart cities", in *Future Generation Computer Systems*, *107*, pp.998-1010.

Chan A.L., Chua G.G., Chua D.Z.L., Guo S., Lim p. M.C., Mak M.T. and Ng W.S., 2018, "February. Practical experience with smart cities platform design", in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 470-475). IEEE.

Chen D., Wawrzynski p. and Lv Z., 2021, "Cyber security in smart cities: a review of deep learning-based applications and case studies", in *Sustainable Cities and Society*, *66*, p. 102655.

Cheng B., Longo S., Cirillo F., Bauer M. and Kovacs E. 2015, "June. Building a big data platform for smart cities: Experience and lessons from Santander", in *2015 IEEE International Congress on Big Data* (pp. 592-599). IEEE.

Chourabi H., Nam T., Walker S., Gil-Garcia J.R., Mellouli S., Nahon K., Pardo T.A. and Scholl H.J., 2012, "January. Understanding smart cities: An integrative framework", in *2012 45th Hawaii international conference on system sciences* (pp. 2289-2297). IEEE.

Colapietro C. 2023, "Intelligenza artificiale e smart cities a mo' di introduzione", in *Smart cities, Diritti, libertà e governance*, pp. XVIII-XXXIV.

Comune di Roma 2024, https:// https://www.comune.roma.it/web/it/attivita-progetto.page?contentId=PRG1163717 (Accessed: May 30, 2024).

Cui L., Xie G., Qu Y., Gao L. and Yang Y. 2018, "Security and privacy in smart cities: Challenges and opportunities", in *IEEE access*, *6*, pp.46134-46145.

da Rosa Lazarotto B. 2022, "The implications of the Proposed Data Act to B2G data sharing in smart cities", available at SSRN.

De Cordes N., de Montjoye Y., Smoreda Z. 2019, *OPAL: reconciling open innovation and data security*.

de Montjoye Y. 2018, "On the privacy-conscientious use of mobile phone data", in *Scientific Data*, 5, Article number: 180286.

Eckhoff D. 2017, Privacy in the Smart City – Applications, Technologies, Challenges and Solutions.

Edwards L. 2016, "Privacy, security and data protection in smart cities: A critical EU law perspective", in *Eur. Data Prot. L. Rev.*, *2*, p. 28.

ENISA 2024, *Engineering Personal Data Protection in EU Sata Space*s. [Online], available at: https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces.

European Commission 2020, *Towards a European strategy on business-to-government data sharing for the public interest.* Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing.

Fiware 2024, https://fiware.org (Accessed: May 14, 2024).

Gharaibeh A., Salahuddin M.A., Hussini S.J., Khreishah A., Khalil I., Guizani M. and Al-Fuqaha A. 2017, "Smart cities: A survey on data management, security, and enabling technologies", in *IEEE Communications Surveys & Tutorials*, *19*(4), pp. 2456-2501.

Grimaldi D. and Fernandez V. 2019, "Performance of an internet of things project in the public sector: The case of Nice smart city", in *The Journal of High Technology Management Research*, *30*(1), pp.27-39.

Hardy K. and Maurushat A. 2017, "Opening up government data for Big Data analysis and public benefit", in *Computer law & security review*, *33*(1), pp. 30-37.

Harrison C., Eckman B., Hamilton R., Hartswick p. , Kalagnanam J., Paraszczak J. and Williams p. 2010, "Foundations for smarter cities", in *IBM Journal of research and development*, *54*(4), pp.1-16.

Hashem I.A.T., Chang V., Anuar N.B., Adewole K., Yaqoob I., Gani A., Ahmed E. and Chiroma H. 2016, "The role of big data in smart city", in *International Journal of information management*, *36*(5), pp.748-758.

Janssen M., Charalabidis Y. and Zuiderwijk A. 2012, "Benefits, adoption barriers and myths of open data and open government", *Information systems management*, *29*(4), pp.258-268.

Kazemargi N., Spagnoletti p. , Constantinides p. , & Prencipe p. 2023, "Data control coordination in cloud-based ecosystems: the GAIA-X case", in C. Cennamo, G. B. Dagnino, & F. Zhu (Eds.), *Handbook of Research on Digital Strategy*, Elgar, pp. 289-307 (https://doi.org/10.4337/9781800378902.00024).

Khan Z., Pervez Z. and Abbasi A.G. 2017, "Towards a secure service provisioning framework in a smart city environment", in *Future Generation Computer Systems*, *77*, pp.112-135.

Khatoun R., & Zeadally S. 2017, "Cybersecurity and privacy solutions in smart cities", in *IEEE Communications Magazine*, *55*(3), 51-59.

King J., Meinhardt C. 2024, *Rethinking Privacy in the AI Era*, Stanford University.

Kitchin R. and Dodge M. 2020, "The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention", in *Smart cities and innovative Urban technologies* (pp. 47-65). Routledge.

Klievink B., Van Der Voort H. and Veeneman W. 2018, "Creating value through data collaboratives", in *Information Polity*, *23*(4), pp.379-397.

Koo J. and Kim Y.G. 2021, "Interoperability requirements for a smart city" in *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (pp. 690-698).

Lévy-Bencheton C. and Darra E. 2015, *Cyber security and resilience of intelligent public transport: good practices and recommendations*.

Lim C., Kim K.J. and Maglio p. P. 2018, "Smart cities with big data: Reference models, challenges, and considerations", in *Cities*, *82*, pp.86-99.

Liu J., Chen N., Chen Z., Xu L., Du W., Zhang Y. and Wang C. 2022, "Towards sustainable smart cities: Maturity assessment and development pattern recognition in China", in *Journal of Cleaner Production*, *370*, p. 133248.

Lučić D., Boban M. and Mileta D. 2018, "An impact of general data protection regulation on a smart city concept", in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 0390-0394). IEEE.

Masnada M. 2023, "I dati al centro della strategia UE: Data Act e Data Governace Act a confronto", in *Agenda Digitale*, 6 settembre.

Mehmood Y., Ahmad F., Yaqoob I., Adnane A., Imran M. and Guizani S., 2017, "Internet-of-things-based smart cities: Recent advances and challenges", in *IEEE Communications Magazine*, *55*(9), pp.16-24.

Mossberger K., Cho S., Cheong p. H. and Kuznetsova D. 2023, "The public good and public attitudes toward data sharing through IoT", in *Policy & Internet*, *15*(3), pp. 370-396.

Paolucci F. e Pollicino O. 2023, "Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarità nella nuova stagione algoritmica?", in *Smart cities, Diritti, libertà e governance*, pp.17-43.

Pierce p. and Andersson B. 2017, *Challenges with smart cities initiatives–A municipal decision makers' perspective*.

Popescul D. and Genete L.D. 2016, "Data security in smart cities: challenges and solutions", in *Informatica Economică 20*(1).

Qu Y., Nosouhi M.R., Cui L. and Yu S. 2019, "Privacy preservation in smart cities", in *Smart cities cybersecurity and privacy*, Elsevier, pp. 75-88.

Ramos G.S., Fernandes D., Coelho J.A.P.D.M. and Aquino A.L. 2023, "Toward Data Lake Technologies for Intelligent Societies and Cities", in *Sustainable, Innovative and Intelligent Societies and Cities*, Cham: Springer, pp. 3-29.

Ritala p. , Keränen J., Fishburn J. and Ruokonen M. 2024, "Selling and monetizing data in B2B markets: Four data-driven value propositions", in *Technovation*, *130*, p. 102935.

Sánchez-Corcuera R., Nuñez-Marcos A., Sesma-Solance J., Bilbao-Jayo A., Mulero R., Zulaika U., Azkune G. and Almeida A. 2019, "Smart cities survey: Technologies, application domains and challenges for the cities of the future", in *International Journal of Distributed Sensor Networks*, *15*(6), p. 1550147719853984.

Silva B.N., Khan M. and Han K. 2018, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities", in *Sustainable cities and society*, *38*, pp.697-713.

Sinaeepourfard A., Krogstie J. and Sengupta S. 2020, "Distributed-to-centralized data management: a new sense of large-scale ICT management of smart city IoT networks", in *IEEE Internet of Things Magazine*, *3*(3), pp.76-82.

Sookhak M., Tang H., He Y. and Yu F.R. 2018, "Security and privacy of smart cities: a survey, research issues and challenges", in *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1718-1743.

Spagnoletti p. , Kazemargi N., Constantinides p. , & Prencipe A. 2025, "Data Control Coordination in the Formation of Ecosystems in Highly Regulated Sectors", in *Journal of the Association for Information Systems,* forthcoming.

Topham S., Boscolo p. and Mulquin M. 2023, *Personal Data-Smart Cities: How cities can Utilise their Citizen's Personal Data to Help them Become Climate Neutral*, Taylor & Francis, p. 365.

Trencher G. and Karvonen A. 2020, "Stretching 'smart': Advancing health and well-being through the smart city agenda", in *Smart and Sustainable Cities?*, Routledge, pp. 54-71.

Trindade E.P., Hinnig M.P.F., da Costa E.M., Marques J.S., Bastos R.C. and Yigitcanlar T. 2017, "Sustainable development of smart cities: A systematic review of the literature", in *Journal of Open Innovation: Technology, Market, and Complexity*, *3*(3), pp.1-14.

Tripodi E. 2024, "Le prospettive potenziali della smart city 'evoluta': la digital twin city", in *Diritto di Internet*, 1/2024, pp. 23-36.

Van Zoonen L. 2016, "Privacy concerns in smart cities", in *Government Information Quarterly*, *33*(3), pp. 472-480.

Vigorito A. 2023, "Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo", in *Media Laws*, *1/2023*, pp. 104-127.

Viitanen, J. and Kingston R. 2014, "Smart cities and green growth: outsourcing democratic and environmental resilience to the global technology sector", in *Environment and Planning A*, *46*(4), pp. 803-819.

Voorwinden A. 2021, "The privatised city: Technology and public-private partnerships in the smart city", in *Law, Innovation and technology*, *13*(2), pp. 439-463.

Weber M. and Podnar Žarko I. 2019, "A regulatory view on smart city services", in *Sensors*, *19*(2), p. 415.

Wirsbinna A. and Grega L. 2021, "Assessment of economic benefits of smart city initiatives", in *Cuadernos de Economía*, *44*(126), pp. 45-56.

Zhang K., Ni J., Yang K., Liang X., Ren J. and Shen X.S. 2017, "Security and privacy in smart city applications: Challenges and solutions", in *IEEE communications magazine*, *55*(1), pp. 122-129.

Matteo Pignatti

La cybersecurity nella digitalizzazione del settore finanziario

Abstract: L'innovazione tecnologica costituisce un fattore che incide sull'economia e assume caratteri particolari nel settore finanziario. Il rapporto di co-dipendenza dal settore ICT che si è venuto a creare comporta rischi sulla stabilità finanziaria del sistema europeo e conferisce un ruolo alle Istituzioni UE nella gestione di fenomeni a carattere sovranazionale. Le cripto-attività, la definizione di misure per garantire un livello comune elevato di cybersicurezza nell'UE, la resilienza operativa digitale per il settore finanziario e dei soggetti critici hanno originato un contesto giuridico in cui l'analisi e la gestione rischi, i regimi contrattuali vincolati e l'attività di sorveglianza costituiscono strumenti volti a garantire la sicurezza e l'efficienza nel Mercato Interno. Il contributo intende analizzare i profili giuridici rilevanti nella gestione del rapporto di co-dipendenza tra ICT e finanza, i principali rischi per il settore finanziario e le possibili criticità ad essi connesse.

Keywords: Cybersecurity; Settore bancario e finanziario; Mercato interno; Vigilanza.

1. La digitalizzazione nel settore finanziario

La transizione digitale nel settore finanziario si inserisce in un contesto in cui la necessità di adeguare e rendere competitivo il Mercato Interno a livello internazionale deve essere bilanciata con la sana e prudente gestione nell'attività finanziaria e la tutela del risparmio, contribuendo a definire un mercato unico digitale dei servizi finanziari[1].

1 Circa la necessità di sostenere il progresso tecnologico nell"economia europea nel settore finanziario, si v.: Commissione UE, *Comunicazione relativa a una strategia in materia di finanza digitale per l'UE*, 24 settembre 2020 COM(2020) 591 final. Per una descrizione dell'evoluzione si v. Bronzetti 2023: 6 e s.; Ruocco 2023: 181 e s. In relazione alla sovranità tecnologica si v.: Commissione UE, *Relazione di previsione strategica 2021*, 8 settembre 2021, 4; European Innovation Council, *Statement to accompany the launch of the full EIC*, allegato I, *Statement on Technological Sovereignty*, 18 marzo 2021. In dottrina: Capriglione 2021: 4 e s.; Celati 2021: (3) 252 e s.; Finocchiaro 2022: 809 e s.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760153

Il rapporto tra settore finanziario e ICT[2] ha generato differenti fenomeni rilevanti per il diritto dell'economia[3] conferendo al *FinTech* un'autonoma rilevanza[4] e ponendo in evidenza nuovi rischi[5].

L'adozione di misure per sostenere settori economici rilevanti per la crescita[6] entra in rapporto con quelle connesse alla sicurezza[7], generando un contesto giuridico particolarmente complesso per gli operatori finanziari che sono chiamati a

2 Già oggi le banche europee dichiarano che il 65% di esse ha *partnership* contrattuale con le aziende *BigTech*. Si v.: Campa 2023: 1 e s. Cfr. anche: Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications*, 14 febbraio 2019; Id., *BigTech Firms in Finance in Emerging Market and Developing Economies Market developments and potential financial stability implications*, 12 ottobre 2020. Cfr. anche: European Supervisory Authorities, *ESAs Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities*, 31 gennaio 2022, ove sono affrontati alcuni profile della digitalizzazione del settore finanziario: catene di valore (*value chains*) sempre più frammentate e non integrate; piattaforme e offerta di prodotti finanziari; rischi per i gruppi che operano in diversi settori integrando differenti attività. Il p. to 4, all'interno della raccomandazione n. 1, pone l'attenzione sui possibili rapporti di dipendenza. Si v. anche European Banking Authority, *Report on the use of digital platforms in the eu banking and payments sector*, 2021, 33 e s., ove ci si riferisce ai rapporti di dipendenza da fornitori terzi di servizi ICT.

3 Tali fenomeni non solo hanno semplificato le attività nel settore finanziario (ove correttamente utilizzati), ma hanno anche inciso sulla diffusione nel mercato degli effetti economici (positivi o negativi) derivanti da essi.

4 *Ex multis*: Lemma 2020: 1 e s.; Lemma 2023: 83 e s.; Annunziata – Minto 2022: 1 e s.; Mazzarisi – Ravagnani – Deriu – Lillo – Medda – Russo 2022: 1-49; Annunziata 2020: 1 e s.; Sciarrone Alibrandi – Borello – Ferretti – Lenoci – Macchiavello – Mattassoglio – Panisi 2019: 1 e s.

5 Si v. Parlamento UE, *Relazione recante raccomandazioni alla Commissione sulla finanza digitale: rischi emergenti legati alle criptoattività – sfide a livello della regolamentazione e della vigilanza nel settore dei servizi, degli istituti e dei mercati finanziari*, 2020; Banca d'Italia, *Comunicazione in materia di tecnologie decentralizzate nella finanza e cripto-attività*, 15 giugno 2022. In dottrina: Rabitti 2023(a): 345 e s.. Cfr. a titolo esemplificativo il caso connesso alla negligenza contabile della società di servizi finanziari *Wirecard*. D. McCrum, *Wirecard made this short seller right but not rich*, in *Financial Times*, 15 luglio 2020.

6 Commissione UE, *The future of European Competitiveness – Part A, A competitiveness strategy for Europe*, 9 settembre 2024, 19 e s., in relazione specificatamente alla digitalizzazione e all'innovazione tecnologica si v. anche *Part B*, 67 e s.

7 Si v. la revisione della disciplina sugli investimenti esteri diretti (Regolamento UE, 2019/452. Si v. anche: Commissione UE, *Proposta di regolamento UE relativo al controllo degli investimenti esteri nell'Unione, che abroga il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio*, 26 gennaio 2024), le previsioni sulla coercizione economica da paesi terzi (Regolamento UE 2023/2675, *sulla protezione dell'Unione e dei suoi Stati membri dalla coercizione economica da parte di paesi terzi*), le previsioni in materia di sovvenzioni estere alle imprese europee volte a prevenire possibili distorsioni economiche (Regolamento UE 2022/2560, *relativo alle sovvenzioni estere distorsive del Mercato Interno)*, nonché per il sostegno alla ricerca e lo sviluppo su tecnologie potenzialmente a duplice uso e controllo sulle esportazioni di quest'ultime (Regolamento UE 2021/821*, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso – rifusione –*).

gestire l'evoluzione di strumenti ICT[8] utilizzati nelle proprie attività, garantendo elevati livelli di sicurezza informatica[9] e una resilienza operativa digitale[10] capace di rispondere in maniera efficace alle esigenze del settore finanziario[11].

L'esternalizzazione a soggetti terzi di funzioni tecniche, se da un lato può consentire di conseguire obiettivi all'interno del mercato (mediante l'acquisizione di un *know-how* specifico), è altresì idonea a generare rapporti di co-dipendenza che possono incidere negativamente sulla continuità dell'attività degli operatori finanziari.

Le previsioni europee in tema di cybersicurezza nell'UE (c.d. direttiva NIS2) e di resilienza operativa digitale per il settore finanziario (c.d. regolamento DORA) si inseriscono tra le misure volte all'armonizzazione della finanza digitale[12], propo-

8 Campa 2023, "Around half of EU banks (covering both corporate and retail segments) have reported that most of their customers (75%-100%) primarily use digital channels for daily banking activities. (…) In the area of Artificial Intelligence (AI), more than 70% of EU banks use AI at least in some areas of activities. Its use is more widespread in creditworthiness assessment and credit scoring, fraud detection, commercial profiling and clustering of clients or transactions, AML/CFT being more wide-spread. An increased use of chatbots or similar solutionsis being noticed. We also see that many financial entities focus on optimisation of internal processes and introducing digitalisation in order to increase efficiencies and cut their operating costs".

9 Direttiva UE, 2555/2022, c.d. NIS2, attuata nell'ordinamento giuridico italiano con il d.lgs. 4 settembre 2024, n. 138.

10 Sulla nozione di "resilienza operativa digitale", si v. Regolamento UE, 2554/2022, *Digital operational resilience for the financial sector* – art. 3, par. I, p. to 1), ove è definita come "la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni"; Commissione UE, *relazione alla direttiva che modifica le direttive 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341*, COM(2020) 596 final, 24 settembre 2020; Comitato economico e sociale europeo, *Parere sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE*, cit., p. to 2.4.

11 *Ex multis*: Casalino 2023: 337 e s.; Baskerville – Capriglione – Casalino 2020: 341 e s.; Alpa 2019: 377 e s.; Miglionico, 2019: 1376 e s.

12 Circa il *Digital Finance Package* si v. Commissione UE, *Comunicazione relativa a una strategia in materia di finanza digitale per l'UE*, 24 settembre 2020; Commissione UE, *Comunicazione relativa a una strategia in materia di pagamenti al dettaglio per l'UE*, 24 settembre 2020. La strategia europea si compone di quattro atti normativi in tema di: cripto-attività (regolamento UE 1114 del 2023, sui mercati delle cripto-attività – MiCA, quali rappresentazioni digitali di valori o di diritti che possono essere trasferiti o memorizzati elettronicamente attraverso una tecnologia che supporta la registrazione distribuita di dati cifrati – tecnologia di registro distribuito, *distributed ledger technology – DLT* su cui si v. Regolamento UE n. 858 del 2022); l'armonizzazione delle principali prescrizioni sulla resilienza operativa digitale (modificando altresì le direttive vigenti in materia di servizi finanziari, per lo più per necessità di adeguare la disciplina concernente i requisiti in materia di rischio operativo e di gestione del rischio al nuovo regolamento DORA, e per aggiornare la definizione di "strumento finanziario" includendo gli strumenti emessi utilizzando la tecnologia DLT (Direttiva UE 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario). A tali atti si aggiunge la disciplina relativa a mercati equi e contendibili nel

nendosi di regolare in maniera uniforme e integrata le misure per la prevenzione e gestione dei rischi relativi ai rapporti con il settore ICT[13].

La direttiva UE NIS2, entrata in vigore il 17 gennaio 2023 il cui recepimento negli ordinamenti giuridici nazionali era previsto entro il 17 ottobre 2024[14], si propone di realizza un'armonizzazione minima in materia di cybersicurezza nell'UE. La norma supera la distinzione tra "Operatori di Servizi Essenziali" (OSE) e "Fornitori di Servizi Digitali" (FSD) in favore di quella tra "Soggetti Essenziali" e "Soggetti Importanti"[15] che operano all'interno dei settori ad "alta criticità" (all. I, in cui rientra il settore bancario) e degli "altri settori critici" (all. II), e su cui ricade la responsabilità di garantire la sicurezza dei sistemi informatici e di rete che utilizzano nelle loro attività.

Il regolamento UE DORA, applicabile a partire dal 17 gennaio 2025, armonizza le regole di *governance* e di gestione del rischio ICT per le istituzioni finanziarie (definizione che ricomprende non solo gli enti creditizi ma anche le imprese di assicurazione e di riassicurazione, istituti di pagamento e moneta elettronica, imprese di investimento, gestori di fondi alternativi e molti altri operatori del nostro sistema finanziario), sino a oggi frammentate in vari corpi normativi, adottati principalmente dalle Autorità Europee di Vigilanza (EBA, ESMA ed EIOPA).

In questo contesto l'attività di sorveglianza interviene a supporto dell'analisi e gestione rischi (in chiave di prevenzione e mitigazione degli eventi) e dell'attività

settore digitale (Regolamento, n. 1925 del 2022, *Digital Markets Act* – DMA), e la proposta di regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*), di una direttiva relativa sull'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (*AI Liability Directive*), riguardante il regime di responsabilità per danni causati con il coinvolgimento di sistemi di intelligenza artificiale. In dottrina: Capriglione 2019: 374 e s.; Sepe 2021: 186 e s.; Canepa 2021: 465 e s.; Urbani 2022: 985 e s. La Banca Centrale Europea e la Commissione UE stanno inoltre proseguendo le attività dei tavoli di lavoro incaricati dello studio di fattibilità del cd. *digital euro project*, ossia dell'istituzione, regolazione ed emissione di una *central bank digital currency* (CBDC) da parte delle Istituzioni europee. Cfr. BCE, *Progress on the investigation phase of a digital euro, 14 luglio 2023*; BCE, *The case for a digital euro: key objectives and design considerations, luglio 2022*.

13 Mediante ad es.: la definizione e il costante aggiornamento di sistemi, protocolli per gestire rischi informatici (Regolamento UE, 2554/2022, art. 7), l'identificazione dei ruoli e responsabilità nelle funzioni svolte dall'operatore finanziario mediante strumenti ICT (Regolamento UE, 2554/2022, art. 8), il controllo costante la gestione dei dati (per prevenire la loro corruzione, perdita e garantirne la riservatezza, Regolamento UE, 2554/2022, art. 9), l'individuazione di punti di vulnerabilità (Regolamento UE, 2554/2022, art. 10), anche mediante test di resilienza operativa digitale (Regolamento UE, 2554/2022, artt. 24-27) e la gestione di eventi di rischio per garantire la continuità mediante apposite piani e procedure di backup (Regolamento UE, 2554/2022, artt. 11 e 12) è coniugata e collegata con l'attività gestione degli incidenti informatici in collaborazione e coordinamento con le Autorità di Vigilanza (europee e nazionali, Regolamento UE, 2554/2022, artt. 17-23. In ambito europeo il riferimento è all'Autorità europea degli strumenti finanziari e dei mercati – ESMA, all'Autorità europea delle assicurazioni e delle pensioni aziendali o professionali – EIOPA e all'Autorità bancaria europea – EBA).

14 L'attuazione nell'ordinamento giuridico italiano è avvenuta con: d.lgs. 4 settembre 2024, n. 138.

15 Direttiva UE, 2555/2022, art. 4.

contrattuale con terzi fornitori di servizi ICT (quale strumento istituzionale di garanzia da asimmetrie informative e a tutela del risparmio).

In questo contesto, l'ordinamento giuridico europeo si propone di garantire "un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno"[16] e bilanciare i differenti interessi e riequilibrare i rapporti di forza tra i due settori mediante la previsione di vincoli contrattuali e in termini di sorveglianza[17], in particolare ove i fornitori di servizi ICT siano qualificati come "critici"[18] o risultino stabiliti in paesi terzi[19].

Il contributo intende analizzare le previsioni in materia di cybersecurity e sulla resilienza operativa digitale per il settore finanziario, approfondendo i rischi connessi alle prestazioni ICT oggetto di esternalizzazione. L'analisi si propone di chiarire i profili giuridici rilevanti nella gestione del rapporto con il settore ICT, i principali rischi per il settore finanziario e le possibili criticità ad essi connesse analizzando il ruolo della vigilanza.

2. La *cybersecurity* e l'affidamento a soggetti terzi di servizi ICT nel settore finanziario

Il rapporto tra il settore ICT e quello finanziario comporta specifici rischi che sovente conseguono ad una asimmetria informativa che può comportare una "cattura" dei soggetti che svolgono la propria attività nel settore finanziario[20].

I rischi connessi alla sicurezza informatica ed alla sua vulnerabilità possono tuttavia assumere differente natura.

16 Direttiva UE, 2555/2022, art. 1.

17 La disciplina europea non impone massimali rigidi o restrizioni rigorose circa il ricorso a fornitori di servizi ICT al fine di non incidere negativamente sull'attività economica del settore limitandone la libertà contrattuale, piuttosto cerca di individuare strumenti, quali l'analisi e gestione dei rischi, la realizzazione di stress test, l'attività di vigilanza, l'attenzione ai contenuti contrattuali con i fornitori terzi di servizi ICT ed i regimi di responsabilità, per equilibrare i rapporti di forza e di dipendenza tra i due settori al fine di tutelare gli interessi degli investitori e del sistema europeo. Tali strumenti, applicati al settore finanziario sulla base di una proporzionalità declinata in termini generali (Regolamento UE, 2554/2022, art. 4, par. I, ove, la disciplina in materia a resilienza operativa digitale per il settore finanziario, trova applicazione "tenendo conto delle (…) dimensioni [degli operatori del settore finanziario] e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività") e in termini specifici in relazione ai rapporti giuridici con i terzi fornitori di servizi ICT (Regolamento UE, 2554/2022, art. 28, par. I, lett. b), ove la gestione dei rischi informatici derivanti da terzi da parte delle entità finanziarie, tiene conto: "i: della natura, della portata, della complessità e dell'importanza delle dipendenze connesse alle TIC; ii) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, tenendo conto della criticità o dell'importanza dei rispettivi servizi, processi o funzioni e del potenziale impatto sulla continuità e la disponibilità delle attività e dei servizi finanziari a livello individuale e di gruppo").

18 Regolamento UE, 2554/2022, art. 3, par. I, p. to 23.

19 Regolamento UE, 2554/2022, art. 3, par. I, p. to 24.

20 Regolamento UE, 2554/2022, artt. 5-16.

I rischi legati alla disciplina normativa costituiscono una categoria generale (che va quindi oltre i servizi resi da fornitori terzi e al settore finanziario), ma assumono peculiarità proprie in un contesto in cui interessi economici nazionali si frappongono a quelli europei.

L'armonizzazione di concetti rilevanti e regole tecniche può costituire elemento di sviluppo del mercato europeo e ridurre possibili distorsioni opportunistiche al suo interno (ad es. derivanti da *bias*[21]), anche in relazione alla frammentazione dei servizi finanziari (che rende complessa la *compliance* per gli operatori finanziari), e tutelare i consumatori (nel corretto utilizzo di servizi finanziari digitali)[22]. Se molti dei principi, requisiti e regole tecniche sono già contenuti all'interno di norme, orientamenti e atti di *soft law* di settore[23], risulta tuttavia necessario garantire la loro armonizzazione e la coerenza con concetti definiti in altri settori (quale ad es. quello bancario[24]) o negli atti normativi UE (come ad es. il regolamento UE in materia di Intelligenza artificiale, che individua nel livello di "rischio" un fattore distintivo all'interno della disciplina)[25].

La definizione di molteplici strumenti o atti, a livello sovranazionale[26] e nazionale[27], e l'interazione tra differenti soggetti (pubblici[28] e privati[29]) deve essere accompagnato da un'uniformità di livelli di tutela, regole tecniche e giuridiche per garantire l'efficiente ed efficace funzionamento del Mercato Interno.

21 Davola 2017: 637 e s.

22 Capriglione 2022: 254.

23 Come quelli elaborati dall'ABE e dall'EIOPA, nonché il progetto di orientamenti dell'ESMA, oggetto di consultazione. In materia di esternalizzazione di servizi, si v. la dicotomia, in termini di ambito di applicazione, tra 'esternalizzazione' e 'servizio di terzi'. La resilienza operativa digitale si riferisce unicamente ai "servizi TIC di terzi" per quanto riguarda i principi fondamentali per la gestione corretta dei rischi relativi alle TIC derivanti da terzi (capo V), mentre l'ambito di applicazione degli orientamenti dell'ABE in materia di esternalizzazione si basa su una definizione di esternalizzazione che implica che l'attività sia eseguita in modo ricorrente o continuativo (par. 26). Gli orientamenti dell'ABE forniscono inoltre un elenco di eccezioni che non sono considerate come rientranti nell'ambito dell'esternalizzazione (par. 28).

24 Comitato di Basilea per la vigilanza bancaria, *Principles for operational resilience* (Principi di resilienza operativa), 6 novembre 2020.

25 Regolamento UE 2024/1689, *che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*.

26 In relazione alla direttiva NIS2, si v., a titolo esemplificativo, direttiva UE, 2555/2022, art. 21, in relazione alla definizione di misure di gestione dei rischi di cybersicurezza ed il d.lgs. 4 settembre 2024, n. 138, art. 24;

27 Direttiva UE, 2555/2022, artt. 1 e 7, in cui si prevede l'obbligo di definire delle strategie nazionali in materia di cybersicurezza. Nell'ordinamento giuridico italiano cfr. d.lgs. 4 settembre 2024, n. 138, art. 9.

28 Si v. le forme di cooperazione previste dalla direttiva NIS2 e dal regolamento DORA.

29 Si v. la definizione del quadro per la gestione dei rischi informatici che deve essere definito dagli operatori finanziari (regolamento UE, 2554/2022, art. 6) ed i sistemi, protocolli e strumenti ICT da utilizzare per "affrontare e gestire i rischi informatici" (regolamento UE, 2554/2022, art. 7).

Gli atti approvati dalla Commissione UE nel 2024 ed in corso di approvazione, possono costituire un importante elemento di armonizzazione di concetti, regole tecniche[30] e documenti[31] nel mercato europeo, che pare assumere carattere di omogeneizzazione dell'attività finanziaria mediante strumenti ICT e di cui oggi si può solo evidenziarne l'opportunità.

Tale auspicio metodologico parrebbe ulteriormente giustificato dai modelli organizzativi fondati sulla cooperazione a livello internazionale, europeo e nazionale previsti dalla direttiva NIS2[32] e dal regolamento DORA[33], nonché dall'approccio orizzontale di gestione dei rischi adottato nella disciplina in materia di resilienza operativa digitale per il settore finanziario e compatibile con la necessità di evitare sovrapposizioni di concetti, duplicazioni e problemi di coordinamento tra norme europee relative a nuove tecnologie rilevanti anche nell'ambito dell'esternalizzazione di prestazioni rilevanti[34] che potrebbero generare ostacoli al funzionamento del mercato unico, a danno degli operatori del mercato e della stabilità finanziaria[35].

La possibile esternalizzazione a "fornitori terzi di servizi ICT", in virtù di ragioni tecniche, contempera la libertà di iniziativa economica (Cost. it., art. 41) con vincoli e controlli di natura pubblica derivanti dalla necessità di tutelare il risparmio e garantire la stabilità (Cost. it., art. 47) e costituisce un elemento di rischio che incide in maniera autonoma e differenziata sul settore finanziario.

La circostanza per cui la dipendenza dallo strumento ICT si riflette nei confronti di soggetti terzi, la cui maggiore conoscenza delle dinamiche tecnologiche può comportare a distorsioni e alterazioni del mercato finanziario, costituisce fondamento dell'analisi e gestione dei rischi.

Ecco come la fase preliminare all'instaurazione di rapporti contrattuali con soggetti terzi diviene fase fondamentale. Una meticolosa analisi precontrattuale

30 Regolamento UE, 2554/2022, art. 15, con riferimento all'armonizzazione di strumenti, metodi, processi e politiche di gestione del rischio informatico (entro il 17 gennaio 2024); art. 18, relativo alla classificazione degli incidenti connessi alle TIC e delle minacce informatiche (entro il 17 gennaio 2024); art. 26, con riferimento ai test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (entro il 17 luglio 2024); art. 28, in relazione alla politica per l'utilizzo dei servizi ICT a supporto di funzioni essenziali o importanti prestati da fornitori terzi, nell'ambito della strategia per i rischi informatici derivanti da terzi (entro il 17 gennaio 2024); art. 30, par. V, con riferimento alle regole tecniche connesse alle funzioni ICT inserite nei contratti tra operatori del settore finanziario e terzi fornitori di servizi ICT (entro il 17 luglio 2024); art. 41, in relazione all'armonizzazione delle condizioni che consentono lo svolgimento delle attività di sorveglianza (entro il 17 luglio 2024).

31 Regolamento UE, 2554/2022, art. 20, con riferimento all'armonizzazione dei modelli e dei contenuti per la segnalazione (entro il 17 luglio 2024); art. 28, in relazione a modelli standard registro di informazioni sugli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi, comprese le informazioni comuni a tutti gli accordi contrattuali per l'utilizzo di servizi ICT (entro il 17 gennaio 2024).

32 Direttiva UE, 2555/2022, artt. 13-19.

33 Regolamento UE, 2554/2022, artt. 28 e s., sulla gestione dei rischi informatici derivanti da terzi.

34 Schneider 2023: 1014 e s.; Arner-Buckley-Zetsche 2022: 147 e s.

35 Regolamento UE, 2554/2022, considerando n. 9.

dovrebbe concentrarsi sui rischi connessi all'utilizzo di strumenti ICT gestiti da fornitori terzi (l'individuazione delle funzioni essenziali o importanti, l'analisi dei rapporti societari di tali soggetti ed i possibili conflitti di interesse, la gestione e la sicurezza dei dati e dei possibili rischi informatici, la realizzazione di test adeguati per verificare la funzionalità e resistenza dei sistemi adottati)[36], che, unitamente alla collaborazione ed al costante rapporto con le autorità di vigilanza costituiscono elementi prodromici e che fondano la diligente gestione dell'attività da parte degli operatori del mercato finanziario e delle loro responsabilità.

In questo modo, mentre la direttiva UE NIS2, distingue tra "soggetti essenziali" e "soggetti importanti"[37] che operano nei settori ad "alta criticità" (tra cui è ricompreso quello bancario)[38] o in "altri settori critici"[39] per definire l'ambito di applicazione soggettivo delle misure comuni europee in materia di cybersicurezza, il regolamento UE DORA suddivide i rischi connessi ai rapporti contrattuali con soggetti terzi, operando una prima distinzione sulla base delle caratteristiche del fornitore del servizio ICT, dell'oggetto delle prestazioni contrattuali e le modalità con cui sono prestate (per poter valutare altresì gli effetti conseguenti gli automatismi degli strumenti ICT). Tra i soggetti che in generale forniscono servizi ICT ad un operatore finanziario[40], assume carattere rilevante la posizione dei terzi fornitori che specificatamente risultano come "critici"[41]. Questi ultimi sono individuati sulla base di criteri quali: l'impatto sistemico sulla stabilità, la continuità o la qualità della fornitura di servizi finanziari (qualora il fornitore terzo sia interessato da una disfunzione operativa); il carattere sistemico o l'importanza delle entità finanziarie che dipendono da un fornitore terzo; la dipendenza delle entità finanziarie dai servizi prestati ed il grado di sostituibilità del fornitore[42], e risultano ulteriormente classificabili, ove ne ricorrano le condizioni, tra terzi che prestano l'attività nell'ambito di rapporti di controllo societario e in gruppi di imprese[43].

36 Regolamento UE 2554/2022, art. 3, par. I, p. to 5, in cui i "rischi informatici" sono definiti come "qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando effetti avversi nell'ambiente digitale o fisico". Financial Stability Board, *Enhancing Third-Party Risk Management and Oversight. A toolkit for financial institutions and financial authorities*, 4 December 2023, 15.

37 Direttiva UE, 2555/2022, art. 3

38 Direttiva UE, 2555/2022, all. I, p. to 3, ripreso nel d.lgs. 4 settembre 2024, n. 138, all. I, p. to 3.

39 Direttiva UE, 2555/2022, all. II, ripreso nel d.lgs. 4 settembre 2024, n. 138, all. II.

40 Regolamento UE 2554/2022, art. 3, par. I, p. to 19.

41 Regolamento UE 2554/2022, artt. 3, par. I, p. to 23 e 31 e s.

42 Regolamento UE 2554/2022, art. 31, par. II.

43 Regolamento UE 2554/2022, art. 3, par. I, p. ti 25, 26 e 27 in cui si distinguono le nozioni di "impresa figlia" e "impresa madre" e di "gruppo" rimandando alla disciplina relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese (Direttiva UE 2013/34).

La distinzione assume una ulteriore importanza ove il fornitore (o subappaltatore[44]) "critico" sia stabilito in uno Stato esterno all'Unione Europea[45].

La declinazione data ai criteri individuati per qualificare un fornitore come "critico" è sintomo di una preoccupazione che la dipendenza degli operatori del settore finanziario da imprese ICT sia amplificato da "concentrazioni" di fornitori ICT[46] e che tali situazioni (non consentendo all'organismo che opera nel mercato finanziario di svolgere le proprie funzioni essenziali o assorbire effetti finanziari conseguenti) si riflettano negativamente sulla stabilità del sistema finanziario europeo[47]. L'impatto delle eventuali disfunzioni connesse all'utilizzo di strumenti ICT, il carattere sistemico delle entità finanziarie, il livello di dipendenza dai servizi ICT forniti in relazione alle funzioni essenziali e il grado di sostituibilità del fornitore terzo evidenziano l'attenzione alla continuità delle attività del settore finanziario e alla necessità di particolari accortezze al fine di evitare che disfunzioni di un fornitore si propaghino sull'intero sistema finanziario europeo.

Ecco come la circostanza che un fornitore "critico" sia stabilito presso un paese terzo, e la dipendenza del settore finanziario non sia più solo verso il settore ICT (o un singolo operatore economico) ma verso le economie che controllano quest'ultimo, comporta ulteriori precauzioni insite nella volontà di garantire una autonomia e indipendenza al sistema finanziario europeo da soggetti esterni (in stretta connessione al concetto di sovranità europea che si sta definendo).

Le caratteristiche dei singoli mercati di riferimento dei servizi ICT rilevano nella definizione dei rischi[48].

44 Regolamento UE 2554/2022, art. 3, par. I, p. to 28, in cui viene definito il subappaltatore stabilito in un paese terzo.

45 Regolamento UE 2554/2022, art. 3, par. I, p. to 24. L'attenzione per i fattori che determinano la dipendenza da fornitori terzi ICT stabiliti fuori dall'UE o con evidenti collegamenti societari esteri all'UE non paiono limitati alla tutela di interessi direttamente connessi al settore finanziario, ma pongono l'attenzione sugli ulteriori interventi Europei volti a garantire una sovranità tecnologica europea (che paiono costituire un interesse superiore che va oltre un singolo settore, comunque complementare ad esso). L'evoluzione del progetto Gaia-X (*https://gaia-x.eu/*), volto a realizzare una governance dei dati dell'UE attraverso una rete *cloud* con sede nell'Unione Europea, potrebbe garantire l'indipendenza dai fornitori esterni di servizi *cloud* rafforzando le modalità di gestione dei dati e delle informazioni del settore finanziario, nonché la sovranità economica, tecnologica e politica europea. La realizzazione di una piattaforma dell'UE per i dati potrebbe consentire l'accesso a fornitori di servizi *cloud* alternativi, anche nel settore finanziario. La Commissione ha chiesto all'Agenzia dell'Unione europea per la cibersicurezza (ENISA) di sviluppare un regime di certificazione della cibersicurezza per i servizi *cloud*, in conformità del regolamento sulla cibersicurezza, che contribuirà ad aumentare la fiducia nell'utilizzo del *cloud*, in particolare da parte dei servizi finanziari e degli organismi di regolamentazione. Parere del Comitato economico e sociale europeo sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE, 24 febbraio 2021, in cui si ritiene che una rete *cloud* europea faciliterebbe inoltre i flussi di dati tra gli Stati UE.

46 Regolamento UE 2554/2022, art. 3, par. I, p. to 29, in cui si definisce il rischio di concentrazione delle TIC e art. 29, sulla valutazione preliminare del rischio di concentrazione.

47 Regolamento UE 2554/2022, art. 31, par. II.

48 I settori di servizi ICT che comunemente rientrano tra le funzioni critiche e importanti del settore finanziario ricomprendono: i servizi di infrastruttura di rete, i servizi di data center.

La circostanza per cui la maggior parte degli operatori finanziari sistemici europei ricorre ai servizi di tecnologia finanziaria forniti da società di paesi terzi (Stati Uniti e Cina)[49] che hanno una posizione dominante in alcuni servizi ICT (quale il *cloud*) espone il Mercato Unico ad una dipendenza che non è solo più tecnologica, ma che genera effetti sulle operazioni finanziarie e nei rapporti politici. La disciplina europea sulla resilienza operativa digitale (DORA) può rivelarsi insufficiente in situazioni in cui le caratteristiche del mercato dei fornitori di servizi ICT sia tale da vincolare il settore finanziario (es. in caso di un numero limitato fornitori di servizi, esterni all'Unione Europea, in presenza di accordi commerciali, vincoli societari o situazioni di controllo e collegamento tra i possibili fornitori).

L'esternalizzazione di servizi ICT comporta inoltre l'accesso alle informazioni sensibili e dati finanziari da parte di soggetti terzi. Possibili violazioni della sicurezza possono incidere sulla stabilità del settore, anche indirettamente (quale conseguenza della limitata affidabilità del sistema europeo). L'incremento dei rapporti contrattuali tra operatori finanziari e aziende ICT, potrebbe creare un'ulteriore complessità dove i fornitori terzi sfruttino le loro infrastrutture e la superiorità nella raccolta dei dati mediante forme di interconnessione.

I rischi operativi, connessi a problemi tecnici o interruzioni nei servizi forniti dai terzi fornitori e la necessità di sostituire un fornitore di servizi ICT, possono incidere direttamente sulle attività delle istituzioni finanziarie (causando ritardi nelle transazioni, perdite di dati o interruzioni dei servizi ai clienti) condizionando la continuità dell'attività. L'allineamento degli strumenti di risposta e recupero dei dati a seguito di incidenti informatici con le previsioni del Consiglio per la stabilità finanziaria (*Cyber Incident Response and Recovery* – CIRR – del *Financial Stability Board* – FSB) pare essenziale per garantire una omogeneità nelle misure.

La costante evoluzione tecnologica e la necessità di correggere, aggiornare strumenti, metodologie e *software* incrementano tali rischi.

I rischi di dipendenza, di concentrazione o di *lock in* da uno (non facilmente sostituibile) o più fornitori terzi (tra loro strettamente connessi) per i servizi rilevanti e per la continuità operativa dell'istituzione finanziaria possono riflettersi negativamente sulla stabilità del sistema finanziario[50]. Il ricorso al medesimo for-

49 Masera 2022: 167, in cui si evidenzia come la Cina, con alcune delle più importanti Fintech Companies del mondo, pone una sfida alla leadership degli US nella Finanza Digitale e al ruolo del dollaro al centro del sistema finanziario internazionale. Per una analisi del contesto italiano: Consob, *FINTECH: Profili di attenzione e opportunità per gli emittenti e il risparmio nazionale*, 6 luglio 2021. Si v. anche: Trautmann 2023: 38(5), 155-161.

50 European Supervisory Authorities, *ESAs Report on the landscape of ICT third-party providers in the EU*, 19 settembre 2023, la cui analisi evidenzia un mercato rilevante composto da circa 15.000 fornitori che prestano servizi ICT a circa 1.600 entità finanziare incluse nel campione d'indagine (tra cui le imprese di assicurazione). Secondo l'analisi, i fornitori più richiesti sono anche quelli che tendono a fornire servizi a supporto del maggior numero di funzioni essenziali o importanti e la difficile sostituibilità dei fornitori ICT che prestano attività in relazione a funzioni essenziali. Si v. anche European Supervisory Authorities, Joint European Supervisory *Authority responsa to a request for technical advice on digital finance and relate issues*, ESA 2022 01, 31 gennaio 2022; European Banking Authority, *Report on the use of digital platforms in the EU banking*

nitore per più tipologie di servizi accresce gli effetti di dipendenza dell'operatore finanziario dal fornitore stesso ponendo quest'ultimo in posizione dominante nel mercato (rendendo altresì possibile, in presenza di un numero limitato di fornitori ICT per specifiche prestazioni contrattuali, la realizzazione di accordi per la suddivisione del mercato rilevante).

Ove più operatori del settore finanziario ricorrano al medesimo fornitore o sussistano interdipendenze societarie tra questi, si possono generare conflitti di interesse riducendo la capacità di prevedere condizioni contrattuali proporzionate alla tipologia di prestazione e rischio. Una particolare attenzione concerne anche la possibile partecipazione di uno o più operatori del settore finanziario al capitale sociale del fornitore di servizi ICT o il ricorso a società che rientrano in gruppi di imprese.

Ulteriori fattori di rischio riguardano i possibili accordi di subappalto e le catene di subappalti, che rendono complessa l'attività di sorveglianza (anche in termini di analisi dei rapporti societari), soprattutto quando siano conclusi con fornitori terzi di servizi ICT stabiliti in un paese terzo[51].

La possibilità che tali eventi si verifichino genera un autonomo rischio che concerne la reputazione dell'operatore finanziario e dell'intero sistema europeo incidendo negativamente sulla fiducia degli investitori. Qualsiasi problema legato alla sicurezza dei dati o alle prestazioni dei servizi ICT da parte di terzi può danneggiare gravemente la reputazione di un'istituzione finanziaria.

L'attività di analisi e gestione del rischio è imputata all'organo di governo dell'operatore finanziario che, nell'ambito dei suoi compiti connessi alla gestione sana e prudente dell'attività, è chiamato ad approvare il "quadro per la gestione dei rischi informatici"[52] che contiene la politica dell'operatore per l'uso di servizi ICT prestati da un fornitore terzo e la predisposizione di canali di comunicazione aziendali idonei ad ottenere informazioni sui rapporti contrattuali con i fornitori terzi e le relative modifiche[53]. Si definisce in questo modo una "strategia per i rischi informatici derivanti da terzi" fondata sulla differenziazione dei fornitori (non solo per ridurre l'incidenza di singoli rischi, ma anche il rapporto di forza sotteso alla dipendenza dall'ICT) e revisioni periodiche dei rischi da parte dell'organo di gestione dell'operatore finanziario[54].

L'analisi e la ponderazione preventiva, equilibrata e precauzionale consente agli operatori del settore di organizzare e migliorare la propria conoscenza

and payements sector, 21 settembre 2021; Palmerini – Aiello – Cappelli – Morgante – Amore – Di Vetta – Fiorinelli – Galli 2018: 35 e s.; Campa 2023.

51 EBA, *Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud*, 28 marzo 2018, 11 e s.

52 Regolamento UE, 2554/2022, art. 5, par. II. Il quadro per la gestione dei rischi informatici trova disciplina specifica nel successivo art. 6. Nel caso in cui ricorrano le circostanze, si v. anche l'art. 16 relativo al quadro semplificato.

53 Regolamento UE, 2554/2022, art. 5, par. II, lett. h) e i).

54 Regolamento UE 2554/2022, art. 28, par. II. La strategia per i rischi informatici derivanti da terzi comporta, per l'organo di gestione, un controllo costante e periodico rischi individuati in relazione agli accordi contrattuali per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti.

delle attività ICT, è contemperata ed integrata da previsioni contrattuali e di sorveglianza idonee.

3. La gestione dei rapporti tra operatori finanziari e fornitori terzi di servizi ICT

La direttiva UE NIS2 definisce un contesto volto a consentire l'efficace gestione di rischi informatici nel Mercato Interno, ed è funzionalmente connessa, con specifica rilevanza per gli operatori finanziari con il regolamento UE DORA. Quest'ultimo individua nel contratto con terzi fornitori di servizi ICT (in relazione a funzioni "essenziali e importanti") e nell'attività di sorveglianza (sull'attività dei fornitori terzi "critici") i due strumenti con cui bilanciare i molteplici interessi in rapporto e riequilibrare la dipendenza del settore finanziario da quello tecnologico.

In un contesto in cui gli operatori finanziari possono avere difficoltà ad imporre determinate clausole all'interno del contratto, rilevano quelli che sono veri e propri obblighi che la disciplina europea pone in capo ai fornitori terzi.

Gli elementi essenziali dei contratti con i fornitori terzi di servizi ICT sono strettamente collegati alla necessità di garantire all'operatore finanziario un controllo sulla sicurezza e sulla corretta gestione operativa dell'attività finanziaria (al fine di tutelare la solidità e la continuità dei servizi finanziari)[55].

Se la previsione normativa di vincoli contrattuali obbligatori per i fornitori terzi di servizi ICT rende ulteriormente percepibile la necessità di tutelare gli operatori finanziari (dalla posizione di forza contrattuale del settore ICT), l'attività delle autorità di vigilanza interviene a supporto dell'analisi e gestione rischi (in chiave di prevenzione e mitigazione degli eventi)[56] e dell'attività contrattuale con terzi fornitori di servizi ICT (quale strumento istituzionale di garanzia da asimmetrie informative e a tutela del risparmio).

Mentre la sorveglianza interna garantisce un livello di autonomia minimo (anche di carattere tecnico) dell'operatore finanziario, rispetto alle altre funzioni interne e ai fornitori ICT[57], la sorveglianza esterna rende i fornitori di servizi ICT (che in linea generale non esercitano attività di natura finanziaria), soggetti alla vigilanza di Autorità che viceversa svolgono il proprio ruolo nell'ambito finanziario, bancario e assicurativo[58]. Tale attività assume un ruolo particolarmente incisivo in relazione ai fornitori terzi "critici"[59], con i quali le Autorità Europee di Vigilanza – AEV (e quella individuata come capofila), istituiscono un rapporto diretto[60].

55 Rilevano quindi la descrizione chiara delle prestazioni oggetto del contratto, i livelli di servizio, ed il luogo della sua esecuzione (anche in un contesto di gestione e conservazione delle informazioni nell'UE), le condizioni di eventuali contratti di subappalto, la gestione delle informazioni e dei dati (anche in relazione ai casi in cui il fornitore terzo risulti impossibilitato a fornire la prestazione).

56 Rabitti 2023(a): 343 e s.

57 Regolamento UE 2554/2022, art. 6, IV.

58 Campa 2023: 5.

59 Regolamento UE 2554/2022, artt. 31-44.

60 Si v.: l'art. 31, par V, in cui si prevede la notifica diretta al fornitore terzo della sua

Le autorità di sorveglianza capofila, individuate direttamente dalle AEV[61] sulla base di criteri aventi ad oggetto i servizi ICT prestati dal fornitore terzo (quali l'impatto sistemico, l'importanza delle entità finanziarie, la dipendenza dai servizi prestati dal fornitore terzo e il grado di sostituibilità)[62], si propongono di acquisire una conoscenza approfondita e completa delle relazioni nei singoli settori della fornitura di servizi ICT[63].

La cooperazione[64] e il coordinamento[65] dell'attività delle Autorità di Vigilanza Europee nell'ambito di una rete comune, costituisce fattore determinante per individuare i possibili soggetti terzi critici e garantire l'effettività della sorveglianza nel Mercato Unico[66].

qualificazione come "critico" (il quale a sua volta deve informare l'operatore finanziario a cui presta servizi ICT); l'art. 31, par. XIII, in cui il fornitore terzo critico è chiamato a notificare direttamente all'autorità di sorveglianza capofila gli eventuali cambiamenti sulla struttura gestionale dell'impresa figlia istituita nell'UE; art. 33, par. I, in relazione ai compiti dell'autorità di sorveglianza capofila, si individua quest'ultima quale "principale punto di contatto per i fornitori terzi critici di servizi ICT"; art. 35, in relazione all'esercizio diretto dei poteri dell'autorità di sorveglianza capofila sul fornitore terzo critico.

61 Su proposta del comitato congiunto delle AEV (per la funzione di coordinamento nell'ambito del Sistema europeo di vigilanza finanziaria) e su raccomandazione del forum di sorveglianza (organo di supporto del comitato congiunto e delle AEV individuate come capofila per il singolo operatore finanziario sulla base della quota principale delle proprie attività).

62 Regolamento UE 2554/2022, art. 31, par. II. Criteri che potranno essere ulteriormente integrati dalla Commissione UE entro il 17 luglio 2024 (si v. il par. VI).

63 In questo contesto sono di interesse (quale anticipazione dei criteri che potranno essere integrati dalla Commissione UE) gli indicatori quantitativi e qualitativi proposti dalle AEV riferiti ad undici criteri di criticità suggeriti ed ai rispettivi livelli di rilevanza. European Supervisory Authorities, *Joint European Supervisory Authorities' Technical Advice to the European Commission's December 2022 Call for Advice on two delegated acts specifying further criteria for critical ICT thirdparty service providers (CTPPs) and determining oversight fees levied on such providers*, 29 settembre 2023, dove, in relazione agli indicatori quantitativi, sono proposte alcune soglie minime di rilevanza. Tali soglie di rilevanza minima costituiscono un requisito minimo al di sopra del quale deve essere effettuata la valutazione sulla criticità.

64 *Ex* art. 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010. Cfr. il Regolamento UE 2554/2022, art. 32, c. VII, in cui si prevede il compito per le AEV di formulare (entro il 17 luglio 2024) "orientamenti sulla cooperazione tra le AEV e le autorità competenti concernenti le procedure e le condizioni dettagliate per la ripartizione e l'esecuzione dei compiti tra le autorità competenti e le AEV, nonché forniscono dettagli sugli scambi di informazioni necessari alle autorità competenti per garantire il seguito da dare alle raccomandazioni a norma dell'articolo 35, paragrafo 1, lettera d) rivolte ai fornitori terzi critici di servizi TIC". Si v. anche gli artt. 48 e 49 in relazione, rispettivamente, alla cooperazione tra l'autorità di sorveglianza capofila e le Autorità Europee di Vigilanza con le competenti autorità amministrative indipendenti nazionali.

65 Regolamento UE 2554/2022, art. 34. Cfr. anche art. 35, par. II e IV in relazione al coordinamento dell'autorità di sorveglianza capofila con la rete di sorveglianza comune.

66 Le AEV raccolgono i dati sui contratti conclusi dagli operatori finanziari con fornitori terzi di servizi ICT, potendo anche accedere al registro informazioni completo (art. 28, par. III), li trasmettono al forum di sorveglianza (art. 31, par. X). Schneider 2023: 1014 e s., in cui si prospetta un coordinamento dell'attività di vigilanza anche con IA. In questo contesto sono di interesse (quale anticipazione dei criteri che potranno essere integrati dalla Commissione UE) gli indicatori quantitativi e qualitativi proposti dalle AEV riferiti ad undici criteri di criticità suggeriti ed ai rispettivi livelli di rilevanza. Cfr. il rapporto tra l'art. 33, par. IV e l'art. 34.

La necessità di garantire l'efficacia dell'attività di sorveglianza anche dei fornitori terzi critici con sede in un paese terzo[67] e la possibile assenza di rapporti di cooperazione con le autorità di vigilanza finanziaria nei paesi terzi comporta (per il fornitore terzo) l'obbligo di assicurare una presenza commerciale nell'UE mediante l'istituzione di un'impresa figlia entro 12 mesi dalla sua designazione come "critico"[68].

Tali attività di sorveglianza includono un potere sanzionatorio[69] nei confronti dei fornitori di servizi ICT che si aggiunge alle sanzioni di natura contrattuale previste dalla disciplina europea[70] e che incide sulla gestione del rapporto con gli operatori finanziari.

Nel rapporto tra Autorità di vigilanza e fornitori terzi di servizi ICT si definisce una relazione volta a completare i vincoli contrattuali (previsti direttamente dall'ordinamento giuridico europeo) al fine di vincolare maggiormente i fornitori terzi di servizi ICT. In tale rapporto risulta peculiare come il ruolo della sorveglianza sia chiamato ad intervenire in relazione a rischi esterni all'attività finanziaria, comportando anche la necessità di dotarsi di una specifica conoscenza.

4. Il ruolo della vigilanza nella cybersecurity per il settore bancario e finanziario

La disciplina dei rapporti tra settore finanziario e ICT, inserendosi in un quadro giuridico più ampio, costituisce una presa di coscienza degli interessi coinvolti dal rapporto di dipendenza dal settore ICT e come risultino necessarie specifiche misure volte a rispondere alle specificità del settore finanziario per gestire efficacemente fenomeni a carattere sovranazionale.

67 Rendendo ad es. difficili le attività ispettive e l'irrogazione di eventuali sanzioni (es. in materia di trasparenza e accesso). Si v. il combinato tra Regolamento UE 2554/2022, art. 35, par. I e VI.

68 Regolamento UE 2554/2022, art. 31, par. XII e XIII. Tale misura tuttavia può non essere sufficiente per garantire gli obiettivi dell'attività di sorveglianza richiedendo la conclusione (da parte delle AEV) di appositi accordi di cooperazione con le autorità dei paesi terzi al fine di rendere possibile l'acquisizione di informazioni e l'esercizio delle funzioni ispettive. Sul punto si v. Regolamento UE 2554/2022, art. 36, ove sono altresì disciplinati i limiti dei poteri delle AEV e il contenuto minimo degli accordi di cooperazione amministrativa. Per assolvere alle funzioni previste dal regolamento DORA, le autorità di vigilanza capofila sono dotate di poteri di indagine, ispettivi e di raccomandazione il cui inadempimento può comportare l'adozione di sanzioni amministrative (penalità di mora quantificate su base giornaliera e parametrata al fatturato medio quotidiano realizzato a livello mondiale dal fornitore terzo), anche a seguito di un contradditorio con i rappresentanti del fornitore terzo critico.

69 Regolamento UE 2554/2022, artt. 50-51. Si v. anche art. 52, in relazione alla possibile rilevanza penale nell'ordinamento giuridico nazionale.

70 Regolamento UE 2554/2022, art. 28, par. VII e VIII. Si v. anche l'art. 42, par. VI e 50, secondo cui alle autorità amministrative indipendenti nazionali è riconosciuto il potere di imporre di richiedere ad un operatore finanziario di sospendere temporaneamente o la risoluzione del contratto con un fornitore terzo critico ICT fino a quando non si sia posto rimedio ai rischi individuati nelle raccomandazioni rese ad un fornitore terzo critico.

L'attività di sorveglianza e la cooperazione tra le autorità di vigilanza risulta strumento essenziale ma non necessariamente sufficiente per prevenire e ridurre eventuali distorsioni in tale settore (che trovano tuttavia origine al di fuori di esso) capaci di incidere negativamente sul rapporto di fiducia con gli investitori.

L'attività di vigilanza è chiamata ad assumere un ruolo centrale a garanzia del corretto funzionamento del settore.

Se, a livello nazionale, la direttiva UE NIS2 prevede un articolato sistema di vigilanza che pone in rapporto l'Agenzia per la cybersicurezza nazionale (individuata quale autorità competente e punto unico di contatto nell'ambito dei rapporti sovranazionali)[71] con il Ministero dell'economia e delle finanze (individuata quale Autorità di settore NIS per i settori bancario e delle infrastrutture finanziarie, "sentite le autorità di vigilanza di settore, Banca d'Italia e Consob")[72], il regolamento UE DORA pone in rapporto diretto i fornitori terzi critici con l'AEV individuata quale autorità capofila[73] (quest'ultima coadiuvata, per quanto concerne i rischi informatici, dal forum di sorveglianza[74] e, in generale, dalle Autorità nazionali competenti[75]).

Si definisce in questo modo un complesso sistema di vigilanza che contempla l'interazione tra soggetti giuridici nazionali ed europei in cui opera un "gruppo di cooperazione" (previsto dalla direttiva UE NIS2[76]) che consente un collegamento con le Autorità competenti ai sensi del regolamento UE DORA[77], rendendo possibile sia uno scambio di informazioni, sia forme di consulenza e assistenza tecnica.

L'utilizzo di poteri impliciti da parte delle autorità di settore (ovvero l'esercizio di competenze che non risultano espressamente da norme giuridiche, ma che si ricavano in via interpretativa per deduzione e che consentono alle autorità di vigilanza il corretto perseguimento dei propri fini istituzionali[78]), oltre ad ampliare il

71 d.lgs. 4 settembre 2024, n. 138, art. 10.

72 d.lgs. 4 settembre 2024, n. 138, art. 11, c. II, lett. b).

73 Regolamento UE, 2554/2022, art 31, par. I, lett. b), individuata tra le AEV sulla base di quella responsabile, "a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, delle entità finanziarie che possiedono complessivamente la quota maggiore delle attività totali rispetto al valore delle attività totali di tutte le entità finanziarie che utilizzano i servizi del pertinente fornitore terzo critico di servizi TIC, secondo quanto risulta dalla somma dei singoli bilanci di quelle entità finanziarie".

74 Regolamento UE, 2554/2022, art. 32, par. I.

75 Regolamento UE, 2554/2022, art. 40.

76 Direttiva UE, 2555/2022, art. 14.

77 Regolamento UE, 2554/2022, art. 47.

78 Cons. St., VI, 14 dicembre 2020, n. 7972, ove, nell'ambito del contenzioso relativo al caso Telecom S.p.A. e Vivendi S.A., sono ricondotti all'Autorità di settore (Consob) poteri impliciti per garantire il "funzionamento del mercato finanziario e l'interesse generale degli investitori e dei risparmiatori": cfr.: Cons. St., VI, 17 ottobre 2005, n. 5827; Cons. St., VI, 24 maggio 2016, n. 2182, che pur annulla il provvedimento impugnato per non aver perseguito le finalità attribuite all'ARERA. Così anche Cons. St., VI, 1 ottobre 2014, n. 4874 che, pur indicano nei presupposti dell'applicazione del principio di legalità "per obbiettivi" anche l'individuazione di limiti entro cui può esercitarsi l'attività amministrativa, finisce per identificare questi limiti negli stessi obiettivi individuati dalla legge; Cons. St., VI, 20 marzo 2015, n. 1532; VI, 2 maggio 2012, n. 2521; Cons. St., VI, 15 luglio 2019, n. 4993, in cui il Giudice, dopo aver fatto una applicazione ampia della teoria

dibattito sulla compatibilità di tali poteri con il principio di legalità, pone ulteriore indeterminatezza nel corretto adempimento dei vincoli gestionali da parte degli operatori finanziari.

Queste criticità possono risultare tali da non consentire la rapida individuazione di un rischio o incidere sulle tempistiche per la sua efficiente gestione.

Ulteriori elementi previsti dalla direttiva UE NIS2 e dal regolamento UE DORA possono rendere il contesto maggiormente complesso.

Se, nell'ambito del regolamento UE DORA, la definizione di un adeguato livello di sicurezza e la mancanza di alternative reali, costituiscono criteri per la qualificazione di fornitore "critico"[79], un errore di valutazione dell'operatore finanziario sulla criticità di un fornitore può ridurre la sorveglianza delle AEV. Tale circostanza potrebbe risultare anche conseguenza di un tentativo di nascondere alcune criticità per evitare effetti sul mercato finanziario (o ritorsioni commerciali dal settore ICT).

La complessità che consegue a possibili catene di subappalto (che contraddistinguono la fornitura di alcuni servizi ICT)[80] pur comportando la previa valutazione dell'operatore finanziario, rende difficilmente monitorabili i rapporti giuridici tra i subappaltatori (ad es. in relazione a controlli volti ad evitare possibili conflitti di interesse tra i terzi fornitori), contribuendo ad incidere sull'equilibrio contrattuale, sul possibile utilizzo distorto di dati e informazioni e sui rapporti di dipendenza. L'attività di vigilanza è resa ulteriormente complessa dalla collaborazione diretta richiesta al fornitore terzo che, nell'ambito dei propri doveri di buona fede e cooperazione, è tenuto a comunicare determinati eventi all'Autorità di sorveglianza capofila[81] (è questo il caso dei contratti di subappalto, in cui l'Autorità di sorveglianza può raccomandare la rinuncia a stipulare il subcontratto[82]).

Tale rapporto diretto può creare distorsioni anche nei confronti dell'operatore finanziario che, da un lato, ha la "responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria"[83] (dovendosi quindi dotare di specifiche com-

dei poteri impliciti con struttura finalistica, individua un limite all'applicazione di questa soluzione ermeneutica nella previsione di sanzioni amministrative e non nell'adozione di misure amministrative inibitorie. In dottrina, *ex multis*: Marra 2023, 697 e s.; Morbidelli 2007, 703 e s.; Bassi 2001, il quale ritiene che "la funzione predeterminata dalla norma quale scopo da perseguire da parte dell'autorità, cioè, funge qui da semplice criterio di esercizio del potere (attraverso la sanzione del c.d. sviamento), ma non da elemento di attribuzione del potere".

79 Regolamento UE, 2554/2022, art 31, par. 2, lett. c) e d).

80 Rese possibili dalla circostanza che 9000 subappaltatori supportano fornitori terzi critici. Cfr. European Supervisory Authorities, *ESAs Report on the landscape of ICT third-party providers in the EU*, cit., p. to 13.

81 Regolamento UE 2554/2022, art. 35, par. I e V.

82 Regolamento UE 2554/2022, art. 30.

83 Circa la responsabilità dell'organo di gestione dell'operatore finanziario si v.: Regolamento UE, 2554/2022, considerando n. 45 e art. 5, par. II. A questo si aggiungono anche le responsabilità dei collaboratori dell'organo di gestione ed a cui quest'ultimo ha conferito un ruolo nell'ambito della governance di resilienza digitale oltre che le responsabilità di natura contrattuale del soggetto terzo fornitore di servizi ICT.

petenze anche all'interno degli organi di gestione) e, dall'altro, non è parte del dialogo con l'Autorità di vigilanza.

Gli stessi meccanismi di funzionamento dell'attività di sorveglianza e i tempi richiesti per gestire le comunicazioni tra le Autorità (europee e nazionali) coinvolte può non consentire una pronta risposta ad un evento che, attraverso gli strumenti tecnologici, genera effetti considerevoli in un limitato intervallo di tempo.

La possibile irrogazione di sanzioni quantificate sul fatturato globale e di natura reputazionale[84] può incidere negativamente sull'interesse degli operatori economici (per i prestatori internazionali di servizi ICT) di operare nel Mercato Interno e sottoporsi ai vincoli previsti dall'ordinamento giuridico europeo.

In tale contesto, una possibile riduzione di tale interesse può riflettersi sul novero di possibili fornitori di servizi ICT (aumentando i rischi di concentrazione) e, nei settori rilevanti in cui opera un numero ristretto di imprese, può generare posizioni 'dominanti' nei singoli mercati di riferimento (riducendo ulteriormente la capacità degli operatori finanziari a inserire vincoli aggiuntivi nei contratti con i fornitori terzi di servizi ICT).

L'ulteriore considerazione per cui, in relazione ai fornitori stabiliti al di fuori dell'UE, sia previsto l'obbligo di costituire un'impresa stabilita nell'UE, è un elemento che non necessariamente pare sufficiente a tutelare gli operatori finanziari o gli investitori, potendo risultare maggiormente opportuna la realizzazione di infrastrutture native nell'Unione Europea.

In questo contesto, permangono tuttavia perplessità sulla efficacia delle misure europee sul settore finanziario, su cui influisce in vario modo il rapporto di dipendenza rispetto al settore ICT.

Bibliografia

Alpa G. 2019, "Fintech: un laboratorio per i giuristi", in *Contratto e Impresa*, 377 e s.

Annunziata F. 2020, "Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE", in *Riv. Dir. Bancario*, 1-15.

Annunziata F. – Minto A. 2022, "Il nuovo Regolamento UE in materia di Distributed Ledger Technology", in *Riv. Dir. Bancario*, 1-8.

Arner-Buckley-Zetsche 2022, "Open Banking, Open Data e Open Finance: Lessons from the European Union", in Jeng (a cura di), *Open Banking*, Oxford: Oxford University Press, 147 e s.

84 Sul regolamento UE DORA, si v. la comunicazione al pubblico delle penalità inflitte (Regolamento UE 2554/2022, art. 35, par. X) o nel caso di mancata risposta alle raccomandazioni formulate (Regolamento UE 2554/2022, art. 42, par. II). Sulla direttiva UE NIS2, si v. il regime sanzionatorio che ricade in capo al soggetto essenziale o al soggetto importante in caso di non conformità rispetto agli obblighi previsti (che può arrivare, per i soggetti essenziali, a €10.000.000 o almeno il 2% del fatturato mondiale totale annuo nell'anno fiscale precedente – su cui direttiva UE, 2555/2022, art. 34, par. IV – e, per i soggetti importanti, fino a €7.000.000 o almeno l'1,4% del fatturato mondiale totale annuo nell'anno fiscale precedente della società a cui appartiene l'entità importante per i soggetti importanti – su cui direttiva UE, 2555/2022, art. 34, par. V –).

Baskerville R. – Capriglione F. – Casalino N. 2020, "Impacts, Challenges and trends of Digital Transformation in the Banking Sector", in *Law and Economics Yearly Review*, 341 e s.
Bassi N., "Principio di legalità e poteri amministrativi impliciti", Giuffrè, Milano, 2001.
Bronzetti A. 2023, "Il diritto europeo della banca e della finanza tra passato e futuribile", in *Riv. trim. dir. dell'economia*, 1: 6-60.
Campa J. M. 10 ottobre 2023, "Operational resilience in EU financial services", keynote speech at the *14th Financial meeting* organised by Expansion, accessibile in https://www.eba.europa.eu/sites/default/documents/files/document_library/Calendar/EBA%20Official%20Meetings/2023/Jos%C3%A9%20Manuel%20Campa%20keynote%20speech%20at%20the%2014th%20Financial%20meeting%20organised%20by%20Expansion/1063659/JM%20Campa%20speech%20on%20digitalisation%20and%20DORA%20at%2010-10-2023.pdf.
Canepa A. 2021, "*Big tech* e mercati finanziari: «sbarco pacifico» o «invasione»? Analisi di un «approdo» con offerta «à la carte»", in *Riv. trim. dir. dell'economia*, 465 e s.
Capriglione F. 2019, "Industria finanziaria, innovazione tecnologica, mercato", in *Riv. trim. dir. dell'economia*, 374 e s.
Capriglione F. 2021, "Diritto ed economia. La sfida dell'intelligenza artificiale", in *Riv. trim. dir. eco*., (3) 4 e s.
Capriglione F. 2022, "Le cripto attività tra innovazione tecnologica ed esigenze regolamentari", in *Riv. trim. dir. eco*., 254.
Casalino N. 2023, "La digitalizzazione del settore finanziario", in M. Pellegrini (a cura di), *Diritto pubblico dell'economia*, Vicenza: CEDAM, 337 e s.
Celati B., "La sostenibilità della trasformazione digitale: tra tutela della concorrenza e «sovranità tecnologica europea»", in *Riv. trim. dir. eco*., 2021, 3, 252 e s.;
Davola A. 2017, "*Bias* cognitivi e contrattazione standardizzata: quali tutele per i consumatori?", in *Contratto e impresa*, 637 e s.
Finocchiaro G., "La sovranità digitale", in *Dir. pub.*, 2022, 809 e s.
Lemma V. 2020, "FinTech Regulation: Exploring New Challenges of the Capital Markets Union", Cham: Springer International Publishing.
Lemma V. 2023, "Solidarietà e regolazione dell'innovazione finanziaria", in *Riv. trim. dir. dell'economia*,, 83-100;
Marra A., "I poteri impliciti", in *Dir. amm*., 2023, 697 e s.
Masera R. 2022, "L'Europa, l'unione europea e l'eurozona: crisi e proposte di soluzione", in *Riv. trim. dir. dell'economia*, 151-184.
Mazzarisi p. – Ravagnani A. – Deriu p. – Lillo F. – Medda F. – Russo A. 2022, "Metodi sperimentali di machine learning per supportare le decisioni nella *detection* degli abusi di mercato", in *Quaderni FinTech – Consob*, (11) 1-49.
Miglionico A. 2019, "Innovazione tecnologica e digitalizzazione dei rapporti finanziari", in *Contratto e Impresa*, 1376 e s.
Morbidelli G., "Il principio di legalità e i c.d. poteri impliciti", in *Dir. amm*., 2007, 703 e s.
Palmerini E. – Aiello G. – Cappelli V. – Morgante G. – Amore N. – Di Vetta G. – Fiorinelli G. – Galli M. 2018, "Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilistici e penalistici. Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori", in *Quaderni FinTech – Consob*, 1-97.
Rabitti M. 2023(a), *Le regole di supervisione nel mercato digitale: considerazioni intorno alla comunicazione Banca d'Itlia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, in D. Rossano (a cura di) *La supervisione finanziaria dopo due crisi. Quali prospettive*, Padova: CEDAM, 345-355.

Rabitti M. 2023(b), "Due diligence sulla sostenibilità e digitalizzazione della catena del valore: l'apporto di blockchain e smart contracts", in *Riv. trim. dir. dell'economia*, 166-185.
Ruocco C. 2023, *"Finanza digitale: opportunità, profili di attenzione e ruolo della supervisione finanziaria"*, in D. Rossano (a cura di) *La supervisione finanziaria dopo due crisi. Quali prospettive*, Padova: CEDAM, 181-187.
Schneider G. 2023, "La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)", in *Resp. civ. e prev*., 1014 e s.
Sciarrone Alibrandi A. – Borello G. – Ferretti R. – Lenoci F. – Macchiavello E. – Mattassoglio F. – Panisi F. 2019, "Marketplace lending Verso nuove forme di intermediazione finanziaria?", in *Quaderni FinTech – Consob*, (5) 1-285.
Schneider G. 2023, "La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)", in *Resp. civ. e prev*., 1014 e s.
Sepe M. 2021, "Innovazione tecnologica, algoritmi e Intelligenza Artificiale nella prestazione dei servizi finanziari", in *Riv. trim. dir. dell'economia*, 186 e s.
Trautmann K. 2022, "EU-DORA regulation as a result of cloud computing adoption by the financial services industry", in *Journal of International Banking Law and Regulation*, 38(5), 155-161.
Urbani F. 2022, "Rassegna dei principali interventi legislativi, istituzionali e di policy a livello europeo in ambito societario, bancario e dei mercati finanziari", in *Riv. delle società*, 985 e s.

Francesca Castaldo and Federico Serini

Public-private collaboration in European cybersecurity. Between organizational and regulatory plans[*]

Abstract: Bringing together considerations straddling organizational business science and public law, the paper aims to provide a multidisciplinary overview of public-private collaboration in the context of cybersecurity. Two profiles are analysed: the public-private partnership, an organizational and legal perspective, and the phenomenon of co-regulation in cyber security technical standardization and certification. The study of the two profiles just mentioned will allow us to analyse the role of private parties, in one case as recipients of the cybersecurity obligations of secondary legislation then translated at the national level, and on the other as actors who promote and participate in the elaboration of technical cyber security standards. The opportunity is to contextualize said phenomenon, as well as to grasp its ongoing evolutionary profiles and criticalities.

Keywords: Cybersecurity; Public and private power; Technical regulation; Public-private partnership; Strategic alliances.

1. Introduction

The legal debate on the governance of cyberspace[1], the well-known interest of States in regulating and controlling this new and unprecedented space that has the characteristic of being a "non-territory", can be generally interpreted as a test of State sovereignty in the globalization time. Indeed, cyberspace represents

* This paper results from a joint reflection by the Authors. However, §§ 2 and 3 are attributable to Francesca Castaldo, while §§ 4 and 5 are attributable to Federico Serini. The introduction in § 1 and the conclusions in § 6 are the product of considerations by both Authors.

1 By cyberspace we mean an agglomeration of products, processes, and services pertaining to information and communication technologies (henceforth "ICT goods") circulating in the global marketplace, which, at the level of services, includes the Internet. On this point may it be granted to refer to Serini 2023a.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760154

a challenge for the public powers that have always been tied to the material element of territoriality[2].

Curious, however, is the genesis of this dimension. Cyberspace was originally a public phenomenon, born with Arpanet project (the prototype of today's network of networks, i.e., the Internet), but later developed and spread through private individuals and outside the States' control[3].

The entry of information technology into the market and society[4] has been an event of little interest to public power[5], which has limited itself to intervening with regulations aimed rather at favouring the economy and investment in this sector, as well as the regulation of the mechanisms of technical operation of the network[6], without ever being interested in intervening in the "political" side of cyberspace[7].

After this initial period of indifference, the increasing social and economic relevance of this environment, caused by the negative consequences arising from cyber-attacks and information technology malfunctions, have led public authorities to turn their attention to this space, demonstrating "not only that they [can] regulate it but also that they 'hyper-regulate'"[8].

The question before us today is how government intervention – successive in time – intends to regulate cyberspace, now understood as a space regulated primarily by forms of self-regulation, first by users themselves, then by large private groups.

In addition to the creation, over time, of an *ad hoc* administrative organization[9], empirical evidence shows that in this dimension it is usual to witness forms of so-called multistakeholder governance, where States are placed on the same level as other actors, often private (i.e. see the Internet regulation)[10].

The framework of security policies, as a typical expression of public sovereignty, in cyberspace, seemed to be a privileged vantage point for analysing the relationship between powers in the digital and reflecting on the peculiar traits of that cooperation between public and private power, which is its essence in this area.

2 Irti, 2006: 4.

3 Bombelli 2017: 26.

4 Heritier 2003.

5 Della Morte 2018: 27.

6 The reference is first of all to the codes, programs and protocols that underlie the functioning of communication in cyberspace, on which point see L. Lessig 1999, where the A. writes «[l]ife in cyberspace is regulated primarily through the code of cyberspace» (p. 83), but also to the centralized management of interconnection standards and the DNS system of domain names, which is delegated to the U.S.-based Internet Corporation for Assigned Names and Numbers-ICANN, governed by a structure in which government representatives, technical organizations, and private companies sit.

7 One is reminded of the rich debate in the early 1990s of the last centuries, animated by criticisms concerning not only the profiles of feasibility, but also the appropriateness and legitimacy of a legal regulation of this "new space". On the point s. Pollicino, Bassini, De Gregorio 2022: 4 ss.

8 Pollicino 2023: 415.

9 On this point, about the Italian and European legal systems, we refer to the work of Rossa 2023.

10 Cerf 2022: 7 ss.

Starting from these brief premises, this paper intends to investigate such collaboration from a multidisciplinary perspective between legal and corporate organizational sciences, according to the academic interests of the authors.

After an initial reflection on the role of private individuals in (cyber)security (§2), the reflection continues by focusing on the transversality of the forms of collaboration, or alliances, public-private for countering cyber threats (§3) arguing on the peculiar and fundamental role assumed by public-private partnerships (PPPs) in cybersecurity from an organizational perspective (§4). as well as subsequently, from the Public Law point of view, on the relevance of standard-setting bodies and technical standardization in this area, as instruments of private origin lent for the regulation of public interests such as security (§ 5). The discussion of these topics will finally allow us to draw some final considerations that refer to the broader question of the relationship between public and private power (§ 6).

2. Private participation in cybersecurity

According to sociological sciences, the globalization process has led to a rearticulation of the State that has effectively transferred some of its functions to private actors[11], including, over time, security[12].

From the legal perspective, this has resulted in a progressive distinction between roles and functions belonging to public (or primary) security, which is made explicit in the exercise of authoritative and repressive powers, and forms of secondary or subsidiary security (itself distinguished into "complementary" and "community" security) where private entities also participate to complement, aid or supplement the police function[13].

In the Italian legal system, the latter securitarian meaning has been made possible by the principle of subsidiarity in Article 118(4) of the Constitution, which opens citizens as well as economic activities to the performance of activities in the general interest, which includes security[14].

At the European level, this openness has been possible on the back of a series of pronouncements since the 1970s by the Court of Justice on the relationship between the activities of public authorities and the framework of European economic freedoms.

The Court has been called upon to resolve questions arising from the conflict between the conditions to which States subject the exercise of private security functions such as citizenship, possession of a license, taking an oath, administrative setting of fees as forms of control and surveillance to which such activities are subjected by the public power of States, with the right of establishment of workers in the European space.

11 Sassen 2008.
12 Abrahamsen 2016.
13 Mosca 2012: 26; Aliquò 2023.
14 Ursi 2022: 204 ss.

With these decisions, the European Court has interpretatively extended European integration in this area, denying that the intervention of private parties in functions of traditional State prerogative should automatically qualify as the exercise of a public power over which market freedoms cannot take effect since the issue must be assessed on a case-by-case basis[15].

In cybersecurity, however, we see a further phenomenon than the one just mentioned of "privatization of security", that is, relating to the involvement of entities that carry out private security activities. Indeed, in this sector, we find the involvement of private organizations that have nothing to do with security in the traditional sense although they are now largely involved in it[16].

One thinks of the various critical infrastructures operating in the sectors of relevance to the society and economy of the states subject to the European NIS framework and, as far as Italy is concerned, falling within the *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC), which are called upon to have to actively participate in the national cybersecurity process as well as the European one.

In other cases, this involvement finds expression in forms of collaboration embodied in public-private partnerships (see §4) that are useful both for countering cybercrime (this is the case with the various information-sharing ecosystems between public authorities and critical)[17], both for technology transfer between universities and industry[18].

3. Facing the cyber threat: the need for alliances

It is widely acknowledged that the cyber threat is multifaceted and diverse. Despite the common perception of cyber-attacks as originating from an invisible enemy, they can be categorized into various types, including malware (viruses, worms, Trojans), phishing, DDoS (Distributed Denial of Service) attacks, ransomware, and social engineering attacks, among others.

The motives behind such attacks are also very diverse, ranging from simple espionage, aimed at gathering sensitive information from governments, companies or individuals, to hacktivism motivated by political or social ideologies; from cybercrime motivated by financial gain, as in the case of ransomware or the theft of banking information, to all-out cyber warfare, with state-sponsored attacks aimed at gathering strategic information or sabotaging critical infrastructure[19].

15 Buzzacchi 2015: 114 ss.

16 Farrand, Carrapico 2018: 197-217.

17 Let it be permissible to refer to F. Serini 2023b, 2024.

18 Reference is made to the European Digital Innovation Hubs (EDIHs), whose aim is to ensure the digital transition of industry, particularly small and medium-sized enterprises (SMEs), and the public administration through the adoption of advanced digital technologies such as artificial intelligence, high-performance computing, and cybersecurity.

19 Castaldo 2019; Eckert 2005.

Cyber-attacks can also hit different targets: critical infrastructure such as power grids, communication systems and other vital infrastructure, a bank, a hospital or a local authority, to name but a few.

The use of botnets and automated scripts to launch large-scale attacks, combined with the ubiquity of Internet connectivity, allows the threat to spread rapidly across global networks.

Furthermore, the use of evasion techniques by hackers, such as encryption or code obfuscation, to mask their activities and evade detection, and the use of anonymity tools and proxies to conceal the origin of attacks, demonstrates why the problem of attribution is so relevant in the cyber sphere.

The cyber threat is, therefore, not only asymmetrical in military terms but also has the potential to cause significant economic damage (loss of data, service interruptions, recovery and compensation costs), operational disruption (interruption of business operations, loss of productivity) and reputational harm (damage to the reputation of affected companies or entities)[20].

The impact of cyber threats extends beyond mere productivity losses. Reputational damage, national security concerns, and the necessity to adapt to the continuous evolution of technology and develop new defence strategies are also significant considerations[21].

In light of the aforementioned considerations, addressing this pernicious threat is a formidable challenge for all stakeholders, public and private, who are unable to ignore it in their operations[22].

The characteristics mentioned collectively constitute a complex and evolving challenge to the cyber threat, necessitating a state of constant vigilance and the implementation of advanced and adaptable defence strategies.

Although the most sophisticated computer systems are now 'resilient by design'[23], i.e. to be able to guarantee their operability in the event of an attack, i.e. to ensure *business continuity* and *disaster recovery*, we must not forget that the main vulnerability in the cyber universe remains the human one, i.e. linked to the intrinsic weakness of the so-called 'human factor'[24].

Considering the current technological landscape, which presents an ever-increasing number of potential attack vectors, no entity, whether private or public, is currently capable of defending itself effectively and remaining resilient against cyber-attacks.

Consequently, there is a pressing need for collaboration between the public and private sectors, as well as the opportunity to form alliances against the common, invisible adversary[25].

20 Castaldo 2018b.
21 Castaldo 2019; Castaldo and Serini 2024.
22 Castaldo 2018b.
23 Castaldo 2021.
24 *Ibidem*.
25 Castaldo 2018a.

In the contemporary globalized, uncertain and interconnected environment, collaboration has become a necessity to address challenges and seize opportunities[26]. This is particularly pertinent in VUCA (Volatile, Uncertain, Complex, Ambiguous) scenarios, which are often employed to describe the highly complex nature of our world[27].

4. A peculiar form of alliance to counter the cyber threat: public-private partnerships

Cooperation can take the form of a public-private partnership, a type of alliance that is not only tactical, arising in response to a contingent risk, but strategic, i.e. long-term, and therefore perfectly suited to dealing with the cyber threat, given its time horizon.

Public-private partnership is a concept based on the idea of combining the resources, skills and perspectives of the public and private sectors to address common challenges and pursue development opportunities[28].

Public-private partnerships (PPPs) have a long history, dating back several decades. However, in recent years they have become more relevant and widespread globally.

These types of partnerships have emerged primarily as a response to the growing complexity of social and economic challenges and the need to develop innovative models for financing and managing infrastructure and public services[29].

Public-private partnerships are in fact cooperation agreements between a public organization and one or more private companies. The objective of a PPP is to design, finance, build, operate and/or maintain infrastructure or provide public services[30].

This model is widely used in sectors such as transport, energy, health, education and water. In essence, PPPs are organizations in which public bodies and private companies work together to achieve common goals. This form of collaboration leverages the strengths of both the public and private sectors, fostering an environment conducive to innovation, efficiency, and sustainability[31].

Public-private partnerships (PPPs) are rooted in theoretical frameworks from various disciplines, including economics, organizational theory, public finance, and public policy theory.

In economics, PPPs are linked to public goods theory and the concept of public sector inefficiency. It is widely believed that private sector involvement can im-

26 Volpe and Castaldo, 2022; 2024.
27 Castaldo 2023; Zanda and Castaldo, 2023.
28 Broadbent and Laughlin 2005; Hemming 2006.
29 George *et al.*, 2024.
30 Broadbent and Laughlin 2005; Hodge *et al.* 2017.
31 George *et al.*, 2024.

prove efficiency in the delivery of public services, especially in areas where the government faces challenges[32].

Organizational theory emphasizes the potential of the private sector to provide specialized management resources and skills to improve the management and efficiency of public operations[33].

Public policy theory focuses on the responsibility and role of government in addressing social issues and providing public services. From this perspective, PPPs can be analyzed as a form of innovation in public governance that involves private actors in the realization of public objectives[34].

These theories, despite their inherent peculiarities, provide the intellectual basis for understanding the underlying motivations behind the emergence of public-private partnerships.

A substantial body of literature exists in the economic, organizational and financial fields which describes the advantages of these alliances. These advantages typically include access to the partner's complementary resources and skills[35].

One of the main issues addressed in the literature when identifying the benefits of PPPs is that of economic efficiency: some scholars argue that these alliances can lead to greater efficiency in the delivery of public services due to the participation of the private sector[36].

One of the main disadvantages of public-private partnerships is the unequal distribution of risk between the public and private sectors, with the state – according to some theorists – bearing a disproportionate share of the burden[37].

Another much-discussed issue is the complexity of managing the relationship between the public and private sectors, two different worlds with different cultures and therefore a potential source of conflict[38].

Another critical factor is the potential for the short-term financial interests of the private sector to conflict with the long-term goals of the public sector in terms of social welfare and environmental sustainability. This is compounded by the risk of overcharging for privately managed services and infrastructure, which can result from inefficiencies in decision-making or a lack of transparency in private partner selection procedures and/or concession contracts[39].

There is a growing interest in assessing the long-term financial sustainability of public-private partnerships, particularly in light of financial risks and their impact on public finances[40]. It is therefore important to address the challenges that these partnerships present through proper design, monitoring, and evaluation, ensur-

32 Grimsey and Lewis 2007; Hemming 2006, Hodge et al. 2017.
33 Hemming 2006.
34 Osborne and Brown 2005.
35 Castaldo 2018a.
36 Broadbent and Laughlin 2005; Grimsey and Lewis 2007; Hodge *et al.* 2017.
37 Rybnicek, Plakolm and Baumgartner, 2020.
38 Castaldo 2018a.
39 Vining and Boardman 2008.
40 Grimsey and Lewis 2007.

ing a balance between public and private interests and maximizing the benefits to society as a whole[41].

Indeed, there is considerable debate surrounding the efficacy of public-private partnerships in ensuring accountability, oversight, and transparency, particularly in light of the involvement of private actors in the provision of essential public services such as health and education[42].

Given the inherent complexity and coordination required for this form of alliance, it is of the utmost importance that public-private partnerships are designed and managed in a transparent, fair and accountable manner if they are to function effectively.

This necessitates the establishment of a robust legal framework, monitoring and evaluation mechanisms, and apparatus to ensure the protection of public interests and the equitable distribution of benefits and risks among all stakeholders. Consequently, it is of paramount importance to conduct a comprehensive assessment of the potential effects of a public-private partnership on the partners and all stakeholders, as well as the allocation of benefits and risks to each party, prior to the establishment of the partnership[43].

While in other sectors, public-private partnerships are the result of a cost-benefit analysis, in the cyber universe the reality is quite different[44]. Here, the challenge is to combat an imperceptible enemy that lurks menacingly in the so-called 'fifth domain'[45], the 'borderless' space.

As previously stated, the cyber threat is not only multifaceted and unpredictable but also continuously changing in technological terms[46].

In such a volatile, uncertain, complex and ambiguous (VUCA) scenario, no player, public or private, can move cautiously and profitably in the face of the threat of cyber-attacks.

Consequently, there is a need to form alliances to fight an asymmetrical battle against a common, invisible, unscrupulous and powerful enemy[47].

In other words, while in other areas public-private partnerships are the result of a well-considered and mutually beneficial decision, in a typical win-win strategic mode, in the cyber sector we are faced with a necessity, a categorical imperative[48].

It is clear that cyber security concerns affect both the public and private sectors. Therefore, public-private partnerships are the most suitable forum for collaboration between the two sectors to develop collective methods to counter

41 Broadbent and Laughlin 2005; Grimsey and Lewis 2007.
42 Dunn-Cavelty and Suter 2009; George *et al.*, 2024.
43 Broadbent and Laughlin 2005; Hodge *et al.* 2017.
44 Thomas 2013.
45 Per 'quinto dominio' si intende il dominio bellico più recente, che si aggiunge ai quattro noti: terra, acqua, aria e spazio.
46 Castaldo 2019; 2021.
47 Castaldo 2021.
48 Castaldo and Serini, 2024.

cyber threats. Attacks on critical national infrastructures have the potential to cause significant damage to citizens' lives, services, operations and continuity. It is therefore essential that the public and private sectors are protected against cybercriminals with effective and adaptable policies, regulations and strategy implementations.

In this context, public-private partnerships represent an organizational effort to protect the common interests of prevention, security and the creation of secure environments.

The issue of cyber security threats is a global problem, which was recognized by the EU and its individual institutions relatively early on. It was agreed that this problem can only be addressed through equally 'global' responses, requiring international communication, harmonized legislation and efforts from both the public and private sectors.

However, cybersecurity issues are complex in nature, which sometimes makes a unified approach difficult to achieve[49].

In order to address this difficulty, the European Commission published a communication in 2001 entitled "Europe's Transition to the Information Society". This communication proposed several actions to protect information and communication infrastructures. It called for the implementation of a comprehensive policy initiative, the establishment of a unified definition of cybercrime, enhanced communication with stakeholders, and increased funding for research and development to address these threats. Since that time, now more than two decades ago, and more intensively in the last decade, there have been several successful PPP models, just as there has certainly been no shortage of failures. Nevertheless, these alliance attempts will continue to be implemented, following the rapidly developing developments in 'attacker' technology[50].

It is only by forming alliances and joining forces that public and private entities can collectively defend themselves against the risk of elimination, to build a better and more resilient world in line with the UN Agenda[51]. The 17th and final Sustainable Development Goal (SDG) for 2030 is 'Partnerships for the Goals'. This identifies partnerships as the optimal means of addressing the challenges facing humanity and the planet as a whole[52].

In conclusion, public-private partnerships represent a powerful tool for addressing the complex and interconnected challenges facing the world today[53]. By fostering a shared commitment and effective collaboration between the public and private sectors, we can achieve significant and lasting results for the common good of our society and our planet.

49 Castaldo 2018b.
50 Laughlin 2015.
51 Castaldo, Porretta and Zanda, 2024.
52 Eweje *et al.*, 2021.
53 Laughlin 2015.

5. The relevance of entities and technical standards in cyber resilience

The cases just mentioned refer to forms of cooperation and collaboration directed toward ensuring cybersecurity in the narrow sense, that is, responding to threats that may pose dangers and, thus certain damage.

Action other than cyber resilience, as a form of security that best fits the needs of the risk society, where harm is a future event, probable and not certain.

Resilience focuses on prevention from threats and minimisation of the effects resulting from the realization of the threat (damage) with an approach that starts from accepting the failure of security measures by providing for mitigation and damage mitigation measures so that the system continues to exist, and its collapse is averted[54].

This is where technical security standards for both products and processes come in since these tools make it possible to make risk calculable (in this case cyber[55]).

These are tools that do not have a legal nature since they are not the result of a legal-political process within Parliaments but are produced within alternative centres of interest aggregation – standard organizations (SO) – which see the participation of both States but also, and above all, of the various private stakeholders operating in the area of interest.

SOs are entities, often private, responsible for producing technical standards. They operate in the multilevel and, for essential historical reasons there are no more than three: one for the electronics sector, one for the telecommunications sector, and one for all other sectors[56].

At the international level, there are the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). At the European level, we find the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). In Italy, the recognized bodies are the Ente Nazionale Italiano di Unificazione (UNI) and the Comitato Elettrotecnico Italiano (CEI).

A relationship exists between technical regulations and the legal system[57], according to which the technical standard acquires relevance for the legal system whenever it is "assumed" within it, and this occurs through the institutes of incorporation and referral. There is incorporation when the content of the technical standard is transposed *sic et sempliciter* within a legal source (usually primary and/or secondary), while referral consists in the explicit reference to a technical standard punctually indicated (fixed or material referral), or in the use of general clauses within a legal provision, such as the reference "to the best available techniques", "to the state of the art", or rather to the "best standards. technical and

54 Bourdeau 2013; Dunn Cavelty, Eriksen and Scharte 2023.
55 Oddenino 2018.
56 Elias 1995: 32.
57 Bombelli 2023: 1-14.

safety standards", referring to compliance with technical regulations as a prerequisite of good practice (mobile or formal referral)[58].

In cybersecurity regulation, the link between technical and legal standards is a characteristic feature that we can already grasp from the definition provided by the European legislator with Regulation (EU) 2019/881 (Cybersecurity Act). Indeed, with this act, the Union introduced – for the first time within a legal norm – the notion of cybersecurity, defining it in Article 2(1) as "the set of activities necessary to protect the network and information systems, the users of those systems and other persons affected by cyber threats".

This formulation not only introduced into the (European) legal system a concept previously relegated to the exclusive domain of technicians but also gave it social and political value.

This can be grasped from the fact that in the first part, the reference to "protection of the network and information systems" can be interpreted as a form of (moving) reference to the confidentiality, integrity and availability (so-called RID) of information and the medium that contains it, as a fundamental feature of information and computer security, already originally defined in the first technical standards in the field between the '80s and '90s[59].

However, is in the second part that we find the innovative feature of this definition, namely the reference to the "security of the human" understood not only as the user, but also as any individual who can be negatively impacted by information technology, or threats conveyed through it.

We believe that with this formulation, the European Union has directed cybersecurity toward the public purpose of protecting individuals beyond the security of the single market and has done so by directing the purpose of industry technical standards, usually directed toward the exclusive protection of the individual organization so that its business is preserved[60].

We find confirmation of this in the document "An EU strategy on standardization Defining global standards in support of a resilient, green and digital EU single market" published by the European Commission in February 2022[61], where the Commission noted that "[o]rder than ever, standards cannot be limited to dealing only with technical components, but must also integrate fundamental democratic values and EU interests as well as ecological and social principles",

58 Greco 1999: 37 ss.

59 Russel, Gangemi 1991: 23. In particular, for the history of the technical standard ISO/IEC 27001, refer to Gallotti 2022: 247 ss.

60 In the ISO/IEC 27001:2013 standard for information security management systems, the definition of an "Information security incident" was "Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security". The recently updated version of the standard, revised considering legislative interventions in the areas of personal data protection and cybersecurity, now defines the concept as "one or multiple related and identified information security event that can harm an organization's assets or compromise its operations".

61 Communication, An EU strategy on standardization: Setting global standards in support of a resilient, green, and digital EU single market, COM (2022) 31 final, 2.2.2022.

and also specifically referred to the "strategic dimension" of technical standards on cybersecurity or critical infrastructure resilience, thus deeming it appropriate for the European standardization system-composed of the three private and independent bodies CEN, CENELEC and ETSI to respect and promote European values and interests[62].

The theme is thus relatable to the broader reflection on the relationship between public and private power at this juncture.

A gradual convergence of the technical standardization system towards compliance with principles with a Public Law vocation has been observed for some time, without going through the "juridicization" of the technical standard or the "publicization" of the bodies that produce said standards, which therefore remain private.

The standardization process at these bodies takes place by the principles dictated by the World Trade Organization (WTO) in 2000[63], namely: coherence (standards cover different technical disciplines, coherence and cohesion between them must be ensured), transparency and openness (all proposed standards and draft standards are made public for comments before the final version is published. Any objection must be discussed with the person who raised it), consensus (the content of standards is defined based on mutual agreement), voluntary application (standards are not mandatory), independence from special interests, and efficiency.

However, although these principles give hope that the process of forming these rules, which are non-legal and produced by entities of a private nature, will be guided by considerations and models of jurisprudential inspiration, the doctrine has had to point out some critical aspects, especially concerning the aspect of participation of social representations, as well as the different weight of certain subjects in voting, which would leave one leaning toward industrial representations[64].

It is worth pointing out, however, that as is evident from the analysis of European strategy documents, the Union's interest is placed on a particular type of technical standard, which is the harmonized standard.

According to Article 2(1)(c) of Regulation 1025/2012 on European standardization, a harmonized standard is "a European standard adopted based on a request from the Commission to apply Union legislation on harmonization", the formation procedure for which is detailed in Article 10 of the same Regulation.

Unlike other technical standards, harmonized standards are not created at the behest of different interest groups but are formulated by the European standards organizations (CEN, CENELEC and ETSI) at the request of the European Commission. The three European bodies can also refuse to comply with that request but, if they accept, they are obliged to respect the content and constraints con-

62 *Ivi*: 4.

63 These are six principles agreed upon by the TBT Committee in 2000, aimed at guiding Members in the development of standardization processes. They can be found on the official WTO page at the following link.:<https://www.wto.org/ english/tratop_e/tbt_e/principles_standards_tbt_e.htm>.

64 Hachez, Wouters 2011: 677-710.

tained therein. The Commission also reserves the right to exercise extensive power of control over these bodies, both during the formulation phase of the standard and during its approval[65].

Given the private nature of the SO and the role of the Commission in the process of forming these standards, usually, the harmonized standard is an example of public-private co-regulatory[66].

These standards will have an increasing importance in the digital policies of the European Union.

In the 2024 version of the Rolling Plan for ICT standardization, the annual document in which the state of the art of ICT standardization activities in the European context is represented, it is envisaged that after the adoption of the proposed Regulation (EU) 2022/272 (also known as the Cyber Resilience Act – CRA), the European Commission will prepare a formal standardization request to support the implementation of the CRA.

The figure is of particular significance because it highlights the Union's strong preference for using this type of technical standard, as opposed to others, in the context of digital technologies.

This, however, led the European legislature to have to intervene in the matter in 2022 by making important changes to Regulation 1025/2012 first and foremost by promoting and encouraging the participation of social representations within the three European bodies[67]. In addition, a communication of the same year introduced the possibility for the European Commission to adopt common technical specifications using implementing acts to ensure the protection of the public interest in cases where there are no harmonized standards or existing ones are insufficient[68].

The latter power finds expression in certain areas, including those of cybersecurity (by the proposed Cyber Resilience Act Regulation)[69] and Artificial Intelligence[70].

6. Concluding remarks

In a few lines, the contribution aimed to draw an overview of the estimation of the relationship between the public and private sectors in the context of cybersecurity in its transversality.

This collaboration represents an inevitable necessity dictated by the very nature of cyberspace, which we can interpret as an agglomeration of ICT products, processes and services, put on the market by private companies active in the field

65 Art. 10 Reg. (UE) 1025/2012.

66 Kamara 2017.

67 Art. 1, Reg. (UE) 2022/2480.

68 Comunicazione, *Una strategia dell'UE in materia di normazione Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, COM (2022) 31 final, 2.2.2022.

69 Comunicazione, *Una strategia dell'UE in materia di normazione* cit.: 5-6.

70 Volpato 2024.

and traded according to the laws of supply and demand, as well as respecting the relevant production and quality standards (commodity cyberspace)[71].

This has led to the need to establish such forms of both public and private intervention, which we can grasp from an organizational perspective, see precisely the aforementioned public-private partnerships (PPPs); as well as at the regulatory level, where in the digital context it is not unusual to witness the phenomenon of so-called co-regulation, or multistakeholder governance, in which states are placed on the same level as other actors, mostly private.

The synergy created in these systems thus makes it possible to cope with the cybernetic threat, on the one hand, from an organizational point of view, by pooling the resources, skills and infrastructure of the public administration and private individuals, and on the other hand, from a regulatory point of view, by dictating regulations of a mixed nature between the legal and the technical, capable of expressing a multitude of interests that can be traced mostly to public interests, usually enforced by States, and economic interests, proper to the sectoral industries that participate in technical standardization.

In addition to the benefits, however, the discussion has also had the opportunity to highlight the negative aspects of this relationship, due to difficulties originating from the very nature of the parties involved.

The economic efficiency of PPPs, demonstrated by better delivery of public services, is matched by the unequal distribution of risk between the public and private sectors, with the state-according to some theorists-bearing a disproportionate share of the burden[72].

Consider also the critical issues posed by the potential conflict between the short-term financial interests of the private sector and the long-term goals of the public sector, which could result in an impediment to the achievement of goals in terms of social welfare and environmental sustainability given by the risk of overcharging for privately operated services and infrastructure.

As will be understood, the topic refers to the complex relationship between public and private powers, which we believe can be easily analysed from the normative perspective.

The assertion of private powers in cyberspace is a well-known fact by now (§ 1) what is of interest here, however, is the ability to express one's interests using technical standardization, as an instrument of a private nature, until not so long ago thought to be neutral in that it was produced outside the circuits of political representation.

However, in the European context, we have had to point out that the Union's interest is to favour a particular type of technical standard, which is the harmonized standard (§ 6). We believe that with this choice the European Union is trying to convey what is already intuited by the definition of European cybersecurity-technical standardization to public ends by pursuing policy objectives.

71 Let it be permissible to refer to Serini 2023a.
72 Rybnicek, Plakolm and Baumgartner, 2020.

Problems arise, however, both on the definitional level, given the labile limit of the nature of these standards, which although technical are strongly close to legal, and on the level of rights protection guarantees. Although since the James Elliott Construction ruling in 2016, the Court of Justice has judged these standards to be an integral part of Union law and, most recently, with the Public.Resource.Org ruling in March 2024, the Court has recognized their free and full accessibility to the public, it is still doubtful whether rights that may be affected by these standards can be enforced through direct judicial action against a harmonized standard.

The issue appears to take on particular significance in the context of security, where the substance of the regulation defines the extent to which freedoms and rights can be constrained for security reasons.

Far from having exhausted such a complex topic, the hope is to have raised questions that may stimulate further studies and in-depth analyses on the subject, thereby fostering scientific debate on the matter.

References

Abrahamsen R., Leander A. 2016., *Handbook of private security studies*, London.

Aliquò G. 2023, "Sicurezza pubblica e sicurezze private", *Polizia moderna*.

Bombelli G. 2017, "Dal moderno all'ultramoderno'? Intorno al nesso diritto-tecnica-sicurezza", in Pizzolato F., Costa p. (a cura di), *Sicurezza e tecnologia*, Milano: Giuffrè.

Bombelli G. Farah p. , "The Interlinkages Science-Technology-Law: Information and Communication Society, Knowledge-Based Economy and the Rule of Law", *Legal Studies Research Series*, n. 43.

Bourdeau p. 2013, "Resiliencism: premises and promises in securitisation research", *Resilience: Inter-national Policies, Practices, and Discourses*, 1(1).

Broadbent J. and Laughlin R. 2005, "Public-private partnerships: An introduction", *Accounting, Auditing & Accountability Journal,* 18 (6): 744-755.

Buzzacchi C. 2015, "Sicurezza e securization tra Stato, Unione Europea e mercato: prerogative dei pubblici poteri o attività economica?", in Pizzolato F., Costa p. (a cura di), *Sicurezza, Stato e mercato*, Milano: Giuffrè.

Carr M. 2016, "Public–private partnerships in national cyber-security strategies", *International Affairs*, 92 (1): 43-62.

Castaldo F. 2018a, "Fronteggiare il nemico in arene competitive turbolente: l'importanza della fiducia e delle capacità dinamiche nelle alleanze strategiche", *Rivista Italiana di Conflittologia*, 35: 10-39.

Castaldo F. 2018b, "I sistemi di gestione del traffico aereo e l'incombente minaccia del crimine: la necessità di un modello cyber security centric", *Rivista Italiana di Conflittologia*, 36: 29-48.

Castaldo F. 2019, "Dalla Cyber Defense alla Cyber Resilience dell'Infrastruttura Critica. Alcune implicazioni strategiche e organizzative", *Rivista di Economia e Politica dei Trasporti*, 3: 1-10.

Castaldo F. 2021, *Resilience by Design and Resilience Embedded. Achieving Proactive Cyber Defense*, Benevento: CUAM University Press.

Castaldo F. 2023, "Traghettare le organizzazioni nell'era delle incertezze", *Sviluppo & Organizzazione*, 311:44-48.

Castaldo F. and Serini F. 2024, "La collaborazione pubblico-privata nell'ambito della Cybersecurity europea. Dal piano organizzativo a quello della normazione tecnica", *Intervento presentato al Convegno Internazionale Interdisciplinare su "Cybersecurity e Istituzioni Pubbliche. Rischi e opportunità della regolamentazione informatico-giuridica di un fenomeno trasversale*", Novara, 23 maggio 2024.

Castaldo F., Porretta p. , Zanda S. 2024, "Recovering the dormant values of accounting to navigate the challenges of the 2030 agenda and beyond", *Meditari Accountancy Research*, 32, 6.

Cerf V. 2022, "Sulla governance di Internet", in Abba L., Lazzaroni A., Pietrangelo M. (a cura di), "La Internet governance e le sfide della trasformazione digitale", in *Rivista Italiana di Informatica e Diritto*, fasc. 4.

Della Morte G. 2018, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018.

Dunn Cavelty M. and Suter M. 2009, "Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, 2 (4): 179-187.

Dunn Cavelty M., Eriksen C. and Scharte B. 2023, "Making cyber security more resilient: adding social considerations to technological fixes", in *Journal of Risk Research*, 26(7): 801-814.

Eckert S. 2005, "Protecting Critical infrastructure: The Role of the Private Sector", in p. Dombrowski (Eds) 2005, *Guns and Butter: The Political Economy of International Security*, Boulder: Lynne Rienner Publishers.

Elias G. 1995*,* "Le regole comunitarie per l'accesso al mercato unico: le misure per l'eliminazione delle barriere tecniche", in Andreini p. , Caia G., Elias G., Roversi-Monaco F.A. (a cura di), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industiali*, Bologna, Il Mulino.

Eweje G., Sajjad A., Nath S.D. and Kobayashi K. 2021, "Multi-stakeholder partnerships: A catalyst to achieve sustainable development goals", *Marketing Intelligence & Planning*, 39 (2): 186-212.

Farrand B., Carrapico H. 2018, "Blurring public and private: cybersecurity in the age of regulatory capitalism", in Bures O., Carrapico H. (a cura di), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham.

Gallotti C. 2022, *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Lulu press.

George G., Fewer T.J., Lazzarini S., McGahan A.M. and Puranam p. 2024, "Partnering for grand challenges: A review of organizational design considerations in public-private collaborations", *Journal of Management*, 50 (1): 10-40.

Greco N. 1999, "Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale", in Aa.Vv., *Crisi del diritto, produzione normativa e demo-crazia degli interessi*, Edistudio, pp. 37 ss.

Grimsey D. and Lewis M. 2007, *Public private partnerships: The worldwide revolution in infrastructure provision and project finance*, Edward Elgar Publishing.

Hachez N., Wouters J. 2011, *A Glimpse at the Democratic Legitimacy of Private Standards: Assessing the Public Accountability of GlobalG.A.P.*, in *Journal of International Economic Law*, 14 (3).

Hemming R. 2006, *Public-private partnerships*, International Monetary Fund.

Heritier p. 2003, *Urbe-Internet. Vol. 1. La rete figurale del diritto*, Torino, Giappichelli.

Hodge G.A., Greve C. and Boardman A.E. (Eds) 2010, *International handbook on public-private partnership*, Edward Elgar Publishing.
Irti N. 2006, *Norma e luoghi*, Roma-Bari: Laterza.
Kamara I. 2017, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate", *European Journal of Law and Technology*, Vol 8, n 1.
Kshetri N. 2015, "India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership", *IEEE Security & Privacy*, 13 (3): 16-23.
Kumar Muthusamy S. 2014, "Role of context and contest in the structuring of alliance governance", *Journal of Strategy and Management*, 7 (2): 172-192.
Laughlin C. 2015, "Cybersecurity in Critical infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations Are Effective", *Journal on Telecommunication and High Technology Law*, 14: 345.
Lessig L. 1999, *Code and Other Laws of Cyberspace*, New York.
Lichtenthaler U. 2016, "Alliance portfolio capability: a conceptual framework for the role of exploration or exploitation alliances", *Journal of Strategy and Management*, 9 (3): 281-301.
Luiijf E., Besseling K. and De Graaf p. 2013, "Nineteen national cybersecurity strategies", *International Journal of Critical infrastructures* 6, 9 (1-2): 3-31.
Min K.S., Chai S.W. and Han M. 2015, "An international comparative study on cybersecurity strategy", *International Journal of Security and Its Applications*, 9 (2): 13-20.
Moore T. 2010, "The economics of cybersecurity: Principal and policy options", *International Journal of Critical infrastructure Protection*, 3 (3): 103-117.
Mosca C. 2012, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova: Cedam.
Mulyani S. 2021, "Critical success factors in public-private partnership", *Journal of Accounting Auditing and Business,* 4 (1): 81-86.
O'Mara M. 2019, *The Code: Silicon Valley and the Remaking of America*, New York.
Oddenino A. 2018, "Digital standardization cybersecurity issues and international trade law", *Questions of International Law*, n. 51.
Pellicelli A.C. 2012, "Strategic alliances", *Economia Aziendale Online*, 2: 1-21.
Pollicino O., Bassini M., De Gregorio G. 2022, *Internet law and protection of fundamental rights*, Milano: Bocconi University Press.
Pollicino O. 2023, *Potere digitale*, Estratto da I Tematici, V-2023, Potere e Costituzione, in *Enc. dir.:* 415.
Rogers J. 2016, *Public-private partnerships: A tool for enhancing cybersecurity* (Doctoral dissertation, Johns Hopkins University).
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli, Editoriale scientifica.
Russel D., Gangemi G.T. 1991, *Computer security basics*, Sebastopol: O'Reilly Media.
Sarmento J.M. and Renneboog L. 2016, "Anatomy of public-private partnerships: their creation, financing and renegotiations", *International Journal of Managing Projects in Business*, 9 (1): 94-122.
Sassen S. 2008, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton.
Serini F. 2023a, "La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana", *Rivista italiana di informatica e diritto*, 2.
Serini F. 2023b, "Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?", *MediaLaws*, 3.
Serini F. 2024, "Collective cyber situational awareness in EU. A political project of difficult legal realisation?", *Computer Law & Security Review*, 55.

Suter M. 2012, "PPPs in Security Policy: Opportunities and limitations", *CSS Analyses in Security Policy*, 111.
Thomas R.N. 2013, *Securing Cyberspace Through Public-Private Partnership: A Comparative Analysis of Partnership Models*, Center for Strategic & International Security.
Ursi R. 2022, *La sicurezza pubblica*, Il Mulino, Bologna.
Vining A.R. and Boardman A.E. 2008, "Public-private partnerships: Eight rules for governments", *Public Works Management & Policy*, 13 (2): 149-161.
Volpato A. 2024, "Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale", *Associazione Italiana Studio di Diritto dell'Unione Europea*, 2.
Volpe A. and Castaldo F. 2021, "Complessità, incertezza e urgenza di agire", *Sviluppo & Organizzazione,* 297: 34-40.
Volpe A. and Castaldo F. 2024, "Rational choice and actors' strategic interdependence: an insight into game theory", *Il Pensiero Economico Moderno*, 1-2: 11-40.
Watkins B. 2014, "The impact of cyber attacks on the private sector", *Briefing Paper, Association for International Affair*, 12: 1-11.
Zanda S. and Castaldo F. 2023, September, "Epistemology of complexity in a state of crisis. Leadership and coordination as catalysts of neghentropy", *16th Annual Conference of the EuroMed Academy of Business*.

Corso Tozzi Martelli

La Cybersicurezza alla prova del Codice dei contratti pubblici (D.lgs. n. 36 del 2023): sfide e opportunità

Abstract: Il presente articolo, dedicato alla cybersecurity nell'ambito del nuovo Codice degli appalti pubblici (D.Lgs. n. 36/2023), intende sottolineare il ruolo cruciale dell'organizzazione amministrativa nella tutela dei diritti e degli interessi. Lo scritto esamina come le disposizioni del Codice, nonostante la loro natura programmatica, rappresentino un'opportunità significativa per rafforzare la protezione dei dati personali e la cybersecurity nel contesto degli appalti pubblici. Per garantire la loro piena efficacia, tuttavia, l'elaborato evidenzia la necessità di integrare queste disposizioni con regolamenti dettagliati e operativi. L'obiettivo è promuovere un approccio olistico alla digitalizzazione, che affronti non solo gli aspetti tecnologici ma anche quelli organizzativi, giuridici e culturali.

Keywords: Pubblica Amministrazione, Organizzazione amministrativa, Digitalizzazione, Cybersicurezza, Appalti pubblici, Codice dei contratti pubblici.

1. Premessa: l'aumento della minaccia *cyber* per l'Amministrazione digitale

In un mondo sempre più digitalizzato, siamo costantemente esposti a un numero crescente di attacchi informatici. Ogni giorno riceviamo numerosi messaggi, email e chiamate che nascondono tentativi di *phishing*, progettati per ingannarci e ottenere informazioni sensibili o accesso non autorizzato ai nostri sistemi informatici.

Quello che desta particolare preoccupazione è tuttavia che questi attacchi sono sempre più indirizzati verso soggetti pubblici[1].

1 V. il Rapporto Clusit 2024 sulla sicurezza ICT in Italia, reperibile al link: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2024_web.pdf, che indica: "Il settore pubblico è stato interessato da un importante aumento del numero degli attacchi fra il 2022 e il 2023.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760155

In tal senso, la Relazione annuale sulla politica dell'informazione per la sicurezza[2], presentata dal Sistema di Informazione per la Sicurezza della Repubblica al Parlamento nel febbraio 2024, evidenzia un "costante interesse degli attori della minaccia [cyber], crescente nei confronti delle infrastrutture digitali di soggetti pubblici, con particolare attenzione verso quelle riferibili alle Amministrazioni Centrali dello Stato e agli Istituti e Agenzie nazionali"[3].

Questa tendenza è ulteriormente confermata dal Rapporto Clusit 2024 dell'Associazione Italiana per la Sicurezza Informatica, che rivela come il 41% degli attacchi informatici "gravi" registrati nel 2023 abbia preso di mira le Pubbliche Amministrazioni[4].

Tale scenario dimostra chiaramente come, nell'attuale fase di trasformazione digitale della Pubblica Amministrazione[5], la cybersicurezza[6] – intesa come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[7] – diventi un requisito imprescindibile per garantire la tutela dei diritti e degli interessi, nonché per mantenere l'operatività dell'Amministrazione.

In effetti, come evidenziato in dottrina, "Una Pubblica Amministrazione che oggi ritenga di non poter essere soggetta ad attacchi di sicurezza, è un'organizzazione senza consapevolezza del livello di digitalizzazione della propria attività istituzionale"[8].

In tale prospettiva, il presente contributo si propone di indagare in che termini il Codice dei contratti pubblici disciplini il tema della cybersicurezza, evidenziando l'importanza dell'aspetto organizzativo delle Pubbliche Amministrazioni per affrontare efficacemente le sfide ad essa connesse.

Tra il 2019 e il 2023 il campione ha incluso 1.149 attacchi noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Globalmente la crescita è all'incirca lineare, con un forte incremento fra il 2022 e il 2023. Nell'arco dei cinque anni si è comunque passati dai 187 attacchi del 2019 ai 282 del 2023, con un incremento complessivo del 50%".

2 Relazione annuale 2023 sulla politica dell'informazione per la sicurezza, reperibile al link: https://www.sicurezzanazionale.gov.it/data/cms/posts/933/attachments/711cf87b-1a38-4864-975a-e253a67cbdba/download?view=true.

3 *Ivi*, p. 84.

4 V. il Rapporto Clusit 2024 sulla sicurezza ICT in Italia, pp. 98 e ss.

5 Sulla digitalizzazione della Pubblica Amministrazione, cfr. *ex multis*: Cavallo Perin e Galetta (a cura di) 2020; Cavallo Perin 2020; Cavallo Perin (a cura di) 2021; Galetta 2022; Galetta 2023; Galetta 2023; Auby, De Minico e G. Orsoni (a cura di) 2023; Torchia 2023.

6 Sulla cybersicurezza, cfr: Montessoro 2019; Bruno 2020; Brighi e Chiara 2021; Renzi 2021; Macrì 2021; Previti 2022; Serini 2022; Ursi 2023; Buoso 2023; Rossa 2023a; Rossa 2023b; Rossa 2024a; Moroni 2024.

7 Art. 2, (1), del Regolamento UE 2019/881 (c.d. *Cybersecurity Act*). Mentre, a livello nazionale, l'art. 1, comma 1, lett. *a*), del d.l. 14 giugno 2021, n. 82, convertito dalla l. n. 109/2021, definisce la "cybersicurezza" come "l'insieme delle attività (…) necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico".

8 V. Macrì 2021: 1196.

2. La protezione dei dati personali e la sicurezza informatica quali principi fondamentali della digitalizzazione degli appalti pubblici

Come noto, una delle principali novità introdotte dal decreto legislativo 31 marzo 2023, n. 36, c.d. Codice dei contratti pubblici[9] (d'ora in poi anche solo "Codice") riguarda la digitalizzazione e l'informatizzazione delle procedure di gara[10], cui è interamente dedicata la Parte II del Libro I (artt. 19-36)[11].

In particolare, il Codice prevede la piena digitalizzazione dell'intero "ciclo di vita" dei contratti pubblici, inteso come l'insieme di tutte le attività che si susseguono dalla programmazione alla definizione del fabbisogno, fino all'esecuzione del contratto[12]. Tuttavia, questa ambiziosa digitalizzazione (*end-to-end*) comporta l'esposizione di ogni fase del processo di approvvigionamento e di ogni dato trattato al rischio di *cyber* attacchi e/o incidenti informatici[13].

Per mitigare tale rischio, il legislatore ha deciso di introdurre specifiche disposizioni in materia di cybersicurezza. Si tratta di una novità 'assoluta', in quanto il precedente Codice (d.lgs. 18 aprile 2016, n. 50) ignorava, *tout court*, tale aspetto[14].

La cybersicurezza viene affrontata sotto un duplice profilo: da un lato, come requisito fondamentale che dovrà essere garantito durante l'intero processo di digitalizzazione delle procedure di gara, impattando l'organizzazione della Pubblica Amministrazione (art. 19, commi 1 e 5); dall'altro, quale elemento da tenere in considerazione nella valutazione della componente tecnica delle offerte nelle gare volte all'acquisto di beni e servizi informatici (art. 108, comma 4)[15], che a loro volta

9 Per alcuni commenti relativi alle norme del Codice dei contratti pubblici, cfr. *ex multis*: Cartei e Iaria 2023; Caringella 2023; Corradino 2023; Dall'Acqua, Meola e Purcaro 2023; Fanti 2023; Giovagnoli e Rovelli 2024; Botto e Castrovinci Zenna 2024; Villata e Ramajoli 2024; Ursi 2024; Tropea 2024.

10 Sul punto, è opportuno ricordare come la digitalizzazione del settore pubblico rappresenti uno degli obiettivi chiave del Piano Nazionale di Ripresa e Resilienza (PNNR), Missione 1, che, con riferimento alle procedure di gara, mira a "definire le modalità per digitalizzare le procedure per tutti gli appalti pubblici e concessioni e definire i requisiti di interoperabilità e interconnettività" (M1C1-70), nonché a realizzare un Sistema Nazionale di e-procurement "interoperabile con i sistemi gestionali delle pubbliche amministrazioni" (M1C1-75). V. link: https://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/Dipartimenti/USG/Misure_attuazione_PNRR_20231231.pdf.

11 Sulla digitalizzazione dei contratti pubblici, cfr. *ex multis*: Cavallo Perin e Lipari, Racca (a cura di) 2022; Racca 2022; Guarnaccia 2022; Gambetta 2023; Corrado 2023; Galetta 2023; Carullo 2023; Forte e Pica 2023; Carlotti: 2023; Bruno 2024; Vesperini: 2024; Mancini Palamoni 2024.

12 V. l'art. 21 del d.lgs. n. 36/2023; nonché l'art. 3, co. 1, lett. p), dell'Allegato I.1 del Codice.

13 V. Rossa 2024a: par. 5.

14 Del resto, anche le Direttive 2014/23-24-25/UE in materia di appalti e concessioni non prevedono né una disciplina generale sugli appalti di *cybersecurity* né disposizioni generali o particolari in merito, rimettendo quindi la relativa previsione alla discrezionalità dei legislatori nazionali. Reperibili al link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L:2014:094:FULL.

15 L'articolo 108, comma 4, del Codice stabilisce che "(…) Nelle attività di approvvigionamento di beni e servizi informatici per la pubblica amministrazione, le stazioni appaltanti,

potranno essere utilizzati per digitalizzare (ulteriormente) l'Amministrazione e la sua attività[16].

Volendo concentrare l'attenzione al profilo organizzativo, l'analisi che segue si focalizza sull'articolo 19 del Codice dei contratti pubblici. In particolare, tale articolo, al comma 1, prevede che:

> Le stazioni appaltanti e gli enti concedenti assicurano la digitalizzazione del ciclo di vita dei contratti nel rispetto dei principi e delle disposizioni del Codice dell'Amministrazione Digitale […], garantiscono l'esercizio dei diritti di cittadinanza digitale e operano secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica.

Al riguardo, si può rilevare come il legislatore, consapevole delle complessità e delle criticità del processo di digitalizzazione, abbia voluto tracciare la direzione degli sviluppi futuri. Infatti, con la norma in commento, non si è limitato a fissare l'obiettivo della "digitalizzazione dell'intero ciclo di vita dei contratti", ma ha stabilito anche quei principi fondamentali che dovranno guidare ed essere garantiti in tale processo[17].

Tra questi principi, spiccano – per quanto qui interessa – quelli di protezione dei dati personali e di sicurezza informatica. Il collegamento tra questi due principi suggerisce un'interpretazione del concetto di "sicurezza informatica" nella sua accezione di "cybersicurezza"[18], ovverosia un sistema di sicurezza in grado di garan-

incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici. Nei casi di cui al quarto periodo, quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento. Per i contratti ad alta intensità di manodopera, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento".

16 Si pensi, in particolare, alle "gare strategiche per la trasformazione digitale", che, secondo quanto indicato nelle Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026 di AGID (reperibile al link: https://www.agid.gov.it/sites/agid/files/2024-05/piano_triennale_per_linformatica_nella_pa_2024-2026_0.pdf), sono "strumenti che consentono alle Amministrazioni di acquisire servizi necessari ad implementare le strategie per la trasformazione digitale della Pubblica Amministrazione" (pp. 38 ss.). Sul punto, si veda anche il Portale informatico Consip Gare Strategiche, al link: https://www.consip.it/attivit/gare-strategiche.

17 Oltre ai principi elencati già al primo comma dell'art. 19, occorre fare riferimento anche ai principi: del "*once only*" (art. 19, comma 2); del "digital by default" (art. 19, comma 3); della "interoperability by default" (art. 19, comma 4); del riuso delle informazioni e di accessibilità e fruibilità dei dati in formato aperto (art. 19, comma 4); di accessibilità e di conoscibilità (art. 19, commi 6 e 7).

18 Si osserva infatti in dottrina come i due termini, di regola, non siano coincidenti o sovrapponibili. Sul punto v. Rossa 2024a, nota n. 21, afferma che "il termine "sicurezza informatica" concerne quel ramo dell'informatica che studia come tutelare le reti informative. Sotto questo punto di vista, pertanto, non vi è completa identità con il concetto di cybersicurezza, posto che con esso si intende un sistema organizzativo finalizzato a proteggere le infrastrutture

tire non solo la protezione dei sistemi informativi e delle infrastrutture, ma anche un'adeguata tutela dei dati personali[19].

In proposito, è bene sottolineare – come evidenziato dal Consiglio di Stato nella Relazione sullo Schema definitivo di Codice dei contratti pubblici – che "tutte le iniziative dovrebbero andare oltre il semplice rispetto del quadro giuridico in materia di protezione dei dati personali e privacy e sicurezza informatica, integrando tali elementi nella fase di progettazione" [20] (o, in inglese, *by design*).

In effetti, la digitalizzazione – come sottolineato nella Relazione –, pur accrescendo l'efficacia e l'efficienza dei processi, "non può implicare un arretramento delle garanzie [di sicurezza informatica] e dei diritti [di protezione dei dati personali e privacy] degli operatori economici né dei doveri che gravano sulle amministrazioni"[21].

3. Il ruolo dell'organizzazione e la formazione continua del personale nel prevenire e gestire gli attacchi *cyber*

Nella prospettiva sopra delineata, il comma 5 dell'articolo 19 assume particolare rilevanza, poiché impone alle stazioni appaltanti, agli enti concedenti e agli operatori economici che partecipano alle attività e ai procedimenti connessi al ciclo vita dei contratti, indipendentemente dal loro settore di attività, l'obbligo di adottare misure tecniche e *organizzative* volte a garantire la sicurezza informatica e la protezione dei dati personali.

Questa disposizione, che si rivolge a tutti i soggetti coinvolti nelle procedure di aggiudicazione, evidenzia il ruolo cruciale dell'organizzazione nella prevenzione e gestione delle minacce informatiche.

È fondamentale, dunque, che tale obbligo non sia inteso come un mero adempimento burocratico, ma piuttosto come un elemento chiave per la costruzione di un sistema di sicurezza di cybersicurezza resiliente, capace di adattarsi alle sfide poste dall'evoluzione delle minacce digitali.

Una gestione efficace dei processi (organizzativi) consente, infatti, di identificare tempestivamente le criticità, implementare soluzioni in via preventiva e reagire prontamente agli incidenti. In altri termini, l'obbligo di adottare "misure tecniche e organizzative" non rappresenta tanto un obbligo formale, quanto un requisito

digitali di organizzazioni complesse, grazie alla predisposizione di misure tecniche idonee a tutelare diritti e libertà fondamentali".

19 In effetti, sebbene la sicurezza informatica e la protezione dei dati personali non siano concetti coincidenti, essi risultano strettamente connessi, come avviene quando una violazione di sicurezza comporta anche una violazione dei dati personali (c.d. "*data breach*").

20 Consiglio di Stato, *Schema definitivo di Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante "Delega al Governo in materia di contratti pubblici". III – Relazione agli articoli e agli allegati*, Roma, 7 dicembre 2022, reperibile al link: https://www.giustizia-amministrativa.it/documents/20142/17550825/3_CODICE+CONTRATTI+RELAZIONE.pdf/d3223534-d548-1fdc-4be4-e9632c641eb8?t=1670936691000.

21 *Ivi*, 40.

sostanziale per proteggere l'integrità dei dati e la continuità operativa delle Pubbliche Amministrazioni.

Un aspetto centrale per una gestione efficace della sicurezza informatica è poi la formazione continua del personale, come espressamente previsto dal comma 5 dell'articolo in esame[22].

Considerando che il panorama delle minacce *cyber* evolve rapidamente, con attacchi sempre più sofisticati, è infatti necessario che il personale sia costantemente aggiornato. Affidarsi esclusivamente a soluzioni tecniche, senza investire nel capitale umano, non può che limitare significativamente l'efficacia delle misure di sicurezza.

Del resto, la formazione e l'aggiornamento costante sono fondamentali per sviluppare una consapevolezza in materia di sicurezza informatica (cosiddetta *cybersecurity awareness*). È infatti da tale consapevolezza che possono derivare le azioni organizzative necessarie a mitigare i rischi relativi alla sicurezza informatica[23].

Investire nella formazione, pertanto, non significa solo elevare il livello delle competenze digitali dei singoli individui, ma anche rafforzare l'intero sistema di difesa contro le minacce informatiche, rendendo ciascun membro di un'organizzazione complessa un attore attivo nella protezione delle risorse informative[24].

L'articolo 19, comma 5, del Codice dei contratti pubblici evidenzia, in sintesi, come la cybersicurezza sia intrinsecamente legata all'organizzazione amministrativa[25] e come l'adozione di misure organizzative adeguate, tra cui la formazione continua del personale addetto, rappresenti un pilastro fondamentale per la sicurezza informatica.

4. Sfide normative: l'articolo 19 del Codice dei contratti pubblici come "norma manifesto" e la necessità di integrazione

Dall'analisi svolta emerge che le disposizioni in materia di cybersicurezza presenti nel Codice dei contratti pubblici rappresentano un significativo passo in avanti nella regolazione della sicurezza informatica all'interno del settore pubblico.

22 A tal fine, l'art. 19, comma 5, precisa che "Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento".

23 Cfr. il Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022, in https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/capitolo_6_sicurezza_informatica.html.

24 Per altro verso, come evidenziato da Rossa 2023a: 219 ss.: "Lo sviluppo delle competenze richieste dalla cybersicurezza pubblica appare necessario, soprattutto all'interno della Pubblica Amministrazione, in particolare nell'ambito degli appalti di tecnologia – come del resto espressamente previsto dal nuovo Codice appalti. E questo per una ragione chiara. Essendovi l'esigenza di instaurare una relazione collaborativa fra i soggetti pubblici e quelli privati, che riequilibri la situazione di disparità che normalmente avvantaggia gli operatori economici e che perciò sia funzionale sul piano concreto, è imprescindibile che i soggetti pubblici siano realmente in grado di possedere le medesime conoscenze dei privati".

25 Sul punto, cfr. Rossa 2023b: 162, afferma che "l'attività organizzativa si pone come fondamento logico del concetto stesso di cybersicurezza".

Tuttavia, tali norme presentano una natura programmatica, configurandosi più come 'norme manifesto'[26] piuttosto che come 'istruzioni operative-pratiche' per la gestione concreta della cybersicurezza da parte delle Pubbliche Amministrazioni[27].

Per esempio, l'articolo 19 sancisce l'obbligo di formare e aggiornare costantemente il personale, ma non ne stabilisce né le modalità né i contenuti minimi, lasciando alle singole amministrazioni l'onere di definire i propri percorsi formativi, in base al principio di auto-organizzazione.

Questo approccio, sebbene flessibile, comporta il rischio di creare livelli di sicurezza disomogenei e talvolta inadeguati, con possibili conseguenze negative sull'efficacia complessiva della protezione cibernetica a livello nazionale.

Infatti, pur stabilendo importanti obiettivi e principi, le disposizioni contenute nel Codice non forniscono indicazioni sufficientemente dettagliate per consentire alle Amministrazioni di tradurre in azioni concrete i principi fissati.

L'assenza di regole chiare e di istruzioni precise può portare a strategie di sicurezza informatica frammentate e non coordinate, compromettendo così la capacità di risposta del settore pubblico alle minacce informatiche.

Di conseguenza, per superare tali criticità e rendere le disposizioni del Codice realmente efficaci, diventa necessario integrarle con normative che offrano un approccio più operativo, come, ad esempio, il Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) ovvero la legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"[28].

In proposito, l'articolo 8 della l. n. 90/2024 prevede che le amministrazioni di maggiori dimensioni – come Regioni, Province autonome di Trento e Bolzano, città metropolitane, comuni con più di 100.000 abitanti (inclusi i capoluoghi di regione), società di trasporto pubblico urbano con bacini d'utenza superiori a 100.000 abitanti, società di trasporto pubblico extraurbano operanti nelle città metropolitane e aziende sanitarie locali – devono individuare una struttura, anche tra quelle già esistenti, dedicata alla cybersicurezza. Questa struttura avrà il compito di sviluppare politiche e procedure di sicurezza, implementare sistemi di analisi e gestione del rischio informatico, definire ruoli e organizzazione per la sicurezza, redigere un piano programmatico per la protezione di dati e infrastrutture, potenziare la capacità di gestione del rischio, adottare le misure previste dalle linee guida dell'Agenzia per la cybersicurezza nazionale, e monitorare costantemente le minacce e le vulnerabilità per mantenere aggiornati i sistemi di sicurezza.

All'interno di tale struttura, è inoltre prevista l'istituzione di un referente per la cybersicurezza, selezionato in base a specifiche e comprovate professionalità e competenze nel settore[29].

26 V. Gambetta 2023: 104.

27 Cfr. Rossa 2024a: parr. 3 e 5.

28 Per un commento al Disegno di Legge n. 1717 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici") si rinvia a Rossa 2024b.

29 V. art. 8, comma 2, della legge n. 90/2024.

Tuttavia, un limite significativo all'attuazione delle misure di sicurezza informatica è rappresentato dall'obbligo di utilizzare esclusivamente le risorse umane, strumentali e finanziarie disponibili a legislazione vigente[30]. Questo vincolo rischia di compromettere la capacità delle Amministrazioni di implementare efficacemente tali misure, specialmente laddove le risorse siano scarse.

Alla luce di ciò, appare chiaro che un cambiamento culturale orientato alla promozione della *cybersecurity awareness* diventa ancor più imprescindibile. In un contesto caratterizzato da risorse limitate, investire nella sensibilizzazione e nella formazione del personale può rappresentare una soluzione 'sostenibile' per innalzare il livello di sicurezza informatica delle Amministrazioni. La consapevolezza dei rischi e delle *best practice*, infatti, deve diventare parte integrante dell'operatività quotidiana.

Inoltre, la natura programmatica dell'articolo 19 del Codice, unitamente alla necessità di promuovere una cultura della cybersicurezza, evidenzia l'importanza di un impegno concreto nella formazione e nella diffusione di conoscenze specifiche. Senza tale impegno, le disposizioni rischiano di rimanere inapplicate, impedendo così il raggiungimento degli obiettivi prefissati.

Pertanto, investire nella cultura della sicurezza informatica, prevedendo specifici ruoli e responsabilità all'interno delle Amministrazioni, non solo supporta l'attuazione pratica delle disposizioni esaminate, ma contribuisce a creare un ambiente più resiliente alle minacce cibernetiche, stimolando al contempo la domanda di soluzioni innovative e di competenze digitali e aprendo così nuove prospettive di crescita per l'intero comparto della cybersicurezza.

5. Riflessioni conclusive: la digitalizzazione dell'organizzazione amministrativa quale presupposto per una buona amministrazione digitale

In conclusione, si può affermare che le disposizioni in materia di cybersicurezza previste dal Codice dei contratti pubblici, in particolare dall'articolo 19, offrono l'opportunità di riflettere sull'impatto della digitalizzazione sulla Pubblica Amministrazione e, in particolare, sulla sua organizzazione.

La crescente digitalizzazione delle attività della Pubblica Amministrazione richiede, infatti, un adattamento della struttura organizzativa per supportare efficacemente le nuove modalità attraverso cui si svolge il potere pubblico.

Nel contesto degli appalti pubblici, se l'intero ciclo di vita dei contratti deve essere svolto digitalmente, allora anche la struttura amministrativa che supporta le procedure di affidamento e gestione dei contratti deve essere adeguatamente organizzata per affrontare i rischi associati alla digitalizzazione.

Di conseguenza, la necessità di garantire una struttura amministrativa impermeabile alle minacce informatiche potrebbe essere considerata una declinazione specifica del principio di buon andamento, sancito dall'articolo 97, comma 2, della

30 V. artt. 8 e 24 della legge n. 90/2024.

Costituzione. In altre parole, la cybersicurezza si configurerebbe come un "corollario" di tale principio, influenzando direttamente l'efficienza, l'efficacia e la sicurezza dell'azione amministrativa.

Pertanto, una Pubblica Amministrazione che intenda conformarsi a un modello costituzionale di "buona amministrazione"[31] deve necessariamente considerare i rischi cibernetici derivanti dalla trasformazione digitale della propria struttura organizzativa. Non può esistere una "buona amministrazione" in senso digitale in assenza di un adeguato livello sicurezza informatica, tanto sul piano materiale quanto su quello organizzativo.

In definitiva, è importante riconoscere che le norme sulla cybersicurezza analizzate hanno il pregio di mettere in luce la necessità di affrontare la trasformazione digitale della Pubblica Amministrazione non solo dalla prospettiva della digitalizzazione dell'azione amministrativa, ma anche da quella dell'organizzazione.

Bibliografia

Auby J.B., De Minico G. e Orsoni G. (a cura di) 2023, *L'amministrazione digitale. Quotidiana efficienza e intelligenza delle scelte*, Napoli: Editoriale scientifica.

Botto A, Castrovinci Zenna S. (a cura di), 2024, *Commentario alla normativa sui contratti pubblici*, Torino: Giappichelli.

Brighi R. e Chiara p. G. 2021, "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea", in *Federalismi.it*, n. 21: 18 ss.

Bruno B. 2020, "'Cybersecurity' tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *Federalismi.it*, n. 14: 11 ss.

Bruno B. (2024), "*Art. 19 Principi e diritti digitali*, in R. Giovagnoli e G. Rovelli (a cura di), *Codice dei contratti pubblici*, Milano, Giuffrè: 212 ss.

Buoso E. 2023, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino: Giappichelli.

Caringella F. (diretto da) 2023, *Nuovo codice dei contratti pubblici*, Milano: Giuffrè.

Carloni E. 2020, "Diritti by design. Considerazioni su organizzazione, autonomia organizzatoria e protezione degli interessi", in *p. A. Persona e Amministrazione*, n. 1: 51 ss.

Cartei G.F. e Iaria D. (a cura di) 2023, *Commentario al nuovo Codice dei contratti pubblici*, Napoli: Editoriale Scientifica.

Carullo G. 2023, "Piattaforme digitali e interconnessione informativa nel nuovo Codice dei Contratti Pubblici", in *Federalismi.it*, n. 19: 110 ss.

Cavallo Perin R. (a cura di) 2021, *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino: Rubettino.

Cavallo Perin R. 2020, "Ragionando come se la digitalizzazione fosse data", in *Dir. amm.*, n. 2: 305 ss.

Cavallo Perin R., Galetta D.U. (a cura di) 2020, *Il Diritto dell'Amministrazione Pubblica digitale*, Torino: Giappichelli.

Cavallo Perin R., Lipari M. e Racca G.M. (a cura di) 2022, *Contratti pubblici e innovazioni. Per l'attuazione della legge delega*, Napoli: Jovene.

31 Sulla digitalizzazione e la buona amministrazione, cfr. su tutti Galetta 2020: 85 ss.

Corradino M. (a cura di) 2023, *La riforma dei contratti pubblici. Commento al d.lgs. 31 marzo 2023, n. 36*, Milano: Giuffrè.
Corrado A. 2023, "I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro", in *Federalismi.it*, n. 19: 128 ss.
Corrado A. 2023, "La digitalizzazione dei contratti pubblici", in Dall'Acqua F., Meola A. e Purcaro A.S. (a cura di), *La nuova disciplina degli appalti pubblici*, Pisa: Pacini giuridica: 119 ss.
Dall'Acqua F., Meola A. e Purcaro A.S. (a cura di) 2023, *La nuova disciplina degli appalti pubblici*, Pisa: Pacini giuridica.
Fanti V. (a cura di) 2023, *Corso sui contratti pubblici riformati dal d.lgs. 31 marzo 2023, n. 36*, Napoli: Edizioni Scientifiche Italiane.
Forte p. e Pica N. 2023, "Principi per la digitalizzazione e l'automazione nel ciclo di vita dei contratti pubblici", in AA.VV., *Studi sui principi del Codice dei contratti pubblici*, Napoli: Editoriale Scientifica: 303 ss.
Galetta D.U. 2020, "Digitalizzazione e diritto ad una buona amministrazione (il procedimento amministrativo, fra diritto UE e tecnologie ICT)", in Cavallo Perin R. e Galetta D.U. (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino: Giappichelli.
Galetta D.U. 2022, "Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal Piano Nazionale di Ripresa e Resilienza e problemi ancora da affrontare", in *Federalismi.it*, n. 7: 118 ss.
Galetta D.U. 2023, "Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono", in *Federalismi.it*, n. 12: iv ss.
Galetta D.U. 2023, "Il procedimento amministrativo come strumento di organizzazione e le conseguenze legate all'uso delle ICT", in *Istit. del Federalismo*, n. 2: 289 ss.
Gambetta D. 2023, "Digitalizzazione (artt. 19-36)", in Fanti V. (a cura di) 2023, *Corso sui contratti pubblici riformati dal d.lgs. 31 marzo 2023, n. 36*, Napoli: Edizioni Scientifiche Italiane: 93 ss.
Guarnaccia E. 2022, "Il processo di digitalizzazione delle gare d'appalto: dal DM n. 148/2021 al Codice dei Contratti Pubblici 2023", in *CERIDAP*, n. 4: 134 ss.
Macrì I. 2021, "Cybersicurezza per la Pubblica Amministrazione", in *Azienditalia*, n. 12: 1196 ss.
Mancini Palamoni G. 2024, "Il paradigma digitale dell'evidenza pubblica", in *CERIDAP*, n. 2.
Montessoro p. L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Ist. del Federalismo*, n. 3: 783 ss.
Moroni L. 2024, "La governance della cybersicurezza a livello interno ed europeo: un quadro intricato", in *Federalismi.it*, 14: 179 ss.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it*, n. 25: 65 ss.
Racca G.M. 2020, "La digitalizzazione dei contratti pubblici: adeguatezza delle pubbliche amministrazioni e qualificazione delle imprese", in R. Cavallo Perin e D.U. Galetta (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino: Giappichelli: 321 ss.
Racca G.M. 2022, "Le innovazioni necessarie per la trasformazione digitale e sostenibile dei contratti pubblici", in *Federalismi.it*, n. 15: 191 ss.
Renzi A. 2021, "La sicurezza cibernetica: lo stato dell'arte", in *Giorn. dir. amm.*, n. 4: 538 ss.
Rossa S. 2023a, *Cybersicurezza e Pubblica Amministrazione*, Napoli: Editoriale Scientifica.

Rossa S. 2023b, "Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario", in *Vergentis. Revista de Investigación de la Cátedra Internacional conjunta Inocencio III*: 161 ss.
Rossa S. 2024a, "Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici", in *CERIDAP*, n. 2.
Rossa S. 2024b, "L'istituzione della figura del "referente per la cybersicurezza" nel d.d.l. 16 febbraio 2024", in *IRPA, Osservatorio sullo Stato digitale – www.irpa.eu*, 8 maggio 2024.
Serini F. 2022, "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", in *Federalismi.it*, n. 12: 241 ss.
Tropea G. (a cura di) 2024, *Lineamenti di diritto dei contratti pubblici*, Napoli: Editoriale Scientifica.
Ursi R. (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: Franco Angeli.
Ursi R. (a cura di) 2024, *Studi sui principi generali del Codice dei contratti pubblici*, Napoli: Editoriale Scientifica.
Vesperini G. 2024, "Art. 19. Della digitalizzazione del ciclo vita dei contratti", in Botto A e Castrovinci Zenna S. (a cura di), *Commentario alla normativa sui contratti pubblici*, Torino: Giappichelli: 200 ss.
Villata R. e Ramajoli M. (a cura di) 2024, *Commentario al codice dei contratti pubblici*, Pisa: Pacini giuridica.

Informazioni sugli autori

Fabio Angeletti, Assegnista di Ricerca di Ingegneria – Sistemi di Elaborazione delle Informazioni nell'Università LUISS Guido Carli

Francesca Castaldo, Ricercatrice a tempo determinato (RTDA) di Organizzazione Aziendale nell'Università degli Studi di Roma "La Sapienza"

Melissa Capelli, Assegnista di Ricerca di Diritto Privato Comparato nell'Università degli Studi di Torino

Bruno Carotti, Consigliere della Corte costituzionale e Professore di Diritto dell'Amministrazione Digitale nell'Università LUISS Guido Carli

Alessandra Galassi, Dottoranda in Information and Communication Technologies nell'Università degli Studi dell'Aquila

Filippo Galli, Dottorando in Diritto e Impresa – Diritto Amministrativo e Pubblico nell'Università LUISS Guido Carli

Massimiliano Malvicini, Ricercatore a tempo determinato (RTDB) di Diritto Costituzionale e Pubblico nell'Università degli Studi del Piemonte Orientale

Maura Mattalia, Professoressa Associata di Diritto Amministrativo nell'Università degli Studi di Torino

Teresa Monaco, Dottoranda in Diritto ed Economia nell'Università degli Studi del Molise

Maria Notaristefano, Dottoranda in Cybersecurity nell'Università degli Studi di Roma "La Sapienza" e Università LUISS Guido Carli

Alberto Oddenino, Professore Associato di Diritto Internazionale nell'Università degli Studi di Torino

Matteo Pignatti, Ricercatore a tempo determinato (RTDA) di Diritto dell'economia nella Scuola Superiore Universitaria ad Ordinamento Speciale – CASD

Federico Serini, Dottore di ricerca in Diritto pubblico, comparato e internazionale nell'Università degli Studi di Roma "La Sapienza"

Esli Spahiu, Ricercatrice in Economia e Gestione delle Imprese nell'Università Bocconi

Stefano Rossa, Ricercatore a tempo determinato (RTDA) di Diritto Amministrativo e Pubblico nell'Università degli Studi del Piemonte Orientale

Corso Tozzi Martelli, Dottorando di Ricerca nel Dottorato Intersettoriale per l'Innovazione (*curriculum* Diritto amministrativo e pubblico) nell'Università degli Studi di Milano