Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 – Anticipazione fascicolo
Intelligenza artificiale e nuove vulnerabilità

Intelligenza artificiale e nuove vulnerabilità. Il difficile bilanciamento tra innovazione e tutela dei diritti fondamentali nella prospettiva del diritto amministrativo

Sveva Del Gatto*

SOMMARIO: 1. Introduzione. – 2. Il bilanciamento tra certezza del diritto e flessibilità nell'approccio regolatorio. – L'efficacia delle soluzioni adottate dall'AI Act per la tutela dei diritti fondamentali. – L'effettiva utilità del coinvolgimento umano: il dibattito sulla riserva di umanità. – 5. Osservazioni conclusive.

1. *Introduzione*

Vorrei ringraziare gli organizzatori di questo interessante Convegno per la squisita ospitalità. Un ringraziamento particolare ai Colleghi e Amici

---

* Professoressa associata di diritto amministrativo nell'Università di Macerata. Il presente contributo è tratto dalla Relazione svolta in qualità di *discussant* del *Panel 1 – IA e tutela dei diritti* nell'ambito del Convegno "Intelligenza artificiale e nuove vulnerabilità: dal diritto europeo della concorrenza e della proprietà intellettuale alla tutela dei diritti fondamentali", Macerata, 8-9 maggio 2025, e si inserisce nell'ambito del progetto "Innovazione e vulnerabilità: problemi giuridici e tutele" del Dipartimento di Giurisprudenza dell'Università di Macerata (finanziamento MUR, programma: Dipartimenti di Eccellenza 2023-2027).

Gianluca Contaldi e Cristina Grieco per avermi invitato consentendomi di svolgere alcune riflessioni, a partire dai *papers* in discussione, sull'impatto dell'intelligenza artificiale sui diritti fondamentali.

Discutere i molti punti trattati nei *papers* al centro di questo primo *Panel* non è cosa facile anche perché trattano, come avete ascoltato dall'introduzione della Presidente, di temi molto diversi tra loro, seppur con alcuni minimi comun denominatori. Per questo ho scelto di concentrare il mio intervento su alcune questioni che mi sembra siano di particolare rilevanza quando si discute di tutela dei diritti fondamentali e intelligenza artificiale (tema oggetto di questo *panel* che mi vede come *discussant*) e che attraversano trasversalmente gli scritti qui in discussione. Svolgerò, poi, nella parte finale ulteriori osservazioni, questa volta più specifiche per alcuni lavori che spero possano essere d'aiuto per il loro successivo sviluppo.

Peraltro io porto in questo autorevole consesso un punto di vista specifico, quello dello studioso del diritto amministrativo, branca che come molte qui rappresentate è stata fortemente interessata (per non dire travolta) dalla rivoluzione digitale[1].

Le riflessioni che mi accingo a fare riguardano la *governance* dell'intelligenza artificiale e il rapporto con i pubblici poteri e, più nel dettaglio, mirano a indagare se e come sia possibile conciliare la promozione dello sviluppo e dell'innovazione con la tutela dei diritti attraverso forme di regolazione tradizionale; e se sia (possa) essere possibile (preferibile) il ricorso a una *regulatory toolbox* diversa e innovativa. Mi interesserò dunque, al tema della regolazione: il potere pubblico che interviene decidendo *se* regolare, *quando* regolare e *come* regolare[2]. Ma anche a quello delle garanzie previste di fronte al potere

---

[1] A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, voll. I-III, Bologna, 2022.

[2] In argomento, G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Rivista trimestrale di diritto pubblico*, 2022, p. 1085 ss.; B. MARCHETTI, L. PARONA, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *DPCE online*, 2022, p. 237 ss.; sia consentito anche il rinvio a S. DEL GATTO, *La "governance" delle nuove tecnologie tra tentativi di regolazione e istanze di "self regulation". Il caso del riconoscimento facciale*, in *RIDPC*, 2023, p. 37 ss.

pubblico che utilizza l'intelligenza e alla concreta efficacia delle stesse. Partiamo dal tema della regolazione guardando al contesto di partenza, al dilemma di base e alle scelte svolte dal legislatore.

Nella scelta se regolare o meno si sono contrapposte, sintetizzando al massimo perché si tratta di argomenti noti, due visioni a cui corrispondono essenzialmente due linee di azione in campo regolatorio riconducibili all'impostazione statunitense (in parte rivista con l'*executive order* di Biden[3]) e a quella dell'Unione europea[4].

Da un lato, la tesi di coloro che ritengono che la regolazione freni l'innovazione, diffuse prevalentemente negli USA anche in ragione delle pressioni delle *big tech* e del mondo degli imprenditori[5] e che hanno portato (e incoraggiato) a fenomeni di *self regulation* da parte delle *big tech*. Dall'altra parte, coloro che invece ritengono che l'innovazione debba essere necessariamente regolata per le implicazioni che ha e che può avere sulla sfera giuridica delle persone, posizione su cui, come tornerò a dire a breve si è da subito attestata l'Unione europea.

---

[3] Il 30 ottobre 2023, il Presidente Biden ha emesso un *Executive Order* ("EO") in materia di Intelligenza Artificiale (AI) con l'obiettivo di promuovere lo sviluppo e l'uso sicuro, protetto e affidabile delle tecnologie di Intelligenza Artificiale. L'EO stabilisce, sulla base di otto principi e priorità, una serie di raccomandazioni e obblighi rivolti tanto ai fornitori dei sistemi di intelligenza artificiale quanto agli utenti (in modo particolare all'amministrazione federale). In argomento le riflessioni di E. CARLONI, *Il sentiero si fa camminando: la strategia statunitense per intelligenze artificiali sicure ed affidabili*, in *Giornale di diritto amministrativo*, 2024, p. 135 ss.

[4] Tre, in verità, sono gli approcci regolatori, essendosi successivamente aggiunta anche l'impostazione cinese. Si vedano al riguardo G. RESTA, *Cosa c'è di "europeo" nella Proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il Diritto dell'informazione e dell'informatica*, 2022, p. 323 ss.; D. CLEMENTI, *Generare e non creare? Spunti per una comparazione sulla regolazione dell'intelligenza artificiale generativa tra Stati Uniti, Repubblica Popolare Cinese e Unione Europea*, in *RDC*, 2024, p. 371 ss.; L. PARONA, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici, "soft law" e "self regulation"*, in *RRM*, 2020, p. 70 ss.

[5] É di recente pubblicazione, il libro di Alexander Karp, imprenditore dell'AI, in cui gli autori riaffermano l'idea che l'intelligenza artificiale è un'attività privata che lo Stato non deve intromettersi pena perdere la battaglia con la Cina. A. C. KARP, N. W. ZAMISKA, *The Technological Republic, Hard Power, Soft Belief, and the Future of the West*, New York, 2025.

Personalmente ritengo che la tutela dei diritti non possa essere mai catalogata come ostacolo allo sviluppo tecnologico. La tutela dei diritti di fronte a poteri tecnologici di elevatissima capacità è piuttosto un *dovere* della società organizzata, per non lasciare il singolo da solo in una lotta impari.

Non si può tentare di incrinare la tutela dei diritti fondamentali (come la *privacy,* ma non solo) di fronte alla necessità di sviluppo: è un non argomento, un falso *trade-off*, che può celare interessi di natura diversa (non a caso sono gli imprenditori a sostenerla in maggior misura). Di contro, come in più occasioni ricordato dal Garante europeo, il rispetto del diritto alla *privacy* (e direi in generale il rispetto dei diritti fondamentali) è l'unico modo per giungere all'uso civilizzato di tali strumenti[6].

La strada della regolazione per tutelare i diritti fondamentali, lo ricordavo poc'anzi, è stata la strada che da subito ha voluto seguire l'Unione europea come è emerso con evidenza sin dal Libro bianco sull'intelligenza artificiale del 2019[7]. Va detto, per inciso, che l'obiettivo di garantire la tutela dei diritti degli individui e dunque, regolare l'intelligenza artificiale affinché questa potesse essere affidabile non è stato l'unico (seppur è stato il principale) motore per una regolazione europea.

La rincorsa a un nuovo "*Brussels effect*"[8] è stata mossa dalla volontà dell'Unione di posizionarsi nello scenario internazionale dell'intelligenza artificiale, dove gli interessi economici sono fortissimi, ma dove l'Unione europea è in difficoltà a raggiungere una posizione di supremazia per quanto riguarda gli avanzamenti scientifici e la produzione. La scelta è stata quindi di puntare ad una sovranità digitale *regolatoria*. Ne è nato, dopo una

---

[6] Osservatorio sullo Stato digitale, B. CAROTTI, *Nulla di nuovo sul fronte artificiale: ChatGPT e gli altri*, in *Osservatorio sullo Stato Digitale*, 10 maggio 2023.

[7] Commissione europea, Un approccio europeo all'eccellenza e alla fiducia, comunicazione COM (2020) 65final. In argomento sia consentito il rinvio a S. DEL GATTO, *Una regolazione europea dell'AI come veicolo di eccellenza e affidabilità. Gli obiettivi del Libro bianco della Commissione europea sull'intelligenza artificiale*, in *Osservatorio sullo Stato Digitale*, 28 aprile 2020.

[8] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, New York, 2020.

lunga gestazione, l'*AI Act*[9], avendo a mente il quale vorrei soffermarmi su tre profili che mi pare intersechino il tema oggetto di questa prima sessione. In primo luogo, l'efficacia delle soluzioni adottate dal regolamento sull'intelligenza artificiale per gestire il problema "tempo" e garantire la certezza del diritto senza sacrificare la necessaria flessibilità della regolazione; in secondo luogo, l'efficacia delle soluzioni adottate dall'*AI Act* per tutelare i diritti fondamentali. In terzo e ultimo luogo, l'effettiva utilità del coinvolgimento umano: è davvero possibile un'IA antropocentrica?

2. *Il bilanciamento tra certezza del diritto e flessibilità nell'approccio regolatorio*

Partiamo dal primo problema che tocca il bilanciamento tra certezza del diritto e flessibilità, ma anche si aggiunge, tra strumenti regolatori tradizionali e strumenti di regolazione innovativi c.d. flessibili capaci di dar vita a regole *future proof*. Perché questo problema? Per una questione di tempo. Il tempo è centrale nel dilemma sul regolare o meno l'IA e sul come regolarla. Quando si tratta di regolare le nuove tecnologie l'estrema velocità dei cambiamenti spariglia le carte della regolazione tradizionale. Non è chiaro a monte *quando* intervenire: mentre all'inizio del processo di evoluzione di un fenomeno tecnologico non sono esattamente conosciuti i suoi effettivi impatti, in termini di rischi e opportunità, cosicché regole nuove sarebbero espressione di approssimazione e inconsapevolezza, all'opposto, quando la tecnologia già si è diffusa l'introduzione di discipline più o meno vincolanti, può diventare molto

[9] 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, *AI Act*). In argomento la dottrina è ormai molto vasta. Senza pretesa di completezza, si rinvia a B. CAROTTI, *Le finzioni dell'intelligenza senza corpo, o dell'"AI Act"*, in *Giornale di diritto amministrativo*, 2025, p. 31 ss.

oneroso per le imprese che devono adeguarvisi "in corsa", e persino inefficace[10].

Vi è un "divario di ritmo" tra la natura lenta della regolamentazione e la velocità del cambiamento tecnologico. Sussiste inoltre, una rilevante asimmetria informativa tra regolatori e regolati aggravata alla riluttanza delle imprese a divulgare informazioni rilevanti. Ce lo ha spiegato la dottoressa Pandolfi nella sua esposizione pocanzi.

Per risolvere questi problemi nell'*AI Act* sono state introdotte le c.d. *sandboxes* regolatorie (a cui accenna Pandolfi nel suo *paper* sul *pacing problem*). La locuzione è evocativa dello spazio di sabbia protetto nel quale i bambini possono giocare e imparare in sicurezza e la metafora può dirsi effettivamente riuscita. Senza addentrarsi in una disamina delle *sandboxes* ci si limita a ricordare che la *regulatory sandbox* può essere descritta come uno spazio di "sperimentazione normativa" che consente agli operatori interessati di testare le innovazioni tecnologiche, in un ambiente reale, ma con due sostanziali peculiarità: beneficiando di deroghe temporanee alla disciplina cui sarebbero sottoposte tali attività e restando sotto la supervisione dell'autorità competente per il settore[11].

Le *regulatory sandbox* quindi, in effetti, risolvono alcuni problemi delle tradizionali forme regolatorie consentendo al regolatore di venire in possesso della conoscenza, delle informazioni e dei dati utili a elaborare regole resilienti ed efficaci rispetto alla specifica tecnologia in questione; d'altro canto, offrendo alle imprese la possibilità di provare le innovazioni, prima di immetterle sul mercato. Vi sono però dei profili critici su cui il *paper* poc'anzi richiamato, in particolare, dovrebbe concentrarsi, a partire dal fatto che manca una definizione univoca di tale istituto nella normativa

---

[10] Sui profili giuridici del problematico rapporto tra diritto "tartaruga" e sviluppo tecnologico "lepre" si veda F. LAVIOLA, *Regolazione della tecnologia e dimensione del tempo*, in *OSF*, 2021, p. 1163 ss.

[11] G. LO SAPIO, *Il regolatore alle prese con le tecnologie emergenti. La regulatory sandbox tra principi dell'attività amministrativa e rischio di illusione normativa*, in *federalismi.it*, 2022, p. 88 ss.; M. TRAPANI, *L'utilizzo delle sandboxes normative: una ricognizione comparata delle principali esperienze di tecniche di produzione normativa sperimentali e il loro impatto sull'ordinamento*, in *OSF*, 2022, p. 215 ss.

e ciò sta generando molta confusione. Andrebbero quindi analizzate le diverse discipline ed esperienze a partire da quella italiana.

Nonostante i vantaggi, poi la stretta collaborazione tra regolatori e regolati (che ha portato a parlare di co-regolazione[12], altro profilo che suggerirei di approfondire nella versione definitiva di alcuni *paper* ora in discussione), può generare la cattura dei regolatori e creare effetti di "porta girevole".

Restando sul tema delle forme di regolazione alternative a quelle tradizionali, andrebbero poi indagate le regolazioni che spontaneamente nascono tra imprese e che determinano modifiche molto interessanti nei comportamenti delle grandi piattaforme (pensiamo all'acquisizione dei dati per l'addestramento. Sempre più frequentemente, anche in assenza di obblighi legali, le piattaforme stanno stringendo accordi e contratti con organizzazione ed aziende – ad esempio Bloomberg e Reuters – che prevedono l'accesso ai dati e agli archivi dietro pagamento)[13]. Come cambiano i comportamenti delle piattaforme di fronte alle lacune normative o alla lentezza normativa?

3. *L'efficacia delle soluzioni adottate dall'AI Act per la tutela dei diritti fondamentali*

Passiamo al secondo profilo, quello dell'efficacia dell'*AI Act* nel tutelare i diritti fondamentali. L'*AI Act* a ben vedere presenta una doppia anima: innovativa e allo stesso tempo tradizionale. Come osservato, la sfida di governare l'ultimo ritrovato della tecnica, infatti, si inserisce nel più classico degli strumenti dell'integrazione europea: le disposizioni relative al funzionamento del mercato unico. Una scelta di peso, ma controversa;

---

[12] Su cui si rinvia a A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, in *RTDP*, 2022, p. 1031 ss.

[13] Su cui si rimanda alle osservazioni svolte da L. TORCHIA, *Regolazione e innovazione nel mondo digitale: un equilibrio dinamico,* in *Osservatorio sullo Stato Digitale*, 3 giugno 2024.

una decisione sui valori, che però poggia su basi di mercato con alcune inevitabili conseguenze in tema di tutela dei diritti[14].

Secondo la logica *risk-based* alla base del regolamento[15], la protezione dei diritti fondamentali sembra seguire in effetti gli stessi metodi di valutazione del rischio utilizzati per la sicurezza dei prodotti (con tutte le storture che ne derivano) piuttosto che rappresentare un limite invalicabile per l'impiego di strumenti di IA potenzialmente nocivi.

L'ottica della c.d. "accettabilità del rischio" che permea la struttura dell'*AI Act* si discosta decisamente dalle aspirazioni e dall'impostazione perseguita dal GDPR, all'interno del quale i diritti fondamentali ricoprono una posizione a mio avviso più centrale.

Un altro timore concerne poi la formulazione di alcune disposizioni che riguardano i sistemi di IA ad alto rischio, che mi pare troppo ampia e astratta, soprattutto se paragonata alla sintassi e al lessico adoperati nella stesura del GDPR. Si pensi al caso del riconoscimento facciale[16].

Sia chiaro, nel complesso, il bilancio può dirsi chiuso in positivo, vi sono però accanto a tante luci alcune ombre di cui tenere conto nelle riflessioni che condurranno alla versione definitiva di alcuni dei *paper* oggetto di questa sessione.

4. *L'effettiva utilità del coinvolgimento umano: il dibattito sulla c.d. riserva di umanità*

Terza e ultima questione. Restando in tema di garanzie per i diritti fondamentali e di tutela del cittadino-utente, mi vorrei concentrare sulla c.d. riserva di umanità o *human in the loop*[17] tema che ricorre in molti *paper*. Il

---

[14] B. CAROTTI, *Punti di vista: l'AI Act*, *ivi*, 25 novembre 2024.

[15] Per cui si veda *ex multis* L. TORCHIA, *Lo Stato digitale. Un'introduzione*, Bologna, 2025.

[16] Su cui sia consentito il rinvio a S. DEL GATTO, *La "governance" delle nuove tecnologie tra tentativi di regolazione e istanze di "self regulation"*, cit., 2023, p. 37 ss.

[17] Il coinvolgimento dell'essere umano, c.d. *human in the loop*, pur non sufficiente è considerato elemento necessario per la legittimità dell'utilizzo di *software* di riconoscimento facciale da parte dei pubblici poteri. Per una definizione di *human in the loop* si vedano gli orientamenti etici per un'intelligenza artificiale affidabile elaborati dal

necessario intervento umano è notoriamente uno dei pilastri originari e mai contestati della strategia regolatoria dell'UE in materia di intelligenza artificiale. Sin dal libro bianco del 2019 prima citato si è parlato di intelligenza artificiale antropocentrica (oltre che affidabile). Ma quanto è efficace questa garanzia ad esempio, quando sono i pubblici poteri che usano gli algoritmi nell'attività decisionale (si pensi a un'amministrazione o a un giudice)?

La risposta cambia ovviamente a seconda che si faccia riferimento all'uso strumentale o all'uso decisorio dell'algoritmo, e soprattutto cambia a seconda che si tratti di algoritmi *model based*, o di algoritmi *machine learning* capaci cioè di auto apprendere e di adottare decisioni in autonomia. Mentre nel primo caso non si creano (salvo quanto si dirà) particolari problemi nel secondo caso le possibilità che l'agente possa effettivamente controllare gli esiti del funzionamento dell'algoritmo ed eventualmente individuarne gli errori sono molto ridotte per varie ragioni[18].

In primo luogo, l'opacità di questi algoritmi. Il Consiglio di Stato ha affermato che quando la p.a. utilizza *software* che influenzano la decisione, per ovviare alla mancanza di altre garanzie è necessario garantire un principio di trasparenza rafforzata[19], ma è difficile immaginare che oltre alla c.d. "*fishbowl transparency*", ovvero la capacità degli interessati di poter osservare le modalità con cui l'amministrazione agisce, ottenendo le indicazioni utili tramite l'esercizio del diritto di accesso a dati, documenti e informazioni, possa essere garantita anche la c.d. "*reasoned transparency*" che concerne invece, la comprensione della logica che muove l'azione e le decisioni dell'amministrazione. Ma solo questo tipo di trasparenza, a mio avviso, può garantire una effettiva forma di controllo sull'operato

---

gruppo di esperti ad alto livello sull'intelligenza artificiale, pubblicati nell'aprile del 2019 e posti a fondamento prima del Libro Bianco sull'AI e poi dell'*AI Act*. In argomento ampiamente G. GALLONE, *Riserva di umanità e funzioni amministrative*, Padova, 2023, *passim.*

[18] Per una maggior dettaglio si rinvia a S. DEL GATTO, *Nuove tecnologie, pubblica amministrazione e rapporto con gli amministrati. Brevi note sulle tendenze in atto*, in *Diritto pubblico*, 2025, p. 155 ss.

[19] Cons. Stato 8 aprile 2019, n. 2270; Cons. Stato 13 dicembre 2019, n. 8472.

dell'amministrazione e dunque garantire la tutela dei diritti dei soggetti coinvolti.

È stato poi osservato, richiamando alcuni studi di psicologia comportamentale, che esiste nel rapporto tra umano e macchina un *anchoring effect* dovuto al forte condizionamento esercitato dalla macchina sull'umano. Sempre dagli studi condotti da alcuni psicologi risulta che una persona sia portata nell'88% dei casi a rimanere della propria opinione se si confronta con un'altra persona, e invece a mutarla più facilmente (la percentuale scende di oltre il 20%) se a pensarla diversamente è un sistema di intelligenza artificiale[20]. Questi dati peraltro sollevano preoccupazioni anche con riferimento ai sistemi *model based,* oltre che rafforzare i timori nel caso di uso di algoritmi *machine learning*[21].

C'è poi un secondo problema che ha a che vedere con la circostanza che le pubbliche amministrazioni generalmente esternalizzano a soggetti privati la costruzione dei sistemi di IA utilizzati, sicché, rispetto alla macchina, occorre domandarsi chi sia – tra il funzionario amministrativo e il costruttore del codice sorgente – l'umano che deve mantenere il controllo sul funzionamento del procedimento[22].

Infine, nell'ambito delle pubbliche amministrazioni, quando un funzionario è chiamato a controllare la correttezza della decisione

---

[20] Così B. MARCHETTI, *La garanzia dello Human in the loop alla prova della decisione amministrativa algoritmica*, in *Biolaw Journal*, 2021, p. 367 ss.

[21] In argomento I. M. DELGADO, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Istituzioni del federalismo*, 2019, p. 643 ss. Come osservato dall'A. con riferimento ai sistemi di auto-apprendimento «[i]l *machine learning* possiede tre note caratteristiche che lo distinguono da altri tipi di tecniche: è basato sull'uso di algoritmi che imparano autonomamente, questi algoritmi hanno natura di *black box* e il sistema ha la capacità di produrre risultati che potrebbero potenzialmente superare la previsione umana. La prima attiene alla "spiegabilità": se le informazioni si trasformano in predizioni attraverso una *black box* in un modo che non è pienamente conoscibile, come motivare il provvedimento? […]». Sul problema della trasparenza nei sistemi di AI e su possibili soluzioni anche alla luce dei principi del nuovo Codice dei Contratti pubblici si rimanda a E. CARLONI, *Transparency within the artificial administration, principles, paths, perspectives and problems*, in *Italian Journal of Public Law*, 2024, p. 8 ss.

[22] Su questi problemi più ampiamente quanto scritto in S. DEL GATTO, *Nuove tecnologie,* cit., p. 155 ss.

algoritmica, per il principio/garanzia dello HITL, occorre riflettere sul tipo di competenze necessarie, competenze di cui la pubblica amministrazione difetta. Bisogna quindi ripensare in primo luogo le procedure di reclutamento nelle pubbliche amministrazioni e in secondo luogo investire in formazione[23].

5. *Osservazioni conclusive*

Poiché il mio tempo si sta per esaurire vorrei concludere con alcune considerazioni più puntuali su alcuni *paper*. Partiamo da quello del dott. Vaira. Il *paper* tocca diversi temi, dalle infrastrutture strategiche, alla *cybersicurezza* e nuove minacce e della relazione tra più stringenti esigenze di sicurezza e tutela del libero mercato. Mi limito a due suggerimenti, uno su *cybersecurity* e uno sul bilanciamento tra sicurezza e libero mercato. Sul tema della cybersicurezza mi limito a osservare che profili da indagare maggiormente sono quelli relativi alla collaborazione pubblico-privato e alla collaborazione tra istituzioni rispetto ai quali la normativa italiana e la direttiva europea che ne è a monte testimoniano un costante rafforzamento. Da un lato, vengono aumentate le forme di collaborazione reciproca, lo scambio di informazioni e le risposte coordinate; dall'altro, sul versante organizzativo, si introduce un sistema reticolare, che pure andrebbe studiato.

Sul profilo del rischio di effetti protezionistici conseguenti al rafforzamento delle norme sulla sicurezza *cyber,* la domanda sottesa al *paper* mi pare riguardi in sostanza come conciliare le garanzie di sicurezza con l'apertura di mercato. Qui vanno in primo luogo studiati e paragonati i diversi approcci normativi. A livello europeo, la strategia per la sicurezza informatica si basa su un equilibrio tra protezionismo strategico e apertura al mercato globale, come dimostrato dall'approccio adottato nel

[23] Sul problema della mancanza di competenza digitali nelle pubbliche amministrazioni cfr. F. DE LEONARDIS, *Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione*, in E. CALZOLAIO (a cura di) *La decisione nel prisma dell'intelligenza artificiale*, Padova, 2020, p. 137 ss.

Cybersecurity Act e nelle direttive NIS2, che pongono l'accento sulla certificazione dei prodotti senza introdurre vincoli di natura protezionistica. Guardando agli ordinamenti nazionali, invece la Francia è molto chiusa mentre l'Italia con la legge 90/2024 ha adottato una soluzione di mezzo abbastanza aperta ma comunque prudente e lo ha fatto attraverso l'introduzione di criteri di premialità per le tecnologie di cybersicurezza sviluppate in Italia o in ambito europeo e NATO. Sempre con riferimento a questo profilo, in Italia è importante vedere l'esperienza del Polo Strategico Nazionale che mi pare una soluzione all'avanguardia e da assurgere a modello.

Sul profilo più strettamente legato al *golden power* e agli investimenti esteri[24] diretti la tendenza che si registra è senza dubbio quella, evidenziata nel *paper* del rischio di un sempre maggiore protezionismo tecnologico, con diverse implicazioni di carattere giuridico. Qui a mio avviso va fatto un ragionamento sulle linee di cambiamento: è evidente mi pare, che la centralità delle tecnologie renderà sempre più anacronistica l'originaria individuazione dei settori strategici. Un primo segnale lo si ebbe già nel 2017 del resto. Questo perché una certa tecnologia, un particolare brevetto o *know-how*, determinati patrimoni informativi, potranno essere presenti in modo trasversale nei diversi settori. Due casi recenti confermano tale rilevanza: la vicenda Pirelli e il caso Verisem-Syngenta dove la strategicità delle società è stata rinvenuta non tanto nella "produzione *core*" quanto nello sviluppo da parte delle stesse società della particolare tecnologia dei sensori *cyber* e del patrimonio informativo, del *know-how* e delle tecnologie detenute dalle due società italiane.

Veniamo infine al *paper* sul *social scoring* della dott.ssa Perlot rispetto al quale comunque rileva già quanto detto a proposito dell'intervento umano e della capacità o meno di saper individuare errori e pregiudizi nelle

---

[24] Su cui senza pretesa di completezza si rinvia a S. CASSESE, *Il controllo degli investimenti esteri*, in *Giornale di diritto amministrativo*, 2025, p. 11 ss.; M. CLARICH, *Concorrenza, regolazione e intervento dello Stato nell'economia*, in *Riv. interd. dir. amm. pubbl.*, 2023, p. 123 ss.; S. DI NITTO, *Il "golden power" nei settori rilevanti della difesa e della sicurezza nazionale: alla ricerca di un delicato equilibrio*, in *Diritto amministrativo*, 2022, p. 553 ss.

decisioni amministrative algoritmiche. Questi sistemi operano in base a meccanismi di punizione e di ricompensa o indici di punteggio, legati ad entrambi[25].

In Italia troviamo i secondi e sarebbe utile tenerne conto nella versione definitiva del lavoro. Si tratta di meccanismi di reputazione che si pongono come sistemi di incentivazione dei cittadini all'adozione di comportamenti virtuosi. Si viene a configurare una sorta di «cittadinanza a punti», anche qui però con conseguenze giuridiche su diritti e le libertà degli interessati, inclusi i soggetti più vulnerabili che andrebbero approfondite. L'altro profilo su cui mi concentrerei nel discutere delle garanzie per i diritti, riguarda l'efficacia del meccanismo/garanzia del consenso su cui ho molte perplessità. Due in particolare i rilievi. Primo: lasciando da parte i sistemi totalitaristici come quello cinese, i problemi sottesi al *social scoring* si pongono anche nei casi di adesione volontaria, come nei casi italiani. La prospettiva di un premio, anche modesto, favorisce la prestazione del consenso a profilazioni anche molto penetranti. Secondo: appare illusorio di fronte a sistemi che mirano a coinvolgere categorie intere di soggetti (per cui la decisione di non partecipare potrebbe essere fonte di pregiudizi, o che propongono premi ed incentivi) parlare di consenso liberamente dato. E ancor più quando il consenso è chiesto da una pubblica amministrazione, considerata l'asimmetria di posizione e lo squilibrio tra p.a. e amministrato, la richiesta del consenso appare come un'opzione *opt out* che presenta numerose criticità[26] e non può assolutamente essere vista, a mio avviso, come una garanzia efficace ed effettiva.

---

[25] Sul tema G. CERRINA FERONI, *Intelligenza artificiale e sistemi di "scoring" sociale. Tra distopia e realtà,* in *Il Diritto dell'informazione e dell'informatica*, 2023, p. 1 ss.; G. SCIASCIA, *Reputazione e potere: il "social scoring" tra distopia e realtà*, in *Giornale di diritto amministrativo*, 2021, p. 317 ss.

[26] Su questi profili e su esperienze che evidenziano siffatta problematica con riferimento al rapporto tra pubblica amministrazione e amministrati si rinvia a S. DEL GATTO, *La "governance" delle nuove tecnologie*, cit., p. 37 ss.

ABSTRACT (ITA)

Lo scritto frutto dell'elaborazione della Relazione svolta in qualità di *discussant* del *Panel 1 – IA e tutela dei diritti* nell'ambito del Convegno "Intelligenza artificiale e nuove vulnerabilità: dal diritto europeo della concorrenza e della proprietà intellettuale alla tutela dei diritti fondamentali", Macerata, 8-9 maggio 2025 mira a indagare i profili della governance dell'intelligenza artificiale e gli effetti che l'utilizzo da parte dei pubblici poteri delle nuove tecnologie e di software di IA può avere sui diritti e sulle libertà fondamentali.

ABSTRACT (ENG)

The paper is the result of the report presented at the conference "Artificial intelligence and new vulnerabilities: from European competition and intellectual property law to the protection of fundamental rights," Macerata, May 8-9, 2025. It aims to investigate the governance of artificial intelligence and the effects that the use of new technologies and AI software by public authorities can have on fundamental rights and freedoms.