UNIVERSITÀ DEGLI STUDI DI TRIESTE

UNIVERSITÀ DEGLI STUDI DI TRIESTE

XXXVIII CICLO DEL DOTTORATO DI RICERCA IN

APPLIED DATA SCIENCE AND ARTIFICIAL INTELLIGENCE

Finanziato dall'Unione europea - NextGenerationEU
Funded by the European Union - NextGenerationEU

La nuova governance della pubblica amministrazione nell'età dell'intelligenza artificiale

Settore scientifico-disciplinare: **IUS/10**

DOTTORANDO
LUCA PELLIZZONI

COORDINATORE
PROF. FRACESCO PAULI

SUPERVISORE DI TESI
PROF. DOMENICO DE STEFANO

CO-SUPERVISORE DI TESI
PROF. ANDREA CRISMANI

ANNO ACCADEMICO 2024/2025

Vis mentis imperat

Sommario

INTRODUZIONE 1

1. La dimensione tecnica nell'organizzazione amministrativa 1

2. L'intelligenza artificiale, nuova frontiera 4

3. I fattori condizionanti l'innovaizone: note sul metodo della ricerca 7

CAPITOLO I

FONDAMENTI TEORICI: UNA RICOSTRUZIONE 9

1. Introduzione 9

2. La *governance* nel contesto digitale 10
   2.1. *New Public Management* e le riforme amministrative degli anni Novanta del secolo scorso 10
   2.2. Digitalizzazione e regolazione: limiti delle categorie tradizionali alla luce delle nuove esigenze di *governance* 15

3. La sovranità dello spazio digitale 20

4. La costruzione di un fondamento giuridico per l'utilizzo delle nuove tecnologie quale presupposto per la *governance* 26
   4.1. Nuove tecnologie e principio di legalità: questioni introduttive 26
   4.2. Algortimo, intelligenza artificiale, *software*: alcune nozioni 29
   4.3. Le ricostruzioni concettuali nelle decisioni del giudice amministrativo 31
   4.4. I principi e i limiti per l'impiego dell'intelligenza artificiale nella pubblica amministrazione 36
   4.5. La base giuridica per l'uso dell'intelligenza artificiale da parte della pubblica amministrazione 42

5. Dati e intelligenza artificiale 45

CAPITOLO II

IL SISTEMA DI *GOVERNANCE* DELL'INTELLIGENZA ARTIFICIALE TRA ORGANISMI GLOBALI, ISTITUZIONI EUROPEE E AUTORITÀ NAZIONALI 51

1. Introduzione 51

2. Il quadro regolatorio delle nuove tecnologie: il *New Artificial Intelligence Advisory Board* delle Nazioni Unite 52

3. L'Unione europea traccia una cornice normativa 54

4. Gli strumenti di *governance* dell'*Artificial Intelligence Act* 60
   4.1. Definizione e classificazione dei sistemi di intelligenza artificiale 60
   4.2. La disciplina per i *general-purpose AI models* 63
   4.3. Gli organisimi europei per l'attuazione dell'*AI Act* 66
   4.4. La desginazione delle autorità nazionali per la vigilanza 70

5. Lo strumento dell'agenzia per vigilare sull'intelligenza artificiale: il requisito dell'indipendenza 73

6. La soluzione nazionale: l'Agenzia per l'Italia Digitale e l'Agenzia per la Cybersicurezza.....

Nazionale, quali autorità designate ai sense dell'*AI Act* 76

7. Il modello della Spagna: l'Agenzia di supervisione dell'Intelligenza Artificiale 84

8. Il ruolo dello Stato nell'ecosistema dell'*AI Act* 88

CAPITOLO III

INFRASTRUTTURE DIGITALI STRATEGICHE NAZIONALI 91

1. Introduzione 91

2. Il *cloud* nella pubblica amministrazione 94
   2.1. Contesto normativo e nozione di *cloud* 94
   2.2. La Strategia *Cloud* Italia 98

3. Gli investimenti per innovare la pubblica amministrazione 94
   3.1. Il *cloud first* come paradigma della trasformazione digitale 102
   3.2. La dimensione dell'investimento nei Comuni italiani: un'analisi a partire dai dati. 105
   3.3. I fattori condizionanti l'adozione del *cloud* 111

4. *Cloud* e sovranità digitale 112

5. L'architettura normativa in materia di cybersicurezza 116
   5.1. Le direttive europee e le leggi italiane per l'istituzione e il governo dello spazio cibernetico ..... sicuro 116
   5.2. La *governance* della cybersicurezza: il ruolo del Presidente del Consiglio dei ministri 120
   5.3. Similitudini e differenze dell'ACN con le altre agenzie presenti nell'ordinamento italiano 126
   5.4. Le funzioni dell'Agenzia per la Cybersicurezza Nazionale e i riflessi sulla gestione del *cloud* ... 127

6. La riorganizzazione degli uffici pubblici per la sicurezza dell'ambiente digitale 130

7. Il legame tra *cloud*, cybersicurezza e intelligenza artificiale 134

CAPITOLO IV

L'INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE 138

1. Introduzione 138

2. Quale intelligenza artificiale? 140
   2.1. Le diverse soluzioni possibili 140
   2.2. Un confronto tra *generative AI models* o *knowledge-based systems* 143
   2.3. *Generative AI models* o *Knowledge-based systems* nel dominio legale 147

3. L'automazione dell'attività amministrativa: considerazioni sul procedimento algoritmico 149

4. Una nuova prospettiva dell'algortimo nella pubblica amministrazione 156
   4.1. L'algortimo come atto di organizzazione 156
   4.2. L'atto organizzativo come insieme di istruzioni: un esperimento 158

5. L'organizzazione e la necessità di nuove figure professionali per la pubblica amministrazione 169

6. La responsabilità amministrativo-contabile del dipendente pubblico tra protezione dei dati personali e intelligenza artificiale 173

CONCLUSIONI 179

BIBLIOGRAFIA 184

INTRODUZIONE

1. La dimensione tecnica nell'organizzazione amministrativa.

Nel 1979 Massimo Severo Giannini presentava al Parlamento il Rapporto[1] sull'amministrazione dello Stato nel quale fotografava i principali problemi che interessavano le pubbliche amministrazioni, sia sotto il profilo organizzativo sia sotto il profilo tecnologico. Giannini osservava che i problemi generali relativi alla tecnologia era riducibili a due aspetti, gli ambienti di lavoro e l'attività informatica, evidenziando l'impreparazione delle amministrazioni al progresso tecnologico che aveva visto gli elaboratori elettronici passare dall'essere semplici apparecchi di registrazione di dati a complessi «apparecchi di accertamento e verificazione, di calcolo, di partecipazione a fasi procedimentali di istruttoria, e infine di decisione»[2]. Tale cambiamento richiedeva la disponibilità di competenze tecniche, presenti solo in poche amministrazioni, anche in ragione del fatto che i sistemi informativi non servivano più alle amministrazioni per la gestione interna, ma anche per amministrare.

Il rapporto Giannini anticipava di quasi mezzo secolo la trasformazione digitale delle amministrazioni pubbliche sotto il profilo sia dell'attività sia dell'organizzazione, avvenuta solamente in anni recenti. Dalla metà degli anni Novanta del secolo scorso alla fine degli anni Dieci del XXI secolo, la pubblica amministrazione è stata interessata dall'introduzione e dell'impiego di nuove tecniche, chiamate digitali, in maniera massiccia, tali da trasformarne il funzionamento[3], ma solo più di recente si è in effetti assistito ad un'innovazione tale da spostare la concezione della tecnica, quale semplice strumentazione operativa al servizio dell'apparato, ad un elemento strutturale dell'organizzazione stessa.

Giannini vedeva inoltre nel legislatore l'attuatore di questa evoluzione dell'amministrazione, invitando il Parlamento ad intervenire, come effettivamente avvenuto a partire dagli anni Novanta attraverso diverse riforme e, da ultimo, grazie agli

[1] M.S. Giannini, *Rapporto sui principali problemi dell'amministrazione dello Stato*, 1979.
[2] M.S. Giannini, *op. cit.*, p. 10.
[3] V. Cerulli Irelli, *La tecnificazione*, in L. Ferrara, D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana*, Vol. IV, S. C. Matteucci, L. Torchia (a cura di), *La tecnificazione*, Firenze University Press, 2016, p. 280.

investimenti del Piano Nazionale di Ripresa e Resilienza[4], che hanno determinato uno sviluppo duale, sia tecnologico sia normativo.

Per quanto attiene al piano tecnico, questa evoluzione vede interessati strumenti nuovi per le amministrazioni, dal *cloud*, alla cybersicurezza, all'intelligenza artificiale, unitamente all'introduzione di una disciplina dedicata, dalla l. 28 giugno 2024 n. 90, in materia di sicurezza cibernetica, alla l. 23 settembre 2025 n. 132 sull'intelligenza artificiale, accanto a linee guida e regole tecniche.

La tecnologia acquisisce quindi una funzione sempre più centrale e una rilevanza autonoma all'interno delle amministrazioni pubbliche, tale da palesare il rischio di un passaggio alla tecnocrazia, intesa quale spossessamento del potere tradizionale, ad opera dei tecnici[5], prevalentemente privati. Questo processo pone inevitabilmente alcuni interrogativi, a cominciare dalla considerazione che la tecnica non è neutra, ma configura essa stessa una specifica forma di potere, potenzialmente capace di influenzare la discrezionalità amministrativa, in un contesto storico dominato dalla presenza in ogni ambito della società delle grandi piattaforme digitali.

L'assetto costituzionale sembra ancora preservare in ogni caso l'organizzazione amministrativa dal rischio di una completa privatizzazione o tecnificazione, almeno in quanto l'art. 28 Cost. impone il principio di immedesimazione organica, per cui la persona deve rispondere delle decisioni[6]. Nondimeno, vi è un processo modificativo dell'amministrazione quale "piattaforma" caratterizzata da elevata tecnificazione, in cui emerge la convinzione che l'innovazione obblighi ad una rivisitazione delle categorie giuridiche[7].

Da queste premesse, il primo capitolo si sofferma sulle teorie della *governance* elaborate nell'ultimo decennio del Novecento, quale parametro di riferimento dell'analisi sviluppata nelle successive parti del presente lavoro. Gli sviluppi sia giurisprudenziali sia legislativi mostrano infatti come la regolazione, in particolare dell'intelligenza artificiale, sia fondata su quelle teorie, tra cui spicca il *New Public Management*. Comprendere i percorsi normativi verso la regolamentazione della tecnologia per la pubblica amministrazione non può prescindere dalle basi culturali in cui si collocano.

---

[4] L. Torchia, *Pubblica amministrazione e transizione digitale*, in *Gior. dir. amm.*, 6, 2024, p. 729.
[5] A. Di Martino, *Tecnica e potere nell'amministrazione per algoritmi*, Ed. Scientifica, Napoli, 2023, p. 23
[6] E. Picozza, *Politica, diritto amministrativo and Artificial Intelligence*, in *Giur. it.*, 7, 2019, p. 1765.
[7] R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm*, 2, 2020, p. 305.

Nel solco della ricostruzione operata nel primo capitolo, viene quindi analizzata nel capitolo 2 la *governance* istituita dall'*Artificial Intelligence Act*, primo regolamento europeo a disciplinare l'intelligenza artificiale, così come gli approcci decisi dal legislatore nazionale nel definire le strutture chiamate a vigilare sull'implementazione e l'uso di questa tecnologia, evidenziando come vi sia una duplice intenzione, da un lato la regolazione, dall'altro la responsabilizzazione, anche attraverso atti programmatici.

L'esperienza italiana, analizzata in particolare in parte nel capitolo 2 e soprattutto nel capitolo 3, mostra infatti un percorso evolutivo della regolazione che va dal Codice dell'Amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82), alle linee guida dell'Agenzia per l'Italia Digitale, ai piani triennali per l'informatica, per l'intelligenza artificiale, la Strategia *cloud* Italia, per menzionarne alcuni. L'insieme di questo testi forma un *corpus* eterogeneo, per certi aspetti anche frammentario, eppure, parte della costruzione del governo delle tecnologie.

Le ragioni della ricerca possono quindi essere sinteticamente spiegate con le parole di Giannini, secondo il quale «la problematica giuridica varia nel tempo a seconda delle sollecitazioni che gli istituti giuridici ricevono dalla realtà sociale»[8]. È indubbio che le sollecitazioni preminenti negli ultimi anni arrivano dal settore tecnologico, la cui complessità ha portato, da un lato, ad uno spostamento della produzione delle regole dalle fonti enunciate in Costituzione, verso altri atti estranei al sistema delle fonti, quali linee guida o piani triennali[9]; dall'altro, si assiste alla creazione di nuove strutture, o l'attribuzione di nuove funzioni a quelle esistenti, per soddisfare le esigenze di governo delle nuove tecnologie. Tutto questo presenta elementi di discontinuità per la pubblica amministrazione[10], che richiede quindi uno studio per comprende la prospettiva verso cui sta evolvendo.

[8] M.S. Giannini, *In principio sono le funzioni*, disponibile al seguente link https://www.eticapa.it/eticapa/wp-content/uploads/2017/08/M-S-GIANNINI-In-principio-sono-le-funzioni.pdf.

[9] E. D'Orlando, *Innovazione tecnologica e fonti del diritto*, in J.B. Auby, G. De Minico, G. Orsoni (a cura di), *L'amministrazione digitale. Quotidiana efficienza e intelligenza delle scelte. Atti del Convegno 9-10 maggio 2022*, *Federico II, Napoli*, Napoli, 2023p. 72.

[10] G. Sgueo, *Governare le macchine. Governare con le macchine*, in *Rivista dello Stato digitale*, 1, 2025, p. 40.

2. L'intelligenza artificiale, nuova frontiera.

L'intelligenza artificiale rappresenta oggi la frontiera della trasformazione dell'amministrazione pubblica, il cui impatto non può essere compreso al di fuori di una riflessione più ampia, in virtù della considerazione secondo cui il diritto amministrativo possiede un carattere aperto, ancorato all'interesse pubblico, la cui definizione avviene in relazione al concreto contesto storico[11].

Questa riflessione guida il percorso argomentativo lungo l'intero lavoro, in cui si vuole coniugare un'analisi sia della recente legislazione dedicata a disciplinare i settori tecnologici centrali per le amministrazioni pubbliche, quindi non solo l'intelligenza artificiale, ma anche l'analisi della normativa e dei dati sui finanziamenti destinati ai Comuni per la migrazione al *cloud*, unitamente alla ricostruzione dell'architettura di *governance* della cybersicurezza, che viene svolta nel capitolo tre. L'intento è di mostrare l'eterogeneità dei processi modificativi, in cui nuove attività e nuove esigenze vengono poste alle pubbliche amministrazioni, nel contesto più ampio della transizione digitale, aggiungendo una riflessione sul differente impatto della normativa. Infatti, la combinazione di investimenti pubblici e legislazione si traduce in un differente impatto della tecnologia. In tale senso, l'esempio evidente è il disomogeneo ambito di applicazione della normativa sulla cybersicurezza ai Comuni, ristretta solamente a quelli capoluoghi o con popolazione superiore ai 100.000 abitanti, nonché la lentezza nell'implementazione della migrazione dei dati e servizi verso ambiente *cloud.*

Da ciò deriva un'ulteriore considerazione. Se il *cloud* costituisce in qualche modo la base del sistema, in tanto in quanto consente l'archiviazione dei dati su cui i modelli di IA possono essere addestrati, e anche operare, mentre la cybersicurezza garantisce l'utilizzo di questi sistemi mitigando od impedendo il rischio di compromissione dell'attività dell'ente, in conseguenza di un attacco informatico, quali sono le prospettive di diffusione dell'intelligenza artificiale negli enti pubblici? Quali effetti può avere sull'organizzazione? Alla prima domanda si prova a rispondere alla fine del capitolo terzo, mentre in risposta alla seconda si formula una possibile ipotesi nel capitolo quarto.

[11] A. Scognamiglio, *Rileggendo la voce "interesse" di Cannada Bartoli, qualche riflessione sul metodo*, in *Dir. amm.*, 4, 2022, p. 982.

Le ragioni di questa ricerca risiedono, quindi, nella considerazione che lo studio dell'impatto dell'intelligenza artificiale non può limitarsi all'attività, ma debba riguardare anche l'organizzazione amministrativa, interessata da anni di riduzione delle componenti tecniche al suo interno[12]. L'introduzione dell'IA nei procedimenti e nei processi decisionali accelera e rende esplicita una riflessione sulle conseguenze per le pubbliche amministrazioni, che si producono in primo luogo per effetto di scelte del legislatore preoccupato di definire le strutture per vigilare sui sistemi di IA e quindi di individuare figure esperte. A ciò si aggiunge una riflessione sul fatto che l'intelligenza artificiale si colloca su un terreno delicato, poiché essa non si limita a supportare l'esercizio del potere, ma incide sulla struttura cognitiva della decisione amministrativa. L'impatto delle nuove tecnologie appare essere duplice; da un lato normativo, ovvero la spinta a legiferare per normare un terreno finora senza regole dedicate, se non settoriali, e dall'altro tecnico, ossia gli impulsi modificativi determinati dall'irrompere nelle organizzazioni non di meri attrezzi facilitatori, bensì strumenti determinativi delle scelte organizzative. Anche per queste ragioni l'intelligenza artificiale costituisce una nuova frontiera.

Il nuovo paradigma è l'ecosistema digitale, in cui pubbliche amministrazioni, fornitori e cittadini interagiscono[13] attraverso piattaforme e strumenti digitali. Tuttavia, la realizzazione di questo obiettivo passa necessariamente per fasi; se si vuole usare l'intelligenza artificiale, come evidenziato nella Strategia italiana per l'Intelligenza artificiale, «sarà particolarmente rilevante sviluppare specifiche analisi verticali, come ad esempio la valutazione dell'impatto di tecniche di IA nell'ambito giuridico o in altri ambiti di specifico interesse per la Pubblica Amministrazione»[14]. Tale scelta non è infatti neutra, poiché non è unica la soluzione tecnica, basti pensare, in termini generali, che sono individuabili almeno due categorie di algoritmi già impiegate da alcuni

[12] A. Di Martino, *op. cit.*, p. 240-241.

[13] F. Conte, *La trasformazione digitale della pubblica amministrazione: il processo di transizione verso l'amministrazione algoritmica*, in *Federalismi.it*, 11, 2023, p. 74.

[14] Strategia italiana per l'Intelligenza artificiale 2024-2026, p. 22, in cui inoltre si aggiunge «Le linee guida definiranno altresì i passi metodologici da dispiegare per definire attività progettuali di innovazione nella Pubblica Amministrazione ove siano presenti strumenti di IA, sia in relazione alle questioni tecnologiche (tecnologie, competenze, rischi) sia in relazione alla definizione dei *framework* etici e regolatori. Inoltre, tali linee guida inquadreranno le diverse applicazioni in classi omogene, caratterizzandone gli standard minimi funzionali e i requisiti di interoperabilità, garantendo pertanto la possibilità di dispiegare soluzioni e applicazioni di IA che collochino ciascun cittadino italiano in una relazione con il proprio ente locale del tutto simile a quello di altri cittadini in altre città e regioni del territorio nazionale».

soggetti pubblici[15]: quelli deterministici (o condizionali)[16] e quelli predittivi. I primi sono formati da un codice contenente una serie di regole predeterminate, per cui al verificarsi di determinate condizioni si ha un risultato[17]. Questa caratteristica rendere quindi prevedibile l'*output*, e per tali ragioni tali algoritmi non si discostano dal ragionamento giuridico[18], di tipo sillogistico, per cui data una norma, al verificarsi di un presupposto di fatto, si avrà un effetto. La loro elasticità di impiego ne consente un uso anche in procedure ripetitive, ad esempio per verificare in maniera automatica il contenuto di un'istanza e i requisiti di essa.

Più complesso appare invece l'impiego di algoritmi di tipo predittivo[19], ossia quelli basati sul *machine learning*[20]. Date le loro caratteristiche, cambia completamente l'approccio della pubblica amministrazione all'utilizzo.

Il diritto amministrativo, che ha già progressivamente riconosciuto la necessità di ricorrere a contributi esterni, da quello sociologico a quello economico, adesso è chiamato a ricorre al contributo degli ingegneri e dei matematici, in grado di aiutare i giuristi ad operare in un nuovo contesto connotato dall'utilizzo delle macchine, in cui per poter sottoporre un problema al sistema di IA deve compiere una riduzione logica simbolica affinché possa ottenere una risposta. Il risultato di questa operazione, come è stato osservato, è il "diritto artificiale", ossia il prodotto di un ragionamento «totalmente tecnicizzato»[21]. L'apertura all'analisi in particolare dei *large language models* porta infatti a ripensare in chiave formale il linguaggio giuridico, solitamente connotato da vasta attività ermeneutica, verso una dimensione formalistica. Su questi aspetti si riflette nel capitolo quattro, in cui viene postulata l'incidenza organizzativa dell'IA, non in termini meramente strumentali, ma quale fattore condizionante le scelte di

---

[15] E. Buoso, *Disruptive technologies and public administration: rethinking administrative law for the brave new world?*, in V. Faggiani, F. J. Garrido Carrillo (a cura di), *Avances en el desarrollo de la inteligencia artificial. Principios éticos y democràticos, concreciones normativas en la uniòn europea, y limites para las administraciones pùblicas*, Aranzadi, 2025, p. 228.

[16] Questo gruppo di algoritmi è stato infatti impiegato dal MIUR nella procedura di assegnazione delle sedi di lavoro per i vincitori.

[17] Questa è la definizione classica di algoritmo, v. dopo capitolo 1.

[18] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. inform*., 3, 2021, p. 435.

[19] I modelli predittivi, basati su tecniche di apprendimento automatico, si addestrano su basi di dati e individuano pattern senza una codifica esplicita; sono impiegati per attività più complesse (come la valutazione di rischio o l'analisi di scenari) ma generano un effetto "*black box*", con scarsa trasparenza del procedimento. In questi casi, la decisione automatica può sfuggire al controllo umano e richiedere specifiche misure di supervisione. V. dopo cap. 1, par. 4.2.

[20] Sulle nozioni di *machine learning,* nonché di *deep learning* v. dopo cap. 1, par. 4.

[21] V. Frosini, *Cibernetica diritto e società*, RomaTre Press, 2023, p. 14.

organizzazione, sulla base della possibilità di costruire un dominio della conoscenza in cui il sistema abbia la possibilità di operare, al fine di decidere, o contribuire a, soluzioni necessarie per migliorare la struttura organizzativa. In questi termini il capitolo quattro propone un'idea alternativa, l'algoritmo non come modello organizzativo, bensì come atto di organizzazione, spostando il momento decisorio del dirigente, o dell'organo politico, alla fase di selezione della soluzione tecnica idonea (il sistema di IA o ancora prima l'algoritmo).

3. I fattori condizionanti l'innovazione: note sul metodo della ricerca.

Il presente lavoro si concentra principalmente sull'analisi giuridica, ed in particolare sulla copiosa produzione normativa degli ultimi anni dedicata a disciplinare diversi campi della tecnologia, estendendo la riflessione a considerazioni sulla sovranità digitale, intesa quale potestà dello Stato di definire le regole applicabili nel proprio territorio, ma anche quale alla capacità di uno Stato o di organismo sovranazionale di controllare e regolamentare le infrastrutture digitali e lo sviluppo tecnologico[22].

Il punto di riferimento del lavoro di ricerca è la *governance* intesa come sistema delle regole e delle strutture per governare le tecnologie e la loro diffusione nella pubblica amministrazione. L'interesse è determinato dall'assunto secondo cui specialmente l'intelligenza artificiale costituisca uno strumento di rottura rispetto alla tradizione burocratica dell'amministrazione pubblica.

L'analisi si concentra sui cambiamenti della pubblica amministrazione in ragione della diffusione dell'IA, e delle tecnologie collegate, seguendo, come metodo di riferimento, il *TOE framework*, un modello elaborato per la prima volta da L.G. Tornatzky, M. Fleischer[23], che analizza il contesto tecnologico, quello organizzativo e quello ambientale, per individuare quali siano i fattori condizionanti l'adozione di soluzioni

[22] G. Papyshev, K.J.D. Chan, *AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities*, in Electron Markets 36, 8, 2026, p. 2 doi.org/10.1007/s12525-025-00870-z. Gli autori riprendono la definizione fornita da H. Roberts, E. Hine, L. Floridi, *Digital sovereignty, digital expansionism, and the prospects for global AI governance*, in M. Timoteo, B. Verri, R. Nanni (Eds.), *Quo Vadis, Sovereignty?: New conceptual and regulatory boundaries in the age of digital China*, Springer Nature Switzerland, 2023, pp. 51–75, doi.org/10.1007/978-3-031-41566-1_4, evidenziando come, tuttavia, non vi sia consenso sulla nozione di sovranità digitale.

[23] L.G. Tornatzky, M. Fleischer, *The process of technological innovation*, Lexington Book. Massachussets/Toronto, 1990.

tecnologiche nelle organizzazioni e come questi non siano autonomamente considerabili, risultando in effetti interconnessi.

Nel presente lavoro, si fa ricorso a questo modello in particolare nei capitoli tre e quattro, analizzando il contesto tecnologico, nello specifico le tecnologie utilizzabili o impiegate dall'amministrazione pubblica, nonché la capacità di introdurne di nuove, concentrando la ricerca sulla triade cybersicurezza, *cloud*, intelligenza artificiale. Viene quindi indagato il contesto ambientale, inteso in senso non coincidente con quello descritto da L.G. Tornatzky, M. Fleischer, bensì il contesto istituzionale, le strutture e i ruoli esistenti nella pubblica amministrazione, e specialmente il sistema regolatorio, in quanto, a differenza delle imprese (punto di riferimento dell'analisi degli autori che hanno elaborato questa metodologia), le pubbliche amministrazioni non sono condizionate (principalmente) dal mercato, ma dal perimetro costituzionale e dalle peculiari funzioni ad esse attribuite, ovvero la cura dell'interesse pubblico attribuito loro dalla legge. Infine, viene specialmente considerato il contesto organizzativo ovvero la capacità delle pubbliche amministrazioni di far fronte alle nuove esigenze, la creazione di ruoli nuovi e l'introduzione di figure esperte, ma anche la decentralizzazione e centralizzazione delle strutture di controllo, i modelli di coordinamento, la necessità di risorse specialistiche. Il contesto organizzativo è quindi l'unità di analisi rispetto alla quale si analizzano i fattori condizionanti l'adozione di soluzioni tecnologiche, unitamente ai fattori inquadrabili nel contesto ambientale ed in quello tecnologico, tutti in qualche modo tesi alla trasformazione tecnologica delle amministrazioni pubbliche e correlativamente alla creazione di un nuovo modello di *governance*.

CAPITOLO I

Fondamenti teorici: una ricostruzione[*]

1. Introduzione.

L'evoluzione tecnologica e digitale ha reso necessario affrontare il tema della *governance*, intesa come l'insieme di principi, modelli e strumenti necessari per assicurare la direzione e il controllo delle innovazioni - di cui anche la pubblica amministrazione si sta dotando - al fine di garantire una gestione efficace, trasparente e responsabile della tecnologia e dei dati. L'impiego di soluzioni tecniche anche di elevata complessità pone infatti il rischio di uno scivolamento verso il controllo privato dell'interesse pubblico.

Il presente lavoro mira quindi ad analizzare il concetto di *governance*, anche con riferimento al contesto digitale, esaminando alcune teorie fondamentali, e come esse hanno trovato declinazione nel contesto giuridico italiano.

Al cuore della discussione vi è la rilevanza assunta dall'intelligenza artificiale nella società moderna, tanto da imporre una riflessione approfondita su come queste tecnologie entrano prepotentemente nel contesto sociale, lasciando agli interpreti, prima ancora che al legislatore, il compito di ricondurre nell'alveo della legalità il loro uso, minimizzando al contempo i rischi associati alla loro diffusione e applicazione.

Vi è infine da considerare il legame intrinseco tra *governance* dei dati e *governance* dell'intelligenza artificiale, su cui l'Unione europea risulta concentrarsi attraverso un approccio regolatorio volto a promuovere la diffusione dei dati e delle tecnologie, ma anche una responsabilizzazione collettiva.

[*] Il presente capitolo è stato pubblicato come contributo sulla rivista scientifica, v. Luca Pellizzoni, *Governance del digitale: fondamenti teorici e il ruolo di legislatore e interpreti*, in *Ceridap*, 3, 2025, p. 376.

2. La *governance* del digitale.

2.1. *New Public Management* e le riforme amministrative degli anni Novanta del secolo scorso.

Il concetto di *governance*, inteso come l'insieme dei processi, delle regole e delle strutture organizzative che presiedono, in un determinato contesto, la definizione dei programmi, delle strategie e delle azioni, acquista nel dominio digitale una complessità e una rilevanza senza precedenti, dovute principalmente alla rapidità con cui le tecnologie e la comunicazione evolvono e si diffondono, trasformando significativamente i modelli sociali e politici tradizionali.

Nell'elaborazione teorica di R.A.W. Rhodes[24], sviluppata negli anni Novanta del secolo scorso, con *governance* si intendono nuove modalità di governare o nuovi metodi con cui la società viene governata. Questa espressione identifica, in particolare, la transizione dal *government* connotato da un'amministrazione centralizzata e burocratica, verso forme decentralizzate, caratterizzate dalla partecipazione di attori diversi, quali enti pubblici, privati ed enti "no" e "non" - profit alla definizione delle politiche pubbliche e all'erogazione di servizi, descrivendo quindi un mutamento organizzativo del settore pubblico. Lo stesso autore individua, inoltre, un ulteriore significato in questa espressione, per descrivere il fenomeno di progressivo svuotamento dello Stato, in cui le funzioni e i poteri pubblici vengono trasferiti ad altri soggetti (come le Autorità amministrative indipendenti e le aziende private[25]) anche sovranazionali[26].

Questa teoria ha il pregio di descrivere un fenomeno verificatosi sul finire del secolo scorso caratterizzato da un profondo mutamento della società[27], e ai fini del discorso viene quindi presa in considerazione. Ma lo stesso Rhodes evidenzia come la parola *governance* venga impiegata anche per identificare una teoria sviluppatasi nel medesimo periodo per descrivere una stagione di riforme chiamata *New Public*

[24] R.A.W. Rhodes, *The New Governance: Governing without Government*, in *Pol. Studies*, 1996. R.A.W. Rhodes, *Foreword: Governance and Networks*, in G. Stoker, *The New Management of British Local Governance*, Macmillan, Londra, 1999.

[25] R.A.W. Rhodes, *Understanding Governance: policy networks, governance, reflexivity and accountability*, Open University Press, Philadelphia, 1997, p. 43.

[26] R. Mayntz, *La teoria della governance. Sfide e prospettive*, in *Riv. it. scienza pol.*, 1, 1999. Cfr. anche D. Cepiku, *Governance: riferimento concettuale o ambiguità terminologica nei processi di innovazione della PA,* in *Azienda pubbl.*, 1/2005.

[27] L. Tronca, *Verso un'analisi strutturale delle forme di* governance, in *Studi sociologia*, 3, 2007, p. 307.

Management (NPM)[28] . Questa si fonda su due assunti, l'equivalenza tra pubblico e privato, per quanto attiene agli approcci gestionali, e l'equiparazione tra dirigenti pubblici e manager delle aziende, connotandosi per alcune caratteristiche, in particolare separazione tra politica e amministrazione, decentralizzazione e maggiore uso delle tecnologie dell'informazione[29]. L'obiettivo è di promuovere una migliore efficienza e qualità dei servizi, in ottica imprenditoriale, sostenendo una riduzione del *government* a favore della *governance*[30].

Il tema del digitale si interseca quindi con la teoria della *governance* di Rhodes, perché promette da un lato di migliorare l'efficienza, paradigma di questi costrutti teorici, e dall'altro solleva questioni per l'avanzare di attori, come le *Big Tech*[31], che per capacità economica e dimensioni sono paragonabili agli Stati sovrani, i quali fornendo servizi, divenuti nel corso del tempo essenziali, possono incidere sulle politiche pubbliche.

Lo sviluppo del digitale, in particolare nella pubblica amministrazione, si configura come un processo trasformativo strutturale e graduale, in grado di incidere sull'efficienza delle pubbliche amministrazioni, ovvero sulle modalità con cui esse organizzano al proprio interno la loro attività, prendono decisioni e si relazionano con cittadini. La digitalizzazione si presenta come un vettore fondamentale per realizzare il principio di buona amministrazione, intesa come legalità, imparzialità, trasparenza e partecipazione, ma al tempo stesso rivela profonde criticità nei processi di implementazione e, ancor più, nei meccanismi di *governance* ad essa associati.

L'affacciarsi di nuove tecnologie, innescanti cambiamenti, come le modalità di interazione dei cittadini con la PA e di erogazione dei servizi, richiede di stabilire soluzioni regolatorie e processi in grado di coordinare e definire l'utilizzo della tecnologia. In questa prospettiva, la *governance* digitale diventa un fenomeno che coinvolge non soltanto aspetti tecnici relativi all'implementazione di infrastrutture IT, ma anche riflessioni più ampie di carattere etico e normativo. L'attenzione non si limita

[28] R.A.W. Rhodes, *The New Governance: Governing without Government*, cit., p. 653. C. Hood, *A Public Management for all seasons?*, in *Public Adm.*, 1, 1991, al quale si deve l'iniziale elaborazione della teoria. Cfr. Anche per una ricostruzione storica F. Rotondo, *Principi di public governance nei sistemi integrati di offerta turistica*, Giappichelli, Torino, 2011, p. 6.

[29] Si veda in particolare G. Gruening, *Origin and theoretical basis of New Public Management*, in *International Public Management Journal*, 4, 2001, il quale traccia le origini teoriche del NPM, evidenziandone le caratteristiche e M. Barzelay, *The New Public Management: Improving Research and Policy Dialogue*, University of California Press, Berkeley, 2001.

[30] R.A.W. Rhodes, *The New Governance: Governing without Government*, cit., p. 654.

[31] Espressione con cui comunemente vengono identificate le grandi *corporations* operanti nel mercato digitale, quali Amazon, Microsoft, Alphabet, Apple, Meta.

quindi all'uso e alla manutenzione degli strumenti digitali, ma si estende al modo in cui tali strumenti determinano le relazioni economiche, influenzano le dinamiche sociali e determinano nuove modalità di esercizio del potere pubblico[32].

Comprendere dal punto di vista analitico, le implicazioni della transizione verso una dimensione cibernetica non è semplice. Non mancano, in questo ambito, proposte di analisi[33] volte a distinguere tra modalità di *governance* analogiche, aumentate e automatizzate. Le prime, fondate su norme, procedure e relazioni fiduciarie, non scompaiono, ma coesistono con nuove forme di *governance* che incorporano algoritmi, sistemi predittivi, *blockchain* e intelligenza artificiale. Le modalità aumentate combinano elementi digitali e tradizionali in cui soggetti e algoritmi si intersecano (un esempio sono le piattaforme digitali), mentre quelle automatizzate si fondano su algoritmi capaci di regolare autonomamente i processi decisionali attraverso l'elaborazione dei dati, modificando il controllo da una struttura gerarchica a una decentralizzata, basata su *checks and balances* previsti all'interno del sistema informatico stesso.

I primi passi volti a definire il conteso attuale possono essere fatti risalire agli anni Novanta del secolo scorso. In particolare, la stagione delle riforme che ha interessato l'Italia[34] è in effetti ispirata alle teorie sulla *governance*, ed in particolare al NPM[35]. Queste sono cominciate con la l. 8 giugno 1990 n. 142, sull'ordinamento delle autonomie locali, seguita dalla l. 7 agosto 1990 n. 241 e s.m.i, che ha sancito i principi centrali sulla trasparenza dell'azione amministrativa, e dalla riforma Bassanini[36], con

---

[32] Cfr. sul punto R. Spagnuolo Vigorita, *Potere amministrativo, poteri e interessi privati*, in *Ceridap*, 2, 2024, la quale analizza il rapporto tra potere pubblico e privato, evidenziando come il potere privato si sia rafforzato anche in ragione dell'arretramento dello Stato e quindi il potere pubblico assume la funzione di contenimento di quello privato (come è il caso del *Golden power*) o le norme in materia di Antitrust, ma anche di indirizzo del potere privato attraverso molteplici strumenti in modo da indirizzare l'attività di impresa verso un interesse pubblico e non solo meramente economico.

[33] M. Hanisch, C. Goldsby, et al., *Digital Governance: A Conceptual Framework and Research Agenda*, in *Journal of Business Research*, 162, 2023, doi.org/10.1016/j.jbusres.2023.113777.

[34] A. M. Petroni, *Le riforme della Pubblica Amministrazione in Italia: una valutazione*, in *Giorn. dir. amm*., 2013, p. 537, il quale distingue le riforme amministrative in tre fasi: dal 1983 al 1993 di semplice riorganizzazione dei Ministeri, dal 1993 al 2001, fase di riforma di portata sistemica; la terza fase invece va dal 2008 al 2011 ed interessa prevalentemente il rapporto di lavoro dei dipendenti pubblici.

[35] G. Rebora, *Public Management: una prospettiva di scienza dell'organizzazione*, in *Riv. it. public management*, 1, 2018, p. 71.

[36] Si intendono i cinque decreti con cui è stata riformata profondamente la Pubblica amministrazione, l. 15 marzo 1997, n. 59, l. 15 maggio 1997, n.127 (Bassanini *bis*), l. 16 giugno 1998, n.191 (Bassanini *ter*), l. 8 marzo 1999, n.50 (Bassanini *quater*). Lo stesso Bassanini, riflettendo sulla stagione di riforme osserva che «Le Amministrazioni pubbliche italiane non hanno bisogno di una nuova rivoluzione normativa, bensì di un complesso di azioni che incidano in modo radicale sulla cultura, sulla organizzazione, sugli

cui sono state introdotte regole ispirate ai principi della distinzione dei ruoli tra politica e amministrazione[37], il principio di autonomia e responsabilità dei dirigenti sul piano dei risultati, e quindi della contrattualizzazione della dirigenza e della valutazione delle *performance*, ed infine l'*e-government*[38]. L'intento del processo riformatore è stato quello di operare un significativo cambiamento dell'organizzazione amministrativa, attraverso la decentralizzazione amministrativa, in ossequio al principio di sussidiarietà, l'istituzione di agenzie governative, l'impiego di strumenti di semplificazione, come l'istituto del silenzio-assenso, la conferenza di servizi e l'introduzione di strumenti di programmazione, di controllo e di gestione; in sintesi modificando l'apparato pubblico in senso aziendalistico[39].

A tali cambiamenti si sono affiancati ulteriori interventi normativi innescati dallo sviluppo dei sistemi informativi. L'incedere della tecnologia ha spinto, infatti, il legislatore ad approvare la legge delega 23 ottobre 1992, n. 421, per istituire l'Autorità per l'informatica nella pubblica amministrazione[40] (formalmente istituita con d.lgs. 12 febbraio 1993 n. 39) attribuendo ad essa le funzioni di coordinamento delle iniziative e di pianificazione degli investimenti in materia di automazione. A questo decreto è seguito il d.lgs. 3 febbraio 1993 n. 29, il cui art. 11 affidava all'ente il compito di definire i modelli e i sistemi informativi utili alla interconnessione tra le amministrazioni pubbliche, con il chiaro intento di assicurare l'adozione generalizzata e «coordinata» delle nuove tecnologie informatiche nell'organizzazione delle pubbliche

---

strumenti, sui processi e sui prodotti delle pubbliche amministrazioni.» E ancora per conseguire gli obiettivi delle riforme occorre «adeguare la macchina amministrativa alle esigenze di un sistema decentrato, che richiede forte capacità gestionale da parte delle amministrazioni territoriali, ma abbisogna anche di una rinnovata amministrazione centrale. Uno Stato centrale che non si ritira, ma si riconverte dalla gestione centralizzata della produzione di beni e servizi pubblici all'esercizio incisivo delle funzioni di regolazione, di promozione, di coordinamento e di supporto, necessarie ad assicurare la coesione, la coerenza e l'efficienza di un sistema multilivello a rete.» , cfr. F. Bassanini, *Lo stato delle riforme amministrative, il "perimetro" della Pubblica Amministrazione, e i problemi del public procurement*, in L. Fiorentino, *Lo stato compratore. L'acquisto di beni e servizi nelle pubbliche amministrazioni*, Il Mulino, Bologna, 2007.

[37] Sancito dall'art. 4 d.lgs. n. 165/2001.

[38] F. Bassanini, *Vent'anni di riforme del sistema amministrativo italiano (1990-2010)*, in *The Journal of European economic History*, 1, 2010, www.astrid.it.

[39] L. Zoppoli, *A dieci anni dalla riforma Bassanini: dirigenza e personale*, in www.astrid.it.

[40] L'ente è stato soppresso con l. 16 gennaio 2003 n. 3 e le sue funzioni trasferite al Centro nazionale per l'informatica nella pubblica amministrazione, poi trasformata in DigitPA Ente nazionale per la digitalizzazione della pubblica amministrazione in forza del d.lgs. 1º dicembre 2009 n. 177. Infine, con d.l. 22 giugno 2012 n. 83, convertito con l. n. 134/2012 DigitPA è stata soppressa ed è stata costituita l'Agenzia per l'Italia digitale.

amministrazioni, per accrescerne l'efficienza[41]. Il legislatore ha inoltre dovuto riconoscere la necessità di regolamentare lo sviluppo tecnologico, ed in particolare, con la l. 15 marzo 1997 n. 59 (la prima legge Bassanini), la diffusione di nuovi strumenti di dirompente novità[42]: il documento informatico e la firma elettronica.

Il primo passo verso la definizione della situazione di fatto è stato quindi un importante intervento riformatore della Pubblica amministrazione. Un processo lungo e complesso, in cui trovare il modello o la soluzione giusta è frutto di tentativi succedutisi nel tempo, come dimostra il susseguirsi di agenzie dedicate alla transizione digitale della p.a.[43].

La graduale evoluzione delle strutture originariamente deputate all'infosfera, dall'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA), alla costituzione di DigitPA e, infine, all'Agenzia per l'Italia Digitale (AGID), quale ente con competenze di coordinamento, monitoraggio e supporto tecnico nel digitale, mostra una stratificazione normativa e organizzativa che, pur avendo come scopo la razionalizzazione dei processi di digitalizzazione, ha prodotto sovrapposizioni di ruoli e una frammentazione dei centri decisionali, generando una sistema di gestione e controllo complesso, in cui la funzione di coordinamento centrale non sempre si integra in modo fluido con altri enti ai quali vengono assegnate funzioni amministrative, come le Regioni e i Comuni[44].

Oltre al NPM, si possono richiamare ulteriori modelli che hanno assunto rilievo con riferimento al digitale: *governance* multilivello e *Open Government*. Con la prima espressione si descrive la scomparsa del ruolo di principale attore nelle decisioni politiche assegnato agli Stati nazionali, i quali diventano compartecipi assieme ad enti sovranazionali (ad esempio l'Unione europea), e altri soggetti sub-statali e non statali,

---

[41] M. Minerva, *Verso l'integrazione dei sistemi informativi pubblici: la rete unitaria della pubblica amministrazione*, in *Dir. inform.*, 3, 1998, p. 623.

[42] L. Albertini, *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. civ.*, 6, 1998, p. 267. R. Borruso, *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (d. lgs. 23 gennaio 2002 n. 10, d.P.R. 7 aprile 2003 n. 137 e l. 29 luglio 2003 n. 229)*, in *Giust. civ.*, 3, 2004, p. 143, il quale rileva che «Se è vero che in tutto il nostro ordinamento giuridico e, in particolare, nel diritto civile (oltreché in quello amministrativo), riveste massima importanza l'atto scritto e la sua sottoscrizione autografa solo grazie alla quale l'atto stesso diventa imputabile ad un determinato soggetto che assume, ad ogni effetto, la responsabilità del suo contenuto, allora dovranno considerarsi di pari importanza le norme di legge recentemente emanate per effetto delle quali diventa giuridicamente e pienamente rilevante un tipo nuovo di documento - il «documento informatico» - e un tipo nuovo di sottoscrizione: la firma elettronica».

[43] C. Notarmuzi, *DigitPA: la terza riorganizzazione dell'informatica pubblica*, in *Giorn. dir. amm.*, 10, 2010, p. 1014 ss.

[44] C. Limiti, *La governance del processo di digitalizzazione della pubblica amministrazione*, in *www.iusinitinere.it*.

dell'esercizio del potere, sviluppando nuove strategie di coordinamento e collaborazione per il perseguimento delle politiche pubbliche[45]. Mentre con la seconda espressione si descrive l'insieme delle politiche volte a promuovere la trasparenza delle amministrazioni pubbliche e la partecipazione dei cittadini[46].

2.2. Digitalizzazione e regolazione: limiti delle categorie tradizionali alla luce delle nuove esigenze di *governance.*

Il richiamo a questi modelli assume rilevanza in ragione delle peculiarità della digitalizzazione. Essa non riveste, infatti, una dimensione nazionale, ma assume estensione globale, poiché scollegata da una dimensione fisica, in cui i dati circolano senza confini e alla quale non si applicano le categorie giuridiche tradizionali[47].

Si presenta quindi un nuovo elemento, la *governance* digitale, intesa quale attività volta a definire, quindi attuare, politiche, procedure e standard per lo sviluppo, l'utilizzo e la gestione dell'infosfera[48]. La presenza di attori diversi rende il contesto digitale privo di rapporti gerarchici e si connota, invece, per una forma decentralizzata, in cui più soggetti sono collegati tra loro[49].

Per definire quale architettura debba avere la *governance* del digitale si devono prendere in considerazione elementi chiave, quali interoperabilità, sicurezza dei dati, servizi centrati sul cittadino, per promuovere trasparenza, *accountability* e innovazione nei

---

[45] M. Saito-Jensen, *Multilevel Governance Theory*, in *Theories and Methods for the Study of Multilevel Environmental Governance*, Center for International Forestry Research, 2015, http://www.jstor.org/stable/resrep02152.5. K.A. Daniell, A. Kay, *Multi-Level Governance: Conceptual Challenges and Case Studies from Australia*, ANU Press, 2017, http://www.jstor.org/stable/j.ctt1zgwjv0. S. Piattoni, *La "governance" multi-livello: sfide analitiche, empiriche e normative*, in *Riv. it. scienza pol.*, 3, 2005, p. 425, il quale sostiene che «Il concetto di governance multi-livello deve intendersi come una specificazione del concetto di governance che mette in particolare risalto la creazione (aspetto strutturale) di livelli di governo di ampiezza giurisdizionale sovra- o sub-nazionale ed il loro coinvolgimento (aspetto processuale) nei processi decisionali ed attuativi ingenerati dalle sfide interne ed esterne al potere di controllo e governo degli stati Nazionali».

[46] La spiegazione si rinviene nel portale https://open.gov.it/governo-aperto.

[47] Cfr. J.S. Bergé, S. Grumbach, V. Zeno-Zencovich, *The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance*, in *Eur. Journal Comparative Law and Governance*, 2, 2018, disponibile in SSRN: https://ssrn.com/abstract=3185943.

[48] L. Floridi, *Etica dell'intelligenza artificiale. Sviluppo, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022, p. 127. Per una ricostruzione storica del concetto di internet *governance* J. Hoffmann, C. Katzenbach, K. Gollatz, *Between coordination and regulation: Finding the governance in Internet governance*, in *New Media & Society*, 2016, disponibile in SSRN: https://ssrn.com/abstract=2836068.

[49] J. Hofmann, C. Katzenbach, K. Gollatz, *op. cit*.

servizi pubblici, garantendo al tempo stesso la conformità degli strumenti digitali alla legge[50].

Questo richiede anche una ridefinizione di categorie del diritto amministrativo (come la motivazione del provvedimento, la pubblicità degli atti e i meccanismi di garanzia partecipativa), nella misura in cui risultano incapaci di regolare strumenti nuovi[51], essendo questi ultimi potenzialmente in grado di scardinare la realtà organizzativa (si pensi all'ipotesi di un procedimento amministrativo totalmente automatizzato, quindi in assenza del funzionario) e ridefinire le responsabilità, in ragione dell'operare di soggetti pubblici e privati[52].

In questo contesto si inserisce un ulteriore tema, quello della diffusione degli algoritmi e dell'intelligenza artificiale[53], che solleva questioni attinenti ai principi di legalità, al rispetto dei diritti fondamentali e alla partecipazione al procedimento amministrativo. Se l'introduzione di sistemi automatizzati promette un incremento di efficienza, risulta imprescindibile una forma di "controllo umano" che assicuri la comprensibilità delle procedure e la responsabilità ultima dei decisori pubblici, così da evitare l'opacità dei processi e la marginalizzazione dei diritti di difesa dei cittadini[54].

Le questioni sollevate da queste tecnologie, hanno portato ad arricchire il dibattito teorico con concetti appartenenti alla dimensione tecnica, come lo *human in the loop*[55],

---

[50] M. Lestari, A. F. Wijaya, M. Chandra, *Enterprise Architecture Model for Smart Government Implementation*, in *Journal of Information Systems and Informatics*, 1, 2025. S. M. Polisetty, S.K. Pendyala, S.P. Prabhakaran, *Strengthening data integrity and security via cloud administration and access control strategies*, in *International Journal of Computer Engineering and Technology*, 3, 2023, p. 283.

[51] Cfr. M.B. Armiento, *Prove di regolazione dell'intelligenza artificiale: il Regolamento della Banca d'Italia sulla gestione degli esposti*, in *Gior. dir. amm.*, 1, 2023, p. 105, la quale osserva come «la regolazione dell'intelligenza artificiale da parte delle pubbliche amministrazioni è stata perlopiù affidata a strumenti di soft law oppure all'opera della giurisprudenza. Limitandosi alla giurisprudenza italiana e nello specifico a quella amministrativa, si può osservare come, nel rilevare la differenza tra l'attività amministrativa "tradizionale" e quella "algoritmica", il giudice amministrativo abbia ritenuto applicabili a quest'ultima non principi e istituti tipici della legge sul procedimento amministrativo, bensì principi e istituti "diversi" e, nel caso di specie, ricavati direttamente dal Regolamento generale sulla protezione dei dati personali».

[52] E. Picozza, *Politica, diritto amministrativo e Artificial Intelligence*, in *Giur. it.*, 7, 2019. A quanto precede si aggiunga la necessità di avere competenze specialistiche nelle amministrazioni pubbliche e un rafforzamento della cooperazione internazionale, al fine di affrontare questioni come la localizzazione dei dati e la tutela della "sovranità digitale" degli Stati, cfr. J.S. Bergé, S. Grumbach, V. Zeno-Zencovich, *op. cit.*, p. 19.

[53] I cui problemi concettuali e definitori dal punto di vista giuridico verranno affrontati nel prosieguo.

[54] Cfr. sul punto A. Puzzanghera, *La sfida tecnologica alla legalità amministrativa*, in *Riv. it. infor. dir.*, 2, 2022.

[55] B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in *Biodiritto*, 2, 2021; V. Neri, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urb. app.*, 5, 2021, p. 581; R. Bovetti, L. Broccardo, G. Materzanin*, Shadow automation:*

che indica quel modello matematico per cui per produrre o validare il risultato è necessaria l'interazione tra uomo e macchina, ma anche principi esistenti, e riscoperti in una nuova prospettiva, come "la riserva di umanità"[56]. Questo principio descrive dal punto di vista teorico l'indispensabilità dell'intervento umano nello svolgimento delle funzioni amministrative automatizzate, in ossequio alla teoria generale della imputazione giuridico-formale dell'attività amministrativa in capo al funzionario persona fisica, per preservare il circuito di responsabilità, costituente elemento indispensabile di legittimazione dei pubblici poteri, un tanto al fine di tracciare un perimetro delle funzioni amministrative automatizzate, in ragione dei limiti e delle incognite che presenta l'utilizzo dell'intelligenza artificiale nel campo della sfera decisionale pubblica [57].

La *governance* del digitale si interseca quindi con quella dell'intelligenza artificiale, nella quale linee guida, *policy* e *framework* normativi vengo elaborati, ridefiniti e aggiornati in maniera costante, anche a causa della mutevolezza del contesto tecnologico in continua evoluzione.

L'incedere di nuove tecnologie rende per questi motivi la sfida della regolamentazione ancora più impervia, soprattutto se non viene affrontata in maniera sistematica. In proposito, basti pensare che l'avvio dell'innovazione tecnologica della pubblica amministrazione può essere collocato temporalmente a partire dal 2005[58] con l'introduzione dell'articolo 3 *bis* nella l. n. 241/1990, ai sensi del quale «per conseguire una maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano

---

l'automazione robotica dei processi come strumento di efficienza per le aziende, in *Controllo gestione*, 5, 2023, p. 29; P. Benanti, *Human in the loop. Decisioni umane e intelligenze artificiali*, Mondadori, Milano, 2022. Si vedano anche T.A.R. Lazio, sez. IV *ter*, 8 aprile 2024, n. 6808, Cons. St., sez. IV, 23.05.2023, n. 5117, Cons. St., Sez. VI, 4 febbraio 2020, n. 881, Cons. St., sez. VI, 13 dicembre 2019, nn. 8472, 8473, 8474.

[56] G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, CEDAM, 2023, G. Gallone*, Riserva di umanità, intelligenza artificiale e funzione giurisdizionale alla luce dell'IA Act. Considerazioni (e qualche proposta) attorno al processo amministrativo che verrà*, in *Judicium*, 2024.

[57] G. Gallone, *Riserva di umanità e funzioni amministrative, op. cit.*, p. 27. In particolare, l'autore rileva come «L'espressione "riserva di umanità", coniata dalla dottrina iberica, sembra ben riassumere, con la forza di una formula evocativa, quest'ultimo concetto. Un concetto che sottende e fonda la teorica classica dell'automazione amministrativa ma che non è mai stato oggetto di una specifica indagine che si soffermi sulle sue radici più profonde e sulle implicazioni che reca con sé. La ragione ultima di questa tradizionale disattenzione verso la "riserva di umanità" nello svolgimento delle funzioni amministrative è, probabilmente, da legare ad un approccio alla tematica che è stato, almeno agli inizi, nello spirito pioneristico dei primordi, comprensibilmente orientato ad evidenziare più le potenzialità offerte dagli stru menti informatici che i limiti giuridici a cui deve rispondere l'automazione», p. 132.

[58] A. Saporito, V*erso una "nuova" amministrazione digitale*, in *Ambientediritto.it*, 2, 2023.

l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati». Una norma programmatica, successivamente modificata dall'art. 12, comma 1, lettera b) della l. n. 120/2020, che ha eliminato il riferimento all'incentivazione sostituendolo con «agiscono mediante strumenti informatici e telematici»[59]. È il legislatore stesso a rimarcare, con il menzionato art. 3 *bis* della l. n. 241/1990, la correlazione tra strumenti digitali ed efficienza[60], paradigma della trasformazione della PA.

Nondimeno, il semplice ricorso a norme di principio appare inutile in assenza di una regolamentazione specifica, per una definizione delle modalità di utilizzo delle nuove tecnologie e di coordinamento tra enti pubblici, enti privati e cittadini[61], soprattutto in un contesto caratterizzato da incessante evoluzione, nel quale si è passati da semplici *software* di video scrittura a soluzioni di intelligenza artificiale come ChatGPT, in grado di produrre interi testi da semplici istruzioni (*prompt*) fornite.

Le difficoltà di coordinamento tra norme fondamentali del diritto amministrativo con la disciplina settoriale, come dimostra la circostanza che la l. 241/1990 abbia nell'art. 3 *bis* l'unica disposizione espressamente dedicata al digitale, laddove la disciplina specifica è contenuta nel d.lgs. 7 marzo 2005, n. 82 (il Codice dell'Amministrazione Digitale), evidenzia le difficoltà di approcciare in maniera sistematica la questione, generando una frammentazione della disciplina[62].

Al contempo, la società digitale pone al centro nuove questioni, quella della tutela dei dati personali, oggetto di attenzione in particolare a partire dal Codice della privacy (d.lgs. 30 giugno 2003, n.196)[63] e infine con il testo fondamentale, il Regolamento 2016/679/UE del Parlamento europeo e del Consiglio del 27 aprile 2016, noto come *General Data Protection Regulation* (GDPR), con cui l'Unione europea ha voluto

[59] La riformulazione denota anche un mutamento dei tempi. Se nel 2005 l'uso della telematica veniva solamente incentivato, poiché si era all'inizio della transizione digitale, nel 2020 lo sviluppo della tecnologia, la sua larga diffusione, ed infine il peculiare contesto storico in cui la modifica è stata apportata (determinato dal *lockdown* deciso per contenere la pandemia da Covid-19) determina la modalità dell'azione amministrativa.

[60] L. Torchia, *Pubblica amministrazione e transizione digitale*, in *Gior. dir. amm.*, 6, 2024, p. 729.

[61] E. Marinică, *Digitalization – The Key for Adapting Good Administration to a Better Governance*, in *Academic Journal of Law and Governance*, 2, 2020.

[62] P.S.L. Falletta, *Le trasformazioni del diritto amministrativo nella complessità dell'ambiente digitale*, in *Federalismi.it*.

[63] Modificato dal d.lgs. 10 agosto 2018, n. 101, per adeguarlo al GDPR, quindi modificato dal d.l. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla l. 3 dicembre 2021, n. 205, dal d.lgs. 10 marzo 2023, n. 24, con effetto a decorrere dal 15 luglio 2023 e dal d.l. 2 marzo 2024, n. 19, convertito, con modificazioni, dalla l. 29 aprile 2024, n. 56.

definire principi e regole comuni a tutti gli Stati membri, per imporre alle imprese e alle istituzioni l'adozione di misure e processi in grado di salvaguardare i diritti dei cittadini e la mitigazione dei rischi di eventuali abusi o fughe di informazioni personali sensibili.

Un aspetto chiave del contesto digitale risulta essere infatti anche la gestione dei dati, risorsa primaria di gran parte dei processi decisionali e di funzionamento dei sistemi di intelligenza artificiale, in quanto l'IA dipende in modo sostanziale dalla disponibilità di dataset di alta qualità, accurati e privi di *bias*[64], su cui poter essere addestrata. In particolare, la *data governance* si preoccupa non solo degli aspetti tecnici, come la definizione di protocolli di sicurezza e l'implementazione di sistemi di controllo degli accessi, ma anche degli aspetti organizzativi, come l'assegnazione di ruoli e responsabilità chiare, la formazione del personale e la promozione di una cultura di responsabilità condivisa in materia di trattamento dati.

Il governo del digitale vede, infatti, da un lato il moltiplicarsi di regole, soprattutto a livello comunitario, e dall'altro la creazione di nuovi enti pubblici di controllo, di certificazione, di nuove figure professionali. È il caso di enti come il Garante per la protezione dei dati personali, l'AgID, l'Agenzia per la Cybersicurezza Nazionale, o di nuove figure all'interno delle pubbliche amministrazioni, quali il Responsabile per la transizione digitale.

Se da un lato la regolazione plasma i comportamenti e definisce le norme alle quali coloro che operano nel digitale, devono attenersi, sono i singoli attori a contribuire alla *governance* del digitale attraverso l'esercizio delle funzioni loro attribuite (come nel caso degli enti pubblici menzionati).

Tracciare quindi un modello unitario di *governance* del digitale non può essere fatto, ma come è stato ben sintetizzato[65] può affermarsi che esso si compone di elementi

---

[64] Secondo la definizione diffusa, con tale parola si indicano, in riferimento ai sistemi automatizzati, «*statistical biases,' which are caused by using data that includes systematic errors which, in turn, skew results. These errors can arise from the algorithm itself and/or from faulty, incomplete, irrelevant, excluded, or biased data sets, thus creating consistent errors in a model, the error being the difference between the ground truth and the average model prediction*» M. Oswald, A. Paul, *'Bias'*, in Kaufmann M., H. M. Lomell, *De Gruyter Handbook of Digital Criminology*, De Gruyter, 2025, p. 101, disponibile in SSRN: https://ssrn.com/abstract=4738337. Cfr. anche L. Floridi, *op. cit.*, p. 160, il quale adotta la nozione di *bias* nel senso di deviazione da uno standard, che può verificarsi in qualsiasi fase di design del *software* a causa dei dati prescelti, o perché campionati in via preferenziali o perché essi stessi contengono un pregiudizio. In tal senso anche G. Massarotto, *What Is Algorithmic Bias and Why Antitrust Agencies Should Care*, in *CPI Antitrust Chronicle*, University of Pennsilvania, Inst. for Law & Econ, paper No. 23-39, 2023, disponibile in SSRN: https://ssrn.com/abstract=4625894.

[65] Così B. Cappiello, G. Carullo, *Blockchain, Law and Governance*, Springer, 2020, in particolare gli autori ipotizzano che la «*Blockchain, in this regard, can be seen as a specific form of regulating code,*

tradizionali ovvero Stati, aziende, organizzazioni internazionali, organizzazioni non governative, organizzazioni della società civile, individui e altre persone giuridiche, i quali agiscono in conformità di leggi, regolamenti, contratti e in forza di mezzi tradizionali di applicazione della legge, come le decisioni dei tribunali e i provvedimenti amministrativi dello Stato e degli altri enti pubblici tradizionali. Nella *governance* digitale a queste componenti si aggiungono nuovi soggetti (come le compagnie tecnologiche) e nuove forme di regolamentazione, come le condizioni d'uso che gli utenti accettano per poter utilizzare un determinato servizio.

Quello che si proverà a fare nel prosieguo del presente lavoro è analizzare alcuni tra i cambiamenti più significativi che le regole e la tecnologia hanno apportato alle pubbliche amministrazioni.

3. La sovranità dello spazio digitale.

La trasformazione digitale della società contemporanea, ed in particolare della pubblica amministrazione, pone al centro del dibattito la questione della sovranità[66] nell'infosfera, in riferimento al rapporto tra autorità pubbliche e poteri privati, determinato dall'assenza di un luogo fisico, quale è la rete, caratterizzata dalla transnazionalità, la quale rende difficile l'esercizio della stessa[67].

Il problema della transnazionalità delle reti e delle piattaforme digitali si intreccia con la questione della sovranità statale, poiché se da un lato gli Stati cercano di stabilire norme per il controllo delle tecnologie, le aziende multinazionali possono spostare i propri server e le proprie attività in giurisdizioni più favorevoli. Questo fenomeno è

---

implying specific design principles and thereby normative principles of governance», nel senso che ogni tecnologia produce un effetto normativo, e questo è particolarmente vero per la *blockchain*, perché produce un decentramento del controllo, che viene assicurato dalla tecnologia (e quindi manca una supervisione esterna), ma anche trasparenza e fiducia, che tale tecnologia, con la sua garanzia di immutabilità produce. Questo esempio, secondo gli autori, mostra come il digitale modifica la *governance*.

[66] Sul concetto di sovranità intesa quale potestà suprema di determinare le regole in un determinato territorio, sulla crisi della sovranità si veda L. Ferrajoli, *La sovranità nel mondo moderno. Nascita e crisi dello Stato nazionale*, Roma-Bari, 1997 e S. Della Valle, *Crisi e ridefinizione della sovranità nel contesto plurilivellare*, in *Costituzionalismo.it*, 3, 2016. Cfr. anche O. Chessa, *Sul rapporto tra Stato e capitalismo. Riflessioni a partire da Hobbes, Schmitt e Mortati*, in *Cosituzionalismo.it*, 3, 2024, p. 35, secondo il quale lo Stato conserva il potere di azione nei confronti del privato, mentre il capitalismo non ha la capacità di eliminare la forma-Stato.

[67] A. Gatti, *Istituzioni e anarchia nella rete. i paradigmi tradizionali della sovranità alla prova di internet*, in *Dir. inform.,* 3, 2019, p. 718.

particolarmente evidente nell'economia delle piattaforme, in cui aziende come Alphabet, Meta, Amazon o Microsoft agiscono su scala globale, generando fatturati di gran lunga superiori a quelli di interi Paesi e potendo influenzare le politiche pubbliche[68].

Il processo di trasformazione tecnologica ha, infatti, innescato processi di concentrazione economica e di riassegnazione di competenze regolative, determinando un ripensamento delle categorie tradizionali del diritto pubblico e mettendo in evidenza i limiti dei principi fondamentali degli Stati democratici, mascherati con nuovi diritti raggruppati sotto il concetto di "costituzionalismo digitale", omettendo, tuttavia, l'elemento fondamentale del diritto costituzionale, ossia la legittimazione democratica[69]. In particolare, la formazione di oligopoli digitali, costituiti da poche *corporations* aventi la disponibilità di ingenti risorse economiche, in grado di raccogliere, elaborare e gestire una quantità enorme di dati, rende necessario per il potere pubblico decidere come vuole normare la tecnologia, intesa quale regolamentazione sia dei poteri privati quanto al loro operare nel mercato sia dell'impiego di strumenti innovativi come l'Intelligenza artificiale nei processi decisionali pubblici[70]. Le grandi piattaforme digitali, in ragione della diffusa idea della *self-regulation* hanno finito per esercitare funzioni di tipo quasi-normativo, sfruttando le clausole d'uso e gli algoritmi di moderazione dei contenuti per definire in maniera svincolata da una legittimazione democratica l'esercizio di diritti (anche fondamentali) come la libertà di espressione[71].

Rispetto a questo fenomeno l'Unione europea ha scelto di adottare un approccio normativo per dettare le regole dello spazio cibernetico, altrimenti dettate dalle *corporations*[72].

In un primo momento, la prevalenza del paradigma della neutralità delle piattaforme e la convinzione di voler promuovere l'innovazione tecnologica hanno spinto i legislatori a lasciare ampi spazi di autoregolazione e di mercato[73]. Tuttavia, l'avvento dei cosiddetti poteri privati digitali ha progressivamente disvelato le fragilità di un modello fondato sulla mera autodisciplina, mettendo in evidenza l'ascesa di attori sovra-statali che

[68] A. Gatti, *op. cit.*, p. 716.
[69] M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Dir. pubbl.*, 3, 2021, p. 747 e ss.
[70] B. Carotti, *Algoritmi e poteri pubblici: un rapporto incendiario*, in *Gior. dir. amm.*, 1, 2020, p. 5.
[71] E. Bruti Liberati, *Poteri privati e nuova regolazione pubblica*, in *Dir. pubbl*, 1, 2023, p. 288.
[72] G. Finocchiaro, *La sovranità digitale*, in *Dir. pubbl.*, 3, 2022, p. 820.
[73] M. Betzu, *op. cit.*, p. 748.

detengono risorse di tipo informativo tali da consentire di influenzare scelte individuali e collettive[74]. Le piattaforme, in questo quadro, non si limitano a fornire servizi, ma assumono il ruolo di vere e proprie "autorità di fatto", che impongono un insieme di regole privatistiche e di procedure di *enforcement* al di fuori di un controllo effettivo da parte di organi pubblici[75].

La vicenda dell'oscuramento del profilo Twitter del Presidente degli Stati Uniti d'America, Donald Trump, è sovente citata quale esempio emblematico del potere contrattuale e decisionale esercitato dalle piattaforme[76]. Ciò dimostra come il privato disponga di capacità d'intervento su diritti fondamentali e libertà politiche, sostituendosi alla funzione pubblica di garanzia e controllo.

Alla luce di questi motivi deve essere letta la scelta dell'Unione europea di superare un modello di sviluppo del digitale basato sul mercato e quindi sull'autoregolamentazione dei privati, verso politiche regolative in particolare relative ai dati e agli algoritmi[77]. Dopo aver inizialmente adottato atti programmatici[78], il legislatore europeo ha scelto una strategia volta ad imporre una *leadership* internazionale, con l'obiettivo di introdurre regole aventi forza globale e quindi tali da condizionare gli standard di sviluppo del mercato[79]. Questo fenomeno, definito "*Brussels Effect*",[80] pur avendo portata più ampia, riguarda anche il digitale e risulta evidente dal succedersi di regolamenti dedicati ad ogni segmento che compone questo settore[81], dal GDPR, (Regolamento 2016/679/UE) al *Digital Services Act* (Regolamento 2022/2065/UE), dal *Digital Markets Act* (Regolamento 2022/1925/UE), fino all'*AI Act* (Regolamento 2024/1689/UE), al *Data Governance Act* (Regolamento 2022/868/UE), e al *Data Act* (Regolamento 2023/2854/UE).

---

[74] M. Santaniello, *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics*, 3, 2021, 587-588.
[75] B. Carotti, *op. cit.*
[76] G. Finocchiaro, *op. cit.*, p. 818.
[77] M. Santaniello, *op. cit.*, p. 580.
[78] Tra cui si possono includere la Strategia europea dei dati e il Libro bianco sull'intelligenza artificiale.
[79] Rientra in questa strategia il "pacchetto digitale" presentato nel 2020 dalla Commissione Europea, contenente una serie di regolamenti (tra cui il *Digitial Market Act* e il *Digital Service Act*). Cfr. sul punto M.R. Allegri, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Riv. it. informatica dir.*, 2, 2021.
[80] A. Bradford, *The Brussels Effect*, in *Northwestern University Law Review*, 1, 2012, disponibile in https://scholarship.law.columbia.edu/faculty_scholarship/271. M. Almada, A. Radu, *Brussels Effect*, in A. Parrish, C. Ryngaert, D. Ireland-Piper, *Elgar Concise Encyclopedia on Extraterritoriality and the Law*, 2025, disponibile in SSRN: https://ssrn.com/abstract=5123680 or http://dx.doi.org/10.2139/ssrn.5123680.
[81] V. Pagnanelli, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Riv. it. informatica dir.*, 1, 2021, p. 19.

L'intento è quello di rivendicare anche una "sovranità digitale" dell'UE, intesa con una duplice valenza, ossia verso l'esterno, ovvero verso i due principali attori globali (USA e Cina), e verso l'interno, verso i singoli Stati membri, col fine di evitare la frammentazione normativa[82] e quindi assicurare l'esercizio di un potere pubblico di governo attraverso la legislazione[83]. Il fine è rivendicare un'autonomia digitale dell'Unione europea e una sovranità regolatoria, quale potere di imporre regole[84].

L'Unione europea contrappone in questo modo a modelli di governo della rete di matrice americana incentrati sul principio del "*laissez-faire*"[85] o di rigido controllo statale (come quello cinese) un approccio antropocentrico[86], ispirato alla tutela della dignità umana e della privacy, definendo un modello di *governance* basato sull'essere umano[87]. Emblematico in questo senso è l'*Artificial Intelligence Act*, che individua fasce di rischio e obblighi di conformità, invocando principi di trasparenza, non discriminazione e controllo umano.

Allo stesso tempo, vi sono settori del digitale in cui gli Stati membri assumono un ruolo diretto in quanto sensibili ed intersecanti altre materie. È il caso della sicurezza cibernetica, ovvero la difesa delle reti e dei sistemi informatici dagli attacchi *hacker*, che si colloca nel più ampio settore della sicurezza nazionale, ancora fortemente appannaggio dei singoli Stati nazionali. Non è un caso che l'UE abbia in questa materia approvato le Direttive NIS1 e 2[88], attribuendo quindi ai singoli Stati membri il compito

---

[82] G. Finocchiaro, *op. cit.*, p. 822.

[83] S. Mangiameli, *La sovranità digitale*, in *Dirittifondamentali.it*, 2, 2023, p. 286.

[84] V. Bertola, *La sovranità digitale e il futuro di Internet,* in *Riv. it. informatica dir.*, 1, 2022, p. 44, in particolare l'autore evidenzia come la «ricerca di 'autonomia digitale', ovvero di disporre sul proprio territorio e dentro la propria giurisdizione di tutti i servizi Internet che possano permettere all'economia e alla società di funzionare anche in caso di conflitto commerciale e geopolitico (o in caso estremo militare) con Paesi esteri, e una ricerca di sovranità vera e propria, ossia della capacità di porre regole e farle rispettare anche ad attori che non sono basati nella propria giurisdizione, ma che comunque possiedono in essa quote di mercato rilevanti o addirittura dominanti, assumendo un ruolo fondamentale nella vita online del Paese».

[85] Il Presidente degli Stati Uniti Joe Biden aveva invero adottato il 30 ottobre 2023 un ordine esecutivo *Executive Order (E.O.) 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* con l'intento di stabilire regole e obiettivi per lo sviluppo dell'intelligenza artificiale, al fine di mitigarne i rischi in particolare per la tutela dei diritti civili. Questo ordine esecutivo è stato abrogato dal successore Donald Trump, il quale il 23 gennaio 2025 ha emanato l'*Executive Order 14179* denominato *Removing Barriers to American Leadership in Artificial Intelligence* il cui intento espressamente dichiarato è preservare la leadership americana nell'IA e a tal fine «*we must develop AI systems that are free from ideological bias or engineered social agendas*».

[86] D. Martire, *Intelligenza artificiale e Stato costituzionale*, in *Dir. pubbl.*, 2, 2022, p. 437.

[87] F. Faini, *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *Federalismi.it*, 2, 2023, p. 13.

[88] Direttiva 2016/1148/UE, nota come Direttiva NIS 1 acronimo di *Network and Information Security*, adottata nel 2016, costituisce il primo intervento normativo a livello europeo avente lo scopo di innalzare

di implementare le regole comunitarie nel proprio ordinamento secondo apposite norme nazionali.

L'approccio fortemente normativo adottate dall'Unione europea risulta quindi eminentemente politico ed emerge con forza nell'individuazione di chi abbia il potere di fissare i criteri e i valori guida per l'innovazione e si accompagna alla definizione di un modello di *governance* diffuso, in cui operano Autorità indipendenti con funzione di vigilanza e di *enforcement*, ma anche di certificazione, con poteri sanzionatori, e la responsabilizzazione dei singoli operatori, privati e pubbliche amministrazioni alla gestione di settori quali la cybersicurezza e la protezione dei dati[89]. Viene tracciato in questo modo un approccio definito "collaborativo", per condividere responsabilità, ma anche competenze, superando in questo modo la dicotomia tra regolazione pubblica e autoregolazione privata, fino ad integrare all'interno della tecnologia stessa i valori costituzionali[90].

La strategia della sovranità digitale europea si connota anche per la costruzione di un mercato interno in cui il potere pubblico viene riaffermato nel rispetto dei principi democratici e dei diritti fondamentali[91], in cui trasparenza, responsabilità e diritti umani sono elementi strutturali della regolazione.

In conclusione, l'emergere della sovranità digitale può essere interpretato come la fase in cui il potere pubblico tenta di riconquistare lo spazio normativo che in precedenza era stato occupato dal potere privato delle piattaforme, spesso attraverso strumenti contrattuali e tecnologici. Il modello europeo, facendo leva su un quadro di principi quali libertà, democrazia, concorrenza e tutela dei diritti, mira a trasformarsi in un riferimento globale di regolazione, nella speranza di indurre un riallineamento delle pratiche commerciali e dell'impiego degli algoritmi. Il quadro che emerge è quindi un

---

la cooperazione tra gli Stati membri e creare un primo livello di armonizzazione in materia di sicurezza cibernetica. Successivamente viene abrogata e sostituita dalla Direttiva 2022/2555/UE, Direttiva NIS 2, per far fronte all'esigenza di aggiornare e rafforzare il quadro normativo previsto dalla Direttiva NIS 1, al fine armonizzare e rafforzare maggiormente i livelli di sicurezza all'interno dell'Unione europea.

[89] La l. 28 giugno 2024 n. 90 e il d.lgs. 4 settembre 2024 n. 138 recanti norme in materia di cybersicurezza e di recepimento della Direttiva NIS2, prevedono l'istituzione di una nuova figura responsabile della materia, all'interno delle organizzazioni, pubbliche e private, per quei soggetti che il decreto legislativo individua come essenziali o importanti.

[90] M. Betzu, *op. cit.*, p. 759.

[91] E. Bruti Liberati, *op. cit.*

insieme di regole per tutelare i diritti fondamentali, ma anche lo sfruttamento economico, in particolare del dato[92].

Sul versante interno agli Stati, la dimensione politica della *governance* tecnologica si manifesta in particolare a partire dai finanziamenti del Piano Nazionale di Ripresa e Resilienza, che mirano ad incoraggiare e facilitare la transizione digitale implementando le IT e la migrazione dei dati delle Pubbliche amministrazioni verso ambienti *cloud* per razionalizzare, consolidare e modernizzare le risorse tecnologiche, migliorando efficienza, sicurezza e gestione delle informazioni[93]. L'effetto di questo piano è imporre un cambiamento significativo del funzionamento e dell'organizzazione della PA[94], tanto che si può affermare di essere di fronte a un mutamento così radicale da richiedere un superamento delle regole esistenti[95]. Anche l'organizzazione amministrativa viene quindi interessata dalla digitalizzazione, da un lato attraverso l'istituzione di nuovi organismi, a cui viene affidata la "materia digitale", come l'Agenzia per l'Italia Digitale e, nel 2021, l'Agenzia per la Cybersicurezza Nazionale e il Comitato interministeriale per la cybersicurezza, dall'altro attraverso la creazione di nuove figure all'interno delle pubbliche amministrazioni quali il responsabile per la transizione digitale[96] e, nel 2024, il referente per la cybersicurezza[97], a cui vengono affidati nuovi compiti in ragione della trasformazione in senso digitale dell'azione amministrativa.

La scelta su dove destinare le risorse europee prevista dal piano *Next generation EU* è certamente politica. L'Italia scontava un significativo ritardo nelle politiche di implementazione digitale, per cui la prima voce del piano approvato dall'Unione europea è dedicata proprio alla trasformazione digitale.

Il quadro così ricostruito richiama l'attenzione alla centralità delle istituzioni tradizionali nel regolare la società, anche attraverso incentivi e sostegno agli investimenti. Tuttavia, questo approccio in parte sconta l'idea per cui solo attraverso massicci investimenti in tecnologia possa aversi progresso della società[98]. Questa

[92] C. Contessa, *Il potere pubblico al tempo dei Big Data*, disponibile in www.giustizia-amministrativa.it.
[93] E. Montagnani, *Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali*, in *Riv. it. informatica dir.,* 1, 2022, p. 190. I. Macrì, *Cloud nella pubblica amministrazione: una casa moderna per i dati degli italiani*, in *Azienditalia*, 11, 2021.
[94] I. Macrì, *Il cloud per le pubbliche amministrazioni*, in *Azienditalia*, 1, 2021, p. 17.
[95] L. Torchia, *Lo stato digitale. Una introduzione*, Il Mulino, Bologna, 2023, p.21.
[96] L. Torchia, *op. cit.*, p. 103.
[97] Previsto dalla l. 28 giugno 2024 n. 90.
[98] M. Mazzucato, *Lo Stato innovatore*, Laterza, Bari, 2014, p. 52.

tensione mostra come governare la tecnologia significhi anche fare scelte politiche di lungo periodo, che influenzano la formazione di competenze e la disponibilità di infrastrutture fondamentali, reti di comunicazione e piattaforme di dati aperti.

4. La costruzione di un fondamento giuridico per l'utilizzo delle nuove tecnologie quale presupposto per la *governance*.

4.1. Nuove tecnologie e principio di legalità: questioni introduttive.

Presupposto della regolazione e quindi anche della *governance* delle nuove tecnologie è la necessaria definizione delle stesse dal punto di vista giuridico. L'aspetto definitorio è sempre presente nello studio del diritto, elemento imprescindibile di ogni analisi. A questo non si sottrae lo strumento tecnico, il quale ancorché ben inquadrato dalla disciplina di riferimento, necessita di una sua enucleazione giuridica, a livello legislativo o frutto dell'elaborazione degli interpreti, in modo da consentire l'utilizzo regolamentato.

Questo problema è particolarmente evidente rispetto a strumenti come l'intelligenza artificiale, l'algoritmo, il *software* e altri. Poiché iniziando ad essere impiegati nelle pubbliche amministrazioni, ad essi viene attribuita la capacità di produrre un effetto giuridico. Come si vedrà nel prosieguo questo aspetto è stato particolarmente evidenziato dalla giurisprudenza amministrativa.

Fino ad anni relativamente recenti il tema dell'intelligenza artificiale era quasi assente nel dibattito pubblico, ristretto a determinati ambiti come quello accademico e delle industrie operanti nel settore delle tecnologie digitali. Tuttavia, a partire dal 2017 è possibile ravvisare un netto cambiamento, che apre la strada alla più ampia discussione sulle tecnologie ricomprese in questa espressione e le prospettive future. In quell'anno si verificano, infatti, due accadimenti significativi. Il primo è la dirompente novità delle reti neurali[99] *transformer* ideate da un gruppo di tecnici di Google e capaci di superare i limiti delle reti neurali fino ad allora utilizzate, aprendo la strada allo sviluppo dei *Large*

[99] Le reti neurali sono un modello matematico elaborato per la prima volta negli anni Quaranta del secolo scorso dai matematici W.S. McCulloch, W. Pitts e D.O. Hebb con l'intento di replicare la struttura dei neuroni cerebrali. Negli anni successivi gli scienziati furono in grado di dimostrare come questi modelli fossero in grado di apprendere sulla base di esempi di apprendimento per svolgere compiti, senza dovere ogni volta riprogrammare. Sul punto W. Ertel, *Introduction to Artificial Intelligence*, Springer, 2017, p. 9.

Language Model[100] il cui esempio più conosciuto è ChatGPT di OpenAi[101]. Il secondo è costituito dalle prime decisioni del Giudice amministrativo in cui viene affrontata la questione dell'uso di algoritmi da parte della Pubblica amministrazione per prendere una decisione[102]. Segno di un cambio di passo anche relativamente al grado di attenzione che si sta ponendo sull'argomento, nel 2017 esce il *Global Risk Report* del *World Economic Forum*, dedicato anche all'intelligenza artificiale e ai pericoli associati alla sua diffusione in particolare nei settori dell'economia, della geopolitica e delle tecnologie[103].

Gli interpreti del diritto sono quindi stati portati a confrontarsi con la rivoluzione tecnologica in atto nella quale il principio di legalità si pone come cruciale, in quanto pietra angolare dello stato di diritto, fondamento e limite del potere, per uno sviluppo dell'IA e quindi di una sua regolamentazione.

Prima ancora del legislatore, con i problemi derivanti dall'applicazione dell'intelligenza artificiale si è dovuto confrontare il Giudice amministrativo, il quale, in assenza di una fonte di rango primario che dettasse regole sull'utilizzo, ha elaborato delle soluzioni applicando i principi e le norme vigenti, in particolare il principio di legalità.

La legalità amministrativa si è affermata per fasi, ma nella sua evoluzione storica non ha mai ottenuto un chiaro riconoscimento in una disposizione, neppure al livello costituzionale[104]. La Costituzione italiana, infatti, non contiene una dichiarazione di tale principio se non indirettamente, quando ad esempio richiede il necessario fondamento

---

[100] I *large language models* sono una categoria di modelli fondativi addestrati su grandi quantità di dati, per renderli capaci di comprendere e quindi generare linguaggio naturale. In particolare, i modelli fondativi sono stati teorizzati da un gruppo di ricercatori che li hanno definiti così: «*A foundation model is any model that is trained on broad data (generally using self-supervision at scale) that can be adapted (e.g., fine-tuned) to a wide range of downstream tasks*», v. R. Bommasani, D. H. Hudson et. al., *On the opportunities and risks of foundation models*, disponibile in https://crfm.stanford.edu/report.html.

[101] Tale invenzione è stata spiegata in A. Vaswani, N. Shazeer et al., *Attention is all you need,* in *Advances in Neural Information Processing Systems*, 2017, pp. 5999-6009, i quali propongono un modello matematico, qualitativamente migliore in termini di capacità e velocità di apprendimento.

[102] Si tratta della sentenza TA.R. Lazio, sezione III *bis*, 22.03.2017 n. 3769, con cui è stato deciso il ricorso presentato da alcuni insegnanti avverso la decisione di assegnazione della sede di lavoro decisa dal Ministero dell'Istruzione mediante affidamento del compito ad un algoritmo.

[103] AA.VV., *The Global Risks Report 2017. 12th Edition*, in www3.weforum.org/docs/GRR17_Report_web.pdf.

[104] B. Sordi, *Il principio di legalità nel diritto amministrativo che cambia. La prospettiva storica*, in *Dir. amm*., 1, 2008, p. 1.

legislativo per ogni prestazione personale o patrimoniale (art. 23) o per l'organizzazione amministrativa dei pubblici uffici (art. 97)[105].

In effetti la dottrina ravvisa una chiara affermazione del principio solamente nell'art. 1 della l. n. 241/1990, ove si statuisce che «l'attività amministrativa persegue i fini determinati dalla legge», quindi vi sarebbe quantomeno un principio di legalità rispetto ai fini.

Di fronte a queste lacune, la legalità nel diritto amministrativo risulta essere piuttosto il frutto di una elaborazione teorica[106], secondo cui in primo luogo essa designerebbe la subordinazione alla legge dei pubblici poteri[107]. Da questa premessa una parte della dottrina ha ravvisato il perno della legalità nella connessione con il principio di sovranità parlamentare, quale garanzia dei diritti[108], mentre altra parte ha sostenuto la maggiore ampiezza di tale principio rispetto a quanto è stato determinato dal legislatore. In particolare, il principio di legalità implicherebbe: la preferenza per la legge, per cui è invalido ogni atto dei pubblici poteri che sia in contrasto con la legge; la legalità in senso formale, secondo cui l'Amministrazione non può provvedere se non le è stato attribuito il potere da una norma; ed infine la legalità sostanziale, in base alla quale la legge attribuisce il potere e determina le modalità del suo esercizio[109].

Corollari del principio di legalità sono il principio di nominatività, ossia è la legge ad indicare quale atto può essere adottato per un determinato fine, e il principio di tipicità, in base al quale la legge determina il contenuto e quindi gli effetti del provvedimento amministrativo.

La domanda che ci si pone è quale possa essere lo spazio di utilizzo dell'intelligenza artificiale da parte della pubblica amministrazione, nel quadro del principio di legalità.

Per poter dare una risposta sembra opportuno partire dalla nozione di intelligenza artificiale, ancorché non giuridica. Ed un tanto appare fondamentale poiché, se è

---

[105] A. Romano, *Amministrazione, principio di legalità e ordinamenti giuridici*, in *Dir. amm*. 1, 1999, p. 113.

[106] I contributi sono molti, F. Satta, *Principio di legalità e pubblica amministrazione nello Stato democratico*, Padova 1969, G. SALA, *Potere amministrativo e principi dell'ordinamento*, Milano, 1993, N. Bassi, *Principio di legalità e poteri impliciti*, Milano 2001. V. Cerulli Irelli, *Principi del diritto amministrativo*, *vol. II*, Giappichelli, Torino, 2005, G. Corso, *Il principio di legalità*, in M.A. Sandulli, *Codice dell'azione amministrativa*, Giuffrè, Milano, 2010, p. 16, S. Toschei, A. Puzzanghera, *La crisi del principio di legalità amministrativa*, in *Dir. pubbl. comp. eur.*, 4, 2022, pp. 897-916.

[107] E. Casetta, *Manuale di diritto amministrativo*, Milano, 2017.

[108] S. Civitarese Matteucci, *Il significato formale dell'ideale del «governo delle leggi» (rule of law)*, in *Dir. amm.*, 1, 2011, p. 29.

[109] R. Giovagnoli, *Compendio di diritto amministrativo*, ita ed., Torino, 2022, p. 326.

necessario dotarsi di concetti sufficientemente precisi per poter applicare le norme, avere una nozione condivisa di IA è indispensabile al fine di distinguere i sistemi informatici intelligenti da quelli che non lo sono, per poter applicare solo ai primi gli istituti e le norme riferibili all'intelligenza artificiale[110].

In generale si può affermare che tutte le macchine funzionano attraverso un algoritmo, concetto più ampio di intelligenza artificiale con cui si intende una sequenza predefinita e finita di istruzioni per eseguire uno specifico compito[111]. Il termine algoritmo viene utilizzato spesso in modo improprio per indicare anche l'IA, si pensi ad esempio alla "decisione algoritmica", mentre invece ha significato più ampio, dal che deriva che tutti i sistemi di IA presuppongono algoritmi, ma non tutti gli algoritmi riguardano l'intelligenza artificiale. Quelli che non riguardano l'IA sono definiti "classici" [112].

4.2. Algoritmo, intelligenza artificiale, *software*: alcune nozioni.

La prima definizione di IA è stata data da John McCarthy[113], tra i primi a dedicarsi alla ricerca in questo campo, secondo il quale «*the goal of AI is to develop machines that behave as though they were intelligent*», successivamente criticata per i limiti concettuali e riformulata da altri studiosi secondo diverse teorizzazioni, raggruppabili in quattro insiemi a seconda dell'approccio seguito[114]. Alcune definizioni danno rilevanza a pensiero e ragionamento, mentre altre si concentrano sul comportamento; altre ancora misurano il successo in termini di fedeltà alle prestazioni umane, o la razionalità, nel

---

[110] G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022, p. 7.

[111] T. H. Cormen, C. E. Leiserson, et al., *Introduction to Algorithms*, MIT Press, 2009, p. 5, in particolare «*an algorithm is any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output. An algorithm is thus a sequence of computational steps that transform the input into the output.*
We can also view an algorithm as a tool for solving a well-specified computational problem. The statement of the problem specifies in general terms the desired input/output relationship. The algorithm describes a specific computational procedure for achieving that input/output relationship». Il *Glossario* del *National Institute of Standards and Technology* definisce algoritmo «*A clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result*»

[112] G. Sartor, F. Lagioia, *Le decisioni algoritmiche tra etica e diritto*, Milano, 2020, p. 64.

[113] W. Ertel, *op. cit.*, p.1.

[114] Per una ricostruzione storica della nozione di intelligenza artificiale cfr. W. Ertel, *op. cit.* che riporta le definizioni elaborate dai matematici, in particolare «*in the Encyclopedia Britannica one finds a Definition that goes like: AI is the ability of digital computers or computer controlled robots to solve problems that are normally associated with the higher intellectual processing capabilities of humans*» e S. J. Russell, P. Norvig, *Artificial Intelligence. A modern approach*, Pearson Ed., 2010.

senso che un sistema è considerato razionale se fa la cosa giusta[115]. Tra le varie formulazioni, quella che merita di essere segnalata è stata elaborata da Elaine Rich, poiché meglio esprime a cosa ci si riferisce con IA: «*Artificial Intelligence is the study of how to make computers do things at which, at the moment, people are better*»[116].

Con tale definizione si designa dunque un settore nel quale sono studiati e sviluppati metodi volti a far svolgere alla macchina cose rispetto alle quali (per il momento) gli esseri umani forniscono prestazioni migliori. E se per l'essere umano l'esecuzione di qualsiasi mansione richiede apprendimento, similmente per l'IA risulta essere centrale il *machine learning*[117], ossia la capacità di una macchina di migliorare la sua performance con l'esperienza, utilizzando algoritmi che apprendono da dati specifici per il problema, permettendo alla macchina di trovare soluzioni e schemi d'azione senza che ciò sia stato programmato in maniera specifica[118]. In base al tipo di attività di apprendimento, si possono inoltre distinguere diverse sottocategorie di algoritmi di *machine learning*, tra cui le *artificial neural networks* (o ANN), ossia un modello matematico rappresentante neuroni connessi tra loro e organizzati in una rete, per trasmettere un segnale; si tratta di un sistema molto diffuso per allenare un algoritmo[119]. Una sottocategoria delle ANN sono le *deep neural networks* (DNN) la cui caratteristica saliente è la capacità di elaborare dati non strutturati. Gli algoritmi basati sul *deep learning* possono processare grandi quantità di dati per svolgere determinati compiti, senza bisogno di doverli prima strutturare e ordinare. Per loro natura gli algoritmi basati sulle ANN e DNN non sono interpretabili e quindi costituiscono una *black box*[120], ossia un sistema di IA opaco, poiché per la sua complessità e per la sua struttura non è possibile comprenderne il funzionamento, non è chiaro il processo per cui dato un input si genera un output. Questa mancanza di trasparenza rende impossibile per l'utente individuare eventuali errori o *bias*[121].

Questo problema diventa decisivo nel momento si utilizzano sistemi di IA nel settore pubblico, dove trasparenza e responsabilità sono requisiti fondamentali. La mancanza di

---

[115] S. Russel, P. Norvig, *op. cit.*, p. 2.
[116] E. Rich, *Artificial Intelligence,* New York, 1983.
[117] W. Ertel, *Introduction to Artificial Intelligence*, 2017, p. 3.
[118] C. Janiesch, P. Zschech, K. Heinrich, *Machine learning and deep learning*, in *Electronic markets*, 4, 2021, p. 686.
[119] S. Russel, P. Norvig, *op. cit.,* p. 728.
[120] C. Janiesch, P. Zschech, K. Heinrich, *op. cit*., p. 688.
[121] V. Hassija, V. Chamola et al., *Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence*, in *Cognitive Computation*, Springer, 2024, p. 47.

esplicabilità mina i principi della buona amministrazione, poiché impedisce a cittadini e funzionari di comprendere le decisioni assunte da o con l'algoritmo, in contrasto col principio della trasparenza e imputabilità delle decisioni alla persona fisica, e quindi di legittimità della decisione[122].

Dalle nozioni di algoritmo e intelligenza artificiale va poi tenuta distinta quella di *software*, atteso che secondo la *World Intellectual Property Organization* con esso si intende «*a set of instructions capable, when incorporated in a machine-readable medium, of causing a machine having information-processing capabilities to indicate, perform or achieve a particular function, task, or result*».

In sintesi, l'algoritmo classico include una sequenza di istruzioni definite, per eseguire un dato compito in maniera efficiente; mentre un algoritmo di intelligenza artificiale elabora a partire dai dati sui quali è stato allenato, nuovi schemi per poter produrre un risultato non necessariamente atteso da chi ha impostato il modello. Infine, il *software* è un insieme di istruzioni per eseguire o fare eseguire un compito.

4.3. Le ricostruzioni concettuali nelle decisioni del giudice amministrativo.

Avere ben specificate queste nozioni risulta importante nel campo del diritto, che richiede certezza definitoria, per poter stabilire il perimetro di rilevanza e conseguentemente applicare le norme. Questo è lo sforzo fatto dalla giurisprudenza amministrativa quando è stata chiamata a pronunciarsi su questi temi.

La strada per l'individuazione di una nozione di algoritmo e di intelligenza artificiale, nonché di *software*, in assenza di una disposizione di rango primario che ne tracci chiare le nozioni, ha visto la giurisprudenza impegnata in attività di elaborazione delle definizioni, onde fare chiarezza.

[122] G. Lo Sapio, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *federalismi.it*, 16, 2021, p. 122, e come evidenzia l'autore, «In mancanza di spiegabilità, anche il principio di responsabilità ultima della decisione resta svuotato, poiché il maccanismo di funzionamento del sistema algoritmico deve essere comprensibile, in primo luogo, per il titolare dell'organo che assume la decisione». In questo senso v. anche A. Cerrillo i Martínez, *How can we open the black box of public administration? transparency and accountability in the use of algorithms*, in *Revista Catalana de Dret Públic*, p. 13-28. doi.org/10.2436/rcdp.i58.2019.3277.

Emblematica è la decisione del giudice amministrativo[123], che volendo formulare una definizione di algoritmo e distinguerla da quello di intelligenza artificiale, afferma che con algoritmo «ci si richiama, semplicemente, a una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato», laddove la nozione di intelligenza artificiale è «riconducibile invece allo studio di 'agenti intelligenti', vale a dire allo studio di sistemi che percepiscono ciò che li circonda e intraprendono azioni che massimizzano la probabilità di ottenere con successo gli obiettivi prefissati. È possibile allora comprendere che esistono anche algoritmi di intelligenza artificiale, vale a dire algoritmi, tecniche computazionali, soluzioni che siano in grado di replicare il comportamento umano: sono tali, ad esempio, quelli che interagiscono con l'ambiente circostante o con le persone, che apprendono dall'esperienza (*machine learning*), che elaborano il linguaggio naturale oppure che riconoscono volti e movimenti».

Tale ricostruzione non è stata esente da critiche. Successivamente il Consiglio di Stato[124], pronunciandosi sull'appello proposto avverso la menzionata sentenza del T.A.R. milanese, spiega «Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo 'tradizionale') ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico».

La questione della nozione non è di secondario rilievo, poiché l'utilizzo improprio delle espressioni algoritmo e intelligenza artificiale genera confusione sul tipo di tecnologia cui si fa riferimento e conseguentemente sui principi e le regole applicabili. Il Consiglio di Stato critica la nozione di algoritmo fornita dal giudice di prime cure, ravvisandone l'errore concettuale di legarla a quella di IA e non a quella di automazione, laddove per automatizzare non è necessario fare ricorso all'IA, ma appare sufficiente far sì che ad un certo input corrisponda un determinato output. Tuttavia, i giudici dell'appello nel tentativo di fare chiarezza su queste nozioni, ancora sfuggenti nel sistema

[123] T.A.R. Lombardia, 31 marzo 2021 n. 843.
[124] Cons. St., sez. III, 25 novembre 2021 n. 7891, che ha deciso sull'appello proposto avverso la sentenza del T.A.R. Lombardia, 31 marzo 2021 n. 843.

amministrativo e capaci di creare dubbi interpretativi[125], riescono solamente in parte a dipanare le incertezze. Ancorché delineino una più comprensibile distinzione tra IA e algoritmo classico, rammentando l'importanza del concetto di automazione riferibile a sistemi tecnologici in generale e non necessariamente a quelli di IA, confondono la nozione di *software* e quella di algoritmo[126]. Il primo si riferisce all'esecuzione di una serie di istruzioni, mentre il secondo indica una sequenza di istruzioni.

Sul tema della natura giuridica del *software*, la sentenza T.A.R. Lazio, sezione III bis, 16 maggio 2023 n. 8384 offre un'interessante prospettiva, qualificandolo come atto amministrativo informatico, ma «solo laddove l'utilizzo del mezzo informatico sia strumentale all'esercizio di un potere autoritativo di stampo pubblicistico» e non in ogni ipotesi di utilizzo del mezzo informatico, per cui «solo laddove il programma informatico sia asservito a un procedimento amministrativo in senso stretto». Nella prospettiva del giudice amministrativo il *software*, quindi, andrebbe considerato quale strumento della volontà dell'amministrazione; tuttavia, se partiamo dalla nozione data nel precedente paragrafo, quale strumento che formalizza un processo logico, espresso in codice algoritmico, è evidente come esso non possa costituire un atto informatico[127], bensì, come ritenuto dal Consiglio di Stato[128], esso va considerato quale «modulo organizzativo-operativo», ovvero uno strumento procedimentale e istruttorio, che l'autorità può scegliere di utilizzare.

Una precisa e chiara distinzione in senso giuridico tra IA, algoritmo e *software*, non risulta esservi, il che ha riflessi sotto il profilo delle norme applicabili (ad esempio quelle sull'accesso) e, come rileva la richiamata sentenza del Tar, anche sotto il profilo della giurisdizione, nonché della legalità di questi strumenti.

Nel 2017 il giudice amministrativo[129] si trova ad affrontare una questione assolutamente nuova, quella dell'accesso all'algoritmo. Questo gruppo di pronunce si inseriscono nel

---

[125] Per un commento sulla decisione del Consiglio di Stato si veda C. Filicetti, *Sulla definizione di algoritmo (nota a Consiglio di Stato, Sezione Terza, 25 novembre 2021 numero 7891)*, in www.giustiziainsieme.it.

[126] S. Cereda, *Il concetto di algoritmo in una recente sentenza del Consiglio di Stato*, in *Medialaws*, 3, 2022, p. 300.

[127] D. Diaco, *Brevi riflessioni sulla natura giuridica del software (a partire da TAR Lazio, sez. III-bis, n. 8384/2023),* in www.giustiziainsieme.it.

[128] In tal senso Cons. St., sezione VI, 13 dicembre 2019, n. 8472, di cui si dirà diffusamente nel prosieguo.

[129] T.A.R. Lazio, sezione III *bis*, 21 marzo 2017 n. 3742 e T.A.R. Lazio, sezione III *bis,* 22 marzo 2017 n. 3769.

filone di decisioni relative alla procedura di mobilità degli insegnanti delle scuole superiori decisa dal Ministero dell'Università e della Ricerca.

Questa, in breve, la vicenda. Nel 2016, in forza della l. 13 luglio 2015 n. 107, il MIUR avvia una procedura di mobilità per gli insegnanti, il cui svolgimento viene demandato ad un *software* che, valutati i requisiti richiesti, attribuisce la sede al docente secondo un meccanismo automatico, senza alcun intervento del Ministero. All'esito della procedura alcuni insegnanti si vedono assegnati a sedi molto distanti dal luogo di residenza, nonostante la presenza di posti vacanti più vicini, risultando oscuri i criteri adottati nella procedura per stabilire la sede di lavoro. Per tali ragioni i sindacati scolastici chiedono al MIUR di poter accedere all'algoritmo e a seguito di diniego presentano ricorso.

Nell'accogliere la domanda dei ricorrenti il giudice amministrativo ha l'occasione di riflettere sulla natura dell'algoritmo e del *software* e sull'atto amministrativo informatico. Il collegio, operando una distinzione tra atto avente forma elettronica e atto ad elaborazione elettronica, ossia l'atto l'elaborazione del cui contenuto viene affidata ad una macchina, superando l'opinione della dottrina per cui solo il primo è suscettibile di accesso, allarga il concetto di atto amministrativo tracciato dall'art. 22 l. n. 241/1990 estendendolo anche all'atto elaborato elettronicamente, riconoscendo peraltro come questa forma di atto sia ammissibile quando si è in presenza di attività vincolata, in cui tutti gli elementi di fatto e i requisiti di diritto sono predeterminati e quindi facilmente programmabili in linguaggio eseguibile dalla macchina.

La soluzione appare certamente innovativa perché, superando concetti consolidati nel tempo come quello di atto o documento amministrativo, reinterpreta le norme alla luce delle nuove tecnologie, ritenendo accessibile il codice sorgente[130], ossia l'insieme delle istruzioni scritte in linguaggio comprensibile all'uomo, eseguibili dalla macchina.

Se queste due pronunce hanno il pregio di aver proposto una prima soluzione ad un problema specifico, quello dell'accesso agli atti, di maggiore interesse si rivelano le sentenze T.A.R. Lazio, sezione III bis, 10 settembre 2018 n. 9224 e T.A.R. Lazio, sezione III bis 10 settembre 2018 n. 9227. In questo caso il giudice amministrativo

[130] Per un vaglio critico delle due sentenze cfr. E. Prosperetti, *Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del Tar Lazio*, in *Dir. inform*, 4, 2019, p. 979, secondo cui il T.A.R. arriva ad ampliare eccessivamente la sua analisi, con la conseguenza che se si applicasse in via generale quanto stabilito in motivazione si determinerebbe un implicito divieto per la PA di utilizzare *software* con codice sorgente chiuso o che comunque non consente di fornirlo in caso di accesso agli atti.

viene chiamato a decidere sulla legittimità del provvedimento con cui sono state decise le sedi di lavoro degli insegnanti, elaborato da un sistema informatico, e conseguentemente a riflettere sull'ammissibilità di una simile determinazione.

Nel caso di specie il GA ha ritenuto dirimente l'argomento secondo cui è mancata nella fattispecie una vera e propria attività amministrativa, «essendosi demandato ad un impersonale algoritmo lo svolgimento dell'intera procedura di assegnazione dei docenti alle sedi disponibili nell'organico dell'autonomia della scuola». In sostanza il giudice critica fortemente l'impiego di un algoritmo in un procedimento amministrativo, affermando che in alcun caso è possibile devolvere l'attività amministrativa ad «un meccanismo informatico o matematico del tutto impersonale e orfano di capacità valutazionali delle singole fattispecie concrete, tipiche invece della tradizionale e garantistica istruttoria procedimentale», poiché un algoritmo non può mai assicurare «la salvaguardia delle guarentigie procedimentali che gli artt. 2, 6,7,8,9,10 della legge 7 agosto 1990 n. 241» violandosi altresì il canone di trasparenza e di partecipazione procedimentale, così come l'obbligo di motivazione.

Inizialmente, quindi, la giurisprudenza mostra chiusura totale nei confronti dell'impiego di algoritmi nel procedimento amministrativo, confermando questa posizione con le sentenze nn. 6606 e 6607 del 2019 del T.A.R. Lazio[131].

Tuttavia, tale posizione viene superata con un mutamento di indirizzo da parte dello stesso del Consiglio di Stato[132]. La novità si coglie nella sentenza n. 2270/2019 ove, riconosciuti gli indiscutibili vantaggi derivanti dalla automazione del processo decisionale, in particolare in quelle procedure seriali che richiedono di elaborare grandi quantità di istanze, quale applicazione dei canoni di efficienza ed economicità (sanciti dall'art. 1 l. 241/1990) e di buon andamento della pubblica amministrazione (stabilito dall'art. 97 Cost.), si pone l'accento sull'ammissibilità della regola algoritmica definita comunque regola amministrativa. Essa deve soggiacere ai principi generali dell'azione amministrativa, non può avere spazi applicativi discrezionali, l'amministrazione deve avere in ogni caso un ruolo di mediazione e composizione degli interessi e deve contemplare la possibilità per il giudice di valutare la correttezza del processo decisionale.

[131] T.A.R. Lazio, sez. III *bis*, 27 maggio 2019 n. 6606 e n. 6607.
[132] Cons. St., sez. VI, 08 aprile 2019, n. 2270, Cons. St., sez. VI, 13 dicembre 2019, nn. 8472, 8473, 8474.

Tuttavia, sono le successive pronunce del Consiglio di Stato, le nn. 8472, 8473, 8474 del 2019, ad esprimere una posizione ancora più chiara rispetto all'automazione del procedimento amministrativo, fornendo un decalogo dei principi per l'ammissibilità della decisione algoritmica[133].

4.4. I principi e i limiti per l'impiego dell'intelligenza artificiale nella pubblica amministrazione.

Premessa la generale ammissibilità di tali strumenti, intesi quale modulo organizzativo di strumento procedimentale e istruttorio, il Consiglio di Stato indica quali debbano essere gli elementi minimi di garanzia in ogni ipotesi in cui vengano utilizzati algoritmi, ossia «a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati; b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo». La piena conoscibilità deve essere assicurata dalla trasparenza, intesa sia per la PA che si avvale di tali strumenti sia per il privato che subisce la decisione presa mediante esso. A questi requisiti minimi, il giudice enuncia tre principi ricavati dal diritto sovranazionale, in particolare dal GDPR (il regolamento europeo sui dati personali), ossia: il principio di conoscibilità, il principio di non esclusività della decisione algoritmica e il principio di non discriminazione algoritmica. Questi principi costituiscono i pilastri della c.d. legalità algoritmica, condizioni indispensabili per la legittimità delle decisioni automatizzate[134].

In base al primo principio ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e ricevere informazioni sulla logica utilizzata. In base al secondo, si impone l'esistenza nel processo decisionale del contributo umano capace di controllare, validare o smentire la decisione automatica; ossia quello che in ambito informatico viene definito *human in the loop*, dove, per produrre il risultato, è necessario che la macchina interagisca con l'essere umano.

[133] Per un commento dettagliato della sentenza Cons. St., 13 dicembre 2019, n. 8472, E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm*. 2, 2020.

[134] F. Nassuato, *Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*, in *Ceridap*, 1, 2022, p. 156.

Infine, secondo il terzo principio è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca effetti discriminatori nei confronti delle persone fisiche.

Con una significativa apertura, il Consiglio di Stato conferma la legittimità dell'uso degli algoritmi, già riconosciuta nella precedente decisione n. 2270/2019, nell'attività vincolata e in via ipotetica anche in quella discrezionale[135]. In assenza di un quadro normativo di riferimento, facendo ricorso alle fonti nazionali e sovranazionali (in particolare il GDPR), il Consiglio enuncia quelli che sono i principi cui deve essere informata l'azione algoritmica dei pubblici poteri.

L'importanza di tale approdo giurisprudenziale si apprezza anche in considerazione del fatto che con il d.lgs. n. 36/2023 (Nuovo codice degli appalti), detti principi sono stati positivizzati.

Nel ragionamento del Consiglio di Stato alla base della legittimazione all'uso di sistemi intelligenti vi è la trasparenza, intesa in senso rafforzato, quale comprensibilità dell'algoritmo. Tuttavia, come è stato evidenziato[136], l'effettiva comprensibilità di un procedimento automatizzato si scontra con un triplice livello di opacità algoritmica: un primo livello è di tipo intenzionale e attiene alla creazione stessa dell'algoritmo da parte del programmatore; un secondo livello è di tipo tecnico, relativo al linguaggio adottato dalla macchina, che è avulso dal linguaggio naturale e pertanto non intelligibile da parte di chi non sia un informatico esperto; infine vi è un terzo livello di opacità intrinseca, relativa a quegli algoritmi che sono stati allenati con tecniche di *machine learning* o *deep learning*, tali per cui nemmeno il programmatore è in grado di avere un controllo puntuale sull'attività. Da un tanto deriverebbe una difficoltà di concreta attuazione dei principi formulati dal Consiglio di Stato.

[135] Cons. St., sez. VI, 13 dicembre 2019, n. 8472, conforme Cons. St., sez. VI, 04 febbraio 2020, n. 881.
[136] A. Mascolo, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giorn. dir. amm.*, 3, 2020, p. 371.

Sulla questione della conoscibilità anche il T.A.R. Campania n. 7003/2022[137] si è inserito nel solco tracciato dalla sentenza n. 8472/2019 del Consiglio di Stato, ribadendo la funzione servente dell'algoritmo, il cui utilizzo non può mai comportare un abbassamento del livello delle tutele garantite dalla legge sul procedimento amministrativo. E tra queste garanzie vi è il principio di trasparenza, che trova il suo corollario nell'obbligo di motivazione. E, prosegue il giudice campano, deve essere sempre assicurato un controllo umano sulla decisione presa da un algoritmo, secondo il modello dello *human in the loop*, per cui «il funzionario possa in qualsiasi momento intervenire per compiere interlocuzioni con il privato, per verificare a monte l'esattezza dei dati da elaborare, mantenendo il costante controllo del procedimento». Concetto già espresso dal Consiglio di Stato nella sentenza n. 881/2020 con cui i giudici di Palazzo Spada avevano affermato che «deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica». Un tanto appare coerente con l'impianto della l. n. 241/1990, che vede come figura centrale il responsabile del procedimento quale personalizzazione dell'azione amministrativa[138]. Il T.A.R. Campania, tuttavia, evidenzia il ruolo centrale dell'amministrazione anche nella selezione e verifica dell'algoritmo impiegato[139].

Affermare la centralità della figura umana anche nel procedimento automatizzato risponde quindi all'esigenza di preservare le garanzie previste dalla l. n. 241/1990, e in particolare la possibilità di interloquire con una figura fisica all'interno della pubblica amministrazione e non con un ente spersonalizzato, cosa che si verificherebbe qualora si lasciasse soltanto alla macchina la funzione amministrativa. In questo contesto il responsabile del procedimento rimane figura fondamentale, dovendo assicurare le garanzie partecipative e di non discriminazione e dovendo rendere intelligibile alle parti la formula tecnica adottata per la decisione, corredata dalle opportune spiegazioni[140].

Alla luce delle sentenze riportate, risulta chiara la posizione favorevole della giurisprudenza maggioritaria, seppur con la precisazione del Consiglio di Stato, per cui

[137] T.A.R. Campania, sez. III, 14 novembre 2022, n. 7003.

[138] M. Sforna, *Le garanzie di conoscibilità degli algoritmi e l'esigenza di assicurare un controllo umano del procedimento amministrativo (c.d. human in the loop). (Nota a Tar Campania, Sez. III, 14 novembre 2022, n. 7003)*, in www.giustiziainsieme.it.

[139] D. Ponte, *Serve conoscenza e comprensione della decisione "automatizzata" (nota a Tar Campania, Sez. III, 14 novembre 2022, n. 7003)*, in *Guida al diritto*, 46, 2022, p. 96.

[140] E. Faletti, *Mai accettare caramelle né atti amministrativi da sconosciuti, ancorché algoritmi (Nota a T.A.R. Napoli, 14 novembre 2022, n.7003, sez. III),* in *Dir. inform.*, 17, 2023, p. 97.

«il ricorso all'algoritmo va correttamente inquadrato in termini di modulo organizzativo, di strumento procedimentale ed istruttorio, soggetto alle verifiche tipiche di ogni procedimento amministrativo, il quale resta il modus operandi della scelta autoritativa, da svolgersi sulla scorta delle legislazione attributiva del potere e delle finalità dalla stessa attribuite all'organo pubblico, titolare del potere»[141].

Già molto tempo fa una parte della dottrina si era interrogata sui processi di automazione della pubblica amministrazione e le possibili implicazioni[142], ma a partire dalle recenti pronunce della giurisprudenza il dibattito si è ampliato e vede una posizione maggioritaria favorevole, anche applicando le norme esistenti.

Con le prime pronunce in materia di IA e decisione amministrativa sono balzati all'attenzione gli interrogativi sulla necessità di una norma che conferisca all'amministrazione il potere di emanare un provvedimento in forma automatizzata o meno. Nello specifico la dottrina si è posta tre domande: serve una norma attributiva del potere, in via generale, in stretta applicazione del principio di legalità? È necessaria una norma che oltre ad autorizzare il ricorso alla decisione automatizzata specifichi anche le modalità del suo impiego? O ancora, è possibile prescindere da una norma apposita?

Come si è visto, a questi interrogativi ha dato una risposta la giurisprudenza, che in via interpretativa si è orientata nel senso di riconoscere l'ammissibilità della decisione algoritmica, nella misura in cui i sistemi di automazione vengono utilizzato in funzione servente, quali moduli organizzativi della PA.

Secondo questa prospettiva, la possibilità di avvalersi di strumenti di IA è implicita nell'attribuzione del potere, alla luce dei principi di imparzialità e buon andamento di cui all'art. 97 della Costituzione, che legittimano l'amministrazione a scegliere i mezzi di cui dotarsi per l'esecuzione dei propri compiti, prediligendo quegli strumenti in grado di massimizzare l'efficienza e l'efficacia e garantire maggiore imparzialità[143]. Gli algoritmi non sono quindi avulsi dal contesto in cui sono utilizzati, essi fanno parte dell'amministrazione e sono strumenti per la decisione[144]. Una dimensione legale può essere ricavata non solo dalle fonti europee, nazionali e dall'attività interpretativa dei

[141] In tal senso Cons. St., sez. VI, 13 dicembre 2019, n. 8472 e Cons. St., sez. VI, 4 febbraio 2020, n. 881.
[142] Tra questi G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996; v. anche A. Masucci, *L'atto amministrativo informatico: primi lineamenti di una ricostruzione*, Napoli, 1993.
[143] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. inform.*, 3, 2021, p. 459.
[144] I. M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Ist. Federalismo*, 3, 2019, p. 658.

tribunali, ma anche dagli strumenti di *soft law*, ad esempio linee guida del gruppo di esperti in materia di IA e la risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale (n. 2018/2088)[145].

Tuttavia, quello che emerge è una posizione (in particolare del Consiglio di Stato) favorevole con riferimento alle decisioni vincolate, e possibilista rispetto a quelle rientranti nell'esercizio del potere discrezionale[146], ma pur sempre con riferimento alle ipotesi in cui si tratti di automazione non attuata attraverso strumenti di intelligenza artificiale; in tale senso va infatti inteso il passaggio della sentenza n. 881/2020, ove si dice «la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima». Per cui quando si tratta di automazione mediante ricorso ad algoritmi tradizionali, i tradizionali istituti sembrano ancora applicabili; viceversa, nel caso in cui impieghino strumenti di IA, ove il grado di automazione è massimo, potrebbero essere necessari nuovi strumenti di garanzia[147].

Un'altra prospettiva offerta dalla dottrina nel tentativo di rendere compatibili queste nuove tecnologie con l'impianto normativo vigente è di fare ricorso allo strumento del *notice and comment*[148], per cui attraverso il coinvolgimento degli interessati sugli esiti cui è giunto l'algoritmo, si apre alla possibilità di contraddittorio e all'esito

---

[145] G. Orsoni, E. D'Orlando, *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Ist. Federalismo*, 3, 2019, p. 606, da questi riferimenti gli autori sintetizzano quelli che sono i punti di essenziali per una legalità algoritmica: *(i) l'algoritmo ha valenza giuridica e deve rispettare i principi dell'attività amministrativa; (ii) non può lasciare spazi applicativi discrezionali, nel senso che la discrezionalità va confinata nel momento dell'elaborazione dello strumento digitale, ove è sempre la PA che svolge ex ante un ruolo di mediazione e composizione di interessi; (iii) deve rispondere a fini predeterminati dalla legge, in ossequio al principio di legalità; (iv) deve essere monitorato e aggiornato nel tempo, attraverso test e perfezionamenti che, in quanto comportanti attività discrezionale, competono parimenti solo alla PA; (v) deve essere sindacabile dal giudice che, per la prima volta sul piano umano, svolge accertamenti e valutazioni fatti prima solo in via automatica e, quindi, verifica la correttezza del processo automatizzato in tutte le sue componenti, secondo il paradigma del giusto processo*".

[146] Dopo un'iniziale limitazione alle sole decisioni vincolate, in Cons. St. n. 2270/2019, si assiste ad una apertura anche per le decisioni discrezionali: «*Né vi sono ragioni di principio, ovvero concrete, per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse*», così Cons. St., sezione VI, n. 8472/2019.

[147] A.G. Orofino, G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giur. it*, 7, 2020, p. 1740.

[148] Strumento mutuato dall'esperienza statunitense e già impiegato specialmente dalle autorità amministrative indipendenti per raccogliere il contributo informativo e valutativo dei soggetti interessati, con cui viene data preventivamente notizia del progetto di atto e viene consentito agli interessati di fare pervenire le proprie osservazioni, M. Filice, *Il sindacato giurisdizionale sull'attività delle Autorità indipendenti*, in *Giorn. dir. amm.*, 4, 2015, p. 560.

l'amministrazione può confermare lo standard algoritmico, motivare la sua deroga o disporne la correzione[149]. In tal modo la base legale del procedimento algoritmico, e conseguentemente dell'atto adottato con questa modalità, verrebbe assicurata attraverso gli istituti di partecipazione previsti dalla L. n. 241/1990 (artt. 7, 8, 10 e 10 *bis*)[150]. Questa soluzione appare percorribile nella misura in cui si ritenga l'atto digitale uguale all'atto amministrativo tradizionale, e quindi manifestazione della volontà dell'amministrazione[151], ed invero non si discosterebbe dall'impostazione giurisprudenziale basata sui tre principi della decisione algoritmica. Sia che si tratti di fare applicazione dei principi di comprensibilità, non esclusività e non discriminazione dell'algoritmo, sia che si opti per il *notice and comment*, si tratta a bene vedere di soluzioni estrinsecanti la legalità procedimentale[152], ossia quella regola per cui il mancato rispetto del principio di legalità sostanziale può essere compensato tramite il rafforzamento delle garanzie procedimentali, come appunto la partecipazione[153], quindi con il contributo umano alla decisione algoritmica.

Un'ulteriore soluzione teorica alla legittimazione dell'esercizio di attività amministrativa mediante sistemi automatizzati, nonostante il deficit di legalità, può altresì essere rinvenuta, eventualmente, nel riferimento alla teoria dei poteri impliciti, locuzione con cui si indica quel potere non espressamente attribuito dalla legge all'amministrazione, ma comunque funzionale al conseguimento del fine pubblico, che la norma di rango primario comanda di perseguire nell'esercizio di poteri espressamente conferiti. È un potere esercitabile per realizzare lo scopo il cui perseguimento è indicato alla Pubblica amministrazione dalla legge[154].

---

[149] R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2, 2020, p. 12.

[150] R. Cavallo Perin, I. Alberti, *Atti e procedimenti amministrativi digitali*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 149;

[151] I. Alberti, *La partecipazione procedimentale per legittimare gli algoritmi nel procedimento amministrativo*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Rubettino Editore, 2021, p. 295.

[152] In tal senso, in riferimento ai principi della decisione algoritmica elaborati dal Consiglio di Stato si veda F. Nassuato, *op. cit*, p. 163.

[153] G. Manfredi, *Legalità procedurale*, in *Dir. amm.*, 4, 2021, p. 749.

[154] R. Garofoli, G. Ferrari, *Manuale di diritto amministrativo*, Molfetta, 2020, p. 554. Sulla teoria anche *ex mulits* Cons. St., sezione III, 01.12.2016, n. 5048.

4.5. La base giuridica per l'uso dell'intelligenza artificiale da parte della pubblica amministrazione.

I ragionamenti fin qui illustrati, pur offrendo soluzioni teoriche alla tecnologizzazione del procedimento, sembrano concentrarsi sull'automazione mediante algoritmi condizionali e non quelli elaborati attraverso il *deep learning*, che pongono maggiori problemi per il sistema normativo.

Se un ordinamento è privo di una norma generale che attribuisca alla pubblica amministrazione il potere di decidere in maniera automatizzata, non è scontato che il sistema di principi ed istituti pensato e costruito intorno al funzionario «essere umano» sia adattabile alle macchine[155].

La premessa concettuale per comprendere il problema passa attraverso la constatazione della diversità tra digitale e intelligenza artificiale, che attengono a due dimensioni non perfettamente sovrapponibili, in quanto la seconda rappresenta una prosecuzione del primo. Se, infatti, si può affermare che, prima dell'entrata in vigore del d.lgs. 31 marzo 2023 n. 36[156], mancava una norma che consentisse esplicitamente l'impiego di sistemi di IA da parte della Pubblica amministrazione, già da tempo vi sono disposizioni che prevedono la digitalizzazione dei procedimenti amministrativi, tra cui l'art. 3 *bis* della l. 241/1990 e gli artt. 12 e 41 del CAD[157].

Muovendo da questa premessa, l'approdo del Consiglio di Stato[158], certamente importante, non sembra superare il problema della inadeguatezza delle attuali regole del procedimento amministrativo, non tanto rispetto agli algoritmi deterministici o condizionali, diffusi da diverso tempo, per cui non sussisterebbero quindi problemi[159],

---

[155] D.U. Galetta, J. G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019, p. 22. S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl.*, 1, 2019, p. 36.

[156] L'art. 30, comma 1 del decreto recita, infatti, «Per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti», introducendo per la prima volta in una fonte di rango primario l'espressione IA.

[157] Sulla distinzione tra amministrazione digitale e amministrazione algoritmica cfr. A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta, *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020.

[158] In particolare, la sentenza Cons. St., n. 8472/2019.

[159] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, cit. p. 459. M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 16, 2019, p. 9; P. Otranto, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in *Federalismi.it*, 7, 2021, p. 198, il quale pur concordando sulla compatibilità tra algoritmi

quanto rispetto all'impiego di algoritmi non deterministici (ossia quelli dei sistemi di IA), dei quali sfugge la logica decisionale. Ed allora non risulta sufficiente la norma attributiva del potere per legittimare l'azione della PA mediante ricorso agli algoritmi[160], in quanto, affidandosi a questi sistemi, si finirebbe per delegare ad una macchina la decisione amministrativa[161], ossia, di fatto, a soggetti (i programmatori), spesso esterni all'amministrazione[162].

Secondo questa impostazione non sarebbe dunque sufficiente a permetterne l'uso la qualificazione dei sistemi intelligenti quali moduli organizzativi, operata dalla giurisprudenza, dovendo invece essere disciplinata con legge apposita la possibilità di delegare alla macchina l'adozione di decisioni amministrative con questi strumenti, nonché i principi e le regole che devono regolamentare tale delega.

Due recenti novità legislative sembrano andare nella direzione auspicata da quella parte della dottrina che ravvisando l'inadeguatezza delle disposizioni vigenti, invocava una minuta regolazione delle novità tecnologiche.

La prima è rappresentata dal richiamato art. 30 del Nuovo Codice Appalti. Mentre la seconda novità è il Regolamento del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale (l'*Aritificial intelligence Act*).

L'art. 30 del Nuovo Codice degli Appalti rappresenta il primo tentativo di regolare con una fonte di rango primario l'automazione dell'attività della pubblica amministrazione, anche attraverso il ricorso all'intelligenza artificiale, indicando altresì i principi ai quali la decisione automatizzata si deve conformare, che sono la positivizzazione di quelli elaborati dal Consiglio di Stato[163], una *constitutional rule* della decisione algoritmica[164].

---

deterministici e principi dell'attività amministrativa, solleva dubbi circa la possibilità di applicare alcune disposizioni della l. 241/1990 anche in caso di algoritmi comprensibili e trasparenti.

[160] P. Otranto, *op cit*., p.197.

[161] P. Otranto, *op. cit*., p. 199, secondo cui si arriva in tal modo ad affidare la cura dell'interesse pubblico ad un sistema fondato su un insieme di regole tecniche (l'algoritmo), in grado di conformare e orientare l'esercizio del potere, fino a far sorgere un vero e proprio centro di potere decisionale.

[162] Sulla esternalizzazione della funzione amministrativa ai privati, cfr. E. Picozza, *Intelligenza artificiale e diritto. Politica, diritto amministrativo and artificial intelligence*, in *Giur. it*., 7, 2019, p. 1657.

[163] L'art. 30, comma 3 recita: «Le decisioni assunte mediante automazione rispettano i principi di:

a) conoscibilità e comprensibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata;

b) non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata;

c) non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici».

Pertanto, pur essendo ristretta al campo degli appalti pubblici, e volta a migliorare la catena di approvvigionamento della pubblica amministrazione, ad esempio, per valutare e selezionare in maniera automatica l'offerta economica più vantaggiosa, si tratta di una norma di ampio respiro[165]. Come emerge dalla lettura della relazione[166] al testo del decreto legislativo, «Si tratta di una disposizione volta a disciplinare il futuro (prossimo), in quanto, allo stato, nell'ambito delle procedure di gara sono utilizzati per lo più algoritmi non di apprendimento, utilizzati per il confronto automatico di alcuni parametri caratterizzanti le offerte e conoscibili. Tuttavia, non si può escludere che, a breve, la disponibilità di grandi quantità di dati possa consentire l'addestramento di algoritmi di apprendimento da applicare alle procedure di gara più complesse; da qui l'utilità dell'inserimento di una disciplina che richiami i principi destinati a governare tale utilizzo, anche alla luce dei principi affermati sia in ambito europeo che dalla giurisprudenza amministrativa».

La questione della legalità algoritmica, in parte affrontata in tanto in quanto vi è una norma che attribuisce alla pubblica amministrazione (in qualità di stazione appaltante) il potere di ricorre all'automazione, mediante sia gli algoritmi, sia l'intelligenza artificiale[167], viene decisa dall'approvazione della l. 23 settembre 2025 n. 132 recante Disposizioni e deleghe al Governo in materia di intelligenza artificiale, che ha fornito altresì una definizione di IA mediante richiamo al Regolamento (UE) 2024/1689, che stabilisce norme armonizzate sull'intelligenza artificiale (*AI Act*), introducendo un'ampia disciplina dell'intelligenza artificiale e, in particolare, ai fini del presente discorso, una definizione normativa di IA. All'art. 3, si legge infatti che: «sistema di IA: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici»[168].

---

[164] L'espressione è utilizzata da G. Carlotti, *I principi nel Codice dei contratti pubblici: la digitalizzazione*, in www.giustizia-amministrativa.it., 2023, per il quale essa è riferibile anche alle ipotesi di utilizzo di intelligenza artificiale.

[165] F. Tallaro, *La digitalizzazione del ciclo dei contratti pubblici*, in www.giustizia-amministrativa.it, 2023.

[166] III – Relazione agli articoli e agli allegati, https://www.camera.it/leg19/682?atto=019&tipoAtto=Atto&idLegislatura=19&tab=2#inizio.

[167] F. Tallaro, *op. cit*.

[168] Una definizione di intelligenza artificiale era stata elaborata anche dall'*High-Level Expert Group on Artificial Intelligence* istituito dalla Commissione europea, secondo cui «*Artificial intelligence (AI) refers*

Si tratta della prima definizione normativa, integrata e specificata, secondo una classificazione dei sistemi di IA basata sul rischio[169]. Proprio il rischio per le libertà e i diritti dei cittadini costituisce l'approccio[170] su cui viene costruita la regolamentazione di questa tecnologia.

L'approvazione dell'*AI Act* intende da un lato colmare il vuoto normativo, per costituire la base legale su cui i sistemi intelligenti saranno sviluppati e opereranno, dall'altro l'UE intende affermare una propria leadership sull'IA basata sul diritto. La regolamentazione diventa quindi strumento di *governance* dell'intelligenza artificiale.

5. Dati e Intelligenza artificiale.

L'*High-Level Expert Group on Artificial Intelligence* incaricato di fornire orientamenti utili per contribuire allo sviluppo di una AI affidabile ed eticamente valida, ha definito i seguenti principi etici: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. Secondo il gruppo di esperti la *governance* dei dati rientra tra tali principi etici fondamentali per lo sviluppo dell'IA.

Dati e intelligenza artificiale rappresentano infatti due elementi strettamente connessi, proprio perché l'IA dimostra il potenziale di essere utilizzata in molti settori diversi e per poter funzionare viene addestrata sui dati. La disponibilità di set di dati, la convalida e la prova di elevata qualità degli stessi rendono necessario attuare adeguate pratiche di

---

to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications) ».

[169] L'AI Act classifica i sistemi di intelligenza artificiale a seconda che il rischio sia:

1. Inaccettabile, in tal caso l'uso è proibito (si tratta di quei sistemi elencati nell'allegato III ad esempio quelli impiegati per l'acquisizione e l'elaborazione di dati biometrici o quelli utilizzati per determinare l'accesso ad una istituzione formativa o un posto di lavoro);
2. Elevato;
3. Limitato;
4. Minimo. In tal caso non viene regolato, e come evidenzia l'Unione europea si tratta della quota maggiore di sistemi di IA attualmente disponibili.

[170] G. Proietti, *Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico*, in *Contr. e impr.*, 3, 2024; A. Gentili, *Regole per l'intelligenza artificiale*, in *Contr. e impr.*, 4, 2024; G. Crialesi, *Verso un'intelligenza artificiale UE antropocentrica e affidabile che garantirà la sicurezza e i diritti di imprese e cittadini*, in *Contr. e impr.*, 4, 2024; C. Pirelli, *L'AI Act: gestione del rischio e tutela dei diritti*, in *Giur. it.*, 2, 2025.

governance e gestione[171]. Se i dataset non sono gestiti in maniera corretta possono, infatti, generare e amplificare errori, ma anche discriminazioni, dei sistemi di intelligenza artificiale. L'IA non può quindi prescindere dalla *governance* dei dati[172], per poter garantire trasparenza, responsabilità e sicurezza nello sviluppo di tecnologie avanzate[173].

La *governance* dell'IA sinteticamente[174] è stata definita così: «*AI governance is a system of rules, practices, processes, and technological tools that are employed to ensure an organization's use of AI technologies aligns with the organization's strategies, objectives, and values; fulfills legal requirements; and meets principles of ethical AI followed by the organization*».

Muovendo da questa definizione, si ricava che l'*AI governance* include la *Data governance*, poiché nel processo di costruzione del modello di IA la gestione appropriata dei dati risulta essere, come già detto, fondamentale, ma ne rappresenta solo una parte[175].

In generale con *governance* dei dati si includono l'insieme di politiche, ruoli e standard volti a gestire in modo corretto e sicuro l'intero ciclo di vita delle informazioni

---

[171] Considerando 67 all'AI Act, in particolare dove si precisa che «le pratiche di governance e di gestione dei dati dovrebbero includere, nel caso dei dati personali, la trasparenza in merito alla finalità originaria della raccolta dei dati. I set di dati dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato». La questione non è irrilevante e, soprattutto presenta delle carenze dal punto di vista normativo, come osservato da G. Carullo, *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in *Ceridap*, 3, 2024, p. 45, il quale nell'analizzare la disciplina sulla privacy italiana con riferimento alla normativa europea, evidenzia che il Codice della privacy consente sempre alla Pubblica amministrazione il legittimo trattamento dei dati personali, un tanto in pregiudizio per i privati con riferimento, tra l'altro, allo «sviluppo ed utilizzo di sistemi di intelligenza artificiale da parte della pubblica amministrazione. Poiché tali sistemi sono basati in sostanza sull'analisi massiva di dati, l'assenza di criteri che definiscano i limiti entro i quali i dati personali possono essere utilizzati per lo svolgimento di funzioni istituzionali pubbliche può determinare una pericolosa apertura ad un uso pressoché insindacabile del patrimonio informativo pubblico».

[172] Per una ricostruzione sistematica della *governance* dell'AI cfr. G. D. Sharma, PhD, A. Yadav, R. Chopra, *Artificial intelligence and effective governance: A review, critique and research agenda*, in *Sustainable Futures*, 2, 2020, disponibile in https://doi.org/10.1016/j.sftr.2019.100004.

[173] E. Bluemke, T. Collins, B. Garfinkel, A. Trask, *Exploring the Relevance of Data Privacy-Enhancing Technologies for AI Governance Use Cases,* disponibile in https://arxiv.org/abs/2303.08956, in cui viene evidenziando come la *governance* delll'IA possa diventare importante per verificare gli output, riconoscendo che «*AI and data governance is now a wide field with increasingly different subtopics and concerns. It is important to consider the various problems in AI governance as a whole, as a system*».

[174] La definizione è una sintesi, tra diverse formulate dai ricercatori, proposta da M. Mäntymäki, M. Minkkinen, T. Birkstedt, M. Viljanen, *Defining organizational AI governance*, in *AI and Ethics*, 2022, p. 604 disponibile in https://doi.org/10.1007/s43681-022-00143-x

[175] M. Mäntymäki, M. Minkkinen, T. Birkstedt, M. Viljanen, *op. cit.*, p. 607.

(raccolta, conservazione, analisi, condivisione), che trova apposita disciplina nel *General Data Protection Regulation*, e a livello nazionale nel Codice della *privacy*[176].

La necessità di protezione dei dati personali, anche al fine di favorirne la circolazione, è stata avvertita come di primaria importanza a livello europeo, ma negli anni successivi il legislatore si è reso conto della necessità di regolare anche un'altra tipologia di dati, quelli che non sono personali, introducendo un regolamento apposito, il Reg. UE 2022/868 (c.d. *Data Governance Act* o DGA) incentrato sui dati, in particolare *non* personali, come quelli relativi alla sanità, ai trasporti e all'energia.

È interessante notare, come si legge nel considerando 4 del Regolamento in questione, come in ogni caso la disciplina debba «lasciare impregiudicati i regolamenti (UE) 2016/679 e (UE) 2018/1725) del Parlamento europeo e del Consiglio, le direttive 2002/58/CE e (UE) 2016/680 del Parlamento europeo e del Consiglio e le corrispondenti disposizioni del diritto nazionale, anche qualora i dati personali e non personali di una serie di dati siano indissolubilmente legati. In particolare, il presente regolamento non dovrebbe intendersi, in particolare, come creazione di una nuova base giuridica per il trattamento dei dati personali per nessuna delle attività regolamentate, né come modifica dei requisiti in materia di informazione stabiliti nel regolamento (UE) 2016/679». L'intento del regolamento non è infatti di tipo protettivo, ma di promozione dell'utilizzo dei dati stessi valorizzandoli[177], al fine di favorire l'innovazione[178] e la

[176] D.lgs. 30 giugno 2003, n. 196, modificato dal d.lgs. 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)» e recentemente novellato con d.l. 2 marzo 2024, n. 19, convertito, con modificazioni dalla l. 29 aprile 2024, n. 56.

[177] D. Poletti, *Il quadro normativo del Data Governance Act: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Nuove leggi civ.*, 3, 2024, p. 535, la quale evidenzia come il regolamento definisca «un nuovo modello di impiego dei dati, alternativo alle pratiche di gestione squisitamente commerciale delle piattaforme Big Tech, per garantire accessi non discriminatori ai soggetti meno attrezzati operanti sul mercato dei dati: piccole e medie imprese, nonché start up, "con mezzi finanziari, giuridici, amministrativi limitati", così da evitare effetti di lock-in. Questo modello separa la fase di fornitura dalla fase di utilizzo, interponendo tra le due il servizio di intermediazione, fondato sui requisiti di neutralità degli intermediari, di esclusività dello scopo di intermediazione e di segregazione dei dati da intermediare rispetto ad altre attività di trattamento eventualmente svolte». V. sul punto anche A. Morace Pinelli, *Dalla Data Protection alla Data Governance: il Regolamento UE 2022/868*, in *Nuova giur. civ. comm.* 2, 2024.

[178] Considerando 3 al *Data Governance Act*, secondo cui «È necessario migliorare le condizioni per la condivisione dei dati nel mercato interno, creando un quadro armonizzato per gli scambi di dati e stabilendo alcuni requisiti di base per la governance dei dati, prestando particolare attenzione a facilitare la cooperazione tra gli Stati membri. Il presente regolamento dovrebbe mirare a sviluppare ulteriormente il mercato interno digitale senza frontiere e una società e un'economia dei dati antropocentriche, affidabili e sicure».

circolazione degli stessi[179], superando la logica del consenso informato[180] (caratterizzante il GDPR), tracciando quindi una *governance*[181] in cui sono coinvolti tutti i portatori di interessi. In particolare, il *Data Governance Act* pone particolare accento sulla natura economica dei dati[182], come si desume anche dall'introduzione di figure nuove: l'utente dei dati[183] e il fornitore dei servizi di intermediazione dei dati[184], nonché le cooperative di dati[185], che il legislatore include tra i soggetti che possono svolgere servizi di intermediazione di dati. Queste ultime assumono particolare rilievo nella *governance*, in quanto, all'interno di esse, gli interessati o le PMI possono esercitare congiuntamente i propri diritti, negoziare le condizioni di trattamento e favorire la creazione di un valore condiviso, alternativo alle prassi delle grandi piattaforme.

---

[179] A. Ricci, *Introduzione al Regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *Nuove leggi civili*, 4, 2024, p. 800.

[180] A. Morace Pinelli, *op. cit.*, p. 491.

[181] Considerando 5 al DGA, in particolare laddove dice che devono essere stabiliti «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».

[182] Cfr. A. Ricci, *op. cit.*, p. 803, la quale evidenzia come la definizione di utente dei dati lo configuri alla stregua di un consumatore.

[183] Ai sensi dell'art. 2 n. 9) si definisce «utente dei dati»: una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del Regolamento 2016/679/UE in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali.

[184] Ai sensi dell'art. 2 n.11) si definisce «servizio di intermediazione dei dati»: un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali, ad esclusione almeno di:

a) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati;

b) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore;

c) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose;

d) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali;

[185] Art. 2, 15) «servizi di cooperative di dati»: servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali.

Con questo regolamento, il legislatore europeo mira a valorizzare la potenzialità di sfruttamento economico da parte delle imprese, anche attraverso la fornitura di servizi incentrati sui dati[186], che vengo quindi considerati beni in senso giuridico (immateriali) negoziabili e trasferibili[187].

Parallelamente, sotto il profilo della *governance*, il DGA indica agli Stati membri di designare una o più autorità competenti per il controllo sugli intermediari dei dati e per la registrazione delle organizzazioni per l'altruismo dei dati (art. 13 del DGA). Tra l'altro il tenore letterale dell'ultimo comma dell'articolo 13, secondo cui «I poteri delle autorità competenti per i servizi di intermediazione dei dati non pregiudicano i poteri delle autorità per la protezione dei dati, delle autorità nazionali garanti della concorrenza, delle autorità responsabili della cibersicurezza e di altre autorità settoriali pertinenti», lascia intendere che gli Stati dovranno nominare un'autorità apposita per questo settore che si va ad aggiungere alle altre già esistenti, incluso il Garante per la protezione dei dati personali e che in tal caso si porranno problemi di coordinamento oppure che tali funzioni possano essere attribuite ad un'autorità già esistente[188].

Anche se non espressamente dichiarato, si rileva l'importanza rivestita dal DGA per promuovere una *governance* dei dati, al fine di sviluppare anche sistemi intelligenti[189].

Dal punto di vista sistematico, la *governance* del digitale emerge sempre più come *governance* dell'Intelligenza artificiale, con strutture multilivello e il coinvolgimento di diversi attori, in cui la regolazione contribuisce a definire la struttura, assegnare ruoli e

---

[186] F. Bravo, *Le cooperative di dati*, in *Contratto impresa*, 3, 2023, p. 767.

[187] A. Morace Pinelli, *La circolazione dei dati personali tra tutela della persona, contratto e mercato,* in *Nuova giur. civ. comm.*, 6, 2022, p. 1326.

[188] A. Morace Pinelli, *Dalla Data Protection alla Data Governance: il Regolamento UE 2022/868,* cit., p. 491.

[189] Un tanto lo si ricava dalla lettura dell'art. 10 dell'AI Act, specificamente dedicato alla *governance* dei dati, in particolare:

§ 3. I set di dati di addestramento, convalida e prova sono pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista. Essi possiedono le proprietà statistiche appropriate anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone relativamente ai quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o a livello di una combinazione degli stessi.

§ 4. I set di dati tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi

particolari dello specifico ambito geografico, contestuale, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

Anche il considerando 2 cpv. al DGA richiamando la comunicazione della Commissione europea sulla strategia europea per i dati valorizza «la visione di uno spazio comune europeo di dati: un mercato interno dei dati nel quale questi ultimi possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione nell'Unione, nel rispetto della normativa applicabile, che tra le altre cose potrebbe essere centrale per il rapido sviluppo delle tecnologie di intelligenza artificiale».

determinare i processi. Il difficile inquadramento delle nuove tecnologie all'interno di un perimetro legale mostra come, anche se vi è una regolamentazione, le frizioni con i principi fondamentali dell'ordinamento non vengono superati, ma si è di fronte a un processo per fasi.

La *governance* genericamente intesa ha certamente il pregio di un'attribuzione condivisa di responsabilità e definizione di *policy*, ma non è in di per sé sufficiente a fare in modo che una tecnologia possa essere applicata. Il ruolo degli interpreti rimane centrale, come mostrato dalle vicende processuali descritte nel paragrafo 2.4, in quanto, confrontandosi con il caso concreto, testano la conformità alla legge di una soluzione tecnologica, definendone il perimetro di utilizzo, e quindi in definitiva contribuendo alla *governance* stessa.

CAPITOLO II

Il sistema di *governance* dell'intelligenza artificiale tra organismi globali, istituzioni europee e autorità nazionali*

1. Introduzione.

Le teorie sulla *governance* di cui si è parlato nel precedente capitolo hanno rappresentato il sostrato culturale, che ha condizionato le riforme in larga parte dell'Europa[1], chiariscono in quale contesto si sia inserito il percorso europeo verso l'approvazione dell'*Artificial Intelligence Act*. Il sistema di regole e specialmente la creazione di strutture dedicata all'applicazione del regolamento possono essere lette alla luce di queste teorie, in chiave evolutiva. Per altro verso, l'*AI Act* può essere analizzato anche con riferimento alla questione della sovranità digitale, affrontato nel capitolo 1. Infatti, la competizione con gli Stati Uniti e la Cina, nonché l'influenza esercitata dalle *Big Tech*, con conseguente dipendenza europea dai *provider* americani, spiega il tentativo dell'Unione europea di affermare una propria autonomia quantomeno sul piano regolatorio, esercitando il *Brussels Effect*.

Risulta allora importante chiarire il contesto ambientale in cui l'innovazione tecnologica si inserisce, nel quale le scelte di definizione delle strutture pubbliche adibite al suo governo trovano spazio, a livello unionale così come a livello nazionale. In particolare, proprio a livello nazionale si vede come il contesto ambientale, costituito dalla tradizione storica amministrativa, unitamente all'influenza del diritto europeo, incidano sulle strutture di governo dell'IA. Questa particolare considerazione avverrà negli ultimi paragrafi del presente capitolo attraverso il confronto sul recepimento del *AI Act* negli ordinamenti di Italia e Spagna. Tale comparazione risulta utile in ragione dell'affinità

* Parti del presente capitolo, in particolare i parr. 3, 4, 6, 7 e 8 sono stati pubblicati, cfr. L. Pellizzoni, (2026). *Divergenze e convergenze nella governance dell'intelligenza artificiale: un confronto sull'attuazione dell'AI Act in Italia e Spagna*, in *DPCE Online*, 73(1), e qui ampliati.

[1] Sul punto v. G. Hammerschmid, S. Van de Walle, R. Andrews et al., *New Public Management Reforms in Europe and their Effects: Findings from a 20-Country Top Executive Survey*, in *International Review of Administrative Sciences*, 3, 2019, pp. 399-418.

tra i due ordinamenti derivanti dalla comune tradizione amministrativa di matrice francese[2].

2. Il quadro regolatorio delle nuove tecnologie: il *New Artificial Intelligence Advisory Board* delle Nazioni Unite.

L'accelerazione dell'innovazione tecnologica, trainata anche dalla diffusione dei *Large Language Models*, ha generato a livello internazionale un dibattito attorno alla questione della regolazione dell'Intelligenza artificiale, col fine di bilanciare il progresso tecnico con la tutela dei diritti fondamentali, la sicurezza e l'equità sociale, nella convinzione che tali tecnologie incidano inevitabilmente sia sugli assetti economici, produttivi, sociali, sia sull'ordine giuridico internazionale, per come è conosciuto e applicato[3].

Questi timori hanno spinto ad una riflessione, a livello globale, sul tema della *governance*, generando proposte, quali la sottoscrizione di atti di indirizzo o accordi internazionali per la creazione di istituzioni dedicate alla materia[4]. In questo contesto, le Nazioni Unite hanno voluto definire un'agenda per la regolazione dell'intelligenza artificiale, come è stato sintetizzato al Vertice di Londra sulla Sicurezza dell'Intelligenza Artificiale del 2023 dal Segretario Generale dell'ONU secondo cui «Promuovere la pace e lo sviluppo sostenibile; proteggere e promuovere i diritti umani. Abbiamo urgentemente bisogno di incorporare questi principi nella sicurezza dell'IA».

---

[2] A. Rallo Lombarte, *Las administraciones independientes: una aproximaciòn constitucional*, in C. P. Chuvi, B.T. Mallén (Eds.), *Las administraciones independientes*, Valencia, 11, 2009, p. 12. E. Ongaro, *The Napoleonic Administrative Tradition and Public Management Reform in France, Greece, Italy, Portugal and Spain*, in M. Painter, B.G. Peters (Eds.), *Tradition and Public administration*, London, 2010, pp. 174-190.

[3] M.M. Maas, *AI, Governance Displacement, and the (De)Fragmentation of International Law*, 2021, disponibile in ssrn.com/abstract=3806624.

[4] Tra gli atti di *soft law* vi sono I principi etici per l'IA elaborati dall'OCSE o la *Global Partnership on artificial intelligence*, un'iniziativa di diversi Paesi per promuovere lo studio e lo sviluppo di un'IA affidabile. Anche il Consiglio d'Europa con la Commissione per l'Efficienza della Giustizia elabora un documento programmatico denominato «*European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*», individuando alcuni principi fondamentali in materia di decisione automatizzate nel contesto della giustizia, quali quello di non discriminazione, di trasparenza, di utilizzo sotto la supervisione umana, visionabile al seguente link https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf. Per una ricostruzione delle varie proposte cfr. M. M. Maas, J.J. Villalobos, *International AI institutions. A literature review of models, examples, and proposals*, *Institute for Law & AI, AI Foundations Report*, 1, 2023, disponibile in www.law-ai.org/international-ai-institutions.

Tale dichiarazione fa seguito alle iniziative avviate a partire dal 2020, quanto all'Assemblea generale il Segretario Antonio Guterres ha presentato il report «*Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*», redatto da un gruppo di esperti incaricati dall'Organizzazione delle Nazioni Unite, in cui viene posto il tema della necessità di adottare soluzioni condivise a livello internazionale per sviluppare standard comuni sull'IA, evidenziando al contempo il bisogno di adottare una *governance*, al fine di garantire la protezione dei diritti umani e accrescere la fiducia nella tecnologia. Il report inoltre presenta l'intenzione del Segretario Generale di istituire un gruppo consultivo «*to provide guidance to myself and the international community on artificial intelligence that is trustworthy, human-rights based, safe and sustainable and promotes peace*»[5].

A seguito di questa dichiarazione di intenti, nel 2023 è stato creato l'*AI Advisory Board* composto da esperti di diversa provenienza e formazione professionale, inclusi accademici ed esponenti politici di trentatré Paesi, con il compito di effettuare analisi e formulare raccomandazioni per la *governance* internazionale dell'IA.

Il frutto del lavoro di questo gruppo di esperti è stato pubblicato nel mese di settembre del 2024 con il titolo *Governing AI for Humanity*[6], ove viene affrontato direttamente il problema del governo dell'intelligenza artificiale muovendo da diverse considerazioni tra cui «*no one currently understands all of AI's inner workings enough to fully control its outputs or predict its evolution. Nor are decision makers held accountable for developing, deploying or using systems they do not understand. Meanwhile, negative spillovers and downstream impacts resulting from such decisions are also likely to be global*». Di qui la necessità di adottare soluzioni di idonee per affrontare tali problemi. Nel rapporto vengono infatti presentate sette raccomandazioni per migliore la *governance*, in particolare la creazione di un Panel composto da esperti internazionali in materia di IA, la cooperazione tra gli Stati per il confronto e lo sviluppo di *best practice* e la creazione di standard comuni attraverso il dialogo continuo tra organismi internazionali e *stakeholders* delle aziende tecnologiche e rappresentanti della società civile.

[5] Cfr. *The Report of the Secretary-General* A/74/821 *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation,* 2020, p. 18.
[6] AI Advisory Body, *Governing AI for Humanity: Final Report. United Nations*, 2024.

Il documento ha certamente il pregio di aver portato all'attenzione globale i diversi problemi dell'IA in riferimento alla generale disparità tra i Paesi economicamente più o meno sviluppati sotto il profilo della capacità infrastrutturale di sostenere la diffusione dell'IA, ma anche i *gap* tra i Paesi che stanno adottando soluzioni regolatorie e altri che invece non lo stanno facendo. Tuttavia, il report non offre soluzioni, ma solamente proposte generiche, tra cui la creazione di un Ufficio dell'IA in seno alle Nazioni Unite, costituendo più un atto di intenti[7], al pari della risoluzione del 2024 dell'Assemblea generale sullo sviluppo dell'IA sicura e affidabile, con la quale i vari Paesi hanno riconosciuto la necessità di prevenire «*the fragmentation of the governance of safe, secure and trustworthy artificial intelligence systems*»[8], evidenziando in ogni caso come questo sia un settore in evoluzione nel quale sono necessarie discussioni approfondite per stabilire quale sia l'approccio da seguire.

3. L'Unione europea traccia una cornice normativa.

Tra i principali attori internazionali ad aver preso una decisione nel senso di una regolamentazione apposita dell'IA vi è l'Unione europea, che ha cominciato a dedicare particolare attenzione al tema attraverso una serie di approfondimenti sfociati in atti programmatici, contenenti dichiarazioni di principio e linee guida. Il primo in ordine di importanza è il Parere del Comitato economico e sociale europeo (CESE) «L'intelligenza artificiale – Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società», pubblicato nella Gazzetta ufficiale dell'Unione europea C 288/1 del 31 agosto 2017, il quale identifica undici aree critiche in cui l'IA pone sfide di rilievo, quali l'etica, la sicurezza, la *privacy*, la trasparenza, la responsabilità, il lavoro, l'istruzione e le competenze, la (dis)uguaglianza e l'inclusività, le disposizioni legislative e regolamentari, ma anche la *governance* e la democrazia, la guerra e la superintelligenza. Il CESE, in particolare, sottolinea l'urgenza di definire nuovi strumenti di normazione tecnica e giuridica volti a

[7] A. Vercelli, *United Nations, artificial intelligences and regulations: analysis of the General Assembly AI Resolutions and the Final Report of the Advisory Body on AI*, in *3rd Workshop on Bias, Ethical AI, Explainability and the Role of Logic and Logic Programming (BEWARE24), co-located with AIxIA 2024, November 25-28, 2024, Bolzano, Italy*, https://ceur-ws.org/Vol-3881/paper11.pdf.
[8] ONU Resolution A/78/L.49, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, 2024, p. 3.

garantire trasparenza, affidabilità e responsabilità etica dei sistemi intelligenti[9], definendo un percorso normativo destinato a portare all'approvazione del Regolamento UE 2024/1689 (*Artificial Intelligence Act*)[10].

A questo documento ha fatto seguito la Comunicazione, COM (2018) 237, «L'intelligenza artificiale per l'Europa», con la quale la Commissione europea ha formulato una prima definizione di intelligenza artificiale[11], affermando esplicitamente la necessità di un quadro giuridico adeguato al fine di sostenere lo sviluppo tecnologico, tutelare i diritti fondamentali e affrontare le conseguenze socioeconomiche derivanti dall'impiego di sistemi autonomi. A questa ha fatto seguito la Comunicazione COM (2019)168 "Creare fiducia nell'intelligenza artificiale antropocentrica" nella quale vengono enunciati i requisiti fondamentali per l'IA affidabile, ovvero intervento e sorveglianza umana, trasparenza, *governance* e sicurezza dei dati, *accountability*.

Questi principi hanno trovato ulteriore sviluppo nel Libro bianco sull'intelligenza artificiale[12] della Commissione europea, in cui viene promosso un approccio integrato alla regolazione, partendo dalla constatazione della necessità di una definizione di IA sufficientemente flessibile da poter adeguarsi al progresso tecnologico e, allo stesso tempo, contemperare l'esigenza di tutela dei consumatori e dei diritti fondamentali con il mercato e gli investimenti. Vengono quindi identificati due obiettivi prioritari, da un lato, incentivare l'adozione dell'IA nei settori strategici, dall'altro, affrontare i rischi associati a utilizzi sensibili della tecnologia, ponendo l'accento su criteri quali

[9] Cfr. Parere, *L'intelligenza artificiale – Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società*, p. 5, in eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52016IE5369.

[10] Nel Parere viene infatti auspicata la definizione di «un dispositivo di normazione per la verifica, la convalida e il controllo dei sistemi di IA, sulla base di un'ampia serie di norme in materia di sicurezza, trasparenza, comprensibilità, rendicontabilità e valori etici» proponendo altresì lo sviluppo di «un'infrastruttura di IA europea, costituita da ambienti di apprendimento a codice sorgente aperto (open source) e rispettosi della privacy, ambienti di collaudo in condizioni reali (real life) e serie di dati di elevata qualità per lo sviluppo e l'addestramento dei sistemi di IA. Il CESE richiama l'attenzione sul vantaggio (concorrenziale) che l'UE può acquisire sul mercato mondiale grazie allo sviluppo e alla promozione di 'sistemi di IA responsabili europei', provvisti di certificazione ed etichettatura europee».

[11] Nella Comunicazione l'IA viene definita «Intelligenza artificiale (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)».

[12] COM (2020) 65, Libro Bianco sull'intelligenza artificiale-un approccio europeo all'eccellenza e alla fiducia.

sicurezza, responsabilità e protezione dei diritti dei consumatori e dei dati personali[13]. Nel Libro bianco si propone, quale soluzione per contemperare queste opposte esigenze, un approccio regolatorio basato sul rischio, nel quale questo deve essere individuato con riferimento al settore interessato, agli interessi in gioco, al pericolo per la sicurezza e i diritti fondamentali [14].

Dopo il susseguirsi dei menzionati atti di *soft law*, con la COM (2021) 206 la Commissione ha presentato al Parlamento e al Consiglio la Proposta di regolamento dell'intelligenza artificiale illustrandone gli obiettivi, ossia «assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione; assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale; migliorare la *governance* e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA; facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato».

L'intento è di rendere l'Unione europea leader nel settore dell'IA, recuperando sul piano giuridico il ritardo tecnologico europeo rispetto ai mercati americano e cinese, attraverso il *Brussels Effect*[15], in una prospettiva orientata verso il mercato[16], ma tenendo in considerazione i diritti fondamentali[17]. Un tanto si può ricavare dalla lettura del Considerando 1 al Regolamento secondo cui «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA)

---

[13] U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. civ.*, 6, 2020, p. 1250.

[14] Cfr. Libro Bianco cit., p. 19 «Tale approccio basato sul rischio è importante per garantire la proporzionalità dell'intervento normativo, ma richiede che siano definiti criteri chiari per distinguere tra le diverse applicazioni di IA, in particolare per stabilire se tali applicazioni siano o meno 'ad alto rischio'. I criteri per stabilire che cosa sia un'applicazione di IA ad alto rischio dovrebbero essere chiari, facilmente comprensibili e applicabili a tutte le parti interessate. Le applicazioni di IA rimangono comunque interamente soggette al diritto vigente dell'UE, anche qualora non siano considerate ad alto rischio».

[15] C. Casonato, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in *DPCE*, 1, 2021, p. 178. Sulla teoria del *Brussels Effect* cfr. A. Bradford, *The Brussels Effect*, in *Northwestern University Law Review*, 1, 2012, disponibile in scholarship.law.columbia.edu/faculty_scholarship/271.

[16] B. Carotti, *Le finzioni dell'intelligenza senza corpo, o dell'AI Act*, in *Giorn. dir. amm*., 1, 2025, p. 35.

[17] O. J. Gstrein, *European AI Regulation: Brussels Effect versus Human Dignity?*, in *Zeitschrift für Europarechtliche Studien (ZEuS)*, 4, 2022, p. 758, disponibile in ssrn.com/abstract=4214358.

nell'Unione», che dichiara l'intento di armonizzazione della normativa degli Stati membri in questa materia[18]. Mentre la seconda parte del considerando fa riferimento alla volontà di protezione dei diritti fondamentali[19]. Si tratta di un compromesso trovato tra Commissione europea e Parlamento, laddove la prima sosteneva una normativa maggiormente incentrata sulla sicurezza del prodotto, mentre il secondo insisteva affinché venisse integrata anche una disciplina (ancorché programmatica) incentrata sulla tutela dei diritti fondamentali[20].

La base giuridica del Regolamento è l'art. 114, implicando, per come affermato nella stessa relazione di accompagnamento alla proposta, la volontà di adottare uno strumento normativo che «prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno […] L'obiettivo principale della presente proposta è assicurare il buon funzionamento del mercato interno fissando regole armonizzate, in particolare per quanto concerne lo sviluppo, l'immissione sul mercato dell'Unione e l'utilizzo di prodotti e servizi che ricorrono a tecnologie di intelligenza artificiale o forniti come sistemi di IA indipendenti», nel quale trova spazio la tutela dei diritti fondamentali, ed in particolare la *privacy* dei dati personali utilizzati per addestrare i sistemi di IA, in forza del richiamo all'art. 16 del TFUE, quale ulteriore base giuridica del Regolamento[21]. Nella relazione illustrativa, la Commissione ha, infatti, ricordato gli obiettivi fissati nel Libro bianco, per cui scopo del regolamento è quello di «sviluppare un ecosistema di fiducia proponendo un quadro giuridico per l'IA affidabile» e di affrontare i rischi associati a determinati usi di tale tecnologia. In particolare, la

[18] R. Scarciglia, *Artificial intelligence and the state from a comparative perspective*, in *IJPL*, 2, 2025, p. 474.

[19] Considerando 1 cpv «[…] promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ('Carta'), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento».

[20] J. Chun, C. Schroeder de Witt, K. Elkins, *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US*, in *arXiv*, 2025.

[21] L'Art. 16 cpv TFUE recita, infatti, che «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano», il cui richiamo viene spiegato dalla Commissione nella sua relazione di accompagnamento in ragione del fatto che, poiché «la presente proposta contiene talune regole specifiche sulla protezione delle persone fisiche per quanto concerne il trattamento di dati personali, in particolare restrizioni sull'utilizzo di sistemi di IA per l'identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico a fini di attività di contrasto, è opportuno basare il presente regolamento, per quanto concerne tali regole specifiche, sull'articolo 16 TFUE».

questione della discriminazione è stata oggetto di una valutazione particolare durante l'elaborazione dell'atto[22], proprio in ragione del potenziale impatto sociale negativo, tenendo conto al contempo dei vantaggi derivanti dal sostegno allo sviluppo dell'IA attraverso la regolamentazione[23]. L'*AI Act* si presenta quindi come una dichiarazione di valori all'interno del settore dell'*artificial intelligence* e uno strumento dedicato alla sicurezza dei prodotti[24], collocandosi entro il pacchetto normativo dell'UE del programma *Digital decade* elaborato dalla Commissione per raggiungere l'obbiettivo di trasformare l'Unione europea e dedicato alla disciplina del digitale[25], ma anche della legislazione sui prodotti[26].

Il regolamento definisce inoltre un'architettura di *governance* costituita da strumenti per gestire la produzione e la diffusione dei sistemi di IA e di organismi istituiti per assicurare l'applicazione e il rispetto delle disposizioni, sia in seno all'UE sia indicando agli Stati membri di designare le autorità volte a vigilare sul rispetto del regolamento e degli obblighi ivi previsti, secondo un modello sovente prescelto dall'Unione europea per l'attuazione del diritto unionale e il perseguimento delle politiche comuni[27.]

Un tanto risulta invero coerente con le finalità perseguite dal legislatore europeo, che nel 2024 ha approvato la Direttiva UE 2024/2853[28] superando la precedente Direttiva 85/37/CE, poiché ritenuta non più idonea a garantire il corretto funzionamento del mercato interno, dovendo «essere rivista alla luce degli sviluppi legati alle nuove

[22] A. Neri, *Uso di un algoritmo discriminatorio nella contrattazione privata*, in *Nuova giur. civ. comm.*, 4, 2021, p. 985.

[23] E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Riv. Regolazione mercati*, 1, 2020, p. 33.

[24] M. Kop, *EU Artificial Intelligence Act: The European Approach to AI*, in *Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments*, Stanford University, 2, 2021, disponibile in ssrn.com/abstract=3930959.

[25] Nel quale vengono ricompresi il *General Data Protection Regulation*, il *Digital Service Act*, il *Digital Market Act*, il *Data Governance Act* e il *Data Act*. Cfr. https://eufordigital.eu/discover-eu/eu-digital-strategy/. V. anche sul punto J. Ruohonen, S. Mickelsson, *Reflections on the Data Governance Act*, in *Digital Society*, 2, 2023, doi.org/10.1007/s44206-023-00041-7.

[26] N. Sousa e Silva, *The Artificial Intelligence Act: Critical Overview*, 2024, disponibile in ssrn.com/abstract=4937150.

[27] H. Hofmann, *European Administration - Nature and Developments of a Legal and Political Space*, C. Harlow, G. della Cananea, L. Sandberg (Eds.), *Research Handbook in EU Administrative Law*, Cheltenham, 2016, p. 30.

[28] Direttiva del Parlamento e del Consiglio sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio.

tecnologie, compresa l'intelligenza artificiale»[29], e tramite la quale viene inclusa per la prima volta all'interno della nozione di prodotto anche il *software*[30].

In questa prospettiva può essere letta la Comunicazione COM (2022)31 *An EU Strategy on Standardisation. Setting global standards in support of a resilient, green and digital EU single market* della Commissione europea, nella quale viene sostenuto lo strumento della standardizzazione, ossia la definizione di requisiti di prodotti e servizi all'interno del mercato unico, quale base per imporre ai soggetti privati le caratteristiche dei prodotti (impedendo una autonomia in tal senso da parte delle aziende, specialmente extra-UE), in conformità con i diritti e i valori dell'Unione europea, e determinare l'omogeneità dei prodotti all'interno dell'UE[31]. L'introduzione di standard europei, specialmente con riferimento ai sistemi di IA, che tengano in considerazione anche i valori e i diritti fondamentali, va a differenziarsi pertanto da altri modelli di standard esistenti come quelli ISO/IEC[32].

Quanto alle disposizioni, di cui si dirà diffusamente nel successivo paragrafo, queste risultano essere il frutto non solo, come accennato, di negoziazioni e compromessi, ma anche di attenzione necessaria all'evoluzione della tecnologia. Inizialmente, infatti il regolamento non contemplava una disciplina dei *general purpose AI model*[33], inserita effettivamente nel maggio 2022 su proposta della Presidenza francese del Consiglio dell'Unione europea.

[29] Considerando 3 della Direttiva 2024/2853.

[30] Art. 4, co. 1 recita, infatti, che con prodotto si intende «ogni bene mobile, anche se integrato in un altro bene mobile o in un bene immobile o interconnesso con questi; include l'elettricità, i file per la fabbricazione digitale, le materie prime e il software», anche se la medesima Direttiva specifica, all'art. 1, che la stessa non si applica al *software* libero e *open source* sviluppato o fornito nel corso di un'attività non commerciale.

[31] Nella relazione di accompagnamento alla proposta di Regolamento si chiarisce che «La presente proposta definisce infatti dei requisiti obbligatori comuni applicabili alla progettazione e allo sviluppo di alcuni sistemi di IA prima della loro immissione sul mercato, che saranno resi ulteriormente operativi attraverso norme tecniche armonizzate. La presente proposta contempla altresì la situazione successiva all'immissione sul mercato dei sistemi di IA armonizzando le modalità secondo cui sono eseguiti i controlli *ex post*».

[32] M. Ebers, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. Di Matteo, M. Cannarsa, C. Poncibò (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, 2022.

[33] Ovvero quei sistemi in grado di svolgere funzioni diverse, come *ChatGPT*, *Gemini*, *Claude*.

4. Gli strumenti di *governance* dell'*Artificial Intelligence Act.*

4.1. Definizione e classificazione dei sistemi di intelligenza artificiale.

Il Regolamento UE 2024/1689 costituisce uno strumento di tutela, ma anche di promozione del mercato dell'IA, e la strategia adottata dal legislatore europeo per coniugare questi due aspetti si regge su un articolato sistema di *governance* composto da strumenti istituzionali, normativi e tecnici per garantire l'utilizzo dell'IA nel rispetto dei diritti fondamentali, della sicurezza e della trasparenza, senza comprimere lo sviluppo tecnologico e il mercato. Questo equilibrio viene conseguito attraverso un approccio basato sul rischio, inteso, ai sensi del Regolamento, come «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso» (art. 3, n. 2), con conseguente adattamento della disciplina, ossia dell'intensità degli obblighi e dei limiti, a seconda dell'intensità e della portata dei rischi[34] dei sistemi di intelligenza artificiale. Nell'adottare un approccio regolatorio basato sul rischio il legislatore sceglie precisamente di fare riferimento ai "sistemi di IA" in luogo della più ampia espressione "intelligenza artificiale". Tale scelta risulta giustificata dal mantenimento di una normativa tecnologicamente neutra[35], che consideri come operano queste tecnologie e non le tecniche con cui sono state progettate e programmate. Ed infatti l'art. 3 definisce il sistema di IA «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisico virtuali». In tal senso il Considerando 12 del Regolamento chiarisce infatti che «La nozione di 'sistema di IA' di cui al presente regolamento dovrebbe essere definita

[34] Cfr. Considerando 26 «Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di IA inaccettabili, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA».

[35] R. Petruso, G. Smorto, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *Nuova giur. civ. com*., 4, 2024, p. 990. Nella relazione al Regolamento redatta dalla Commissione si legge infatti che «Il titolo I definisce l'oggetto del regolamento e l'ambito di applicazione delle nuove regole concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA. Stabilisce inoltre le definizioni utilizzate in tutto l'atto. La definizione di sistema di IA nel quadro giuridico mira ad essere il più possibile neutrale dal punto di vista tecnologico e adeguata alle esigenze future, tenendo conto dei rapidi sviluppi tecnologici e di mercato relativi all'IA. Al fine di fornire la necessaria certezza del diritto, il titolo I è integrato dall'allegato I, contenente un elenco dettagliato di approcci e tecniche per lo sviluppo dell'IA che deve essere adattato dalla Commissione in linea con i nuovi sviluppi tecnologici».

in maniera chiara e dovrebbe essere strettamente allineata al lavoro delle organizzazioni internazionali che si occupano di IA al fine di garantire la certezza del diritto, agevolare la convergenza internazionale e un'ampia accettazione, prevedendo nel contempo la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici in questo ambito. Inoltre, la definizione dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi *software* o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati». La caratteristica fondamentale del sistema di IA è quindi la capacità inferenziale, ovvero la capacità di dedurre autonomamente il percorso logico per generare un *output*.

Considerata questa premessa definitoria, il Regolamento adotta un criterio di classificazione dei sistemi di IA basato sulla distinzione in quattro categorie di rischio, ossia inaccettabile, alto, limitato, minimo[36], che si riflette sull'assetto regolatorio diversificato per ciascuna categoria. Nel caso dei sistemi classificati come a rischio inaccettabile, l'art. 5 stabilisce espressamente il divieto[37] di talune pratiche, fornendo un elenco tassativo[38]. Viceversa, per i sistemi a rischio limitato il Regolamento impone unicamente un obbligo di trasparenza, ovvero i produttori e soprattutto gli utilizzatori devono rendere edotti i consumatori o utenti di un servizio che stanno interagendo con

[36] Definiti dal Regolamento come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Per una ricostruzione schematica del Regolamento v. G. Crialesi, *Verso un'intelligenza artificiale UE antropocentrica e affidabile che garantirà la sicurezza e i diritti di imprese e cittadini*, in *Pratica Fiscale e Professionale*, 14, 2024, p. 45.

[37] L'art. 5 fa riferimento alle pratiche vietate, piuttosto che alle tecnologie, poiché infatti la disciplina è finalizzata a mitigare i rischi per i diritti, la salute e la sicurezza, invece di vietare specifiche tecnologie viene posto un divieto a quegli strumenti tecnologici dotati di caratteristiche specifiche, quali, ad esempio, *software* che utilizzano tecniche subliminali o che sono in grado di compiere classificazioni delle persone o di gruppi sociali.

[38] N. Zorzi Galgano, *Il Regolamento UE 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contratto impresa*, 1, 2025, p. 49.

uno strumento di IA (ad esempio una *chatbot*). Mentre nel caso dei sistemi a rischio minimo non vengono stabiliti particolari adempimenti.

La parte più complessa della disciplina riguarda quindi i sistemi ad alto rischio per i quali il Regolamento prevede specifici criteri di classificazione, stabiliti secondo una duplice modalità dall'art. 6, ovvero da un lato se il sistema è componente di sicurezza di un prodotto o è prodotto soggetto alla normativa di armonizzazione e ad una valutazione di conformità da parte di terzi, dall'altro mediante rinvio alle varie ipotesi in cui un sistema di IA può essere considerato ad alto rischio, mediante rinvio agli allegati I (contenente l'elenco della normativa di armonizzazione) e III (contenente una casistica dedicata alle funzioni che tali sistemi possono svolgere, come la biometria, classificazione delle persone o dei gruppi sociali, o valutazione delle persone). Rispetto a questa categoria di sistemi, l'AIA introduce, all'art. 7, una serie di requisiti che questi sistemi debbono avere, oltre a obblighi per i produttori, quali la redazione della documentazione tecnica, nonché la registrazione automatica degli eventi (denominata "*log*") per tutto il ciclo di vita del sistema (art. 12), nonché obblighi di verifica della qualità dei dati impiegati per l'addestramento del sistema onde mitigare i rischi di discriminazione e garantire la trasparenza, intesa quale obbligo di consentire ai *deployer*, ossia coloro che impiegano tali sistemi, di poter interpretare l'*output* (art. 13). Inoltre, viene prevista l'utilizzo di detti sistemi solo se è possibile la supervisione umana[39]. La disciplina, quindi, responsabilizza i produttori anche attraverso un controllo di gestione dei rischi, inteso come «un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici», comprendente le seguenti fasi:

«a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista;

[39] L'art. 14 par. 3 recita, in particolare, «Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti:
a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile;
b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal *deployer*».

b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile;
c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72;
d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lettera a)».
Parimenti vengono previsti obblighi anche in capo ai fornitori e ai *deployer*, come assicurare la conformità dei sistemi ai requisiti previsti dal regolamento, nonché la predisposizione di un sistema di gestione della qualità (art. 16).

4.2. La disciplina per i *general-purpose AI models*.

Accanto alla disciplina basata sul rischio, l'AIA ne prevede una apposita per i *general-purpose AI model*. Tale distinzione si coglie nel Considerando 97 laddove si specifica «La nozione di modelli di IA per finalità generali dovrebbe essere chiaramente definita e distinta dalla nozione di sistemi di IA per consentire la certezza del diritto. La definizione dovrebbe basarsi sulle principali caratteristiche funzionali di un modello di IA per finalità generali, in particolare la generalità e la capacità di svolgere con competenza un'ampia gamma di compiti distinti», un riferimento, come poi viene specificato al successivo Considerando 99, ai modelli generativi[40], come GPT[41]. Tale distinzione viene introdotta nell'art. 3 n. 63 laddove si definisce un modello di IA a finalità generale quel «modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o

[40] I grandi modelli di IA generativi sono un tipico esempio di modello di IA per finalità generali, dato che consentono una generazione flessibile di contenuti, ad esempio sotto forma di testo, audio, immagini o video, che possono rispondere a un'ampia gamma di compiti distinti.
[41] Ovvero *General Pre-trained Transformer*, una tipologia di *Large Language Model*, una categoria di modelli fondativi addestrati su grandi quantità di dati, per renderli capaci di comprendere e quindi generare linguaggio naturale.

applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato».

Il Regolamento distingue tra modelli di IA per finalità generali e quelli che presentano un rischio sistemico[42], stabilendo obblighi aggiuntivi per i fornitori della seconda tipologia, che, ai sensi dell'art. 51, viene individuata al verificarsi di due condizioni, ovvero se il modello:

«a) presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento;

b) sulla base di una decisione della Commissione, ex officio o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XII[43]».

Il medesimo articolo introduce inoltre, al paragrafo 2, una presunzione di impatto elevato, che si verifica «quando la quantità cumulativa di calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 10^{25}» (art. 51, par. 2)[44]. I modelli a rischio sistemico vengono quindi inseriti in un apposito elenco mantenuto aggiornato dalla Commissione.

---

[42] Definito dall'art. 3 n. 65 «un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore».

[43] Ovvero i seguenti criteri: il numero di parametri del modello, la qualità o la dimensione del set di dati, ad esempio misurata mediante token, la quantità di calcolo utilizzata per addestrare il modello misurata in operazioni in virgola mobile o indicata da una combinazione di altre variabili quali il costo stimato dell'addestramento, il tempo stimato necessario per l'addestramento o il consumo energetico stimato per l'addestramento, le modalità di input e output del modello, come da testo a testo (modelli linguistici di grandi dimensioni), da testo a immagine, multimodalità e soglie di punta per determinare le capacità ad alto impatto per ciascuna modalità, nonché il tipo specifico di input e output (ad esempio sequenze biologiche); i parametri di riferimento e le valutazioni delle capacità del modello, anche tenendo conto del numero di compiti, che non richiedono un addestramento aggiuntivo, la capacità di apprendere nuovi compiti distinti, il livello di autonomia e scalabilità e gli strumenti a cui ha accesso, se il modello ha un alto impatto sul mercato interno in considerazione della sua portata, che viene presunta quando il modello stesso è stato messo a disposizione di almeno 10.000 utenti commerciali registrati stabiliti nell'Unione, il numero di utenti finali registrati.

[44] Il parametro indicato nella disposizione (in inglese *floating point operation*) viene utilizzato nella *computer science* per indicare il numero di operazioni con numeri decimali eseguite per secondo. Questo viene utilizzato per misurare la capacità di calcolo di un sistema e quindi valutarne la *performance*. Tale metodo classificatorio viene spiegato nel Considerando 111, laddove si afferma l'opportunità di «stabilire una metodologia per la classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischi sistemici. Poiché i rischi sistemici derivano da capacità particolarmente elevate, si dovrebbe considerare che un modello di IA per finalità generali presenti rischi sistemici se ha capacità di impatto elevato, valutate sulla base di metodologie e strumenti tecnici adeguati, o se ha un

Infine, l'art. 52, par. il par. 3 introduce una sorta di clausola di salvaguardia, conferendo alla Commissione europea potere di delega «per modificare le soglie di cui ai paragrafi 1 e 2 del presente articolo, nonché per integrare parametri di riferimento e indicatori alla luce degli sviluppi tecnologici in evoluzione». Una soluzione per ovviare alla rigidità derivante dall'adozione di un parametro quantitativo ai fini dell'inclusione di un modello nell'ambito di applicazione del Regolamento, anche se, come è stato osservato[45], a contrario vi è il rischio della moltiplicazione dei modelli assoggettabile alla disciplina dell'AIA, con conseguente difficoltà di monitoraggio o di eccessiva regolazione.

Con riferimento all'IA con finalità generale, ulteriore aspetto preso in considerazione è la scelta di normare i modelli e non i sistemi, come si ricava dall'art. 3, n. 63, secondo cui il modello non è un sistema di IA, ma è parte di esso. L'inclusione di un modello nella disciplina applicabile viene determinata sulla base di un parametro quantitativo (ovvero il numero di operazioni eseguibili dal modello), in luogo dell'impatto che lo stesso può avere; in altre parole, viene normata la tecnologia stessa invece delle sue applicazioni[46]. Ed un tanto può essere spiegato sulla base della difficoltà di stabilire a priori quale possa essere il rischio specifico[47]. Correlativamente, a differenza dei sistemi di IA, per cui vengono contemplati diversi destinatari della normativa, i soggetti obbligati a conformarsi alla disciplina relativa ai *general-purpose AI models* risultano essere espressamente i fornitori[48]. In particolare, i fornitori di modelli a finalità generale sono tenuti ad osservare obblighi di trasparenza[49] e di tutela del diritto d'autore (art. 53), mentre per i modelli con rischio sistemico si aggiungono ulteriori obblighi in ragione del potenziale impatto sulla salute, la sicurezza e i diritti fondamentali. I fornitori devono, infatti, compiere una valutazione di conformità dei modelli al fine di attenuare i

---

impatto significativo sul mercato interno a causa della sua portata». V. sul punto R. Cingolani, D. Andresciani, *Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive*, in G. Alpa (cur.), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 27.

[45] Sul punto cfr. I. Kumar, S. Manning, *Trends in Frontier AI Model Count: A Forecast to 2028*, in *arXiv*. 2025.

[46] F. G'sell, *An Overview of the European Union Framework Governing Generative AI Models and Systems*, 2024, disponibile in https://ssrn.com/abstract=4762804.

[47] O.J. Gstrein, N. Haleem, A. Zwitter, *General-purpose AI regulation and the European Union AI Act*, in *Internet Policy Rev.*, 3, 2024, https://doi.org/10.14763/2024.3.1790.

[48] M. Ricolfi, *L'impiego di opere protette come input e come output dell'intelligenza artificiale*, in *Dir. ind.*, 2024, 5, p. 417.

[49] Gli specifici obblighi di trasparenze vengono elencati nell'allegato XII.

rischi sistemici e documentare e riferire all'Ufficio per l'IA e le autorità nazionali circa il verificarsi di incidenti gravi[50].

4.3. Gli organismi europei per l'attuazione dell'*AI Act*.

L'ampia e complessa disciplina, in particolare quella dedicata ai sistemi di IA ad alto rischio, prevede la predisposizione di una *governance* al fine di assicurarne l'effettiva osservanza. L'Unione europea si è preoccupata infatti di istituire strutture dedicate a livello sia unionale sia dei singoli Stati membri[51], per coordinare ed assicurare l'applicazione uniforme del Regolamento.

Il regolamento istituisce a livello unionale l'Ufficio per l'Intelligenza artificiale (art.64), il Consiglio europeo per l'intelligenza artificiale (art. 65), il Forum consultivo (art. 67) e il Gruppo di esperti scientifici indipendenti (art. 68). Il primo è un ufficio amministrativo creato in seno alla Commissione europea ed è responsabile dell'attuazione, della supervisione e del monitoraggio del regolamento, nonché del coordinamento tra gli Stati membri, ed è responsabile della supervisione dei modelli di IA per uso generale[52]. Gli altri organismi europei istituiti dal regolamento sono invece organismi consultivi. Il Consiglio europeo per l'IA (disciplinato dagli art. 65, 66) è

[50] L'art. 55 par. 1 elenca tra gli obblighi, l'effettuazione di una valutazione di conformità dei modelli ai protocolli e strumenti standardizzati, anche tramite *adversarial testing*, al fine di individuare e attenuare i rischi sistemici; tenere traccia e comunicare all'ufficio per l'IA e, se del caso, alle autorità nazionali competenti, le informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio; garantire un livello adeguato di protezione della cibersicurezza per quanto riguarda il modello di IA per finalità generali con rischio sistemico e l'infrastruttura fisica del modello.

[51] Il Considerando 148 dice che: «Il presente regolamento dovrebbe istituire un quadro di governance che consenta di coordinare e sostenere l'applicazione dello stesso a livello nazionale, nonché di sviluppare capacità a livello dell'Unione e integrare i portatori di interessi nel settore dell'IA. L'attuazione e l'esecuzione efficaci del presente regolamento richiedono un quadro di governance che consenta di coordinare e sviluppare competenze centrali a livello dell'Unione. L'ufficio per l'IA è stato istituito con decisione della Commissione (45) e ha la missione di sviluppare competenze e capacità dell'Unione nel settore dell'IA e di contribuire all'attuazione del diritto dell'Unione in materia di IA. Gli Stati membri dovrebbero facilitare i compiti dell'ufficio per l'IA al fine di sostenere lo sviluppo di competenze e capacità dell'Unione a livello dell'Unione e di rafforzare il funzionamento del mercato unico digitale. È inoltre opportuno istituire un consiglio per l'IA composto da rappresentanti degli Stati membri, un gruppo di esperti scientifici volto a integrare la comunità scientifica e un forum consultivo per raccogliere il contributo dei portatori di interessi all'attuazione del presente regolamento, a livello dell'Unione e nazionale».

[52] L'art. 3, n. 47 definisce infatti l'ufficio per l'IA «la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA prevista dalla decisione della Commissione del 24 gennaio 2024. I riferimenti all'ufficio per l'IA contenuti nel presente regolamento si intendono fatti alla Commissione». Il richiamo è alla decisione COM., Dec. 24 gennaio 2024, n. C/2024/1459.

composto da un rappresentante di ciascuno Stato membro e alle sue riunioni partecipano anche un rappresentante dell'Ufficio per l'IA, nonché il Garante europeo della protezione dei dati in qualità di osservatore[53]. Tra le diverse funzioni attribuite all'organismo vi è quella di contribuire al coordinamento delle autorità designate dagli Stati membri per l'applicazione del regolamento (art. 66, par. 1 lett. a), assicurare la cooperazione tra gli Stati membri attraverso la condivisione delle migliori pratiche e conoscenze. Inoltre, svolge funzione consultiva sull'attuazione del regolamento, oltre ad assistere la Commissione formulando raccomandazioni e pareri in relazione all'attuazione del regolamento, in particolare nell'elaborazione di linee guida e progetti di misure normative future, ma anche in relazione a questioni internazionali connesse all'IA.

Il Forum consultivo è un organo tecnico istituito per fornire consulenza al Consiglio per l'IA e alla Commissione ed è composto da «una selezione equilibrata di portatori di interessi, tra cui l'industria, le start-up, le PMI, la società civile e il mondo accademico. La composizione del forum consultivo è equilibrata per quanto riguarda gli interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, per quanto riguarda le PMI e le altre imprese» (art. 67, co. 2), al fine di garantire un equilibrio tra rappresentanza commerciale e non commerciale[54]. L'equilibrio di rappresentanza viene garantito dalla Commissione europea, alla quale ai sensi del medesimo art. 67 compete la nomina dei membri tra i portatori di interessi, che rimangono in carica due anni fino a massimo quattro anni. Ai componenti nominati dalla Commissione si aggiungono anche quattro membri permanenti, ossia l'Agenzia per i diritti fondamentali, l'ENISA (Agenzia europea per la cybersicurezza), il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo per le norme di telecomunicazione (ETSI).

[53] Inoltre, ai sensi dell'art. 65, co. 6 «Il consiglio per l'IA istituisce due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e notificare le autorità su questioni relative rispettivamente alla vigilanza del mercato e agli organismi notificati».

[54] L'intento perseguito nel Regolamento con l'istituzione del Forum è chiarito nel Considerando 150, nel quale viene ritenuto importare coinvolgere in maniere costante i portatori di interessi «nell'attuazione e nell'applicazione del presente regolamento, è opportuno istituire un forum consultivo per fornire consulenza e competenze tecniche al consiglio per l'IA e alla Commissione. Al fine di garantire una rappresentanza diversificata ed equilibrata dei portatori di interessi che tenga conto di interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, con riferimento alle PMI e alle altre imprese, il forum consultivo dovrebbe comprendere, tra l'altro, l'industria, le start-up, le PMI, il mondo accademico, la società civile, comprese le parti sociali, nonché l'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo delle norme di telecomunicazione (ETSI)».

Il Consiglio per l'IA ed il Forum consultivo assolvono alla funzione di garantire la rappresentanza degli Stati membri e della società civile raccogliendo anche il contributo dei portatori di interessi all'attuazione del regolamento, in tal modo coadiuvando la Commissione[55], in questo assicurando una *governance* condivisa.

Infine, il Gruppo di esperti scientifici indipendenti (art.68) è composto da soggetti selezionati dalla Commissione in base alle competenze scientifiche o tecniche nel settore dell'IA necessarie per svolgere i compiti di assistenza e sostegno all'Ufficio IA e alle autorità nazionali di controllo, con particolare riferimento ai modelli *general-purpose AI*, proponendo strumenti e metodologie per la classificazione dei sistemi di IA.

Il modello di *governance* adottato dal regolamento appare quindi finalizzato al coinvolgimento di tutte le componenti fondamentali della società, dagli Stati, attraverso loro rappresentanti, ai portatori di interessi, fino agli esperti del settore. Tutti questi soggetti, attraverso gli organi consultivi, sono chiamati a contribuire alla *governance* dell'IA, coadiuvando la Commissione nell'applicazione dell'*AI Act*, anche con riferimento all'esercizio dei poteri delegati[56] previsti dall'art. 97, che consente alla Commissione europea di adottare atti delegati con riferimento a diversi aspetti del Regolamento, inclusa la possibilità di modificare la procedura di valutazione di conformità dei sistemi ad alto rischio o di integrare o modificare i criteri di classificazione degli stessi. Infine, a completamento vi è la previsione contenuta nell'art.

[55] Cfr. Considerando 121 «In sede di elaborazione della richiesta di normazione, la Commissione dovrebbe consultare il forum consultivo e il consiglio per l'IA al fine di ottenere le competenze pertinenti», ovvero la possibilità dei vari portatori di interesse della società di fare richiesta alla Commissione di normazione, per fornire le soluzioni tecniche migliori e la conformità alle norme armonizzate. Il considerando 121 è collegato a quanto viene poi stabilito dall'art. 40, 2, a mente del quale «In conformità dell'articolo 10 del regolamento (UE) n. 1025/2012, la Commissione presenta senza indebito ritardo richieste di normazione riguardanti tutti i requisiti di cui alla sezione 2 del presente capo e, se del caso, richieste di normazione riguardanti gli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento. La richiesta di normazione chiede inoltre prodotti relativi a processi di comunicazione e documentazione intesi a migliorare le prestazioni dei sistemi di IA in termini di risorse, come la riduzione del consumo di energia e di altre risorse del sistema di IA ad alto rischio durante il suo ciclo di vita, e allo sviluppo efficiente sotto il profilo energetico dei modelli di IA per finalità generali. Nel preparare una richiesta di normazione, la Commissione consulta il consiglio per l'IA e i pertinenti portatori di interessi, compreso il forum consultivo». La finalità risulta essere quella di promuovere attraverso il diritto le norme tecniche dei sistemi e prodotti tecnologici.

[56] L'esercizio del potere delegato è previsto dall'art. 290 TFUE, che consente, tramite atto legislativo, di conferire una delega alla Commissione per l'adozione di atti non legislativi di portata generale, che integrano o modificano determinati elementi non essenziali dell'atto legislativo.

70 ai sensi del quale gli Stati membri devono indicare un'autorità di notifica e un'autorità di vigilanza del mercato[57].

Per come delineato, il sistema di *governance* risulta essere strutturato per i sistemi ad alto rischio[58]. Viceversa, per i *general purpose AI models* viene invece previsto una *governance* peculiare, caratterizzata dalla centralizzazione in capo alle istituzioni dell'Unione europea. Ai sensi dell'art. 52, qualora il modello ricada nei requisiti previsti dall'AIA, il fornitore deve seguire una procedura per informare la Commissione europea, che quindi rispetto ai modelli a finalità generale costituisce autorità di notifica. Il monitoraggio avviene anche grazie al supporto del Gruppo di esperti scientifici indipendenti, che segnala «all'ufficio per l'IA i possibili rischi sistemici a livello dell'Unione dei modelli di IA per finalità generali» (art. 68, par. 3, lett. a), i) avvalendosi dei criteri indicati nell'allegato XII[59]. Inoltre, rispetto a questi modelli, nel momento in cui sono presenti sul mercato, la Commissione, ovvero l'Ufficio per l'IA, è altresì autorità di vigilanza del mercato (art.75)[60], operante in cooperazione con le autorità nazionali aventi la stessa funzione, le quali vigilano sui sistemi ad alto rischio che incorporano un modello a finalità generale.

---

[57] Il Considerando 153 recita, infatti, che «Gli Stati membri svolgono un ruolo chiave nell'applicare ed eseguire il presente regolamento».

[58] Dal momento che sono la categoria maggiormente interessata dalla disciplina di valutazione del rischio e di monitoraggio successivo.

[59] Cfr. nota 46. Inoltre, l'art. 68, par. 3 specifica i compiti del gruppo di esperti scientifici, ovvero di fornire consulenza e sostegno all'Ufficio per l'IA per:

«a) sostenere l'attuazione e l'esecuzione del presente regolamento per quanto riguarda i modelli e i sistemi di IA per finalità generali, in particolare:

i) segnalare all'ufficio per l'IA i possibili rischi sistemici a livello dell'Unione dei modelli di IA per finalità generali, conformemente all'articolo 90;

ii) contribuire allo sviluppo di strumenti e metodologie per valutare le capacità dei modelli e sistemi di IA per finalità generali, anche attraverso parametri di riferimento;

iii) fornire consulenza sulla classificazione dei modelli di IA per finalità generali con rischio sistemico;

iv) fornire consulenza sulla classificazione di vari modelli e sistemi di IA per finalità generali;

v) contribuire allo sviluppo di strumenti e modelli;

b) sostenere il lavoro delle autorità di vigilanza del mercato, su richiesta di queste ultime;

c) sostenere le attività transfrontaliere di vigilanza del mercato di cui all'articolo 74, paragrafo 11, fatti salvi i poteri delle autorità di vigilanza del mercato;

d) sostenere l'ufficio per l'IA nello svolgimento delle sue funzioni nell'ambito della procedura di salvaguardia dell'Unione di cui all'articolo 81».

[60] Art. 75, par. 1 «Qualora un sistema di IA si basi su un modello di IA per finalità generali e il modello e il sistema siano sviluppati dallo stesso fornitore, l'ufficio per l'IA ha il potere di monitorare e supervisionare la conformità di tale sistema di IA agli obblighi di cui al presente regolamento. Per svolgere i suoi compiti di monitoraggio e supervisione, l'ufficio per l'IA dispone di tutti i poteri di un'autorità di vigilanza del mercato prevista dalla presente sezione e dal regolamento (UE) 2019/1020».

L'approccio anche in questo caso è collaborativo, ma a differenza dei sistemi di IA, la supervisione sui modelli a finalità generale è svolto dall'organo esecutivo dell'Unione, che accentra una funzione regolatoria, anche attraverso la predisposizione di linee guida, codici di condotta o di buone pratiche[61], ed una di controllo. Tale architettura stride con quanto richiesto agli Stati membri. Infatti, da un lato si domanda l'indipendenza delle autorità di controllo nazionali designate[62], mentre tale caratteristica viene meno con riferimento all'Ufficio per l'IA, creando quindi un duplice scenario, in cui i sistemi di IA vengono monitorati da enti indipendenti, mentre i modelli di IA con finalità generale sono, potenzialmente, soggetti all'agenda politica della Commissione europea[63].

4.4. La designazione delle autorità nazionali per la vigilanza.

Con la COM/2021/205 la Commissione europea aveva già puntualizzato l'importanza della cooperazione tra istituzioni europee e Stati membri per assicurare «un'attuazione tempestiva e agevole del quadro giuridico dell'UE per l'IA». Questo obiettivo viene realizzato con l'obbligo per gli Stati membri di istituire o designare le autorità nazionali[64].

Il Regolamento prevede infatti un coinvolgimento diretto degli Stati membri, i quali ai sensi dell'art. 70 devono designare almeno due autorità, una di notifica e una di vigilanza del mercato. La prima è «l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio» (art.

[61] Art. 56.
[62] Art. 70, di cui si parlerà nel prosieguo.
[63] Cfr. sul punto C. Novelli, P. Hacker, et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *Eur. J. Risk Reg.*, 2024, doi:10.1017/err.2024.57.
[64] Considerando 153 «Gli Stati membri svolgono un ruolo chiave nell'applicare ed eseguire il presente regolamento. A tale riguardo, è opportuno che ciascuno Stato membro designi almeno una autorità di notifica e almeno una autorità di vigilanza del mercato come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del presente regolamento. Gli Stati membri possono decidere di nominare qualsiasi tipo di entità pubblica per svolgere i compiti delle autorità nazionali competenti ai sensi del presente regolamento, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali. Al fine di incrementare l'efficienza organizzativa da parte degli Stati membri e di istituire un punto di contatto unico nei confronti del pubblico e di altre controparti sia a livello di Stati membri sia a livello di Unione, è opportuno che ciascuno Stato membro designi un'autorità di vigilanza del mercato come punto di contatto unico».

3, n. 19), mentre la seconda è «l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2019/1020»[65] (art. 3, n. 26), ossia le attività svolte e le misure adottate dalle autorità di sorveglianza del mercato per garantire che i prodotti siano conformi ai requisiti della normativa di armonizzazione dell'Unione applicabile e tutelino l'interesse pubblico[66]. Con tale disposizione, viene perseguito lo scopo di rendere la vigilanza, e quindi il monitoraggio sull'applicazione del regolamento, diffusi, garantendo al contempo un coordinamento tra le varie autorità nazionali attraverso il Consiglio sull'IA.

L'autorità di notifica viene compiutamente disciplinata dagli artt. 28 e seguenti e svolge la funzione di vigilare sugli organismi di valutazione di conformità dei sistemi di IA. Essa è responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità, nonché per il loro monitoraggio (art. 3, n. 19). Si tratta di organismi che svolgono, per conto di terzi, attività di valutazione della conformità (ossia se i requisiti previsti dal regolamento con riferimento ai sistemi ad alto rischio sono stati soddisfatti), incluse prove, certificazioni e ispezioni. Questi compiono quindi un'attività di verifica *ex ante* sui sistemi di IA, in particolare dei sistemi ad alto rischio, come si ricava dalla lettura dei considerando 123, 124 e 125[67]. I soggetti che intendono proporsi quali

[65] Il riferimento è al 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, finalizzato a rafforzare la sorveglianza sui prodotti immessi sul mercato anche attraverso la vigilanza del mercato da parte di autorità designate, le quali vigilano sui prodotti immessi sul mercato e ove occorra indicano all'operatore economico quali azioni correttive adottare per eliminare eventuali difformità rispetto alla normativa unionale.

[66] Nella relazione alla Proposta di regolamento, infatti, la Commissione spiega che «Il titolo VIII stabilisce gli obblighi in materia di monitoraggio e segnalazione per i fornitori di sistemi di IA per quanto riguarda il monitoraggio successivo all'immissione sul mercato e la segnalazione di incidenti e malfunzionamenti correlati all'IA nonché le indagini in merito».

[67] Considerando 123: «Al fine di garantire un elevato livello di affidabilità dei sistemi di IA ad alto rischio, è opportuno sottoporre tali sistemi a una valutazione della conformità prima della loro immissione sul mercato o messa in servizio».

Considerando 124: «Al fine di ridurre al minimo l'onere per gli operatori ed evitare eventuali duplicazioni, la conformità ai requisiti del presente regolamento dei sistemi di IA ad alto rischio collegati a prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione basata sul nuovo quadro legislativo dovrebbe essere valutata nell'ambito della valutazione della conformità già prevista da tale normativa. L'applicabilità dei requisiti del presente regolamento non dovrebbe pertanto incidere sulla logica, la metodologia o la struttura generale specifiche della valutazione della conformità a norma della pertinente normativa di armonizzazione dell'Unione».

Considerando 125: «Data la complessità dei sistemi di IA ad alto rischio e i rischi ad essi associati, è importante sviluppare un'adeguata procedura di valutazione della conformità per quanto riguarda i sistemi di IA ad alto rischio che coinvolgono organismi notificati, la cosiddetta valutazione della conformità da parte di terzi. […]».

valutatori della conformità dei sistemi di IA al regolamento europeo devono, ai sensi dell'art. 29, presentare domanda di notifica all'autorità designata, dimostrando di essere in possesso dei requisiti previsti dall'art. 31 e di essere indipendenti. L'autorità, quindi, valuta la richiesta e in caso positivo designa tali organismi, sui quali esercita un'attività di monitoraggio costante al fine di verificare la permanenza dei requisiti necessari.

L'autorità di vigilanza del mercato è invece l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento UE n. 2019/1020 (art. 3 n. 26), vigilando sui sistemi di IA immessi sul mercato, i quali ancorché conformi possano costituire un rischio elevato, monitorando il reale funzionamento e l'eventuale verificarsi di incidenti gravi (art. 73), e controllando l'esito della valutazione di impatto dei sistemi di IA che devono essere impiegati da enti di diritto pubblico o enti privati fornitori di pubblici servizi (art. 27).

Tale soluzione mostra un modello di *governance* oltreché multilivello anche diffuso e che si articola su un sistema di controllo sia *ex ante* sia *ex post*. Da un lato, gli organismi a cui è demandato il compito di valutare la conformità dei sistemi di IA, vigilati dall'autorità di notifica, effettuano un controllo sui sistemi che devono essere immessi sul mercato, verificandone la conformità al regolamento nonché alle linee guida adottate dalla Commissione. Dall'altro l'autorità di vigilanza del mercato verifica il rispetto dei requisiti prescritti dalla normativa europea dei sistemi presenti sul mercato.

Alla possibilità di istituire o designare un'autorità di vigilanza del mercato, il Regolamento introduce tuttavia alcune eccezioni e deroghe. Quanto alla prima eccezione, l'art. 74, par. 6 precisa che per i sistemi di IA ad alto rischio, immessi sul mercato, a servizio o usati da istituti finanziari, l'autorità di vigilanza del mercato è l'autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di IA siano direttamente collegati alla fornitura di servizi finanziari. La seconda eccezione è invece prevista dall'art. 74, par. 8, in base al quale il Garante per la protezione dei dati è designato autorità di vigilanza del mercato con riferimento a quei sistemi impiegati ai fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III. Mentre l'art. 74, par. 3 individua quale

autorità di vigilanza del mercato specifica per i sistemi ad alto rischio quella designata ai sensi della normativa di armonizzazione prevista dall'allegato I, sezione A.
Il sistema di controllo diffuso risulta molto articolato, soprattutto in considerazione delle molteplici autorità di controllo previste, il cui coordinamento viene centralizzato a livello unionale, come si è detto nel precedente paragrafo, attraverso il Consiglio per l'IA in cui siedono i rappresentanti degli Stati membri e della Commissione europea[68].
Il modello organizzativo delineato dall'*AI Act* può essere fatto rientrare in quello delle reti e sistemi comuni[69] (laddove le reti costituiscono una forma di cooperazione tra l'amministrazione europea e le amministrazioni nazionali, dando vita a sistemi comuni), nella variante in cui i sistemi sono caratterizzati da indipendenza, ma in cui la Commissione riveste un ruolo centrale di coordinamento delle autorità nazionali (ciò è vero specialmente con riferimento ai modelli di IA a finalità generale). Mentre per altro verso presenta elementi collaborativi e di supporto all'azione della Commissione. Questo è vero se si guarda agli organismi istituiti per dare supporto all'attività dell'istituzione, e il costante riferimento alla collaborazione richiesta alle autorità nazionali e assicurata dal Consiglio per l'IA.

5. Lo strumento dell'agenzia per vigilare sull'intelligenza artificiale: il requisito dell'indipendenza.

Sotto il profilo ricostruttivo, circa la natura di queste autorità, un'indicazione viene fornita dall'art. 70, secondo cui le autorità istituite o designate devono esercitare i loro poteri in modo indipendente, imparziale e senza pregiudizi. Viene lasciata libertà di scegliere se creare un'autorità nuova oppure assegnare le funzioni ad un ente esistente, fatte salve le eccezioni e deroghe previste, ma le autorità nazionali devono essere indipendenti nell'esercizio delle loro funzioni.
Come debba essere inteso il requisito dell'indipendenza può essere ricavato da quanto già espressamente previsto nel *General Data Protection Regulation* (reg. UE n.

[68] V. art. 66.
[69] Per spiegare il modello organizzativo tracciato dall'*Artificial Intelligence Act*, si fa riferimento alla classificazione dei modelli organizzativi europei proposta da F. Giglioni, *La composizione dei sistemi amministrativi comuni*, in S. Del Gatto, G. Vesperini (a cura di), *Manuale di diritto amministrativo europeo*, Torino, 2024, pp. 159-174 e G. Vesperini, *Il diritto amministrativo europeo e le trasformazioni istituzionali dell'Unione europea*, in *Gior. dir. amm.*, 6, 2024.

2016/679), con riferimento alla figura del Garante per la protezione dei dati personali. L'art. 51 del GDPR stabilisce testualmente l'istituzione di autorità di controllo indipendenti, nel senso specificato dal successivo art. 52, quale assenza di pressioni o istruzioni esterne dirette o indirette da parte dei suoi componenti[70]. Nel caso del regolamento sulla *privacy* l'esplicitazione dei corollari, ha fatto parlare di indipendenza piena, quindi non solo assenza di un rapporto gerarchico, ma anche assenza di influenze indirette[71]. Un tanto ha trovato giustificazione nelle funzioni fondamentali di protezione dei dati delle persone fisiche[72], per cui si è inteso in senso rafforzato il concetto di potere indipendente, diversamente da quanto accade per altre autorità di controllo, per cui l'indipendenza è intesa quale neutralità tecnico scientifica e autonomia dalle interferenze rispetto alla cura degli interessi affidati[73].

Già da tempo si registra una tendenza nell'Unione europea alla creazione di poteri indipendenti, europei e nazionali, ma collegati[74], iniziata a partire dagli anni Novanta del secolo scorso e giustificata dall'assicurare maggiore uniformità nell'applicazione del diritto europeo[75] e coordinamento tra una molteplicità di attori[76].

L'*Artificial Intelligence Act* non si discosta da questo percorso, tuttavia l'autorità di vigilanza, in senso lato, contemplata nel regolamento sull'IA presenta aspetti peculiari. Il primo elemento caratterizzante sta nelle funzioni assegnate ad essa, poiché oltre a vigilare sulla conformità al regolamento dei prodotti, assicura la tutela dei cittadini rispetto alle violazioni dei diritti causate dai sistemi di IA. Il secondo elemento caratterizzante risiede nella previsione di più autorità di vigilanza del mercato. Non solo

---

[70] Tale definizione è stata codificata a partire dall'interpretazione data dalla Corte di giustizia UE, Grande Sez., 9 marzo 2010, C-518/07, sul punto v. commento di F. Fabbrini, *Il diritto dell'UE e l'indipendenza delle autorità nazionali garanti della protezione dei dati*, in *Gior. dir. amm*., 10, 2010, p. 1028.

[71] M. Macchia, C. Figliolia, *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, in *Gior. dir. amm*., 4, 2018, p. 424.

[72] M. Macchia, C. Figliolia, *op. cit*., p. 426.

[73] A. Magliari, *L'indipendenza delle autorità di vigilanza finanziaria: le esigenze di uniformazione e l'uso (improprio) della soft law*, in *Gior. dir. amm*., 3, 2024. G. Grasso, *L'anomalia di un «modello»: le autorità (amministrative) indipendenti nei paesi membri dell'unione europea*. *Prime ipotesi per un «inventario»*, in *Il Politico*, 2000, p. 263.

[74] C. Franchini, *Autonomia e indipendenza nell'amministrazione europea*, in *Dir. amm*., 1, 2008.

[75] E. Vos, *EU Agencies, Common Approach and Parliamentary Scrutiny*, in *European Parliamentary Research Service*, 2018, 19, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/627131/EPRS_STU(2018)627131_EN.pdf . G. Napolitano, *Autorità amministrative indipendenti e agenzie amministrative*, voce in M. Clarich, F. Fonderico (a cura di), *Dizionario di diritto amministrativo*, Milano, 2007, p. 86. V. Turchini, *Le autorità amministrative indipendenti oggi. La necessità di un approccio storico e comparato*, in *Quad. Corte conti*, 1, 2022, pp. 33-45.

[76] H. Hofmann, *op. cit.*, p. 30.

quelle designate, ma quelle *ex lege* previste, come il Garante della *privacy* oppure quelle di vigilanza bancaria e finanziaria. Il terzo elemento caratterizzante riguarda specificamente l'Ufficio per l'IA. Come visto, ed esplicitato nel regolamento stesso, il riferimento a questo ufficio va inteso alla Commissione, costituendo un'articolazione interna. A questo ufficio vengono tuttavia assegnate anche funzioni di autorità di vigilanza del mercato con riferimento ai *general-purpose AI models*[77], cosa che implica una frizione in primo luogo con il grado di indipendenza che si vorrebbe avere per lo svolgimento di questo tipo di funzione, scevro da condizionamenti politici; in secondo luogo l'osservanza delle regole generali previste dalla Commissione in tema ad esempio di trasparenza, poiché il Regolamento 2001/1049/CE[78] prevede eccezioni al diritto di accesso ai documenti delle istituzioni europee se ciò può danneggiare gli interessi di una persona giuridica o fisica, tra cui la proprietà intellettuale[79]. Questo tema emerge dalla lettura dell'art. 75, par. 3 ai sensi del quale «Qualora non sia in grado di concludere la propria indagine sul sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali […], un'autorità di vigilanza del mercato può presentare una richiesta motivata all'Ufficio per l'IA, che garantisce l'accesso a tali informazioni», per cui non solo vi è un tema di accesso da parte dei cittadini, ma anche da parte delle autorità di controllo nazionali.

Il quarto elemento risiede nel diverso grado del requisito dell'indipendenza. Come accennato nel caso del GDPR, viene espressamente prevista tale caratteristica per l'autorità di controllo, esplicitando come debba essere intesa e assicurata. Mentre in riferimento all'autorità ai sensi dell'*AI Act*, si parla solo di esercizio delle funzioni in maniera indipendente e imparziale.

Il richiamo alle funzioni rinvia a una nozione di indipendenza intesa nel senso classico[80] delle agenzie indipendenti dell'Unione europea, ossia indipendenza tecnica e assenza di

[77] L'art. 75 par. 1 cpv. recita, infatti, che «Per svolgere i suoi compiti di monitoraggio e supervisione, l'ufficio per l'IA dispone di tutti i poteri di un'autorità di vigilanza del mercato prevista dalla presente sezione e dal regolamento UE 2019/1020».

[78] Regolamento 1049/2001/CE del Parlamento europeo e del Consiglio, relativo all'accesso del pubblico ai documenti delle istituzioni dell'Unione europea.

[79] C. Novelli, P. Hacker, et al., *op. cit.*, p. 21.

[80] A. Magliari, *op. cit.* C. Massa, *L'indipendenza delle autorità nazionali di regolamentazione dal potere politico: recenti sviluppi nel settore dei media in Italia*, in *Quaderni AISDUE - Rivista quadrimestrale*, 1, 2024, p. 125.

influenza politica[81], in vista delle finalità perseguite, quali la necessità di competenze tecniche per affrontare le questioni in settori specifici, la credibilità e stabilità delle scelte adottate (indipendentemente dal mutare del contesto politico)[82].

Come si vedrà nei paragrafi seguenti, tramite il confronto tra Italia e Spagna, il requisito dell'indipendenza trova una declinazione differente e si traduce in scelte apparentemente distanti, ma simili. Il punto di partenza della comparazione muove dalla funzione (come descritto poc'anzi) cui sono chiamate a svolgere le autorità nazionali e si sofferma sugli elementi caratterizzanti l'indipendenza, quali la nomina dei vertici di questi enti e l'autonomia organizzativa e di bilancio[83], come parametri di confronto tra i due casi analizzati.

6. La soluzione nazionale: l'Agenzia per l'Italia Digitale e l'Agenzia per la Cybersicurezza Nazionale, quali autorità designate ai sensi dell'*AI Act*.

Il 23 aprile 2024 il Governo ha licenziato il disegno di legge n. 1146 contenente principi e regole in materia di intelligenza artificiale, al fine di disciplinare lo sviluppo, l'applicazione e l'uso di sistemi di IA (art. 1), in un contesto finora connotato dall'assenza di una regolamentazione apposita e, come è stato osservato[84], soggetto invece alle regole del mercato.

La presentazione del disegno di legge ha di fatto anticipato l'entrata in vigore dell'*AI Act*, avvenuta in parte il 2 agosto 2024[85], ponendosi, quantomeno sotto il profilo dei

[81] R. Rustichelli, *L'autorità garante della concorrenza e del mercato: origini e prospettive*, in *Riv. Corte conti*, 1, 2022, p. 65. G. Scarselli, *Autorità amministrative indipendenti: appunti per una possibile riforma*, in *Il Foro Italiano*, 126(11), 231/232-249/250. http://www.jstor.org/stable/23197926. G. Amato, *Le autorità indipendenti nella Costituzione economica*, in AA.VV., *Regolazione e garanzia del pluralismo. Le Autorità amministrative indipendenti*, Milano, 1997, p. 16.

[82] M. Manetti, *Sull'autonomia e indipendenza delle autorità*, in *Riv. AIC*, 2023, 2, 33. C. Sartoretti, *Le* authorities *al tempo del covid-19. Riflessioni sul ruolo delle autorità indipendenti: modello in declino o consolidato?*, in *DPCE*, 2, 2021, p. 2138.

[83] L. Orlando, *Genesi delle autorità amministrative indipendenti: natura e funzioni principali*, in https://www.ildirittoamministrativo.it/Genesi-delle-autorit%C3%A0-amministrative-indipendenti-natura-funzioni-principali-Luigi-Orlando/stu524, 4-7-2019.

[84] M. Macchia, A. Mascolo, *Intelligenza artificiale e regolazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, p. 97.

[85] Il regolamento infatti prevede un'entrata in vigore progressiva delle varie disposizioni in modo da consentire l'adeguamento graduale degli ordinamenti, tra cui la designazione delle autorità nazionali entro il 2 agosto 2025.

principi[86], in coerenza con esso, anche apparentemente sotto il profilo della *governance*. Sull'opportunità di stabilire regole nazionali prima ancora del dispiegarsi degli effetti di quelle comunitarie, sono sorte perplessità, come il rischio di stratificazione normativa o incompatibilità tra norme interne e comunitarie[87]. Su questo aspetto la Commissione europea ha manifestato alcuni dubbi, inviando il parere (C (2024) 7814) [88] al Governo italiano con cui ha richiesto di rendere più esplicito il richiamo al regolamento, in special modo nella parte relativa alle definizioni, al quale il legislatore si è conformato aggiungendo una norma di rinvio contenuta nell'art. 2, co. 2, secondo cui «Per quanto non espressamente previsto, si rimanda alle definizioni di cui al regolamento UE 2024/1689», Il disegno di legge è stato quindi definitivamente approvato divenendo legge dello Stato n. 132 del 23 settembre 2025, con cui si introduce nell'ordinamento per la prima volta un insieme di regole espressamente dedicate all'IA, che vanno ad integrare e dettagliare quanto previsto dall'*AI Act*.

La nuova legge da un lato enuncia i principi generali nel campo della ricerca, sperimentazione, sviluppo, adozione, applicazione e utilizzo dell'IA (art. 3, co. 1) garantendo sempre la sicurezza cibernetica[89], che assurge quindi a principio fondamentale[90], dall'altro, stabilisce regole settoriali[91], per ciascun ambito della società, dal lavoro alle professioni intellettuali, alla Pubblica amministrazione[92].

---

[86] G. Barone, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Dir. pen. proc.*, 8, 2024 p. 993.

[87] Per una analisi sul punto cfr. C. Burelli, *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?*, in *Quad. AISDUE*, *Fascicolo speciale*, 2 2024.

[88] Si tratta di un parere reso ai sensi della Direttiva (UE) 2015/1535, sull'informazione nel settore delle regolamentazioni tecniche e dei servizi della società dell'informazione, derivante dall'obbligo degli Stati membri di comunicare alla Commissione europea ogni progetto di regola tecnica. È possibile visionare le osservazioni della Commissione nel resoconto approvato dal Senato consultabile al seguente link https://www.senato.it/show-doc?id=1435866&leg=19&tipodoc=SommComm&part=doc_dc-allegato_a:1.

[89] Il comma 5 dell'art. 3 statuisce infatti che debba «essere assicurata, quale precondizione essenziale, la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale, secondo un approccio proporzionale e basato sul rischio».

[90] Nella relazione tecnica al testo, p. 20, si legge infatti che gli articoli da 1 a 6 hanno carattere ordinamentale, in quanto norme di principio.

[91] L'art. 6, anch'esso contenente norme di principio, esclude dall'ambito applicativo della legge le attività di cui al menzionato art. 3, comma 1, quando svolte per scopi di sicurezza nazionale o di cybersicurezza e resilienza indicate dall'art. 1, comma 1 lett. a) e b) del d.l. n. 14 giugno 2021 n. 82 (istitutivo dell'Agenzia per la Cybersicurezza Nazionale), ossia quelle volte a proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche.

[92] Con particolare riferimento a quest'ultimo ambito vengono dettate, all'art. 14, tre regole per l'utilizzo dell'IA, ossia promozione del suo uso per incrementare l'efficienza e la qualità dei servizi erogati, strumentalità rispetto all'attività provvedimentale e all'autonomia e al potere decisionale della persona, adozione di misure tecniche, organizzative e formative per garantire un uso responsabile. In parte, come si può notare, vengono richiamati i principi dettati dalla nota sentenza del Consiglio di Stato del 13

Accanto alle norme di principio, anche il legislatore italiano decide di dedicare alcune disposizioni al Capo III al tema della *governance*. All'art. 19 viene prevista la predisposizione della strategia nazionale per l'intelligenza artificiale da parte di apposita struttura della Presidenza del Consiglio dei ministri competente in innovazione e transizione digitale, alla quale viene anche affidato il compito di coordinamento e monitoraggio dell'attuazione di detta strategia[93]. Mentre, recependo quanto previsto nell'*AI Act*, l'art. 20 della l. 132/2025 designa le autorità nazionali per l'intelligenza artificiale individuandole in due strutture esistenti: l'Agenzia per l'Italia Digitale, quale autorità di notifica (comma 2) e l'Agenzia per la Cybersicurezza Nazionale, quale autorità di vigilanza del mercato e punto di contatto unico (comma 2 cpv.). Alla prima viene assegnata la responsabilità di definire le procedure e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di IA (comma 1 lett. a) oltre alla promozione dell'innovazione e dello sviluppo dell'IA, mentre alla seconda viene attribuito il compito di vigilanza con poteri ispettivi e sanzionatori, oltreché della promozione e dello sviluppo dell'IA relativamente ai profili di cybersicurezza (comma 1 lett. b). Nel dossier del Servizio studi del Senato[94] viene chiarita tale scelta in ragione delle competenze e delle strutture già disponibile in queste due Agenzie[95], in conformità con la clausola di invarianza finanziaria prevista all'art. 26 del medesimo disegno di legge.

---

dicembre 2019, n. 8472, successivamente codificati nell'art. 30 del d.lgs. 31 marzo 2023 n. 36, in materia di appalti.

[93] Ancor prima dell'entrata in vigore di questa legge, il Governo, attraverso l'Agenzia per l'Italia digitale ha elaborato una strategia italiana per l'IA 2024-2026. Il comma 1 dell'art. 19 dichiarando «La strategia nazionale per l'intelligenza artificiale è predisposta e aggiornata dalla struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale, d'intesa con le Autorità nazionali per l'intelligenza artificiale di cui all'articolo 20» consolida questa centralità dell'organo politica.

[94] Dossier XIX Legislatura, *Disposizioni e delega al Governo in materia di intelligenza artificiale del Servizio Studi del Senato*, p. 141, consultato al seguente link https://documenti.camera.it/leg19/dossier/Pdf/ID0010d.pdf.

[95] Per quanto attiene all'ACN queste sono individuate nel dl 82/2021 all'art. 7 e specificamente al comma 1 lett. r) «perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.

L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di

Un ulteriore possibile spiegazione, quantomeno con riferimento alla designazione dell'ACN può trovare fondamento nel fatto che la cybersicurezza si salda inevitabilmente con l'intelligenza artificiale. L'IA non solo può essere un efficace strumento per prevenire e mitigare i rischi informatici, grazie alla capacità di analizzare in tempo reale grandi quantità di minacce e predisporre risposte automatiche agli attacchi[96], attenuando il rischio derivante dal fattore umano, ma può essere anche elemento vulnerabile agli attacchi o strumento di penetrazione dei sistemi informatici. Per questo lo sviluppo e l'utilizzo di sistemi di IA non può prescindere dal considerare la sicurezza dei dati e delle infrastrutture critiche, su cui si concentra l'azione dell'ACN.
Alle due agenzie designate si affiancano la Banca d'Italia, la Consob e l'IVASS. Infatti, l'art. 20, co. 2 recepisce e richiama espressamente l'art. 74, par. 6 del Regolamento, ove si indicano quali debbano essere le autorità di vigilanza per quei sistemi di IA ad alto rischio immessi sul mercato o usati da istituti finanziari. Tale recepimento risulta essere obbligato, se si legge il par. 7 del medesimo articolo, che consente allo Stato membro di derogare quanto previsto dal par. 6 in determinate circostanze (anche se non è chiaro quali), così come quello di preservare, ancorché non fosse necessario farlo esplicitamente, le competenze del Garante per la protezione dei dati personali.
Infine, stante la coesistenza di diverse autorità di controllo, viene previsto un Comitato di coordinamento, composto dai direttori generali di AgID e ACN e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, per assicurare il coordinamento tra le due agenzie. Al medesimo comitato possono partecipare rappresentanti delle di Banca d'Italia, CONSOB e IVASS, quando si tratta di questioni di rispettiva competenza (art. 20, co. 3).
Il legislatore recepisce quindi quanto previsto dalla normativa europea. L'ACN e l'AgID diventano quelle autorità previste dal regolamento, dotate, tra l'altro, di poteri di vigilanza dei soggetti intenzionati ad utilizzare un sistema di IA, i quali devono compiere una valutazione di impatto sui diritti fondamentali che il sistema può avere e comunicare i risultati di questa valutazione all'autorità di vigilanza del mercato (art. 27). Inoltre, AgID venendo designata quale autorità di notifica, dovrà verificare il possesso

analisi valutative finalizzati a tale scopo». Mentre per quanto attiene all'AgID il richiamo è alle competenze previste dall'art. 14 *bis* del CAD, in particolare al comma 2.
[96] A. Rugolo, *Intelligenza Artificiale: la rivoluzione della Cybersecurity*, in *Difesa online,* 22 agosto 2024, https://www.difesaonline.it/2024/08/22/evidenza-cyber-intelligenza-artificiale-la-rivoluzione-della-cybersecurity/.

dei requisiti degli organismi di valutazione della conformità dei sistemi di IA, ivi incluso il possesso di idonei requisiti di cybersicurezza (ai sensi dell'art. 31 *dell'AI Act*). Pertanto, si demanda ad ente non preposto alla materia relativa alla sicurezza cibernetica la verifica di requisiti in questa materia da parte degli organismi chiamati a valutare la conformità dei sistemi di intelligenza artificiale ad alto rischio.

La designazione di queste due Agenzie pone il tema della compatibilità rispetto al comma 1 cpv dell'art. 70, secondo cui «Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi». Il requisito dell'indipendenza richiesto risulta infatti stridere con il modello organizzativo dell'Agenzia per l'Italia digitale ed in particolare dell'Agenzia per la Cybersicurezza Nazionale.

Per comprendere se un tanto sia vero, si può muovere da due ordini di considerazioni. La prima attiene al diritto dell'Unione europea, in cui un riferimento all'indipendenza degli enti lo si trova nell'art. 298 TFUE, con riferimento all'assolvimento dei compiti, nondimeno nelle varie fonti di rango secondario, ovvero le direttive e i regolamenti istitutive delle agenzie, l'indipendenza ha trovato varie declinazioni più o meno marcate[97]. La seconda riguarda i requisiti di cui deve essere in possesso un'autorità indipendente elaborati in letteratura, quali il possesso di poteri e responsabilità propri conferiti dal diritto pubblico, essere dotata di autonomia organizzativa rispetto ai ministeri o ai loro vertici e non essere soggetta né a elezione diretta, né alla gestione da parte di rappresentanti politici[98]. Da queste considerazioni si può svolgere un'analisi sulle caratteristiche delle due agenzie designate in Italia.

Con riferimento all'ACN, con il d.l. 82/2021 istitutivo il legislatore ha voluto dare una sistemazione alla disciplina e riorganizzare le competenze nel settore della *cybersecurity*[99] definendo una *governance* unitaria attraverso l'istituzione dell'Agenzia per la Cybersicurezza Nazionale[100] (art. 5) avente personalità giuridica di diritto pubblico, con autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. L'organo di vertice dell'Agenzia è il direttore generale, il quale,

[97] C. Massa, *op. cit.*, p. 127.

[98] M. Kozak, O. Batura, *Study on the NRA independence Final Report*, 2022, p. 17, https://www.berec.europa.eu/system/files/2023-02/BoR%20%2822%29%20189%20_Report%20on%20NRAs%20Independence.pdf, in cui viene ricostruita la nozione di indipendenza.

[99] Prima distribuite tra l'Agenzia per l'Italia digitale, il DIS e il Ministero dello Sviluppo economico.

[100] M. Ridolfi, *Servizi di informazione e cybersicurezza*, in *Gior. dir. amm.*, 2, 2023, p. 176.

unitamente al vicedirettore, viene nominato dal Presidente del Consiglio, previa deliberazione del Consiglio dei ministri[101].

Ai sensi del comma 4 dell'art. 5, l'attività dell'Agenzia è regolata dal decreto-legge stesso e da appositi atti, mentre per quanto attiene all'organizzazione, il successivo art. 6 stabilisce che «L'organizzazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento» adottato con decreto del Presidente del Consiglio dei ministri. Al Presidente del Consiglio viene attribuita in via esclusiva, oltre al potere di nominare il vertice dell'Agenzia, «a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza; b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4;» (art.1, comma 1). Quanto previsto dalla lettera a) viene esplicitato dal successivo comma 2, secondo cui il Presidente «impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale». Inoltre, allo stesso spetta il compito di determinare la dotazione finanziaria annuale dell'ACN (art.11, comma 1), oltre a adottare con proprio decreto il regolamento di contabilità.

Appare evidente il ruolo centrale svolto dal capo del Governo, il quale esercitando un controllo e una funzione di indirizzo incisivo, dispone di un potere di direzione sull'ente [102], che quindi rispetto all'organo politico adempie, si può concludere, una funzione strumentale[103]. Infatti, nel regolamento, adottato con DPCM 9 dicembre 2021 n. 223, viene evidenziato il ruolo strumentale dell'ACN, che ai sensi dell'art. 3, comma 1 svolge le funzioni previste dal decreto-legge «e da altre disposizioni di legge, sulla base delle direttive emanate dal Presidente del Consiglio dei ministri o dall'Autorità delegata».

Il rapporto di direzione tra l'Agenzia e l'organo politico si desume altresì dall'art. 5 del DPCM, il quale indica il direttore generale quale diretto referente del Presidente del Consiglio (o dell'autorità delegata se istituita), attribuendogli la legale rappresentanza dell'ACN, la responsabilità di curare i rapporti esterni dell'Agenzia, adottare i

[101] Tra soggetti scelti tra i magistrati delle giurisdizioni superiori ordinaria ed amministrativa, gli avvocati dello Stato, i dirigenti generali dello Stato ed equiparati, i professori universitari di ruolo, ovvero tra estranei alla pubblica amministrazione, di cui all'art. 18, co. 2 della l. 23 agosto 1988 n. 400.

[102] S. Rossa, *Cybersicurezza e Pubblica amministrazione*, Ed. scientifica, Napoli, 2023, p. 95.

[103] I. Forgione, *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in *Dir. amm.*, 4, 2022, p. 1119.

provvedimenti necessari per il funzionamento dell'agenzia, definendone gli indirizzi e coordinandone l'attività[104]. Inoltre, l'art. 16 gli attribuisce il potere di adottare ogni provvedimento, anche regolamenti, necessario all'attuazione delle funzioni dell'Agenzia.

Infine, l'incisività dell'influenza politica si desume dal potere attribuito al Presidente del Consiglio dei ministri di adottare il regolamento di contabilità ai sensi dell'art. 11, comma 3 del D.L. 82/2021, anche in deroga all'art. 17 della l. 400/1988[105].

Il potere di direzione esercitato dal Presidente del Consiglio dei ministri appare in effetti coerente rispetto alla specifica funzione per cui è stata istituita l'ACN, essendo la sicurezza cibernetica inserita nell'alveo della disciplina più ampia della sicurezza nazionale, in cui il Presidente del Consiglio rappresenta il vertice istituzionale in materia di sicurezza e di digitale[106].

Un discorso analogo può essere fatto per l'AgID, istituita con l'art. 19 del d.l. 22 giugno 2012 n. 83. Essa è espressamente soggetta al potere di vigilanza e indirizzo del Presidente del Consiglio dei ministri o di un Ministro delegato. Il potere di vigilanza sulle agenzie si esplica, ai sensi del d.lgs. 300/1999, nel potere del ministro competente di emanare gli statuti, nel caso dell'AgID con DPCM 8 gennaio 2014; mentre quello di indirizzo consiste, ai sensi dell'art. 2, co. 5 dello Statuto, nel perseguimento dei fini

[104] In base all'art. 4 del DPCM sono organi dell'Agenzia, il direttore generale, il vicedirettore e il collegio dei revisori dei conti. In quanto organi, questi sono gli unici soggetti titolari di poteri e capaci quindi di esprimere all'esterno la volontà dell'ente. Sul concetto di organo, F.G. Scoca, *La pubblica amministrazione come organizzazione*, in L. Mazzarolli, G. Pericu, A. Romano, F.A. Roversi Monaco, F.G. Scoca (a cura di), *Diritto amministrativo*, Bologna, 1998. M.S. Giannini, *Diritto amministrativo*, Milano, 1993.

[105] Il quale, invece, prevede in questi casi l'adozione di regolamenti con Decreto del Presidente della Repubblica.

[106] L'art. 14 del CAD dispone infatti che «In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime». In base alla Costituzione è dunque attribuita allo Stato la competenza in materia di digitalizzazione ed in particolare relativamente alla sicurezza informatica. Tale compito vede il Presidente del Consiglio dei ministri rivestire un ruolo centrale nelle politiche di trasformazione e innovazione digitale, come si evince dalla lettura dell'art. 16 CAD (modificato dal d.lgs. 13 dicembre 2017, n. 217), il quale attribuisce a quest'ultimo il compito di garantire un coordinamento nel processo di digitalizzazione e nello sviluppo di sistemi informativi da parte delle amministrazioni centrali, nonché di promozione e sostegno di progetti aventi grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale. Parimenti l'art. 1 della L. 3 agosto 2007 n. 124 assegna «Al Presidente del Consiglio dei ministri sono attribuiti, in via esclusiva: a) l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento; […]».

istituzionali secondo gli indirizzi impartiti dal Presidente del Consiglio dei ministri o dal Ministro da lui delegato. Come si desume anche dall'art. 14 bis CAD, AgID è preposta alla realizzazione degli obiettivi dell'Italia digitale, in coerenza con gli indirizzi dettati dal Presidente del Consigli dei ministri.

L'interrogativo da porsi è dunque se la designazione di ACN e AgID sia conforme all'art. 70 dell'*AI Act*.

Se si volge lo sguardo al requisito dell'indipendenza dal potere politico, anche nella declinazione attenuato di chi sostiene che essa debba tradursi nell'assenza di un rapporto gerarchico[107], il dato che emerge è lo stretto rapporto tra organo politico e direttore, da che quest'ultimo è considerato un referente e sebbene possa sostenersi l'esistenza di un'autonoma organizzazione delle due agenzie, il potere del Presidente del Consiglio di incidere mediante proprio decreto sull'organizzazione delle stesse, specialmente dell'ACN, fa venire meno anche questo requisito.

Ed infatti, non sono mancati rilievi da parte della Commissione europea, sull'opportunità di ripensare la designazione di queste due agenzie proprio per la carenza di indipendenza[108]. Dubbi sollevati con il menzionato parere C (2024) 7814, con il quale l'istituzione europea ha ricordato che le autorità nazionali devono possedere lo stesso livello di indipendenza previsto dalla Direttiva UE 2016/680 per le autorità preposte alla protezione dei dati nelle attività delle forze dell'ordine, nella gestione delle migrazioni e controllo delle frontiere, nell'amministrazione della giustizia e nei processi democratici. Tale direttiva specifica, all'art. 42, il requisito di indipendenza, intendendolo quale indipendenza dei membri dell'autorità di controllo, ovvero assenza di pressioni esterne, né dirette, né indirette, o di istruzioni, nonché divieto per gli stessi di compiere azioni o svolgere attività incompatibili con le loro funzioni.

Se è pure vero che l'art. 70 fa riferimento all'esercizio delle funzioni in maniera indipendente, non precludendo in maniera netta un collegamento con le autorità politiche[109], lo stretto rapporto di direzione esistente tra Presidente del Consiglio e autorità designate è sufficiente a far ritenere una possibile influenza del potere politico nell'azione di ACN e AgID.

---

[107] G. Sgueo, *Le autorità amministrative indipendenti: genesi, funzioni e ruolo*, in *www.diritto.it*, 14 giugno 2007.

[108] G. Barone, *op. cit*., p. 994.

[109] F. Resta, *Articolo 70*, in A. Mantelero, G. Resta, G.M. Riccio (a cura di), *Intelligenza artificiale. Commentario*, Milano, 2025, p. 638.

7. Il modello della Spagna: l'Agenzia di supervisione dell'Intelligenza Artificiale.

Il caso della Spagna presente alcune similitudini con quello italiano, pur muovendo da una premessa differente. Infatti, ancor prima dell'approvazione dell'*Artificial Intelligence Act*, la Spagna ha deciso di dotarsi del primo ente dedicato alla supervisione dell'Intelligenza artificiale, istituendo un'apposita agenzia[110]. Infatti, nello stesso anno in cui la Commissione europea presentava la proposta di un regolamento sull'intelligenza artificiale, il Parlamento spagnolo con la Legge dei Bilanci Generali dello Stato, 28 dicembre 2021 n. 22 dava autorizzazione al Governo alla creazione di un'agenzia nazionale di supervisione dell'IA[111]. La base giuridica dell'autorizzazione è contenuta nell'art. 91 della Ley 1° ottobre 2015 n. 40, *de Régimen Jurídico del Sector Público*[112], il quale prevede la creazione di enti pubblici unicamente mediante legge, che ne definisce altresì le finalità generali, il Dipartimento da cui dipende, nonché la natura giuridica, il regime patrimoniale e fiscale. Su queste basi la Ley 22/2021 attribuisce alla nuova agenzia personalità giuridica di diritto pubblico, patrimonio proprio e autonomia gestionale, con potestà amministrativa, con l'obiettivo di promuovere lo sviluppo e supervisionare i progetti relativi all'intelligenza artificiale inseriti nella Strategia Nazionale sull'Intelligenza Artificiale, così come quelli promossi dall'Unione europea, sotto il controllo della Segreteria di Stato alla Digitalizzazione e all'Intelligenza artificiale, inquadrata nel *Ministero de Asuntos Económicos y Transformación Digital*.

---

[110] Il contesto spagnolo si mostra proattivo sotto il profilo della regolamentazione dell'IA. Lo dimostra anche il fatto che anche le Comunità territoriali abbiano avviato iniziative. Ad esempio la Comunità autonoma della Galizia ha approvato la Ley 2 del 2 aprile 2025 con l'obiettivo di definire (art.1) un «quadro per la progettazione, l'acquisizione, l'implementazione e l'uso dell'intelligenza artificiale nell'amministrazione generale della Comunità autonoma di Galizia e nel suo settore pubblico, in conformità con la normativa dell'Unione europea e con la normativa fondamentale dello Stato in materia, di cui costituisce lo sviluppo e l'implementazione nella Comunità autonoma di Galizia». Si tratta di una legge avente lo scopo di regolare l'uso dell'IA nel settore pubblico galiziano promuovendo altresì l'adozione di una IA incentrata sull'uomo, sicura e affidabile, che offra un elevato livello di protezione della salute e dei diritti fondamentali e sia anche rispettosa dell'ambiente. Per perseguire questi fini, la legge ha previsto anche l'istituzione di un Consiglio dell'IA, un organo collegiale avente finalità consultiva e di promozione dell'IA nella Galizia, attraverso l'identificazione di strategie per migliorare le politiche pubbliche nel campo dell'IA.

[111] L'autorizzazione è contenuta nella *Disposición adicional centésima trigésima. Creación de la Agencia Española de Supervisión de Inteligencia Artificial.*

[112] D. Fierro Rodriguez, *Luces y sombras en el panorama de la Agencia Española de Supervisión de Inteligencia Artificial*, in *eXtoikos*, 26, 2023, p. 18. Questa legge unitamente alla Ley 39/2015, del 1° ottobre 2015, *del Procedimiento Administrativo Común de las Administraciones Públicas*, costituiscono i due testi normativi fondamentali del diritto amministrativo spagnolo, approvati nel 2015 con lo scopo di semplificare e razionalizzare la materia; cfr. sul punto R. G., Vioque, *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público [BOE n.o 236, de 2-X-2015]*, in *Ars Iuris Salmanticensis*, nùm. 1, 2016, p. 224.

L'effettiva creazione di questo organismo è avvenuta grazie ai finanziamenti previsti nel *Plan de Recuperación, Transformación, y Resiliencia*, Componente 16, Investimento 1 (dedicato alla digitalizzazione), tramite l'impegno di spesa deciso con l'Orden PCM/1203/2022, del 5 dicembre 2022 del Consiglio dei ministri. L'Agenzia è stata quindi formalmente istituita con il Real Decreto 729/2023, del 22 agosto 2023, recante l'approvazione dello Statuto, il quale consta di 51 articoli in cui si definiscono gli obiettivi, le funzioni e l'organizzazione dell'ente.

Dal punto di vista sistematico, l'AESIA è un'agenzia rientrante nella disciplina dalla Ley 1° ottobre 2015 n. 40[113]. Inizialmente prevista dalla Ley 19 luglio 2006 n. 28, tale espressione identificava una nuova forma organizzativa della pubblica amministrazione per l'assolvimento di funzioni connotate da natura tecnica[114]. Tale legge consentiva la costituzione di nuovi organismi, previa autorizzazione parlamentare, e con l'approvazione dello statuto, dipendenti dal Ministro che ne aveva promosso la creazione[115], per l'assolvimento delle politiche generali pubbliche.

Questo approccio incentrato su un modello di organizzazione amministrativa applicabile in via generale è stato superato dalla Ley 40/2015, con la quale è stata operata una riforma dell'organizzazione, successivamente modificata dalla Ley 30 dicembre 2020 n. 11, con cui è stata introdotta un'apposita disciplina delle agenzie (agli art. 108*bis* e seguenti)[116] ridefinendone la nozione, non più in termini di modello organizzativo, bensì includendole tra gli Enti Statali collegati o dipendenti dall'Amministrazione Generale dello Stato[117], e quindi tra quelli che in generale compongono la Pubblica amministrazione[118]. L'art. 84 della Ley 40/2015 distingue infatti «*Los organismos públicos vinculados o dependientes de la Administración General del Estado*» in tre tipologie, organismi autonomi, enti commerciali pubblici e agenzie statali, quale categoria diversa dagli organismi pubblici così detti "separati" come le autorità

[113] J.J. Montero Pascual, *Articulo 70*, in M. Barrio Andrés (dir.), *Comentarios al Reglamento Europeo de Inligencia Artificial*, Madrid, 2024, p. 671.
[114] A. Boto, *La agencia como forma organizativa de optimización de servicios públicos. Pasado, presente y futuro en una España en crisis*, in *Revista digital de Derecho Administrativo*, 2015, p. 51.
[115] J.B. Gomez Moreno, *Agencias estatales: el modelo consolidado en sistemas jurídicos de tradición anglosajona que fracasó en españa,* in *Revista Aragonesa de Administración Pública*, nùm. 58, 2022, p. 359.
[116] La modifica è stata apportata con la *Disposición final trigésima cuarta. Modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*, che ha introdotto una nuova sezione nella *Ley* 40/2015, interamente dedicata alle agenzie.
[117] Definita, mediante elenco delle amministrazioni di cui si compone, dall'art. 55 della *Ley* 40/2015.
[118] J.B. Gomez Moreno, *op. cit.*, p. 373.

amministrative indipendenti[119]. Le agenzie rientrano quindi negli organismi pubblici comuni, sono soggette alla Ley 40/2015, sono organismi di diritto pubblico, dotati di personalità giuridica pubblica, patrimonio proprio e autonomia gestionale, autorizzati a esercitare poteri amministrativi (art. 108 *bis*), possono essere create solo con legge e, in particolare, sono al servizio dell'Amministrazione Generale dello Stato[120].

L'AESIA rientra pertanto nella categoria dell'agenzia statale, come espressamente indicato nell'art. 1 dello Statuto, ai sensi del quale «*La Agencia Española de Supervisión de Inteligencia Artificial […] es una entidad de derecho público regulada en los artículos 108 bis a 108 sexies de la Ley 40/2015*», dotata di autonomia e indipendenza tecnica, intesa quale specializzazione, professionalità e responsabilità individuale del personale[121], come stabilito dall'art. 8 dello Statuto.

Per quanto attiene agli obiettivi, questi vengono definiti nell'art. 4, secondo cui l'AESIA promuove un uso dell'intelligenza artificiale responsabile, sostenibile e affidabile, offrendo consulenza e supporto ai cittadini e agli attori istituzionali e privati coinvolti nello sviluppo e nell'applicazione di sistemi di IA, assicurando altresì la protezione degli utilizzatori dei sistemi di IA al fine di evitare discriminazioni[122]. Tuttavia, la sua competenza in materia non è esclusiva, poiché le altre agenzie (ad esempio *Agencia Española de Medicamentos y Productos Sanitarios*) conservano la competenza anche rispetto all'utilizzo dell'IA nei settori specifici cui sono preposte[123].

Quanto all'organizzazione lo Statuto distingue tra organi di governo e organi esecutivi. I primi sono costituiti dal Presidente e dal Consiglio direttivo, mentre gli organi esecutivi

---

[119] R. Caballero Sanchez, *Téoria general de la organizaciòn administrativa*, in F. Velasco Caballero, M. M. Darnaculleta Gardella (a cura di), *Manual de Derecho administrativo*, 2024, p. 216.

[120] F. B. Lòpez-Jurado, *Administracòn y sector pùblico estatal,* in F. Velasco Caballero, M. M. Darnaculleta Gardella (a cura di), *Manual de Derecho administrativo*, 2024, p. 243.

[121] D. Fierro Rodriguez, *op. cit.*, p. 24.

[122] L'art. 4, co. 3 dello Statuto elenca infatti gli obiettivi dell'Agenzia:
«*Asimismo, la actuación de la Agencia responderá a los siguientes fines:*
a) La concienciación, divulgación y promoción de la formación, y del desarrollo y uso responsable, sostenible y confiable de la inteligencia artificial.
b) La definición de mecanismos de asesoramiento y atención a la sociedad y a otros actores relacionados con el desarrollo y uso de la inteligencia artificial.
c) La colaboración y coordinación con otras autoridades, nacionales y supranacionales, de supervisión de inteligencia artificial.
d) El fomento de entornos reales de prueba de los sistemas de inteligencia artificial, para reforzar la protección de los usuarios y evitar sesgos discriminatorios.
e) La supervisión de la puesta en marcha, uso o comercialización de sistemas que incluyan inteligencia artificial y, especialmente, aquellos que puedan suponer riesgos significativos para la salud, seguridad, la igualdad de trato y no discriminación, en particular entre mujeres y hombres, y para los demás derechos fundamentales».

[123] D. Fierro Rodriguez, *op. cit.*, p. 24.

sono la Direzione, il Segretariato generale, la Sotto-direzione di Certificazione, valutazione delle tendenze, coordinamento e formazione in materia di intelligenza artificiale. Il ruolo del Presidente viene dallo Statuto assegnato al Segretario per la digitalizzazione e l'intelligenza artificiale, il quale inoltre presiede il Consiglio direttivo, che è composto da otto membri nominati dal Ministero dell'Economia.

Con l'approvazione dell'*AI Act*, il tema della designazione delle autorità di controllo ivi prevista si è posto anche per il legislatore spagnolo. L'aver istituito un'agenzia con le descritte funzioni prima dell'entrata in vigore del regolamento ha generato uno scollamento con quanto previsto dall'art. 70 del regolamento, per due ragioni. In primo luogo, la previsione dell'istituzione di autorità nazionali di vigilanza del mercato ha richiesto al Governo di licenziare un disegno di legge, nel marzo 2025, «*Para un uso ético, inclusivo y beneficioso de la inteligencia artificial*» con cui designare l'AESIA quale autorità di vigilanza del mercato, altrimenti ente non inquadrabile nel perimetro normativo unionale. In secondo luogo, il quadro giuridico in cui si colloca l'AESIA mostra una divergenza rispetto a quanto indicato nell'*AI Act*, ove si specifica, come già ribadito, che le autorità nazionali agiscono nel quadro del Regolamento UE 2019/1020 relativo alle autorità di vigilanza del mercato[124]. Anche nel caso dell'Agenzia spagnola di supervisione dell'intelligenza artificiale si pone infatti il tema dell'indipendenza.

Muovendo da un confronto con quegli elementi caratteristici dell'indipendenza sopra richiamati, appare evidente come non possa parlarsi di autonomia dal potere politico. Come si è già avuto modo di evidenziare, l'Agenzia di Supervisione dell'Intelligenza artificiale rientra nella categoria degli organismi pubblici strumentali, e quindi dipendenti dell'Amministrazione Generale dello Stato. Tale vincolo di dipendenza si evince altresì sotto un duplice profilo. In primo luogo, dalla lettura dell'art. 108 *ter*, co. 3 *Ley* 40/2015 (espressamente richiamato dallo Statuto dell'Agenzia), in base al quale l'azione dell'ente avviene in conformità con il contratto pluriennale di gestione, nel quale vengono definiti gli obiettivi da perseguire, i piani d'azione e i risultati attesi, che ai sensi dell'art. 39 dello Statuto viene approvato dal Ministero degli Affari Economici. In secondo luogo, il vincolo con l'amministrazione centrale emerge con più forza dalla lettura degli artt. 12 e seguenti dedicati agli organi di governo dell'ente. In particolare, l'art. 12 espressamente prevede che il Presidente dell'agenzia è il Segretario di Stato

[124] J.J. Montero Pascual, *op. cit.*, 670.

della Digitalizzazione e dell'Intelligenza artificiale, il quale presiede e dirige il *Consejo Rector*, composto da sei rappresentanti, di cui quattro del Ministero degli Affari Economici, uno del Ministero delle Finanze e della Funzione Pubblica, uno del Ministero dell'Industria, del Commercio e del Turismo e solamente un rappresentante indipendente selezionato tra gli esperti in materia di IA dal *Consejo Asesor de Inteligencia Artificial y la Comisión Permanente de Digitalización de la Economía, la Administración y la Ciudadanía*.

Alle considerazioni che precedono vale la pena aggiungere un'ulteriore considerazione. Lo Statuto dell'AESIA non richiama l'art. 109 della *Ley* 40/2015 rubricato *Les autoritats administratives independents d'àmbit estatal*, collocando in effetti tale ente al di fuori degli organismi indipendenti, similmente a quanto avviene per l'Agenzia per la Cybersicurezza Nazionale e l'Agenzia per l'Italia Digitale.

8. Il ruolo dello Stato nell'ecosistema dell'*AI Act.*

Anche nel campo dell'intelligenza artificiale il diritto europeo si pone l'obiettivo di avvicinare gli ordinamenti nazionali verso una disciplina comune, anche mediante la creazione di nuovi organismi. Tuttavia, il confronto tra i casi di Italia e Spagna, per quanto riguarda le autorità di vigilanza e notifica, mette in luce come le modalità di recepimento dell'*AI Act* adottate dai due Paesi, pur divergenti, conducano a esiti simili in concreto, discostandosi dallo statuto di indipendenza descritto dall'art. 70 del regolamento. L'opzione italiana di designazione, quali autorità, di due agenzie esistenti (ACN e AgID), e quella spagnola istitutiva di un ente nuovo e specializzato, l'AESIA, mostrano un paritetico problema di interferenza del potere politico, nel primo caso potenziale, nel secondo evidente. Le due soluzioni ripropongono un modello di autorità strumentali, fortemente integrate nell'apparato governativo, ma se nel caso dell'Italia un tanto si deve a una scelta del legislatore di declinazione del requisito di indipendenza, per la Spagna sembra piuttosto frutto della scelta di aver anticipatamente istituito un ente dedicato all'IA. Eppure, in entrambi i casi si pone un problema di autonomia dell'esercizio delle funzioni, che in considerazione del ruolo di vigilanza del mercato, si ripercuoterà sulla tutela dei consumatori e dei diritti delle persone.

La costruzione della *governance* nazionale dell'intelligenza artificiale in questi termini appare come un tentativo di rispondere alla crisi degli Stati nazione e della loro sovranità, causata dal moltiplicarsi delle norme e istituzioni sovranazionali[125], riaffermando il controllo dello Stato in un campo chiave per lo sviluppo futuro, in cui si misurano anche le tensioni geopolitiche sulla proiezione ultra europea del regolamento e gli interessi delle compagnie private specialmente nord americane[126].

[125] L. Casini, *Lo Stato (im)mortale*, Mondadori, 2022, p. 38.
[126] V. sul punto S. Řezníková, *Regulating AI – borders of freedom and sovereignty*, in *Ceridap*, 2026.

CAPITOLO III
Infrastrutture digitali strategiche nazionali

1. Introduzione.

Come spiegato nel capitolo precedente il sistema di *governance* costruito dall'*Artificial Intelligence Act* rappresenta il tentativo di contemperare le contrapposte esigenze di assicurare una regolazione uniforme ed in chiave collaborativa tra gli Stati membri per preservare il funzionamento del mercato unico e al contempo preservare la sovranità nazionale, se non altro attraverso la possibilità di normare specifici settori (senza ovviamente entrare in conflitto con il regolamento).

Il tema della sovranità pur manifestandosi probabilmente con maggiore preponderanza sul terreno dell'IA, investe tutto il dominio digitale, ed in particolare due ambiti in cui questo tema si presenta sotto aspetti peculiare, ossia il *cloud* e la cybersicurezza, nei quali la necessità regolatoria e di una *governance* esprimono l'esigenza di riaffermare la sovranità intesa quale controllo territoriale, o meglio localizzazione nel territorio delle infrastrutture digitale e correlativamente garantire la sicurezza.

Il *cloud computing,* come infrastruttura portante dei sistemi informativi, nonché la cybersicurezza, costituiscono per i motivi che verranno illustrati dei settori complessi per gli enti pubblici, e per il diritto amministrativo.

Le pubbliche amministrazioni sono chiamate a rendere disponibili i propri servizi tramite piattaforme informatiche, da cui deriva la necessaria dotazione di infrastrutture materiali e immateriali[1] a tale scopo. La conseguenza è da un lato l'urgenza di sviluppare l'ecosistema digitale per la pubblica amministrazione, dall'altro l'interconnessione strutturale tra servizi *cloud* e la loro diffusione nelle pubbliche amministrazioni ha l'effetto di trasformare ogni vulnerabilità potenziale, in un rischio sistemico. Un incidente informatico o fisico alla infrastruttura che fornisce servizi *cloud* può infatti riverberarsi sull'erogazione dei servizi pubblici essenziali e sulla protezione dei dati cittadini.

[1] G. Carullo, *L'amministrazione quale piattaforma di servizi digitali*, Editoriale Scientifica, Napoli, 2022, p. 15.

Di fronte a simili questioni, a livello unionale la risposta legislativa si è articolata attraverso una pluralità di atti tra loro complementari, ossia la Direttiva UE 2022/2555 (Direttiva NIS 2), il Regolamento UE 2024/2847 (*Cyber Resilience Act*) e il Regolamento UE 2024/1689 (*AI Act*)[2]. Mentre il legislatore italiano ha provveduto a dare attuazione a questi testi con la l. 28 giugno 2024 n. 90 ed in particolare il d.lgs. 4 settembre 2024 n. 138, con cui è stata recepita la direttiva NIS 2.

La particolare attenzione dedicata dal legislatore nazionale ed europeo a questi ambiti, segnala l'importanza riconosciuta ad essi per assicurare la sovranità europea[3], e il ruolo di ogni organizzazione per preservare i sistemi informatici dalle minacce criminali e dai rischi geopolitici.

Il presente capitolo esamina quindi lo sviluppo dei servizi *cloud*, e l'evoluzione normativa collegata e di quella dedicata alla cybersicurezza, nell'ordinamento italiano, dall'istituzione del perimetro di sicurezza nazionale cibernetica definito dal d.l. 21 settembre 2019, n. 105, unitamente alla Strategia Nazionale di Cybersicurezza 2022-2026, al ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN).

Come si avrà modo di spiegare il sistema di *governance* della sicurezza cibernetica si innesta con quello dell'*AI Act*, anche per l'identità degli attori coinvolti, su tutti l'ACN. La sicurezza cibernetica investe, infatti, nodi fondamentali dello Stato, quali i confini della sovranità digitale, la distribuzione di responsabilità, la tutela dei dati personali e di quelli detenuti dalle pubbliche amministrazioni.

Le direttrici dell'analisi seguono l'implementazione delle soluzioni *cloud* in particolare per i Comuni, il recepimento della NIS2 e le funzioni dell'ACN come autorità qualificante i servizi *cloud*, nonché ente preposto alla sicurezza dello spazio digitale. L'approccio adottato segue la tesi secondo cui la cybersicurezza non è riducibile a una questione meramente tecnica, riguardando piuttosto tanto le organizzazioni quanto il contesto normativo.

L'analisi delle interazioni tra le tecnologie *cloud* disponibili, il quadro normativo in materia di cybersicurezza e gli oneri organizzativi per le pubbliche amministrazioni

[2] Questi testi insieme costituiscono il corpus normativo dedicato al digitale. Unitamente agli altri regolamenti disciplinanti il settore del digitale, ossia il *Digitale Market Act*, il *Digitale Service Act*, il *Data Act*. In proposito cfr. cap. 1.

[3] Sul punto v. M. Burri, Z. Zihlmann, *The EU Cyber Resilience Act – An Appraisal and Contextualization*, in *Zeitschrift für Europarecht*, 2, 2023, B1-B45, disponibile in SSRN: https://ssrn.com/abstract=4375552.

segue lo schema del *TOE framework*, il quale risulta particolarmente adatto per comprendere la complessità del fenomeno in esame[4]. Vengono quindi considerate le tre dimensioni di questo modello di analisi, ossia tecnologica, organizzativa e ambientale, ed in particolare i fattori abilitanti di ognuna per comprendere quali sono i fattori critici per lo sviluppo tecnologico della pubblica amministrazione.

In particolare, la dimensione tecnologica tiene in considerazione le soluzioni *cloud* disponibili, nonché i principi di *digital by default* e *security by design* e *lifecycle security*, oltre ai criteri di qualificazione dei servizi *cloud*. L'analisi della dimensione organizzativa si concentra, invece, sia sulla dimensione dell'organizzazione stessa sia sulla capacità di preparazione dei dipendenti e dei dirigenti di gestire la transizione, a ma anche sulle nuove figure professionali necessarie per un'implementazione concreta delle tecnologie. Questi fattori emergono nella possibilità e capacità per l'ente di adottare tali soluzioni facendo ricorso ai finanziamenti messi a disposizioni con il PNRR, unitamente alla capacità, in determinati casi influenzata dalla legislazione, di istituire una *governance* interna, specialmente in ambito cybersicurezza, con l'individuazione di nuove figure, al fine di rispondere agli obblighi di *reporting* alle autorità competenti, come si avrà modo di spiegare nel prosieguo.

Infine, la dimensione ambientale è quella in cui il quadro normativo europeo e italiano risulta emergere quale fattore esercitante l'influenza determinante. Gli investimenti pubblici, la NIS2 e la legislazione nazionale compongono un contesto regolatorio di crescente complessità che indirizza e guida necessariamente le scelte organizzative e di riflesso l'adozione di soluzioni tecnologiche.

Tale analisi può essere così sintetizzata:

Contesto	Fattori
Tecnologico	*Cloud computing*; IaaS, PaaS, SaaS; Polo Strategico Nazionale;
Organizzativo	Capacità organizzativa; programmazione spesa; utilizzo fondi; riorganizzazione (referente sicurezza, notifica incidenti); strutture di governance (ruolo ACN);

[4] Tale approccio metodologico è stato seguito per evidenziare i fattori che condizionano l'adozione del *cloud computing* nel settore pubblico, cfr. E. Entsiea, F.K. Frempong Aidoo, A. Vaz, *Systematic review of cloud computing adoption in the public sector: Insights from the TOE framework and DOI theory*, in *Multidisciplinary Reviews*, 9(2), 2025, https://doi.org/10.31893/multirev.2026091. Applicando lo stesso approccio, nel presente capitolo si è voluto estenderlo all'analisi dei fattori condizionanti la diffusione del *cloud* e degli strumenti di cybersicurezza nelle pubbliche amministrazioni locali, ossia i Comuni, come esempio di studio concreto dei fattori condizionanti.

Ambientale	Direttiva NIS2, l. 90/2024, d.lgs. 138/2024; *soft law* tecnica (linee guida ACN, documenti programmatici AgID); requisiti di localizzazione dati; tassonomia dati ACN (ordinario/critico/strategico); sovranità digitale;

A differenza di precedenti analisi, che prendono in considerazione i singoli fattori per comprendere quali siano quelli condizionanti l'adozione di una data tecnologia, qui dopo aver applicato tale modello analitico allo studio dell'implementazione delle soluzioni di *cloud computing*, si procederà a considerare il *cloud* e la cybersicurezza alla stregua di fattori condizionanti l'adozione dell'IA nella pubblica amministrazione.
Per queste ragioni è coerente applicare questo modello per indagare i fattori che condizionano l'adozione di soluzioni di IA da parte delle pubbliche amministrazioni. Come si avrà modo di chiarire, la disponibilità di infrastrutture *cloud* qualificate, l'esistenza di un quadro normativo definito e la capacità organizzativa degli enti si intrecciano, rendendo il successo della transizione verso l'IA un fenomeno multifattoriale che non si riduce alla mera disponibilità di tecnologie avanzate.

2. Il *cloud* nella pubblica amministrazione.

2.1 Contesto normativo e nozione di *cloud*.

Il tema della *governance* dell'intelligenza artificiale, analizzato nei precedenti capitoli, si innesta con il peculiare contesto storico in cui l'innovazione sta richiedendo un approccio organico, tale da necessitare riforme normative per adeguare l'ordinamento alla transizione anche in riferimento ad altri settori tecnologici collegati.
Per comprendere il contesto normativo, in cui questa trasformazione ha preso avvio, è opportuno partire dalla fonte di riferimento[5], ossia il d.lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale (CAD), il quale costituisce il testo fondamentale per la disciplina dell'informatizzazione della pubblica amministrazione.
Stante la risalenza nel tempo della sua prima versione, il CAD è stato oggetto di numerosi interventi modificativi. Tra questi, quelli maggiormente rilevanti, rispetto all'economia del presente discorso, sono stati operati dai decreti-legge approvati nel 2012, che hanno costituito un importante cambiamento di approccio del legislatore al

[5] F. Notari, *Il percorso della digitalizzazione delle amministrazioni pubbliche: ambiti normativi mobili e nuovi modelli di governance*, in *Giorn. dir. amm.*, 1, 2020, p. 27.

tema del digitale. Il d.l. 9 febbraio 2012 n. 5 (convertito con l. 4 aprile 2012 n. 35) con l'art. 47, rubricato Agenda digitale italiana, al comma 2 ha indicato l'istituzione della cabina di regia dell'agenda digitale (con decreto del Ministro dello Sviluppo Economico)[6], assegnando a tale ufficio, tra i vari compiti[7], anche quello di promuovere la diffusione e il controllo di architetture di *cloud computing* per le attività e i servizi delle pubbliche amministrazioni. Il successivo d.l. 18 ottobre 2012, n. 179 (convertito con modificazioni dalla l. 17 dicembre 2012, n. 221), ha avviato un significativo processo di informatizzazione dei servizi pubblici[8], introducendo il domicilio digitale del cittadino, l'uso del fascicolo elettronico nelle scuole e quello sanitario. Inoltre, modificando il comma 1 dell'art. 68 del CAD, quest'ultimo decreto-legge ha reso possibile per le pubbliche amministrazioni ricorrere al mercato, nel rispetto dei principi di economicità, efficienza e neutralità tecnologica, per l'approvvigionamento di *software* a seconda delle esigenze, incluse soluzioni di *cloud computing*[9]. Trattasi, quest'ultima ipotesi, di un modello di infrastruttura informatica che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad esempio reti, server, risorse di archiviazione, applicazioni *software*) che possono essere rapidamente erogate come servizio, semplificando la gestione dei sistemi informativi, sia eliminando la gestione relativa ad applicativi fruibili direttamente online, sia trasformando le infrastrutture fisiche in servizi virtuali fruibili in base al consumo di risorse[10].

---

[6] Comma modificato nel 2014, con il quale è stata stabilita per legge l'istituzione della cabina di regia presso la Presidenza del Consiglio dei ministri e successivamente abrogato con d.lgs. 26 agosto 2016, n. 179. Le funzioni della cabina di regia sono state quindi assorbite dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri.

[7] Tra cui la promozione del paradigma dei dati aperti, il potenziamento delle applicazioni di amministrazione digitale, infrastrutture per favorire l'accesso alla rete. Il comma è stato successivamente abrogato con d.lgs. 26 agosto 2016, n. 179.

[8] V. Pagnanelli, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Riv. it. infor. dir.*, 1, 2021, p. 12.

[9] I. Macrì, *Il cloud per le pubbliche amministrazioni*, in *Azienditalia*, 1, 2021, p. 18.

[10] Cfr. sul punto il Manuale di Abilitazione al Cloud dell'Agenzia per l'Italia Digitale, consultabile al seguente link https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/v1.2/index.html). La definizione di *cloud computing* contenuta nel manuale di abilitazione redatto da AgID riprende quella elaborata dal *The National Institute of Standards and Technology* (NIST), istituto di ricerca, facente parte dell'*U.S. Department of Commerce* secondo cui «*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*». Mentre lo stesso istituto definisce il *cloud* come «*the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer,*

Il quadro normativo iniziale mostra quindi una apertura del legislatore per questo tipo di soluzioni, relegandola però ad alternativa tra le altre percorribili, come si evince dall'elenco di soluzioni possibili, quali *software* già in uso ad altre amministrazioni, oppure mediante acquisto di licenze. Solo successivamente si è presa piena contezza dell'importanza della tecnologia *cloud* per lo sviluppo e l'innovazione dell'apparato pubblico, a partire dal Piano Triennale per l'informatica nella Pubblica amministrazione 2019-2021[11] e soprattutto con la Strategia *cloud* per l'Italia[12]. In quest'ultimo documento viene evidenziato come «l'irreversibile processo di trasformazione digitale della società, […], ha reso improcrastinabile un'analoga trasformazione della Pubblica Amministrazione. […]. In questo processo trasformativo, il ricorso al Cloud Computing, o Cloud, riveste un ruolo centrale in ragione delle sue caratteristiche abilitanti per la semplificazione e ottimizzazione della gestione delle risorse IT, la riduzione dei costi, e l'introduzione di nuove tecnologie digitali»[13] individuando quindi nel *cloud computing* «un nuovo paradigma di utilizzo e gestione di risorse computazionali e di servizi informatici erogati su richiesta tramite internet». Per dare concreta attuazione a questi documenti programmatici l'Agenzia per l'Italia Digitale ha quindi approvato un regolamento[14] apposito volto a stabilire i requisiti minimi di sicurezza delle infrastrutture destinate ad ospitare i dati e servizi delle pubbliche amministrazioni, nonché le modalità di qualificazione dei servizi *cloud*.

Pur definendo il percorso per le pubbliche amministrazioni per la migrazione verso le "nuvole", fino al 2024 è mancata una definizione normativa di servizio di *cloud computing*. Infatti, è solamente il d.lgs. 4 settembre 2024 n. 138 (di cui si parlerà nel

---

which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer».

[11] Ove si afferma che «Il cloud, nell'ambito della trasformazione digitale, rappresenta una delle tecnologie cosiddette disruptive, che comporta notevoli vantaggi in termini di incremento di affidabilità dei sistemi, qualità dei servizi erogati, risparmi di spesa realizzabili attraverso l'opportunità della migrazione dei servizi esistenti verso il cloud e la possibilità di pagare soltanto gli effettivi consumi (*pay-per-use*). L'adozione del paradigma cloud rappresenta la chiave della trasformazione digitale consentendo una vera e propria rivoluzione del modo di pensare i processi di erogazione dei servizi della PA verso i cittadini», v. Piano Triennale per l'Informatica nella Pubblica amministrazione 2019-2021, p. 33.

[12] Documento realizzato dal Dipartimento per la trasformazione digitale presso la Presidenza del Consiglio dei ministri.

[13] Strategia *cloud* Italia, p. 1.

[14] Con Determinazione n. 628/2021 del 15 dicembre 2021. Adozione del Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi *cloud* per la pubblica amministrazione.

prosieguo) a definirlo «un servizio digitale che consente l'amministrazione su richiesta di un *pool* scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni[15]». A questa definizione contenuta in una fonte primaria, si affianca quella contenuta nel Regolamento dell'Agenzia per la Cybersicurezza Nazionale[16] approvato nel 2024, che sostituisce quello precedente dell'AgID, il quale distingue la nozione di *cloud computing*, che rappresenta un «paradigma che abilita l'accesso via rete ad un insieme condivisibile, scalabile ed elastico di risorse fisiche o virtuali attivabile autonomamente su richiesta dall'utente», dai servizi *cloud* definiti quali servizi «informatici e risorse computazionali erogati mediante il paradigma *cloud computing* su richiesta dell'utente tramite internet da un fornitore di servizi *cloud* differenziati, sulla base del modello computazionale offerto, in tre categorie di servizi». I due concetti, anche a livello normativo, risultano dunque essere distinti.

Quando si parla di *cloud* il riferimento non è peraltro solamente ad una infrastruttura fisica, ossia un insieme di *server* connessi a Internet, ma un sistema di erogazione di servizi[17], *self-service on-demand*, per la condivisione elastica e rapida di dati e servizi. Il regolamento dell'Agenzia per la Cybersicurezza Nazionale provvede a classificare tali servizi, distinguendoli in tre tipologie, ossia:

1. *Infrastructure-as-a-Service* (IaaS), servizi sistemistici infrastrutturali per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati;
2. *Platform-as-a-Service* (PaaS), servizi di piattaforme computazionali, per l'erogazione di ambienti preconfigurati e amministrati per lo sviluppo di specifiche applicazioni, ad esempio per lo sviluppo software, la gestione di dati o di applicazioni containerizzate;
3. *Software-as-a-Service* (SaaS), servizi applicativi, per l'erogazione di un'applicazione agli utenti finali, ad esempio la posta elettronica o altri sistemi di collaborazione remota[18].

---

[15] Purtroppo, la definizione presente nel decreto legislativo (art. 2 lett. bb) non risulta essere chiara, apparendo imprecisa e vaga.

[16] Regolamento per le infrastrutture digitali e per i servizi *cloud* per la pubblica amministrazione, adottato con Decreto Direttoriale n. 21007/24, ai sensi dell'articolo 33 *septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, pubblicato il 27 giugno 2024 e applicabile dal 1° agosto 2024.

[17] A. Garlassi, *Il* cloud*: opportunità di crescita per i sistemi di controllo digitali*, in *Controllo gestione,* 3, 2022, p. 50.

[18] Questa classificazione discende da quella elaborata dal *National Institute of Standard and Technology* secondo cui «*Software as a Service (SaaS). The capability provided to the consumer is to use the*

2.2. La Strategia *Cloud* Italia.

La Strategia *Cloud* Italia[19] pubblicata nel 2021 rappresenta il primo atto con cui il Governo ha definito un piano organico per la transizione digitale delle pubbliche amministrazioni, individuando tre direttrici per realizzarlo[20]: la classificazione di dati e servizi, la qualificazione dei servizi *cloud* e la creazione del Polo Strategico Nazionale.
La prima direttrice è la distinzione dei dati e servizi in tre categorie sulla base del danno che «una loro compromissione, [può arrecare] in termini di confidenzialità, integrità e disponibilità»[21], in ordinari, critici e strategici[22], e risulta essere strettamente connessa alla qualificazione dei servizi *cloud.* Il documento indica alle pubbliche amministrazioni di differenziare i dati in loro possesso in base a questa categorizzazione in funzione della scelta dei servizi *cloud* che possono essere non qualificati oppure qualificati. La qualificazione descritta nel documento individua quindi i servizi *cloud*, in base al livello di sicurezza e controllo dei dati, in "cloud pubblico non qualificato", offerto da provider sia extra-UE sia UE, e "*cloud* pubblico qualificato", disponibile nell'UE, e conforme ai

---

provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)».

[19] Si tratta di un documento di indirizzo realizzato dal Dipartimento per la trasformazione digitale, della Presidenza del Consiglio dei ministri volto a definire gli indirizzi strategie per l'adozione del *cloud* da parte delle pubbliche amministrazioni, con il fine di garantire l'autonomia tecnologia del Paese, garantire il controllo dei dati e la resilienza dei servizi digitali.

[20] I. Macrì, *Cloud della Pubblica Amministrazione: una casa moderna per i dati degli italiani*, in *Azienditalia*, 11, 2021, p. 1848.

[21] Strategia *cloud* Italia, 2021, p. 13.

[22] Ordinari: dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese. Critici: dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese. Strategici: dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale; Cfr. Strategia *Cloud* Italia, 2021, p. 14.

regolamenti GDPR e NIS[23], che garantisce la localizzazione dei dati all'interno dell'Unione e adotta sistemi di sicurezza avanzati, come la cifratura gestita dal fornitore. A questa distinzione si aggiungono il "*cloud* pubblico con controllo *on-premise*" (o *cloud* criptato), dotato di un ulteriore livello di protezione grazie al controllo *on-premise* dei meccanismi di sicurezza, e il "*cloud* privato e ibrido",[24] che consentono la localizzazione dei dati in Italia e un isolamento più marcato dalle aree geografiche dei grandi *provider*, con gestione operativa affidata a fornitori soggetti a vigilanza pubblica. Dalla diversa qualificazione discende la possibilità di migrazione dei dati delle pubbliche amministrazioni. Solo i dati ordinari possono essere ospitati su *cloud* pubblico generico, mentre i dati critici e strategici devono risiedere in infrastrutture con alti requisiti di sicurezza, come i servizi *cloud* qualificati in conformità ai requisiti stabiliti dal regolamento ACN del 2024[25]. Tale regolamento con riferimento ai requisiti delle infrastrutture, nonché dei servizi, prescrive i requisiti di sicurezza, anche con riferimento alle categorie di dati. L'art.17 stabilisce infatti quale debba essere la

[23] Ovvero il Regolamento generale sulla protezione dei dati (Reg. UE 2016/679) e il Regolamento europeo sui sistemi informatici, dedicato alla cybersicurezza.

[24] Anche la distinzione tra *cloud* pubblico e privato non è priva di rilievo. Il documento programmatico riporta infatti che «Nel *Cloud* pubblico l'infrastruttura è di proprietà di un CSP che, avendone il pieno controllo, mette a disposizione di utenti, aziende ed enti pubblici i propri sistemi, distribuiti in diverse aree geografiche (o regioni) del mondo, con la condivisione di capacità elaborativa, applicazioni e storage. Tale distribuzione permette agli utenti dei servizi *cloud* di beneficiare di capacità computazionali resilienti e scalabili a seconda delle effettive esigenze.» Si tratta in altre parole dei grandi service provider principalmente degli Stati Uniti.
«Il *Cloud* privato consiste in un ambiente *Cloud* riservato ad un singolo cliente per suo utilizzo esclusivo. Questo può essere *on-premise*, ovvero basato su infrastrutture che si trovano interamente nel dominio del cliente, che detiene il controllo e la totale responsabilità sulla manutenzione e la gestione della sicurezza dei dati e dei servizi ospitati, oppure può essere gestito presso i *data center* di un terzo soggetto, presso cui il cliente dispone di risorse dedicate. Fra i vantaggi di un *Cloud* privato c'è sicuramente il maggior controllo che il cliente può esercitare sulle caratteristiche dell'infrastruttura e dei servizi *Cloud*, soprattutto per quanto riguarda la sicurezza. Al contrario, fra gli svantaggi di questa soluzione, soprattutto nel caso di *cloud on-premise*, occorre considerare il fatto che l'infrastruttura può non essere in grado di garantire l'adeguata scalabilità per gestire picchi non previsti di domanda.
Cloud ibrido: Combinazione del modello di *cloud* pubblico e di quello privato, il *cloud* ibrido si configura come un singolo ambiente creato a partire da più ambienti connessi in cui, a seconda delle necessità, sono messe a disposizione degli utenti risorse sia di un *cloud* privato che di un *cloud* pubblico. Tale modello consente, infatti, di estendere le capacità di un *cloud* privato per utilizzare, su richiesta, le risorse di larga scala disponibili su un *cloud* pubblico, ad esempio, per gestire improvvisi picchi di lavoro e garantire risparmi in termini di banda di trasmissione necessaria per lo scambio dei dati, rispetto a quanto sarebbe possibile con una connessione ad un data center».

[25] I. Macrì, *Dalle infrastrutture digitali delle amministrazioni al cloud, il nuovo regolamento per la sicurezza dei dati e dei servizi pubblici*, in *Azienditalia*, 3, 2022, p. 488. Inizialmente il regolamento di riferimento era quello di AgID del 2021, approvato con la Determinazione 628/2021, successivamente sostituito dal Decreto Direttoriale 2 dicembre 2023 n. 29 del Direttore dell'Agenzia per la Cybersicurezza Nazionale ed infine dal Regolamento per le infrastrutture digitali e per i servizi *cloud* per la pubblica amministrazione, adottato con Decreto Direttoriale n. 21007/24 del Direttore dell'Agenzia per la Cybersicurezza Nazionale.

qualificazione cui sono tenuti i fornitori dei servizi *cloud* per le PA, suddividendola in quattro livelli, QC1, QC2, QC3, QC4, laddove il livello QC1 consente di trattare dati classificati come ordinari, il QC2 quelli critici, il QC3 quelli strategici e l'ultimo ancora quelli strategici, ma con specifici requisiti di elevata sicurezza previsti dagli allegati 3 e 4 del Regolamento[26]. Gli operatori, per poter fornire servizi *cloud* alla pubblica amministrazione, devono quindi ottenere la qualificazione dall'ACN, per ogni livello[27]. Mentre le pubbliche amministrazioni possono ricorrere a soluzioni *cloud* esclusivamente qualificate da ACN.

L'ultimo tassello di questa strategia è la costituzione del Polo Strategico Nazionale. Si tratta di un'infrastruttura ad alta affidabilità, geograficamente distribuita, destinata a ospitare dati e servizi strategici della PA, e promossa dal Dipartimento per la trasformazione digitale al fine di sanare la situazione di arretratezza e frammentazione delle infrastrutture esistenti[28]. Sotto il profilo operativo la realizzazione del Polo è stata finanziata con la Missione 1 Componente 1 del PNRR, attraverso la costituzione di una società per azioni, denominata Polo Strategico Nazionale S.p.A., partecipata da TIM, Leonardo, Cassa Depositi e Prestiti e Sogei, secondo il modello del partenariato pubblico privato[29]. Si tratta di un'infrastruttura costituita da diversi *data center*[30] distribuita in località differenti[31] in cui far confluire i dati e i servizi critici e strategici

[26] Gli allegati descrivono in particolare i requisiti tecnico-operativi necessari per poter ricevere la qualificazione a livello richiesto, presupposto per poter erogare servizi di *hosting* o altra tipologia alle pubbliche amministrazioni.

[27] Viene richiesto inoltre al fornitore il possesso di certificazioni ISO (ovvero quelle certificazioni rilasciate da un organismo indipendente che certificano la conformità della gestione e dei processi agli standard stabiliti dall'*International Organization for Standardization*), diverse a seconda del livello di cui si chiede la qualificazione.

[28] G. Napolitano, *Il partenariato pubblico-privato per la realizzazione del Polo strategico nazionale*, in *Gior. dir. amm.*, 6, 2021, p. 704.

[29] G. Napolitano, *op. cit.*, p. 705.

[30] Termine che indica un'infrastruttura fisica che ospita server e strumenti IT (*hardware* e *software*) per la connessione e l'accesso da remoto. Ve ne sono di vari tipi, in particolare quelli di *cloud computing* ospitano le risorse per una gestione condivisa di dati e servizi da parte di più clienti (cfr. sul punto "Strategia Cloud Italia", 2021 di AgID e il Regolamento *Cloud*, 2024 dell'ACN). I più grandi *data center* sono gestiti da grandi aziende quali Alphabet, Amazon Web Services, Microsoft e IBM e vengono chiamati *hyperscale*. Non esiste una definizione ufficiale di questo tipo di strutture, tuttavia secondo quanto si legge nella libreria virtuale del Congresso degli Stati Uniti con tale termine si indicando quei data center contenenti almeno 5.000 server in uno spazio di circa 3000 metri quadri, con una domanda di energia superiore a 100 megawatts/h, cfr. al seguente link https://www.congress.gov/crs-product/IF12899.

[31] Tale infrastruttura rispecchia quanto previsto nel documento Strategia cloud Italia, in cui si legge «Il PSN ha infatti l'obiettivo di dotare la PA di tecnologie e infrastrutture Cloud che possano beneficiare delle più alte garanzie di affidabilità, resilienza e indipendenza. A tal fine, si prevede che il PSN sia distribuito geograficamente sul territorio nazionale presso siti opportunamente identificati, al fine di garantire adeguati livelli di continuità operativa e tolleranza ai guasti. La gestione operativa del PSN sarà affidata a un fornitore qualificato sulla base di opportuni requisiti tecnico-organizzativi. Il fornitore dovrà

delle amministrazioni centrali, delle ASL, nonché delle principali amministrazioni locali, quali Regioni, città metropolitane e Comuni con più di 250.000 abitanti.

La base giuridica per la creazione di questi impianti tecnologici destinati ad ospitare il patrimonio informativo della pubblica amministrazione è l'art. 33 *septies* del d.l. 179/2012[32], modificato dal d.l. 16 luglio 2020 n. 76, il quale attribuisce alla Presidenza del Consiglio dei ministri il compito di promuovere la realizzazione di un'infrastruttura ad alta affidabilità localizzata nel territorio italiano, al fine di assicurare l'autonomia tecnologica del Paese, imponendo altresì alle amministrazioni locali di migrare i centri di elaborazione dati e i relativi sistemi informatici propri verso questa nuova infrastruttura o altre qualificate, qualora i propri *data center* non rispettino i requisiti minimi di sicurezza ed efficienza[33].

Le pubbliche amministrazioni possono avvalersi dei servizi offerti dal PSN, che sono in particolare di tipo *IaaS* e *PaaS*, sottoscrivendo un contratto con la società Polo Strategico Nazionale S.p.A. sulla base della convenzione stipulata tra questa e il Dipartimento per la trasformazione digitale[34].

---

garantire il controllo sui dati in conformità con la normativa in materia, nonché rafforzare la possibilità della PA di negoziare adeguate condizioni contrattuali con i fornitori di servizi Cloud».

[32] Introdotto dalla legge di conversione n. 221/2012. Nella sua originaria formulazione l'articolo affidava all'Agenzia per l'Italia Digitale il compito di effettuare un censimento dei CED (centri elaborazione dati), definiti ai sensi del medesimo articolo «un sito che ospita un impianto informatico atto alla erogazione di servizi interni alle amministrazioni pubbliche e servizi erogati esternamente dalle amministrazioni pubbliche», con l'obiettivo di razionalizzare le risorse e favorire il consolidamento delle infrastrutture digitali.

[33] I. Macrì, *Polo Strategico Nazionale*, in *Azienditalia*, 3, 2023, p. 460.

[34] L'art. 5 della Convenzione definisce l'oggetto dell'accordo stabilendo in particolare che «La Convenzione definisce la disciplina generale relativa alla Concessione relativa alla prestazione in favore delle singole Amministrazioni Utenti, in maniera continuativa e sistematica, di servizi altamente dedicati e con focus su sicurezza, connettività ed affidabilità […] con messa a disposizione di un'infrastruttura appositamente progettata, predisposta ed allestita ad alta affidabilità, localizzata sul territorio nazionale, con caratteristiche adeguate ad ospitare la migrazione delle infrastrutture, delle applicazioni e dei dati frutto della razionalizzazione e del consolidamento dei Centri di elaborazione Dati e dei relativi sistemi informatici delle pubbliche amministrazioni di cui all'articolo 33 *septies* del d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, come modificato dall'art. 35 del d.l. 16 luglio 2020, n. 76, nonché come ulteriormente modificato dall'art. 7, d.l. 6 novembre 2021, n. 152, ed a ricevere la migrazione dei detti dati affinché essi siano poi gestiti attraverso una serie di servizi da rendere alle amministrazioni titolari dei dati stessi». Cfr. "Concessione per la realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012", consultata al seguente link www.datocms-assets.com/38008/1671199163-convenzione-dtd_polo-strategico-nazionale.pdf.

3. Gli investimenti per innovare la pubblica amministrazione.

3.1 Il *cloud first* come paradigma della trasformazione digitale.

La realizzazione di quanto definito nella Strategia *Cloud* Italia si deve specialmente al Piano Nazionale di Ripresa e Resilienza[35]. Tale strumento è stato approvato per far fronte alle conseguenze economiche e sociali derivanti dalla crisi pandemica da SarsCov2 (*Coronavirus disease*). L'Unione europea ha infatti istituito, nell'ambito del programma straordinario *Next Generation EU*, il Dispositivo per la ripresa e la resilienza (*Recovery and Resilience Facility* – RRF), al fine di sostenere la ripresa economica degli Stati membri[36], i quali per poter accedere a questo piano di finanziamenti, hanno sottoposto un programma di investimenti e di riforme strutturali. Quello italiano è stato approvato il 13 luglio 2021 con Decisione di esecuzione del Consiglio dell'Unione Europea, corredata da un Allegato tecnico in cui sono stati dettagliati, per ciascuna misura di riforma o investimento, i relativi traguardi (*milestones*) e obiettivi (*targets*), il cui raggiungimento ha costituito e costituisce condizione necessaria per l'erogazione progressiva delle risorse finanziarie. Per l'Italia il piano di investimenti[37] ha previsto una somma pari a 194,4 miliardi di euro (di cui 122,6 miliardi in prestiti e 71,8 miliardi in sovvenzioni), comprendente 66 riforme e 150 investimenti, articolati in 618 traguardi e obiettivi.

Conformemente ai target europei, il Piano di Nazionale di Ripresa e Resilienza italiano vede tra gli obiettivi l'ammodernamento della Pubblica amministrazione, attraverso la modernizzazione, in particolare, delle infrastrutture tecnologiche delle amministrazioni pubbliche, anche attraverso la migrazione dei sistemi informativi verso soluzioni *cloud* sicure e interoperabili, e la creazione di un Polo Strategico Nazionale (PSN). Inoltre,

[35] I. Macrì, *Cloud della Pubblica Amministrazione: una casa moderna per i dati degli italiani*, cit., p. 1848.

[36] Il funzionamento di questo strumento è disciplinato dal Regolamento (Ue) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, che ha previsto una dotazione iniziale massima pari a 672,5 miliardi di euro, di cui 312,5 miliardi sotto forma di sovvenzioni e 360 miliardi come prestiti agevolati. A seguito delle modifiche introdotte con il Regolamento (UE) 2023/435 (cd. REPowerEU), è stato inoltre previsto un incremento delle sovvenzioni disponibili per un importo pari a 20 miliardi di euro. Cfr. G. Lonero, *Relazione sul Regolamento UE 241 del 2021. Una panoramica comprensiva delle disposizioni e delle implicazioni,* in *Il Diritto Amministrativo*, disponibile al seguente link https://www.ildirittoamministrativo.it/Relazione-sul-Regolamento-UE-241-del-2021-Una-panoramica-comprensiva-delle-disposizioni-delle-implicazioni/gamm1090.

[37] Frutto della modifica apportata con la Decisione di esecuzione dell'8 dicembre 2023 con cui il Consiglio dell'Unione europea ha riprogrammato il PNRR dell'Italia.

viene promossa l'interoperabilità dei dati e dei servizi, declinazione in concreto dei principi *once only*, *digital by default* e *cloud first*[38], già enunciati nel Piano Triennale per l'Informatica nella Pubblica amministrazione 2019-2021[39]. A supporto degli investimenti, sono state previste riforme normative[40] e organizzative orientate alla semplificazione delle procedure di acquisizione di servizi ICT, alla promozione dell'approccio *cloud first* e alla rimozione degli ostacoli giuridici allo scambio di dati tra amministrazioni. Il risultato di questo insieme di investimenti, è la trasformazione dell'amministrazione in chiave artificiale, dotata di un potere digitale[41].

Al centro del processo innovativo vi è quindi, in primo luogo, la creazione di una grande infrastruttura informatica sostenuta con i fondi previsti dalla missione M1.C1 – Digitalizzazione, innovazione e sicurezza nella PA del PNRR, in particolare alla voce 1.2 Abilitazione e facilitazione migrazione al *Cloud*, per realizzare «il sistema operativo del Paese»[42]. Si tratta di un progetto finalizzato a trasformare la pubblica amministrazione in un sistema operativo interconnesso, nel quale operino dati e applicazioni, per fornire ai cittadini servizi più efficienti e accessibili[43].

Tale obiettivo, già fissato nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019[44], e ribadito nel documento programmatico Strategia *Cloud* Italia, identifica il *cloud* come uno dei fattori abilitanti della trasformazione

[38] Secondo il Piano triennale con il principio *once only* si indica alle pubbliche amministrazioni di evitare di chiedere ai cittadini e alle imprese informazioni già fornite, mentre con *digital by default* si impone alle PA di fornire servizi digitali come opzione predefinita. Infine, con il principio *cloud first* si richiede alle pubbliche amministrazioni, in fase di definizione di un nuovo progetto, o di sviluppo di nuovi servizi, di valutare in via prioritaria l'adozione del paradigma *cloud* prima di qualsiasi altra tecnologia, tenendo conto della necessità di prevenire il rischio di *lock-in*. Dovranno altresì valutare il ricorso al *cloud* di tipo pubblico, privato o ibrido in relazione alla natura dei dati trattati e ai relativi requisiti di confidenzialità.

[39] Si tratta di un documento strategico aggiornato periodicamente dall'Agenzia per l'Italia Digitale. Nel documento del 2019 vengono enunciati i principi cardine della trasformazione digitale della Pubblica amministrazione.

[40] Il primo intervento in tal senso è rappresentato dal d.l. 31 maggio 2021 n. 77 (c.d. Decreto semplificazioni), v. G. Sgueo, *La transizione digitale*, in *Gior. dir. amm.*, 6, 2021.

[41] E. Carloni, *Dalla legalità algoritmica alla legalità (dell'amministrazione) artificiale. Premesse ad uno studio,* in *Riv. it. infor. dir.*, 2, 2024.

[42] Questa frase compare sul portale cloud.italia.it in cui vengono illustrati la strategia *cloud* per le pubbliche amministrazioni e i passaggi attraverso cui queste e i fornitori possono realizzare tale progetto. Come descritto nel Piano Nazionale di Ripresa e Resilienza (pag. 18) «il passaggio al *cloud* faciliterà lo sviluppo di un nuovo ecosistema di prodotti e servizi per la PA».

[43] V. *Piano Nazionale di Riprese e Resilienza, Next Generation EU*, p. 90.

[44] Al punto 3.2.1. del Piano viene individuato tra gli obiettivi strategici da perseguire quello di realizzare «un ambiente cloud della PA, omogeneo dal punto di vista contrattuale e tecnologico, riqualificando le risorse interne alla PA già esistenti o facendo ricorso a risorse di soggetti esterni qualificati». L'obiettivo è conseguire un risparmio di spesa derivante dal consolidamento dei data center e migrazione dei servizi verso il *cloud*.

digitale del Paese, per permettere di semplificare e ottimizzare la gestione delle risorse[45], ma anche razionalizzare, consolidare e modernizzare le risorse tecnologiche, migliorando efficienza, sicurezza e gestione delle informazioni[46].

La transizione delle pubbliche amministrazioni verso il *cloud* è necessariamente collegata all'intenzione di rendere non solo i dati accessibili, ma anche attiene anche alla modalità di erogazione dei servizi, ovvero stabilire che le prestazioni fornite dalla pubblica amministrazione siano digitali[47]. Tale principio è quindi divenuto paradigma del progetto di trasformazione degli uffici pubblici, per l'erogazione ai cittadini di servizi non solo efficienti, ma anche sicuri e di qualità[48].

L'investimento contemplato dal PNRR si colloca in questa direzione, allocando risorse per quasi un miliardo di euro[49]. L'assegnazione avviene con la pubblicazione di un avviso di finanziamento, al quale gli enti attuatori (amministrazioni centrali e locali) possono aderire inviando un progetto di migrazione dei dati e servizi della pubblica amministrazione verso soluzioni *cloud*[50]. L'importo finanziabile per ogni progetto, con particolare riferimento alle p.a. locali, viene definito secondo due criteri: modalità di migrazione al *cloud* (trasferimento in sicurezza dell'infrastruttura IT o aggiornamento in sicurezza di applicazioni in c*loud*)[51] e classe di popolazione residente di riferimento del

---

[45] Strategia *cloud* Italia, 2021, p. 4.

[46] E. Montagnani, *Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali*, in *Riv. it. infor. dir.,* 1, 2022, p. 190. I. Macrì, *Cloud nella pubblica amministrazione: una casa moderna per i dati degli italiani*, cit. Il rapporto su «La spesa ICT nella PA italiana. Percorsi e trend in atto 2022-2025», redatto da AgID, mostra come la spesa per il digitale nelle PA centrali sia enormemente cresciuto grazie ai fondi del PNRR, mentre per le PA locali e le Regioni l'andamento sia costante, cfr p. 14 del rapporto.

[47] G. Carullo, *op. cit.*, p. 8. Viene in questo modo data attuazione al principio sancito nell'art. 3 del Codice dell'Amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82) per cui «I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice».

[48] I. Macrì, *Dalle infrastrutture digitali delle amministrazioni al cloud, il nuovo regolamento per la sicurezza dei dati e dei servizi pubblici*, in *Azienditalia*, 3, 2022, p. 488.

[49] L'importo esatto è pari a 954.511.199,00. Tale dato viene reso noto dal portale Pa Digitale 2026, consultabile al seguente link www.padigitale2026.gov.it/open-data.

[50] Gli avvisi pubblicati sono rivolti alle amministrazioni centrali e locali.

[51] L'opzione trasferimento, detta anche *re-host* o trasferimento di *host* consente la migrazione al *cloud* dell'infrastruttura già esistente. Tale soluzione, detta anche strategia di *Lift and Shift*, consiste nel prendere (*Lift*) l'intero servizio, inclusa l'infrastruttura, architettura, dati e traffico, e spostarlo su un *hosting cloud* (*Shift*) senza modifiche al *core* dell'applicativo. Spesso il *re-host* è una strategia che permette di fare un primo step verso il *cloud* valutando poi successivamente ulteriori miglioramenti all'applicativo che permettano di sfruttare ulteriormente i vantaggi del *cloud*. Mentre l'opzione aggiornamento si attua mediante le soluzioni *re-purchase* o sostituzione, che consente nel sostituire un applicativo installato e gestito *on-premise* con la controparte SaaS oppure *re-platform* o trasferimento di piattaforma, consistente nel trasferimento di un applicativo sul *cloud* (come nel *re-host*), ma sostituisce

medesimo soggetto attuatore[52] (ossia il numero di abitanti), distinguendo sette classi differenti, da quella con popolazione inferiore ai 2.500 abitanti a quella con popolazione superiore ai 250.000. Sulla base della conformità ai requisiti[53] stabilita negli avvisi il Dipartimento per la trasformazione digitale ammette i progetti.

3.2. La dimensione dell'investimento nei Comuni italiani: un'analisi a partire dai dati.

Tra il 2022 e il 2025 sono stati pubblicati diversi avvisi[54] destinati a finanziare la migrazione dei dati e dei servizi delle pubbliche amministrazioni, non solo centrali, ma anche di quelle più prossime ai cittadini. Sulla base di queste aperture di finanziamento sono state stabilite finestre temporali entro cui gli enti hanno potuto presentare i loro progetti e richiedere i contributi.

Per comprendere la dimensione e gli effetti di questo investimento nel prosieguo dell'analisi ci si è concentrati sui Comuni, in quanto connotati da arretratezza sotto il profilo della digitalizzazione dei servizi[55], a partire dai dati resi disponibili in formato aperto nella *repository* disponibile su "dati.gov.it" del Dipartimento per la trasformazione digitale e sul sito ItaliaDomani. Il primo dataset[56] preso in considerazione contiene tutte le informazioni relative all'importo del finanziamento per ciascun Comune italiano, la finestra temporale di riferimento dei decreti di erogazione

---

nel processo di migrazione alcune componenti per meglio sfruttare le specificità della piattaforma di destinazione. Cfr. sul punto Manuale di abilitazione al *cloud* di AgID consultabile al seguente link https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/v1.4/index.html.

[52] V. l'avviso per la presentazione di domande di partecipazione a valere su PNRR - Missione 1 - Componente 1 investimento 1.2 "Abilitazione al cloud per le pa locali", pubblicato a luglio 2025.

[53] Un requisito prodromico all'ammissibilità del progetto è l'avvenuta classificazione dei dati e servizi in conformità agli artt. 3 e 5 del Regolamento AGID di cui alla Determinazione AGID n. 628/2021.

[54] Il primo avviso è dell'aprile 2022, mentre l'ultimo pubblicato è di luglio 2025, ogni informazione è reperibile al seguente link https://areariservata.padigitale2026.gov.it/Pa_digitale2026_avvisi.

[55] La relazione della Commissione parlamentare di inchiesta sul livello di digitalizzazione e innovazione delle pubbliche amministrazioni e sugli investimenti complessivi riguardanti il settore delle tecnologie dell'informazione e della comunicazione del 2017 rilevava che su 23 Comuni di grandi dimensioni o capoluogo, poco più della metà aveva indicato un responsabile per la transizione digitale (cfr. p. 104 della relazione al link documenti.camera.it/apps/nuovosito/Documenti/DocumentiParlamentari/parser.asp?idLegislatura=17&categoria=022bis&tipologiaDoc=documento&numero=014&doc=pdfel). Tale dato, unitamente agli altri analizzati, secondo la relazione della Commissione dimostra quanto l'innovazione digitale nella pubblica amministrazione fosse sostanzialmente assente.

[56] Consultato da ultimo in data 23 novembre 2025.

dei fondi, l'importo finanziato e se il progetto è stato accettato (A), respinto (R) o eseguito (E)[57]. Tali dati sono stati analizzati al fine di descrivere il quadro dei finanziamenti destinati ai Comuni per la migrazione dei dati e servizi nel *cloud*.

Attraverso una prima analisi dei dati è possibile evidenziare l'andamento dei contributi ammessi, raggruppati per regione e divisi per macro aree geografiche in relazione alle finestre temporali di ciascun avviso di finanziamento.

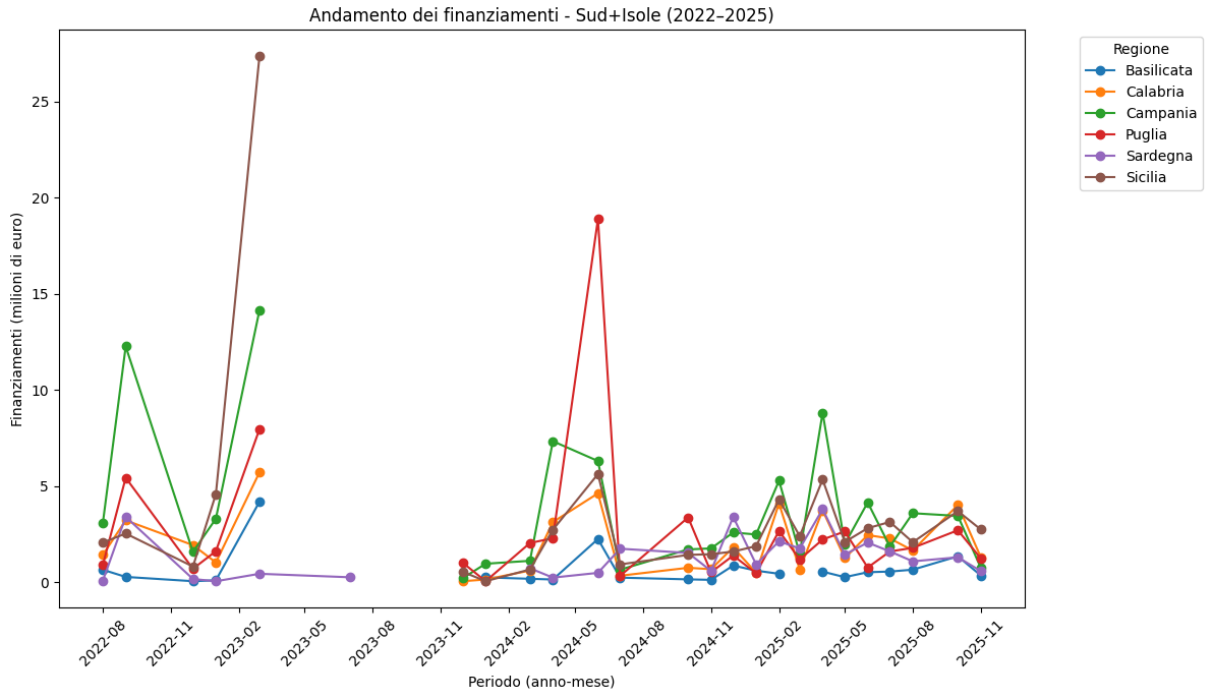


Figura 1

[57] Reperito al seguente link dati.gov.it/view-dataset?groups=scienza&organization=pcm-dipartimento-trasformazione-digitale.

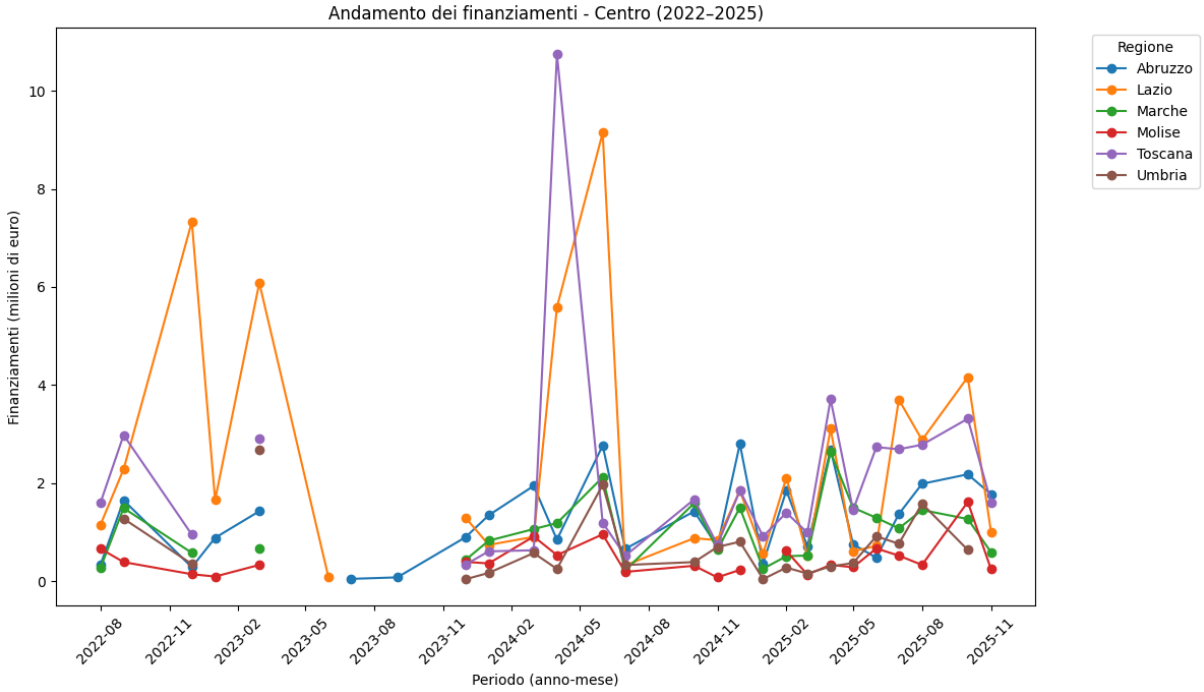


Figura 2

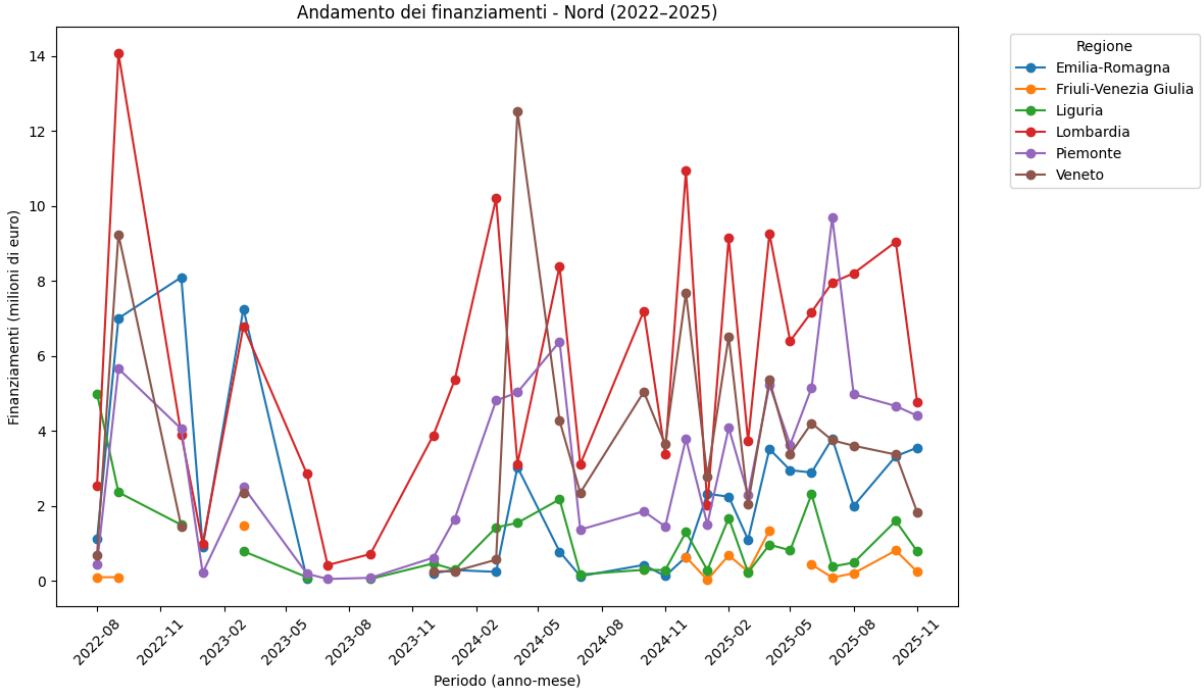


Figura 3

Le figure mostrano come la maggior parte delle risorse allocate sia stata messa a disposizione nel 2022, mentre successivamente il numero di finanziamenti sia andato

calando, mostrando anche una certa disomogeneità tra le regioni circa la dimensione dei finanziamenti assegnati. Una prima considerazione che risulta possibile svolgere attiene al numero variabile dei Comuni per ogni regione. Ne consegue che una volta approvato il progetto, con relativa assegnazione dei fondi, oltre a un generale divieto previsto nei bandi successivi di presentare domanda di partecipazione da parte dei soggetti già finanziati, sempre meno sono state le municipalità che hanno chiesto l'accesso alla misura prevista dal PNRR. In ogni caso risulta interessante rilevare come vi sia stato un acceso interesse verso soluzioni *cloud*, che, come si vedrà nel prosieguo, rappresenta una tecnologia centrale per la modernizzazione delle pubbliche amministrazioni anche nella prospettiva dell'adozione dell'intelligenza artificiale.

Il secondo dataset al quale si è attinto per comprendere l'andamento degli investimenti è stato reperito sul sito ItaliaDomani[58] che contiene numerose informazioni sui progetti di migrazione al *cloud*, tra cui anche lo stato di avanzamento e la data di conclusione effettiva del progetto finanziato.

Al fine di rendere l'analisi più approfondita, al dataset iniziale è stata aggiunta un'ulteriore colonna contenente i codici delle aree interne di ciascun Comune, che costituisce un sistema sintetico utilizzato per descrivere l'ente rispetto alla vicinanza ai servizi pubblici. La mappa delle aree interne, redatta dall'Istat, prende infatti in considerazione l'intero territorio italiano nella sua articolazione a livello comunale, e classifica i Comuni sulla base dell'offerta congiunta di tre tipologie di servizio (ad esempio salute, istruzione, mobilità), distinguendoli in poli, poli intercomunali, a cui si aggiunge un'ulteriore classificazione, determinata sulla base della distanza da questi poli, in quattro fasce a crescente distanza relativa, ossia cintura, intermedi, periferici, ultraperiferici, e, quindi, con un potenziale maggior disagio nella fruizione di servizi[59].

L'inserimento di questa ulteriore informazione ha consentito di approfondire l'analisi dei dati per comprendere i tempi medi di conclusione dei progetti, determinati sulla base della data di inizio e di fine effettiva presente nel dataset, raggruppando le informazioni relative, in base alla classificazione menzionata e stabilire se vi fosse una relazione tra

[58] Il dataset di riferimento, aggiornato al 14 ottobre 2025, è reperibile al seguente link https://www.italiadomani.gov.it/content/sogei-ng/it/it/catalogo-open-data.html?orderby=%40jcr%3Acontent%2FobservationDateInEvidence&sort=desc

[59] Cfr. La geografia delle aree interne nel 2020: vasti territori tra potenzialità e debolezze elaborata dall'Istat, consultata al seguente link https://www.istat.it/wp-content/uploads/2022/07/FOCUS-AREE-INTERNE-2021.pdf.

tipologia di ente e tempi di conclusione dei progetti. Tale scelta si giustifica in ragione della diversità dimensionale delle amministrazioni comunai in termini di dipendenti, di capacità di spesa e anche di numero di servizi che in base agli avvisi PNRR potevano essere migrati. Ad esempio, nel caso di Comuni con popolazione da 5000 a 20.000 abitanti possono essere migrati un range di servizi da 1 a 14, mentre per i Comuni con popolazione superiore a 250.000 abitanti fino a 21.

Il risultato di questa analisi mostra come non vi sia una significativa differenza nei tempi medi di conclusione dei progetti; si va infatti dagli 892 giorni per i Poli agli 818,8 giorni per i Comuni ultraperiferici. Tale dato può essere, tuttavia, indice della difficoltà di conclusione dei progetti per i piccoli centri dotati di personale ridotto. Viceversa per i Poli, la lunghezza dei tempi di conclusione può essere spiegata in ragione della complessità della migrazione, sia per la mole di dati da migrare sia per il numero di servizi che è necessario migrare per poter accedere ai finanziamenti[60].

Un altro dato osservato è il basso tasso di completamento dei progetti dei Poli (che arriva al 13,2% a novembre 2025); un valore che si discosta drasticamente dalla media nazionale del 54,0% e dal tasso delle classi B–F, le quali si attestano in un intervallo compresso tra il 54,6% (F — Ultraperiferico) e il 59,9% (C — Cintura).

Quello che i dati restituiscono è come i grandi comuni capoluogo costituiscono una categoria a sé stante, con tempi di completamento strutturalmente più lunghi rispetto a tutti gli altri tipi di ente comunale. Questo risultato è coerente con le caratteristiche progettuali dei Polo urbani, il cui finanziamento medio dei progetti supera i 4,8 milioni di euro, a fronte di una media nazionale di 67.759 euro, riflettendo una complessità architetturale e organizzativa della migrazione incomparabilmente maggiore. Il basso tasso di completamento dei progetti riguardanti i Poli non è indice di un ritardo sistemico, bensì della complessità degli stessi in virtù della loro dimensione.

L'ulteriore analisi conferma come proprio il tasso di completamento dei progetti destinati ai Comuni classificati come Poli sia il più basso, senza differenze tra aree geografiche (figura 4), indicando che la migrazione al *cloud* dipende specialmente dalla complessità del progetto, piuttosto che dalla posizione geografica degli enti.

[60] Ad esempio nel bando Avviso Investimento 1.2 "Abilitazione al Cloud per le PA Locali" Comuni settembre 2024, per i Comuni di piccole dimensioni si consente di migrare fino a 9 servizi, mentre per i Comuni con popolazione sopra i 250.000 abitanti il limite viene esteso fino a 21 servizi. Peraltro, come chiarito negli allegati al bando una volta selezionato il servizio, il percorso di migrazione deve includere tutti gli applicativi e sistemi afferenti allo stesso.

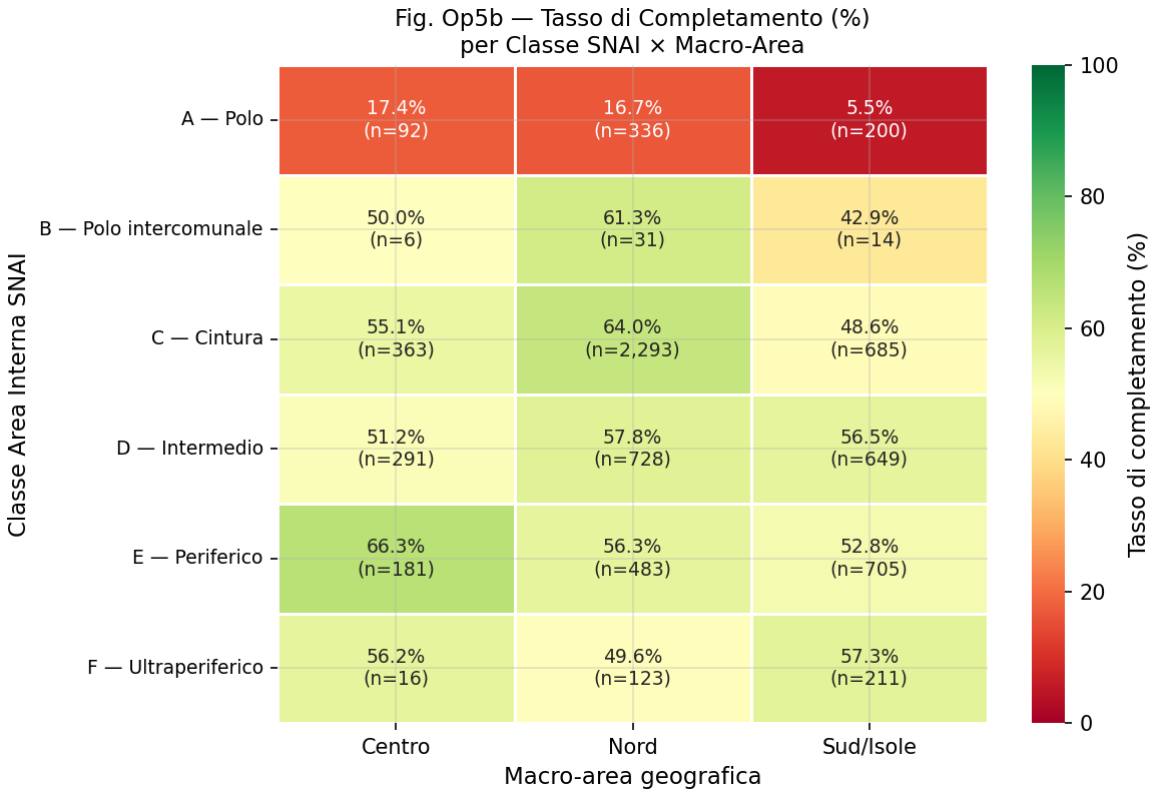


Figura 4

Mentre se si guarda ai tempi di conclusione dei progetti rispetto alla media nazionale, emerge una differenza tra le Regioni, anche in questo caso non legato al tradizionale discorso del divario Nord/Sud (figura 5).

Il risultato è influenzato dal fatto che tiene in considerazione solamente i progetti conclusi. Tuttavia, risulta possibile compiere una valutazione dell'impatto degli investimenti del PNRR sulla migrazione al *cloud* delle pubbliche amministrazioni locali, anche in considerazione delle stringenti regole previste dagli avvisi di finanziamento[61].

Il quadro che emerge è un'elevata attenzione per questa tecnologia, che rappresenta un tassello per rendere i servizi pubblici immediatamente fruibili, migliorando efficienza

[61] L'Avviso Investimento 1.2 "Abilitazione al Cloud per le Pa locali" Comuni ha previsto l'obbligo per gli enti di costruire un progetto di migrazione individuando i servizi, *software* in uso e dati da migrare, scegliendo i servizi/le attività da svolgere tra una serie di opzioni (in funzione della specifica misura) offerte dalla Piattaforma PA digitale 2026 (cfr. Linee Guida per i Soggetti attuatori individuati tramite avvisi pubblici *a lump sum* del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri).

ed efficacia dell'azione amministrativa, ma anche che l'effettiva realizzazione dei progetti si scontra con le difficoltà di esecuzione di un intervento di transizione tecnologica di questo tipo, mostrando come i tempi di esecuzione siano in taluni casi molto lunghi, con significativo divario nel tasso di completamento tra le Regioni (fig. 5).

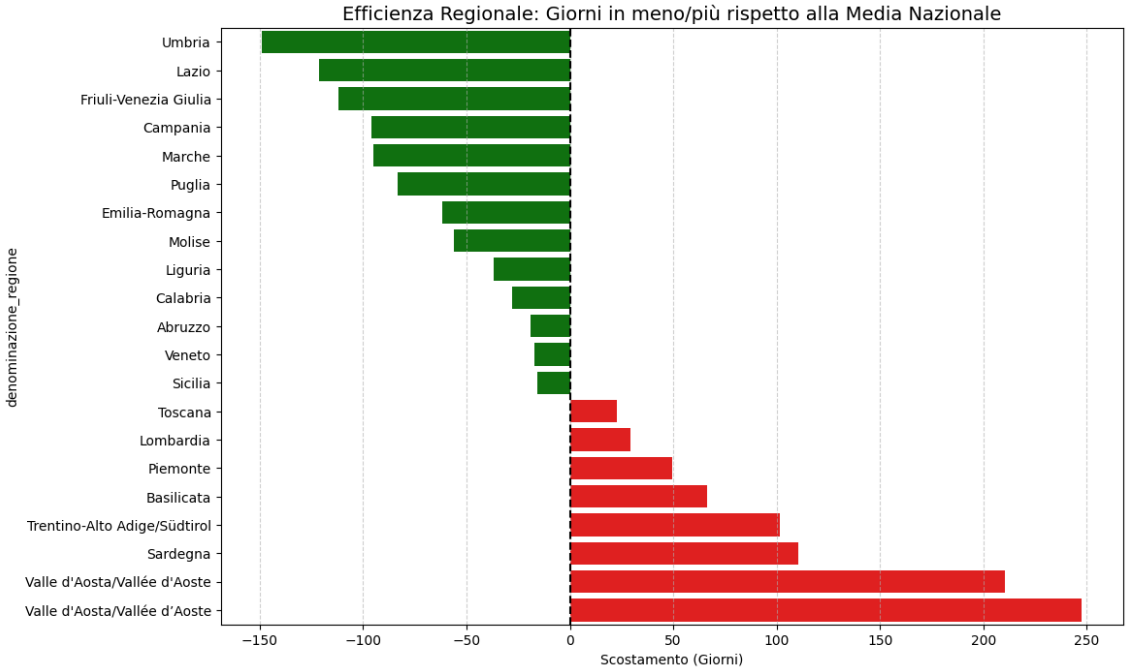


Figura 5 Efficienza regioni: giorni in meno/più rispetto alla media nazionale

3.3. I fattori condizionanti l'adozione del *cloud*.

L'analisi dei progetti di adozione del *cloud* restituisce un punto di osservazione empirico, a partire anche dai dati, dei diversi fattori che determinano questa transizione tecnologica della pubblica amministrazione. Adottando, quindi, quale chiave di lettura, il *TOE framework*, è possibile classificare nelle tre dimensioni i fattori determinati.

Per quanto attiene alla dimensione tecnologica emergono chiaramente due rilevanti fattori, ossia le soluzioni *cloud* disponibili (IaaS, PaaS e SaaS), nonché il vincolo di qualificazione dei fornitori di queste tecnologie, che devono essere certificati dall'ACN. Un primo risultato ricavabile dall'analisi è dunque il perimetro entro il quale può

avvenire l'implementazione tecnologica, ovvero la scelta del *cloud* è circoscritta alle tecnologie messe a disposizione unicamente da soggetti qualificati.

Tuttavia, sono specialmente i fattori ambientali ad influenzare maggiormente il piano di adozione di queste tecnologie. E questi sono identificabili nei finanziamenti sia negli atti programmatici, nonché nella legislazione, ma anche nelle linee guida e negli atti programmatici. Difatti la spinta all'innovazione data dai fondi PNRR, nonché le finestre temporali per poter avviare i progetti, hanno senza dubbio contribuito all'implementazione di questa tecnologia, unitamente agli indirizzi stabiliti dal legislatore.

Più complesso appare, invece, lo studio dei fattori rientranti nella dimensione organizzativa. L'analisi fa emergere come questi non siano univoci, intanto in quanto i tempi di completamento dei progetti molto elevati per i piccoli comuni sono uguali a quelli dei grandi centri, con la differenza che quest'ultimi hanno una percentuale di completamento più bassa, in ragione della complessità dei progetti, superiore a quella di piccoli enti. La conclusione ricavabile è che vi sia una questione non solo di disponibilità di risorse umane, ma anche la capacità di gestione dei progetti, specialmente complessi, quali fattori incidenti[62] direttamente sull'adozione del *cloud*.

Certamente lo studio dei progetti attraverso il modello TOE, rivela come l'interazione di diversi fattori abbia accelerato la trasformazione digitale delle pubbliche amministrazioni.

4. *Cloud* e sovranità digitale.

L'implementazione tecnologica, specialmente nel settore descritto nei precedenti paragrafi, vede un ulteriore elemento che assume rilevanza nelle scelte del legislatore, e conseguentemente dalle amministrazioni pubbliche, ossia la sovranità digitale, tema già affrontato nel primo capitolo, che con riferimento al *cloud* si pone in termini di controllo delle infrastrutture da parte dello Stato, in cui si trovano i dati e i servizi e, in generale su cui si regge l'ecosistema digitale[63]. Il *cloud* rappresenta un potenziale

[62] Questi fattori vengono evidenziati in particolare nel contributo di V. E. Entsie, F. K. Frempong Aidoo, A. Vaz, *op. cit.*, p. 7.

[63] V. I. K. Kwentoa, *Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology*, in *Journal of Next-Generation Research 5.0*, 2025.

rischio in ragione della presenza dei dati delle pubbliche amministrazioni e dei cittadini detenuti dalle pubbliche amministrazioni[64], poiché il ricorso a questa tecnologia significa affidare a soggetti privati, spesso con sede al di fuori dei confini nazionali[65], il patrimonio informativo pubblico e soprattutto i dati personali delle persone, con conseguente perdita di controllo su dati e innovazione e dalla dipendenza da giganti tecnologici[66].

Tale questione è stata posta già nel Piano Triennale per l'Informatica 2019-2021, così come nella Strategia *Cloud* Italia e nelle Raccomandazioni e proposte sull'utilizzo del *cloud computing* nella Pubblica amministrazione[67]. Questi tre documenti evidenziano tutti l'esigenza di garantire il controllo delle infrastrutture da parte dello Stato o comunque di assicurare la sovranità digitale, intesa quale protezione di dati e servizi dalle possibili ingerenze di Paesi stranieri[68]. Viene per altro verso evidenziato il pericolo dell'impossibilità di gestire pienamente il processo di digitalizzazione, e per tali ragioni nel Piano Triennale 2019-2021 si menziona l'importanza della costituzione di poli strategici, localizzati nel territorio nazionale, per soddisfare l'esigenza di controllo da parte dello Stato sulle infrastrutture. Mentre nel documento relativo alle Raccomandazioni sul ricorso al *cloud computing*, si evidenzia anche la possibilità di utilizzare le soluzioni offerte dal privato purché siano rese nazionali al fine di rendere più semplice risolvere problemi di normativa, conformità e sovranità.

Queste due componenti sono inscindibilmente legate. L'aumento di soluzioni tecnologiche legate alla rete, comporta inevitabilmente la crescita della superficie d'attacco, ovvero il moltiplicarsi di obiettivi di attacchi informatici, tanto da rendere necessario un corposo susseguirsi di interventi normativi, per adeguare l'ordinamento al

---

[64] V. S. Leucci, S. Girella, J. L. a Beccara, *Pubblica amministrazione e protezione dei dati personali nelle "nuvole": criticità e soluzioni*, in *Inform. dir.*, 2, 2014, p. 32.

[65] Il tema della minima quota di mercato nel *cloud* detenuta dagli operatori con sede nell'Unione europea, con conseguente dipendenza da fornitori di Paesi extra-UE viene rilevato dalla Commissione europea con la comunicazione COM (2020) 66 *Una strategia europea per i dati* con cui viene annunciato il progetto di una infrastruttura europea per la condivisione dei dati basato sulla federazione europea di infrastrutture *cloud* accanto ad un sistema di *governance*.

[66] Tra i principali fornitori vi sono Amazon Web Service, Microsoft Azure, Google, IBM, aziende con sede negli Stati Uniti. V. sull'argomento T. Madiega, *Digital sovereignty for Europe*, European Parliamentary Research Service, 2020.

[67] Tre documenti programmatici redatti da AgID dedicati in generale alla digitalizzazione della PA, ma che dedicano ampio spazio alla questione della costruzione e gestione dei data center in cui i dati e i servizi pubblici dovranno essere destinati.

[68] I. Macrì, *Polo Strategico Nazionale*, cit., p. 462.

mutato contesto in cui la pubblica amministrazione si trova a dover operare[69]. E si rende necessario, inoltre, una funzione pubblica di *cybersecurity*, in cui gli Stati esercitano poteri di controllo e protezione delle reti e dei sistemi informatici per salvaguardare infrastrutture e dati sensibili[70].

Sovranità e sicurezza nel contesto europeo assumono inoltre una dimensione sovranazionale a carattere cooperativo. Difatti, l'Unione europea ha ravvisato la necessità di un rafforzamento da un lato della sovranità del *cloud*, attraverso una corposa legislazione volta a promuovere il mercato interno costituita dal *Digital Market Act*, *Digital Service Act*, *Data Act*, *Data Governance Act* [71], dall'altro della cybersicurezza, con la Direttiva UE 2016/1148, nota come Direttiva NIS (ossia *Network Information System*) volta a rafforzare la sicurezza delle reti e dei sistemi informativi dell'UE, recepita in Italia con d.lgs. 18 maggio 2018 n. 65. Successivamente è stato approvato il Regolamento Europeo del Parlamento e del Consiglio n. 2019/881 volto a definire gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA, (l'Agenzia dell'Unione europea per la cybersicurezza), oltre a stabilire un quadro comune per l'introduzione di sistemi europei di certificazione della cybersicurezza al fine di garantire un livello adeguato di sicurezza dei prodotti, servizi e processi TIC[72] nell'Unione.

Il fine di assicurare un servizio *cloud* sicuro per gli enti pubblici costituisce certamente un obiettivo ineludibile nel momento in cui si decide di trasferire tutto il patrimonio conoscitivo e di informazione della PA verso soluzioni offerte dal mercato oppure da soggetti (come nel caso del PSN) a partecipazione societaria mista pubblico-privato. Tuttavia, tale scopo pare cozzare con la pretesa di preservare la sovranità nazionale, nel momento in cui la gestione dei dati viene affidata a operatori economici soggetti alla

[69] Nella Relazione annuale al Parlamento 2023, pubblicata nel 2024 l'Agenzia per la Cybersicurezza Nazionale descrive la superficie d'attacco come l'insieme di dispositivi e servizi esposti su Internet (p. 28).

[70] S. Mangiameli, *La sovranità digitale*, in *dirittifondamentali.it*, 3, 2023, p. 292-293.

[71] Al fine di assicurare la sovranità dei dati. V. sul punto F. Gualtiero Blancato, *The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem*, in *Policy & internet*, 2023.

[72] Secondo la definizione fornita dal Regolamento UE 2019/881 e ripresa dal d.lgs. n. 138/2024 con «prodotto TIC» si definisce un elemento o un gruppo di elementi di una rete o di un sistema informativo; «servizio TIC» un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi; «processo TIC» un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC;

giurisdizione di uno Stato estero, anche extra UE. Come è stato osservato[73], la problematica si pone ad esempio con riferimento alla legislazione degli Stati Uniti dove nel 2018 è stato approvato il *Cloud Act* (*Clarifying Lawful Overseas Use of Data*), il cui scopo, chiarito nel documento stesso, «*The Purpose and Impact of the CLOUD Act*» è il seguente: «*U.S. law requires that CSPs subject to U.S. jurisdiction must disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data*». Le autorità statunitensi possono quindi richiedere ad un *provider* di fornire i dati anche se questi sono conservati in un *data center* collocato all'estero, qualora vi sia la necessità di svolgere indagini e perseguire reati, con conseguenze non solo sotto il profilo della *privacy*, ma anche della sovranità nazionale dello Stato in cui il *data center* è ubicato.

Proprio la predominanza sul mercato di grandi aziende americane mette in crisi la sovranità, siccome a questi attori gli enti pubblici sono costretti a rivolgersi. Gli investimenti nel *cloud* specialmente quelli finalizzati alla creazione del Polo strategico nazionale (i cui *data center* sono nel territorio nazionale), sono anche conseguenza della presa di consapevolezza di questo problema gestito. Tuttavia, l'assenza di aziende europee capaci di competere con le aziende americane in termini di investimenti in ricerca e sviluppo comporta una rivendicazione apparente di sovranità. Il PSN rappresenta un esempio in questo senso, come evidenziato nel report[74] del *Future of Technology Institute*. L'infrastruttura è localizzata in territorio italiano e controllata da soggetti pubblici e privati con sede in Italia, ma per operare si avvale di *Google Assured Workload* and *Oracle Alloy* ovvero tecnologie di proprietà di Alphabet e Oracle, due aziende americane.

La sovranità digitale ribadita nella Strategia *cloud* Italia e attuata con l'investimento per la realizzazione del PSN, rimane quindi molto labile.

[73] V. Pagnanelli, *op. cit.*, p. 19.

[74] Future of Technology Institute (2026) *Cloud Defence: An exposed European flank*, p. 10, https://futureinstitute.tech/assets/doc/FOTICloudDefenceReport26.pdf

5. L'architettura normativa in materia di cybersicurezza.

5.1. Le direttive europee e le leggi italiane per l'istituzione e il governo dello spazio cibernetico sicuro.

Il tema dello spazio digitale richiama necessariamente la sicurezza, intesa come sicurezza cibernetica o *cybersecurity*, quale condizione in cui lo spazio *cyber* (ossia l'insieme delle infrastrutture informatiche interconnesse[75]) risulti protetto rispetto ad eventi «consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittime ovvero nel blocco dei sistemi informativi, grazie ad idonee misure di sicurezza fisica, logica e procedurale»[76].

Negli ultimi anni lo sviluppo del digitale ha acceso l'attenzione sul problema della sicurezza, a cui ha risposto l'approvazione della Direttiva NIS sulla sicurezza delle reti e dei sistemi informativi dell'Unione, che ha perseguito l'obiettivo di raggiungere un livello comune elevato in materia di sicurezza delle reti e dei sistemi di informazione in tutta l'UE, per rendere affidabili e sicuri le reti, i sistemi e i servizi informativi in ragione del ruolo vitale svolto nella società, dalle attività economiche e sociali, e, in particolare, ai fini del funzionamento del mercato interno[77]. L'obiettivo perseguito attraverso la direttiva è stato creare una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi mediante un approccio globale a livello di Unione, che contemplasse la creazione di una capacità minima comune e disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali[78]. Veniva così per la prima volta affrontato il tema della sicurezza delle reti in termini generali, anziché per settori, come la finanza o il crimine informatico[79], demandando agli Stati membri[80] il compito di adottare una strategia nazionale in

[75] Voce *Cyberspace*, in Sistema di informazione per la sicurezza della Repubblica, *Glossario intelligence*, www.sicurezzanazionale.gov.it/comunicazione/glossario/101.

[76] Voce *Cybersecurity*, in Sistema di informazione per la sicurezza della Repubblica, *Glossario intelligence*, https://www.sicurezzanazionale.gov.it/comunicazione/glossario/100. Per una ricostruzione approfondita della nozione v. S. Rossa, *Cybersecurity e pubblica amministrazione*, Ed. scientifica, 2023, p. 10 e ss.

[77] Considerando 1 della Direttiva NIS.

[78] Considerando 6 della Direttiva NIS.

[79] S. Rossa, *op. cit.*, p. 77.

[80] Cfr. Direttiva 2016/1144, art. 1, co. 1. In Italia la direttiva è stata recepita con il d.lgs. 18 maggio 2018, n. 65, che inizialmente, con l'art. 7, designava quali autorità competenti il Ministero dello sviluppo economico per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture

materia mirata al raggiungimento di obiettivi di sicurezza comuni minimi consistenti nell'istituzione o designazione di autorità nazionali competenti, nonché di gruppi di intervento per la sicurezza informatica in caso di incidenti, ossia cyberattacchi o malfunzionamenti (CSIRT).

Parallelamente, l'Unione europea, con il Regolamento UE del Parlamento e del Consiglio n. 2019/881, ha definito gli obiettivi, i compiti e gli aspetti organizzativi dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA), oltre a stabilire un quadro comune per l'introduzione di sistemi europei di certificazione della cybersicurezza al fine di garantire un livello adeguato di sicurezza dei prodotti, servizi e processi TIC[81] all'interno del mercato unico.

L'ultimo tassello di questo processo normativo è stata l'approvazione della Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (cd. Direttiva NIS2) con cui si è deciso di superare la direttiva NIS in ragione della poca chiarezza circa l'ambito di applicazione per gli operatori economici e l'ampia discrezionalità concessa agli Stati membri nell'individuazione dei requisiti di sicurezza e di segnalazione di incidenti[82].

---

digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali, il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada, il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze, il Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza. Infine, era designato il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile. Di fatto il decreto frazionava per settori le autorità competenti in materia di sicurezza cibernetica.

[81] In base al Regolamento UE 2019/881 con «prodotto TIC» si definisce un elemento o un gruppo di elementi di una rete o di un sistema informativo; mentre con «servizio TIC» si identifica un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi. Infine, con «processo TIC» si indica un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC;

[82] Cfr. COM (2020) 823 della Commissione europea, avente ad oggetto la Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, nonché il considerando 2, ultimo cpv. della direttiva 2022/2555, laddove viene riportato che «la revisione della direttiva (UE) 2016/1148 ha rivelato carenze intrinseche che le impediscono di affrontare efficacemente le sfide attuali ed emergenti in materia di cibersicurezza» e il successivo considerando 5.

Tale direttiva, che doveva essere recepita negli ordinamenti nazionali entro il mese di ottobre 2024, amplia l'ambito applicativo del precedente NIS, estendendolo anche ai servizi e alle infrastrutture digitali[83], rafforzando altresì la cooperazione transfrontaliera tra autorità competenti.

Per quanto riguarda la normativa nazionale italiana, al d.lgs. n. 65/2018 di recepimento della Direttiva NIS, ha fatto seguito il d.l. 21 settembre 2019 n. 105, convertito con l. 18 novembre 2019 n. 133 con il quale è stato istituito e definito il perimetro di sicurezza nazionale cibernetica[84], inteso quale limite oggettivo e soggettivo, costituito dalle funzioni essenziali dello Stato, svolte da soggetti, pubblici e privati, per i quali operano le misure di sicurezza cibernetica[85]. Da un lato, vi sono i soggetti pubblici titolari di poteri di controllo e individuazione dei soggetti che svolgono un servizio essenziale, dall'altro i soggetti (pubblici e privati) inclusi nel perimetro, e quindi obbligati ad approntare le misure per minimizzare il rischio di attacchi informatici e notificare alle autorità competenti eventuali incidenti.

I due richiamati decreti hanno istituito il sistema di *governance* e di difesa unitaria[86], da applicare a tutti i soggetti pubblici (incluso lo Stato) e privati, esercenti una funzione o un servizio considerato essenziale. Se il decreto legislativo recependo la Direttiva NIS ha definito il sistema di competenze e responsabilità in materia, di fatto attribuendo il compito della sicurezza delle reti e dei sistemi informatici agli stessi organi già deputati alla sicurezza nazionale (quali Presidente del Consiglio dei Ministri, Ministero della Difesa, AISI, AISE, DIS, Ministero degli Esteri, Ministero della Giustizia, oltre ad aver istituito il Nucleo per la difesa cibernetica)[87], il decreto legge n. 105/2019 ha definito l'ambito soggettivo dei destinatari degli obblighi in materia di sicurezza cibernetica.

La definizione di un perimetro di sicurezza cibernetica dimostra quindi un'evoluzione del concetto tradizionale di sicurezza nazionale, legato alla dimensione territoriale

[83] Cfr. *Shaping Europe's digital future, NIS2 Directive: securing network and information systems*, Commissione europea, digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[84] Art. 1 « Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica».

[85] B. Carotti, *Sicurezza cibernetica e Stato-nazione*, in *Giorn. dir. amm.*, 5, 2020, p. 629.

[86] A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. dir. amm.*, 4, 2021, p. 543.

[87] Cfr. art. 7 Art. 7 rubricato Autorità nazionali competenti e punto di contatto unico d.lgs. n. 65/2018, vigente al 1° novembre 2020.

statuale, spostandosi verso uno spazio indefinito geograficamente, individuato attraverso una precisa scelta del legislatore. Da un lato, vi sono i soggetti pubblici titolari di poteri di controllo e individuazione dei soggetti che svolgono un servizio essenziale, dall'altro i soggetti (pubblici e privati) inclusi nel perimetro, e quindi obbligati ad approntare le misure per minimizzare il rischio di attacchi informatici e notificare alle autorità competenti eventuali incidenti.

Ai menzionati interventi normativi si sono succeduti, in ordine di tempo, il d.l. 14 giugno 2021 n. 82, convertito dalla l. 4 agosto 2021 n. 109, con cui è stata istituita l'Agenzia per la Cybersicurezza Nazionale[88] e contestualmente si è proceduto ad un riordino delle disposizioni in materia, a cui ha fatto seguito la l. 28 giugno 2024 n. 90 e il d.lgs. 4 settembre 2024 n. 138, di recepimento della Direttiva NIS 2, che ha abrogato il d.lgs. n. 65/2018, per effetto dell'abrogazione della Direttiva NIS 1 da parte della nuova Direttiva in materia di cybersicurezza (NIS 2).

Si affacciano quindi nell'ordinamento concetti giuridici nuovi come "cybersicurezza" e "resilienza nazionale nello spazio cibernetico". Il primo trova la sua definizione normativa nell'art. 1, comma 1, lett. a) del d.l. 82/2021 secondo cui con questo termine si intende «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», mentre con la seconda espressione (art. 1, comma 1, lett. b) viene inteso l'insieme delle attività volte a prevenire «un danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale»[89]. Si tratta di concetti ampi, di difficile inquadramento giuridico; il richiamo alla "sicurezza nazionale" risulta essere un concetto politico piuttosto che giuridico, laddove il termine "resilienza" indica la prevenzione dalle minacce e la minimizzazione

[88] E conseguentemente è stato modificato il d.lgs. 65/2018.

[89] La definizione è data mediante rinvio all' art. 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131.

degli effetti dannosi causati da una minaccia, per preservare il continuo funzionamento dello Stato[90].

Unitariamente considerati, queste disposizioni rappresentano l'architrave normativo in materia di sicurezza cibernetica, creando un ente preposto alla sicurezza della dimensione cibernetica, e al contempo istituendo un sistema di obblighi e adempimenti cui sono tenuti tutti i soggetti più o meno interessati dai rischi di attacchi informatici, tracciando un modello di *governance* non limitato alla cybersicurezza, secondo un approccio multilivello in cui sono coinvolti sia attori pubblici sia operatori privati, e nel quale il Presidente del Consiglio dei ministri riveste un ruolo centrale, di vertice, che va oltre la semplice responsabilità politica[91].

5.2. La *governance* della cybersicurezza: il ruolo del Presidente del Consiglio dei ministri.

Con l'obiettivo di costituire un sistema comune di difesa dello spazio digitale, il legislatore europeo ha imposto agli Stati membri di costituire anche un sistema di *governance* designando autorità competenti ed individuando azioni e comportamenti che i soggetti interessati devono osservare.

Nel recepire la normativa europea, il legislatore italiano ha quindi optato per un modello verticistico in cui il Governo assume un ruolo centrale nella tutela dello spazio *cyber*.

Il punto di partenza di questa analisi può essere individuato nell'art. 14 del CAD, a mente del quale «In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime». In base alla Costituzione è dunque attribuita allo Stato la competenza in materia di digitalizzazione, in particolare relativamente alla sicurezza informatica. Tale compito vede il Presidente del Consiglio

[90] M. A. Rizzi, F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Riv. it. infor. dir.*, 2, 2024.
[91] T. F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quad. cost.*, 2, 2024.

dei ministri[92] rivestire un ruolo centrale nelle politiche di trasformazione e innovazione digitale, come si evince dalla lettura dell'art. 16 CAD (modificato dal d.lgs. 13 dicembre 2017, n. 217), il quale attribuisce a quest'ultimo il compito di garantire un coordinamento nel processo di digitalizzazione e nello sviluppo di sistemi informativi da parte delle amministrazioni centrali, nonché un ruolo di promozione e sostegno di progetti aventi grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale. Dalla lettura combinata degli artt. 14 e 16 può allora rilevarsi come anche il settore della cybersicurezza risulti inquadrabile tra le funzioni assegnate alla Presidenza del Consiglio, atteso lo specifico ambito della materia, ossia quello della tutela dei sistemi informatici. Infatti, con DPCM del 17 aprile 2017 veniva emanata la Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, con cui veniva regolata l'architettura istituzionale deputata alla sicurezza e protezione cibernetica ed informatica, nella quale, ai sensi dell'art.3, il Presidente del Consiglio rivestiva un ruolo centrale «quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica».

Seguendo questa impostazione, appare coerente la scelta operata dal legislatore quando, istituendo il perimetro di sicurezza nazionale cibernetica con d.l. 21 settembre 2019 n. 105[93], ha previsto poteri significativi in capo al Presidente del Consiglio, il quale con proprio decreto definisce «modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati»[94] da includersi nel perimetro di sicurezza nazionale cibernetica; un atto amministrativo segretato con il quale vengono individuati i soggetti inclusi nel perimetro.

---

[92] Per una ricostruzione delle norme riguardanti le funzioni e i poteri del Presidente del Consiglio nello sviluppo e gestione del digitale si veda L. Golisano, *Il governo del digitale: strutture di governo e innovazione digitale*, in *Gior. dir. amm.*, 6, 2022.

[93] Art. 1, co. 1: «Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica».

[94] Art.1, co. 2 lett. a), che specifica altresì i criteri in base ai quali si deve procedere all'individuazione, ossia: «1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; 2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici; 2-bis) l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti».

Il potere più incisivo viene invece attribuito dall'art. 5, comma 1[95] del menzionato d.l., in base al quale, in presenza di un rischio grave e imminente per la sicurezza nazionale legato alla vulnerabilità di reti, sistemi informatici o servizi digitali, il Presidente del Consiglio può ordinare, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, se indispensabile e per il tempo strettamente necessario a eliminare o ridurre il rischio, la disattivazione totale o parziale di apparati o prodotti usati nelle reti, nei sistemi o nei servizi coinvolti. Questo provvedimento può avvenire in deroga alle norme vigenti, ma nel rispetto dei principi generali dell'ordinamento, purché sia proporzionato.

Al Presidente del Consiglio quale autorità preposta alla sicurezza nazionale (come già stabilito dalla l. 3 agosto 2007 n. 124)[96] viene di fatto attribuito un potere rilevante, pur con la previsione del coinvolgimento del Comitato interministeriale, esercitabile in presenza di un rischio grave e imminente per la sicurezza nazionale. Stante la natura di questo atto, ci si può domandare se sia possibile ascriverlo alla categoria delle ordinanze *extra ordinem*. Le caratteristiche di questo provvedimento emanabile dal Presidente del Consiglio ricordano infatti quelle delle ordinanze contingibili e urgenti[97], i cui presupposti sono la contingibilità, intesa quale imprevedibilità che richiede il ricorso a mezzi straordinari stante l'insussistenza di rimedi tipici, oppure l'inadeguatezza di quelli esistenti, e l'urgenza, consistente nella materiale impossibilità di differire l'intervento. Questa tipologia di ordinanze implica la «sussistenza di un pericolo irreparabile ed imminente per la pubblica incolumità, non altrimenti fronteggiabile con i mezzi ordinari apprestati dall'ordinamento», indipendentemente dal fatto che il pericolo sia nuovo o imprevedibile, purché rivesta il carattere dell'urgenza[98], al quale è necessario far fronte con provvedimento connotato dalla provvisorietà, temporaneità e

[95] Comma modificato dalla legge di conversione 18 novembre 2019, n. 133 e, successivamente, dall'art. 29, comma 5 del d.l 21 marzo 2022, n. 21, convertito, con modificazioni, dalla l. 20 maggio 2022, n. 51.

[96] Il cui art. 1 prevede «Al Presidente del Consiglio dei ministri sono attribuiti, in via esclusiva:
a) l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento;». Già il DPCM 24 gennaio 2013 recante indirizzi per la sicurezza nazionale, anche nello spazio cibernetico, indicava nel Presidente del Consiglio dei ministri il vertice dell'architettura istituzionale di sicurezza informatica.

[97] Sui presupposti e caratteristiche delle ordinanze *extra ordinem* si è in più occasione pronunciato il giudice amministrativo; cfr. e*x multis*, Cons. St., sez. V, 3 gennaio 2024, n. 105, Cons. St., sez. IV, 25 marzo 2022, n. 2193, Cons. St., sez. II, 11 luglio 2020, n. 4474, Cons. St., sez. IV, 23 giugno 2021, n. 4802.

[98] Nota a Cons. St., sez. V, 8 maggio 2007, n. 2109, in *Giur. it.*, 1, 2008, p. 227.

proporzionalità. La peculiarità delle ordinanze *extra ordinem* è l'atipicità, in quanto la legge nulla dispone circa il contenuto, l'oggetto e gli effetti delle stesse[99].

Se è vero che l'art. 5 definisce quale sia il contenuto del potere, ossia la disattivazione, e quindi, sotto questo profilo, si esulerebbe dalla nozione di ordinanza atipica, appare generica l'indicazione delle circostanze in cui esso è esercitabile. Inoltre, il carattere di temporaneità, la possibilità di derogare alla norme dell'ordinamento, pur nel rispetto dei principi generali, nonché il requisito della proporzionalità, renderebbero ascrivibile a questa categoria l'ordinanza di disattivazione, la quale per altro verso si connota per una caratteristica non contemplata negli altri casi di ordinanze contingibili e urgenti, ovvero il rischio di sottrazione ad un controllo giurisdizionale, ad esempio nel caso di responsabilità per danni cagionati ad un operatore economico, attesa la natura segreta dell'atto amministrativo che identifica i soggetti ricompresi nel perimetro della sicurezza cibernetica[100].

Nel quadro delineato si colloca l'approvazione del d.l. 14 giugno 2021 n. 82, con cui il legislatore ha voluto sistemare la disciplina e riorganizzare le competenze nel settore della *cybersecurity*[101] definendo una *governance* unitaria attraverso l'istituzione dell'Agenzia per la Cybersicurezza nazionale[102] avente personalità giuridica di diritto pubblico, con autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. L'organo di vertice dell'Agenzia è il Direttore generale, il quale, unitamente al vicedirettore, viene nominato dal Presidente del Consiglio, previa deliberazione del Consiglio dei ministri. Entrambi sono scelti tra i soggetti di cui all'art. 18, comma 2 della l. 23 agosto 1988 n. 400, ossia tra i magistrati delle giurisdizioni superiori ordinaria ed amministrativa, gli avvocati dello Stato, i dirigenti generali dello Stato ed equiparati, i professori universitari di ruolo, ovvero tra estranei alla pubblica amministrazione.

Al Presidente del Consiglio viene attribuita in via esclusiva, oltre al potere di nominare il vertice dell'Agenzia, «a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza; b) l'adozione della strategia nazionale di cybersicurezza, sentito il

[99] S. Maglia, M.V. Balossi, *Le ordinanze contingibili e urgenti dopo le modifiche operate dal d.l. n. 90/2008*, in *Ambiente & sviluppo*, 8, 2008, p. 705.
[100] B. Carotti, *op. cit.*, p. 639.
[101] Distribuite tra diversi enti, già menzionati, a cui si aggiungevano il Dipartimento delle Informazioni per la Sicurezza e l'Agenzia per l'Italia Digitale.
[102] M. Ridolfi, *Servizi di informazione e cybersicurezza*, in *Giorn. dir. amm.*, 2, 2023, p. 176. Cfr. art. 86.

Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4» (art.1, comma 1). Quanto previsto dalla lettera a) viene esplicitato dal successivo comma 2, secondo cui il Presidente «impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale». Inoltre, allo stesso spetta il compito di determinare la dotazione finanziaria annuale dell'ACN (art.11, comma 1), oltre a adottare con proprio decreto il regolamento di contabilità.

Appare evidente il ruolo centrale svolto dal capo del Governo, il quale attraverso un controllo e un indirizzo incisivo, svolge un'attività di direzione sull'ente [103], che rispetto all'organo politico assume, quindi, una funzione strumentale[104].

Secondo l'art. 5, comma 4 l'attività dell'Agenzia è regolata dal decreto legge stesso e da appositi atti, mentre per quanto attiene all'organizzazione, il successivo art. 6 stabilisce che «L'organizzazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento» adottato con decreto del Presidente del Consiglio dei ministri, nello specifico emanato con DPCM 9 dicembre 2021 n. 223. Nel regolamento viene ribadito il ruolo strumentale dell'ACN, come si evince dall'art. 3, comma 1, per cui l'ente svolge le funzioni previste dal decreto-legge «e da altre disposizioni di legge, sulla base delle direttive emanate dal Presidente del Consiglio dei ministri o dall'Autorità delegata». Mentre il comma 2, nell'elencare i principi ispiratori dell'organizzazione e del funzionamento dell'agenzia, richiama in particolare l'autonomia e il miglior conseguimento dei risultati attesi, l'efficienza e il razionale impiego delle risorse disponibili, l'imparzialità e la trasparenza dell'azione amministrativa.

Quanto alla struttura organizzativa, la norma primaria che definisce l'articolazione interna è contenuta nel d.l. 82/2021, ossia l'art. 6, comma 1, secondo cui l'ACN si articola fino ad un «numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale». L'organizzazione viene dettagliata dall'art. 4 del DPCM, che richiama l'art. 6 del decreto-legge indicando quali organi dell'Agenzia il direttore generale, il vicedirettore e il collegio dei revisori dei conti. In quanto organi, questi sono gli unici

[103] S. Rossa, *op. cit.*, p. 95.

[104] I. Forgione, *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in *Dir. amm.*, 4, 2022, p. 1119.

soggetti titolari di poteri e capaci quindi di esprimere all'esterno la volontà dell'ente[105]. In particolare, l'art. 5 nell'indicare il direttore generale quale diretto referente del Presidente del Consiglio (o dell'autorità delegata se istituita), gli attribuisce la legale rappresentanza dell'ACN, la responsabilità di curare i rapporti esterni dell'Agenzia, adottare i provvedimenti necessari per il funzionamento dell'agenzia, definendone gli indirizzi e coordinandone l'attività, oltre a disporre delle nomine, delle promozioni, delle assegnazioni e dei trasferimenti del personale. L'art. 16 attribuisce poi al direttore il potere di adottare ogni provvedimento, anche regolamenti, necessario all'attuazione delle funzioni dell'Agenzia. A sua volta l'art. 12, comma 5 (che richiama il precedente art. 6 del decreto legge) dettaglia ulteriormente l'organizzazione interna dell'ACN elencando sette servizi[106], o uffici, ciascuno con specifici compiti. Infine, al collegio dei revisori dei conti spettano, ai sensi dell'art. 7 del DPCM 223/2021, le funzioni di controllo e verifica della gestione finanziaria, esprimendo parere sul progetto di bilancio preventivo e sul rendiconto annuale.

Al Presidente del Consiglio dei ministri spetta, inoltre, il potere di adottare il regolamento di contabilità in base all'art. 11, comma 3 del D.L. 82/2021, anche in deroga all'art. 17 della l. 23 agosto 1988 n. 400, in base al quale, invece, si prevede in questi casi l'adozione di regolamenti con Decreto del Presidente della Repubblica.

Ulteriore carattere distintivo è il controllo democratico sull'operato dell'ACN, assicurato in ragione del sistema costituzionale per cui il Governo deve ricevere la fiducia del Parlamento eletto dai cittadini, unitamente[107] a quanto stabilito dal d.l. n. 82/2021, che attribuisce al Comitato parlamentare per la sicurezza della Repubblica (COPASIR) il potere di audire il direttore generale, esprimere pareri sui regolamenti, oltre a ricevere una relazione annuale sull'operato dell'Agenzia.

---

[105] Sulla teoria dell'organo, S. Romano, *Organi*, in *Frammenti di un dizionario giuridico*, M. Croce, M. Goldoni (a cura di), Quodlibet, 2019, p. 147; F. G. Scoca, *La pubblica amministrazione come organizzazione*, in L. Mazzarolli, G. Pericu, A. Romano, F.A. Roversi Monaco, F.G. Scoca (a cura di), *Diritto amministrativo*, Bologna, 1998. M.S. Giannini, *Diritto amministrativo*, Giuffré, Milano, 1993.

[106] Ossia: a) Gabinetto; b) Autorità e sanzioni; c) Certificazione e vigilanza; d) Operazioni; e) Programmi industriali, tecnologici, di ricerca e formazione; f) Risorse umane e strumentali; g) Strategie e cooperazione.

[107] L. Moroni, *La governance della Cyber sicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, p. 191.

5.3. Similitudini e differenze dell'ACN con le altre agenzie presenti nell'ordinamento italiano.

Da quanto descritto emerge un modello organizzativo apparentemente simile a quello delle Agenzie istituito con il d.lgs. 30 luglio 1999 n. 300, in ragione delle specifiche attività tecniche che l'ACN è chiamata a svolgere, salvo discostarsene proprio per il decisivo potere esercitato da parte dell'autorità politica[108]. Difatti, a differenza del modello previsto dal decreto legislativo n. 300/1999, l'organo politico ha il potere di emanare un regolamento relativo all'organizzazione, manca un comitato di gestione (presente nelle agenzie amministrative) e il Presidente del Consiglio ha potere di direzione, in luogo dei poteri di vigilanza e controllo ministeriali previsti per le agenzie[109]. L'ACN presenta quindi caratteristiche peculiari rispetto al modello tradizionale di agenzia[110].

Ci si può altresì domandare se il modello organizzativo dell'ACN costituisca una novità nel panorama dell'ordinamento italiano. Secondo la dottrina[111] in materia di organizzazione della pubblica amministrazione a livello costituzionale i principi di imparzialità e buon andamento fondano una distinzione tra l'agire amministrativo e l'agire politico, offrendo all'amministrazione una legittimazione autonoma rispetto a quella di cui gode il potere esecutivo. Tali principi hanno trovato significativa attuazione con una serie di decreti legislativi, 3 febbraio 1993 n. 29, 31 marzo 1998 n. 80, 30 luglio 1999 n. 286[112], con cui è stata sancita la distinzione tra indirizzo politico spettante agli organi di governo e gestione attribuita ai dirigenti, intesa quale esistenza di sfere di autonomia d'azione. Ebbene, il modello organizzativo dell'ACN si allontana da questa distinzione poiché l'indirizzo politico e la gestione sono concentrati nell'autorità politica, pur con il riconoscimento in capo al direttore di poteri gestionali.

---

[108] T. F. Giupponi, *op. cit.*, p. 289.
[109] I. Forgione, *op. cit.*, p. 1120.
[110] Dossier 22 giugno 2021 del Servizio Studi di Camera e Senato, Disposizioni urgenti in materia di Cyber sicurezza, definizione dell'architettura nazionale di Cyber sicurezza e istituzione dell'agenzia per la Cyber sicurezza nazionale. Dl 80/2021-A.C. 3161, https://documenti.camera.it/leg18/dossier/pdf/D21082.pdf.
[111] M. S. Giannini, *Parlamento e amministrazione*, in *Amm. civ.*, 1961. M. Nigro, *La pubblica amministrazione fra costituzione formale e costituzione materiale*, in *Riv. trim. dir. proc. civ.*, 1985, ora in Scritti giuridici, III, Milano, Giuffrè, 1996.
[112] M. D'Orsogna, *Programmazione strategica e attività decisionale della Pubblica amministrazione*, Torino, 2001, p. 85 e p. 114.

Il modello di riferimento è in qualche modo quello previsto dalla legge 3 agosto 2007 n. 124, relativi ai Servizi di informazione per la sicurezza della Repubblica, in base al quale il Presidente del Consiglio svolge un ruolo centrale, quale organo a cui è attribuita l'alta direzione e responsabilità generale della politica di informazione e sicurezza. Tuttavia, il d.l. n. 82/2021 crea una struttura separata[113] da quelle tradizionalmente dedicate alla sicurezza dello Stato, in cui l'organo politico riveste un ruolo centrale, dotato di incisivi poteri, pur nella garanzia di un'autonomia operativa dell'ente.

5.4. Le funzioni dell'Agenzia per la Cybersicurezza Nazionale e i riflessi sulla gestione del *cloud*.

A fronte dell'obbligo per le pubbliche amministrazioni di adottare soluzioni *cloud*, si rende necessario assicurare la sicurezza dei dati, scopo della l. n. 90/2024 sulla cybersicurezza e dei regolamenti di AgID[114] e ACN[115], attraverso un meccanismo di classificazione degli stessi in ordinari, critici e strategici[116] e un sistema di qualificazione delle infrastrutture ospitanti o fornitori di servizi, in un'era in cui si moltiplicano gli attacchi informatici.

Il d.lgs. n. 138/2024 va a completare il quadro normativo, recependo la Direttiva (UE) 2022/2555 in materia cybersicurezza e prevedendo ulteriori obblighi, oltre a quelli già previsti dalla l. n. 90/2024, sia per le Pubbliche amministrazioni sia per i soggetti privati, individuati nel dettaglio dall'art. 3 (rubricato "Ambito di applicazione") e dagli

[113] Costituita appunto dall'ACN e dal Comitato Interministeriale per la Cybersicurezza.

[114] Regolamento «recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione», adottato da AGID con Determinazione 628 del 15 dicembre 2021, in conformità alle previsioni di cui all'articolo 33*septies*, comma 4, del D.L. 179/2012 e all'articolo 17, comma 6, del D.L. 82/2021.

[115] Regolamento che sostituisce quello precedente di AgID, adottato con Decreto Direttoriale n. 21007/24 del Diretto dell'ACN ed emanato in data 28 giugno 2024, entrato in vigore il 1° agosto 2024. Tale atto è l'ultimo, in ordine di tempo, dedicato alla regolazione delle infrastrutture *cloud*, e segue il menzionato Regolamento Cloud per la PA n. 628/2021 dell'AgID, successivamente modificato con Decreti del Direttore dell'ACN n. 20610 del 28 luglio 2023 e n. 2927 del 30 gennaio 2024, quando a questa agenzia sono stati affidati i compiti prima attribuiti all'AgID, in forza dell'art. 7 del d.l. 14 giugno 2021 n. 82, convertito dalla l. 4 agosto 2021 n. 109.

[116] In particolare, come accennato più sopra, sono considerati «strategici» i dati la cui compromissione può determinare un pregiudizio alla sicurezza nazionale; sono «critici» quelli la cui compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese; mentre sono «ordinari» i dati che sono compromessi non determinano i pregiudizi contemplati per quelli strategici e critici.

allegati al decreto medesimo. Da un lato vengono previste ulteriori competenze e funzioni in capo all'Agenzia per la Cybersicurezza Nazionale, dall'altro si assiste ad una diffusione delle responsabilità in questa materia a tutta una serie di soggetti pubblici e privati.

Si nota che nel contesto della *cybersecurity* l'Agenzia è, ai sensi dell'art. 7 del d.l. n. 82/2021, autorità nazionale per la cybersicurezza competente NIS, ossia autorità competente in materia di sicurezza delle reti e dei sistemi informativi, ed è punto di contatto unico NIS a livello nazionale, svolgendo la funzione di collegamento per garantire la cooperazione transfrontaliera con altre autorità nazionali preposte al medesimo compito e con l'*European Union Agency for Cybersecurity* (ENISA) già prevista con la Direttiva (UE) 2016/1148 (Direttiva NIS 1) poi recepita con d.lgs. n. 65/2018, quindi sostituita dalla Direttiva (UE) 2022/2555 ora recepita con il d.lgs. n. 138/2024, che ha abrogato il d.lgs. n. 65/2018. L'ACN è altresì, ai sensi dell'art. 7, comma 1 d *ter*), CSIRT nazionale, ossia *Computer Security Incident Response Team*. Si tratta di una struttura inquadrata all'interno dell'Agenzia preposta alle funzioni di gestione degli incidenti di sicurezza informatica, i cui compiti, inizialmente previsti dal d.lgs. n. 65/2018, sono ora definiti dal d.lgs. n. 138/2024 all' art. 15[117]. In particolare, il CSIRT monitora le minacce, analizza le vulnerabilità e gli incidenti a livello nazionale, fornisce assistenza ai soggetti cui si applica il decreto legislativo sia per quanto riguarda il monitoraggio sia in caso di incidenti, effettua scansioni dei sistemi informativi e di rete per verificare l'esistenza di vulnerabilità.

L'ACN è anche autorità di certificazione della cybersicurezza (art. 4, comma 1 d.lgs. 3 agosto 2022, n. 123), competente a rilasciare certificati a coloro che ne facciano richiesta (art. 6), conformemente al Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 (cd. *Cybersecurity Act*).

L'Agenzia è altresì ente di controllo della sicurezza delle infrastrutture informatiche e del rispetto degli obblighi previsti in particolare dalla l. n. 90/2024 e dal d.lgs. n. 138/2024, con il potere di disporre ispezioni e comminare sanzioni in caso di violazioni.

[117] In particolare, ai sensi dell'art. 15, il CSIRT monitora le minacce, analizza le vulnerabilità e gli incidenti a livello nazionale, fornisce assistenza ai soggetti cui si applica il decreto legislativo sia per quanto riguarda il monitoraggio sia in caso di incidenti, effettua scansioni dei sistemi informativi e di rete per verificare l'esistenza di vulnerabilità.

È titolare delle funzioni previste dall'art. 51 CAD, prima attribuite all'AgID[118], oltre a svolgere i compiti previsti dall'art. 33 *septies*, comma 4 del d.l. 179/2012, ovvero stabilire livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, tra cui i CED.

L'altro aspetto emergente è la centralità dell'Agenzia per la Cybersicurezza Nazionale, la quale assume le funzioni di ente regolatore e certificatore, di coordinamento e supervisione, nonché sanzionatore, rendendola un'agenzia amministrativa unica nel panorama dell'ordinamento italiano[119]. Da un lato essa è infatti responsabile della gestione e del monitoraggio degli incidenti di cybersicurezza rilevanti per le infrastrutture pubbliche e private strategiche, assicurato dall'obbligo di notifica degli incidenti previsto dall'art. 1 della l. 90/2024. Dall'altro è dotata del potere di irrogare sanzioni per violazioni degli obblighi ivi previsti. Ma svolge, anche, funzione di coordinamento e consulenza, indicando alle PA i casi di vulnerabilità rilevati, con la possibilità di comminare sanzioni in caso di mancato adeguamento.

A queste funzioni si affiancano quelle di autorità di certificazione cybersicurezza (designata con d.lgs. 3 agosto 2022 n. 123, in forza dell'art. 58 del Regolamento (UE) 2019/881 del 17 aprile 2019), attraverso l'Organismo di Certificazione della Sicurezza Informatica, per quanto riguarda la concessione di certificazione con elevato livello di affidabilità. E, come visto, l'Agenzia qualifica i servizi *cloud*, oltre a definire standard di sicurezza[120] e linee guida, supervisionando la sicurezza dei sistemi crittografici e promuovendo l'adozione di algoritmi sicuri, con un'attenzione alla tutela delle informazioni sensibili e all'autonomia tecnologica italiana.

Proprio in assolvimento della funzione regolatoria assegnatale, l'Agenzia il 27 giugno 2024 ha emanato il Regolamento per le infrastrutture digitali e per i servizi *cloud* per la pubblica amministrazione, ai sensi dell'articolo 33 *septies*, comma 4, del d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, al fine di stabilire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e

[118] L'AgID prima e ora l'ACN predispongono linee guida per l'individuazione delle soluzioni tecniche volte a garantire protezione, disponibilità, accessibilità, integrità e riservatezza dei dati, oltre ad attuare il Quadro strategico nazionale per la sicurezza dello spazio cibernetico. Cfr. art. 17, comma 6 d.l. 82/2021.

[119] S. Rossa, *Cybersicurezza e pubblica amministrazione,* cit., p. 94.

[120] Infatti, ai sensi dell'art 14 l. 90/2024 l'Agenzia ha il compito di assicurare che beni e servizi IT acquistati dal settore pubblico rispettino determinati criteri di cybersicurezza. Questo include il controllo sulle forniture per garantire l'uso di tecnologie conformi a standard di sicurezza definiti, specie in settori critici per la sicurezza nazionale, e prevede incentivi per l'adozione di tecnologie sviluppate in ambito europeo e NATO.

affidabilità delle infrastrutture digitali per la pubblica amministrazione. Questo regolamento è stato adottato alla luce della Strategia *Cloud* Italia e del Piano di implementazione 2022-2026 pubblicato il 1° giugno 2022. Riprendendo e aggiornando le linee guida e i regolamenti emanati da AgID in materia, il menzionato Regolamento definisce le caratteristiche di qualità, sicurezza, performance, scalabilità, interoperabilità e portabilità dei servizi *cloud* destinati alle amministrazioni pubbliche, fornendo altresì le linee guida per la migrazione verso infrastrutture e servizi *cloud* sicuri e certificati. Come accennato, i dati e i servizi digitali della pubblica amministrazione devono essere classificati (provvedendo all'aggiornamento con cadenza almeno biennale) in tre categorie, ordinari, critici e strategici, in base all'impatto potenziale che la loro compromissione potrebbe avere sulla sicurezza e sulle funzionalità pubbliche, determinando così i livelli di sicurezza richiesti. Conseguentemente, il regolamento prescrive quali requisiti di sicurezza le infrastrutture digitali e i servizi *cloud* devono rispettare a seconda della classificazione dei dati trattati. Ad esempio, le infrastrutture che gestiscono dati critici devono soddisfare criteri più stringenti rispetto a quelle che gestiscono dati ordinari. Una volta eseguita la classificazione, le PA devono procedere alla migrazione verso soluzioni *cloud* nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa. In particolare, in conformità alle previsioni dell'articolo 33 *septies*, commi 1 e 1 *bis*, del d.l. n. 179 del 2012, i dati e servizi digitali migrano verso le infrastrutture digitali (art. 9).

6. La riorganizzazione degli uffici pubblici per la sicurezza dell'ambiente digitale.

Come riportato nel Piano triennale per l'informatica 2024-2026 (aggiornato nel 2025) «La trasformazione digitale richiede un processo integrato, finalizzato alla costruzione di ecosistemi digitali strutturati sostenuti da organizzazioni pubbliche semplificate, trasparenti, aperte, digitalizzate e con servizi di qualità, erogati in maniera proattiva per anticipare le esigenze del cittadino»[121]. La diffusione di soluzioni come il *cloud computing* e i relativi adeguamenti normativi, dedicati soprattutto all'esigenza di garantire la sicurezza cibernetica, incide necessariamente anche sull'organizzazione amministrativa, interessata sia dalla creazione di nuove figure specializzate all'interno

[121] V. Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, p. 25.

delle pubbliche amministrazioni come il responsabile per la transizione digitale[122] e, nel 2024, il responsabile per la cybersicurezza (quest'ultimo obbligatorio per ogni soggetto destinatario degli obblighi previsti dalla l. 90/2024, individuato dall'art. 1 della stessa), sia dalla necessità di averne di nuove.

In particolare, tanto la l. n. 90/2024 quanto il d.lgs. n. 138/2024 stabiliscono una serie di obblighi per le amministrazioni[123], con correlate sanzioni in caso di inosservanza, nell'intento di rendere la difesa cibernetica una responsabilità diffusa, coinvolgente tutti i soggetti interessati, al fine di assicurare una maggiore resilienza[124].

L'art. 8 della l. 90/2024 impone, in particolare, alle amministrazioni di provvedere alla riorganizzazione interna, individuando una struttura, anche tra quelle esistenti[125], nell'ambito delle risorse disponibili, dedicata allo sviluppo delle politiche e procedure di sicurezza delle informazioni, implementazione di sistemi di analisi del rischio informatico, pianificazione e attuazione di interventi di potenziamento della capacità di gestione dei rischi informatici, adozione di misure previste dalle linee guida per la cybersicurezza emanate dall'ACN, produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema della cybersicurezza, nonché di un piano

[122] Figura prevista come obbligatoria per tutte le pubbliche amministrazioni ai sensi dell'art. 17 CAD, ai sensi del quale «Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le Linee guida. A tal fine, ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità». L. Torchia, *op. cit.*, p. 103.

[123] La l. n. 90/2024 impone alle pubbliche amministrazioni (inclusi i Comuni sopra i 100.000 abitanti) l'obbligo di segnalazione e notifica degli incidenti informatici, aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici, all'Agenzia per la Cybersicurezza Nazionale, entro termini molto brevi (dal momento in cui ne sono venute a conoscenza), ossia 24 ore per segnalare e 72 ore per notificare tutti gli elementi informativi disponibili. Il mancato rispetto di tali prescrizioni comporta l'invio di ispettori da parte dell'Agenzia e la possibilità di comminare sanzioni pecuniarie in caso di reiterazione dell'inosservanza di questi obblighi.

[124] Sul concetto di resilienza, in particolare nazionale, come notato più sopra l'art. 1, comma 1 lett. b) del d.l. 82/2021 la definisce come «le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131», il quale definisce un pregiudizio per la sicurezza nazionale qualsiasi «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale di cui all'articolo 2», ossia quell'insieme di compiti attribuiti ai soggetti il cui assolvimento è essenziale per assicurare la continuità operative degli organi costituzionali, la sicurezza interna ed esterna, e per il mantenimento delle attività civili, sociali ed economiche.

[125] Il comma 3 dell'art. 8 prevede a tal fine la possibilità di individuare il referente e la struttura deputati alla cybersicurezza, nell'ufficio e nel responsabile per la transizione digitale.

programmatico per la sicurezza di dati, sistemi e infrastrutture. Inoltre, alle amministrazioni è fatto obbligo di dotarsi di un referente per la cybersicurezza, dipendente dell'amministrazione stessa o di altra amministrazione (secondo la procedura prevista dall'art. 53 del d.lgs. 30 marzo 2001 n. 165, Testo Unico degli Enti Locali), il quale, ai sensi del comma 2, «svolge anche la funzione di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale». L'art. 8 della l. 90/2024 va letto unitamente all'art. 7 del d.lgs. 138/2024, il quale prescrive alle pubbliche amministrazioni (nonché ai privati) di registrarsi su un'apposita piattaforma dell'ACN, indicando, tra le varie informazioni richieste, anche il punto di contatto unico. Dal combinato di questi due articoli è possibile stabilire un duplice adempimento per le pubbliche amministrazioni, ossia la comunicazione del nominativo del soggetto referente per la *cybersecurity*, il quale deve essere indicato altresì come punto di contatto unico.

Alla figura del referente e punto di contatto unico, se ne è aggiunta un'ulteriore, quella di referente CSIRT, introdotta con la determina del Direttore generale dell'Agenzia per la cybersicurezza nazionale del settembre 2025[126]. Si tratta di un soggetto, persona fisica, designato dal punto di contatto, al quale vengono affidati il compito di interloquire con CSIRT Italia ed effettuare le notifiche di cui agli art. 25 e 26 d.lgs. 138/2024, relative agli incidenti informatici[127]. Tale figura si differenzia dal referente per la cybersicurezza, in quanto la determina prescrive che debba possedere «almeno competenze di base in materia di sicurezza informatica e di gestione di incidenti informatici, nonché una conoscenza approfondita dei sistemi informativi e di rete del soggetto per conto del quale operano», senza specificare se la persona designata debba essere obbligatoriamente un dipendente dell'amministrazione. Si tratta in ogni caso di figura dotata di competenze tecniche, che utilmente può essere individuato in un soggetto esterno all'amministrazione, similmente a quanto avviene in materia di

[126] Reperibile al seguente link www.acn.gov.it/portale/documents/d/guest/detacn_piattaformanis_250916-v5_signed.

[127] L'art. 7 della determina consente altresì la designazione di uno o più sostituti al fine di assicurare la prontezza e celerità delle comunicazioni. Tale figura si differenzia dal referente per la cybersicurezza per un duplice profilo, da un lato (in base alla determina) essa deve possedere «almeno competenze di base in materia di sicurezza informatica e di gestione di incidenti informatici, nonché una conoscenza approfondita dei sistemi informativi e di rete del soggetto per conto del quale operano», non facendo alcun riferimento al fatto se debba essere o meno l'incarico non sembra debba essere necessariamente un dipendente dell'amministrazione.

protezione dei dati personali, per cui, ai sensi dell'art. 37 del GDPR, il responsabile per la protezione dei dati può anche essere un professionista esterno all'organizzazione.

Ai soggetti cui si applica il decreto legislativo è fatto altresì obbligo, ai sensi dell'art. 24, di adottare misure tecniche, operative e organizzative per assicurare un livello adeguato di sicurezza dei sistemi informativi, proporzionato al grado di esposizione a rischi del soggetto stesso, ossia, detto altrimenti, di predisporre misure idonee rispetto al rischio e alla probabilità di un incidente informatico[128].In altre parole, le strutture delle amministrazioni pubbliche competenti in materia cybersicurezza devono realizzare misure idonee secondo un approccio multirischio, volto a proteggere da incidenti i sistemi informativi e di rete, nonché il loro ambiente fisico[129]. Alle amministrazioni viene infatti richiesto di elaborare processi di gestione dei rischi informatici, impiegando risorse anche per rafforzare le difese informatiche, *firewall* e strumenti di crittografia.

Dal dettato normativo si comprende la richiesta di uno sforzo riorganizzativo attraverso, in primo luogo, l'adozione di politiche di sicurezza relative all'ambiente fisico, cosa che comporta l'impiego di risorse per formare il personale dipendente sui rischi informatici e sulle procedure per mitigarli, iniziando dalla gestione corretta delle password di accesso al terminale e dalla condivisione di documenti e dati sensibili attraverso internet o la rete interna dell'ente. Questo, unitamente alla individuazione di una figura responsabile, appare necessario atteso che il fine della tutela dei diritti passa attraverso una riorganizzazione amministrativa[130].

---

[128] I. Macrì, *Cybersicurezza, le novità per il 2024*, in *Azienditalia*, 1, 2024, p. 23.

[129] In particolare, art. 24, comma 2 d.lgs. 138/2024: «a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete; b) gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26; c) continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi; d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità; f) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica; g) pratiche di igiene di base e di formazione in materia di sicurezza informatica; h) politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura; i) sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti; l) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno».

[130] S. Rossa, *Cyber attacchi e incidenti nella pubblica amministrazione, tra organizzazione amministrativa e condotta del funzionario*, in *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio III*, 17, 2023, p. 165.

Il complesso di prescrizioni ed obblighi connessi al processo di digitalizzazione vanno quindi a determinare una complessità organizzativa, sia attraverso l'istituzione di nuove figure sia con la ridefinizione dei ruoli in funzione dei processi digitali, procedendo all'individuazione di soluzioni tecnologiche idonee alle necessità, tenendo conto dell'utilizzo di esse nei processi interni, ma allo stesso tempo anche delle esigenze dei cittadini[131].

7. Il legame tra c*loud*, cybersicurezza e intelligenza artificiale.

L'analisi sulla diffusione del *cloud* attraverso l'indagine sugli investimenti, così come la ricostruzione dell'architettura di *governance* della sicurezza cibernetica rappresentano due ambiti importanti per comprendere quali siano le prospettive di diffusione dell'intelligenza artificiale. Questi tre settori tecnologici sono infatti strettamente intrecciati, poiché l'IA è in somma sintesi un sistema informatico, che opera su dispositivi fisici, ed è pertanto esposta ad attacchi informatici. A ciò si aggiunga che essa può costituire altresì uno strumento per incrementare le capacità delle infrastrutture digitali come il *cloud*, attraverso analisi automatica dei dati o interfacce utenti basate sul linguaggio naturale[132], ma parallelamente risulta essere uno strumento utile per implementare la sicurezza delle infrastrutture[133], attraverso l'analisi delle vulnerabilità dei sistemi informatici.

Questo stretto legame viene cristallizzato a livello normativo, all'art. 3, comma 6 della l. 23 settembre 2025 n. 132, in cui la cybersicurezza viene posta al centro di tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generale[134], mentre

[131] G. Carullo, *op. cit*, p. 47.

[132] Z. Engin, J. Crowcroft, et al., *The Algorithmic State Architecture (ASA): An Integrated Framework for AI-Enabled Government*, in *arXiv*, 2025, p. 5.

[133] Lo studio condotto per l'ENISA da S. Ntalampiras, G. Misuraca, P. Rossel, *Artificial Intelligence and Cybersecurity Research*, 2022, p. 20, rileva che gli strumenti e le metodologie basati sull'intelligenza artificiale possono essere impiegati per individuare e identificare gli attacchi informatici e attenuarne le conseguenze. Tali strumenti offrono prestazioni soddisfacenti a basso costo, in tempo reale, oltre a consentire l'adozione di numerose tecniche di protezione, come la sicurezza di rete e dei dati, la protezione dei terminali e la gestione degli accessi. Secondo uno studio condotto da Thales, società francese specializzata nei settori della sicurezza, aerospazio e difesa, la sicurezza del *cloud* e dell'intelligenza artificiale costituiscono due priorità per le organizzazioni, cfr. Thales, *Cloud Security Study*, 2025.

[134] Nello specifico la disposizione recita «Al fine di garantire il rispetto dei diritti e dei principi di cui al presente articolo deve essere assicurata, quale precondizione essenziale, la cybersicurezza lungo tutto il

all'art. 5 comma 1 lett. d), stabilisce che lo Stato e le autorità pubbliche devono indirizzare le piattaforme di *e-procurement* in modo che venga privilegiata la scelta di fornitori che garantiscono la localizzazione e l'elaborazione dei dati strategici «presso *data center* posti nel territorio nazionale, le cui procedure di *disaster recovery* e *business continuity* siano implementate in *data center* posti nel territorio nazionale, nonché modelli in grado di assicurare elevati standard in termini di sicurezza e trasparenza nelle modalità di addestramento e di sviluppo di applicazioni basate sull'intelligenza artificiale generativa, nel rispetto della normativa sulla concorrenza e dei principi di non discriminazione e proporzionalità». Con quest'ultima norma, in particolare, il legislatore ha inteso fornire le linee strategiche alle pubbliche amministrazioni[135], sulla consapevolezza dell'ambiente digitale, verso l'adozione di soluzioni di intelligenza artificiale in maniera responsabile.

Accanto al dato normativo, la connessione tra *cloud*, sicurezza e IA emerge anche dalle Linee guida per l'adozione dell'IA nella PA[136], volte a fornire un quadro di riferimento delle tecnologie digitali rilevanti e indicazioni, ma anche prescrizioni[137] alle pubbliche amministrazioni per l'adozione di sistemi di IA. Dalla lettura di esse risulta come il *cloud* venga identificato tra i fattori abilitanti per lo sviluppo di sistemi intelligenti. Infatti, l'adozione di infrastrutture sicure, qualificate in conformità al regolamento ACN, è una precondizione per sviluppare modelli di IA e per condividere risorse tra enti diversi, riducendo costi e tempi di implementazione.

Proprio in ragione dei potenziali rischi per la sicurezza, le linee guida, con riferimento ai sistemi di IA, individuano una catena del valore composta da quattro livelli[138]: fornitori

---

ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza».

[135] Cfr. Dossier 289/1 del Servizio studi del Senato al seguente link https://www.senato.it/service/PDF/PDFServer/BGT/1447651.pdf. Tuttavia, la collocazione dell'articolo nel Capo 1 dedicato ai principi, nonché la sua formulazione rendono questa norma debole sotto il profilo precettivo, oltre ad essere confinata ai soli dati strategici, non considerando le altre due categorie di dati, ossia quelli critici e ordinari.

[136] Approvate in sede di Conferenza Unificata il 10 settembre 2025.

[137] Significativamente nel documento, al paragrafo 2.1 si riportano le note di lettura del documento, con cui si chiarisce il carattere prescrittivo delle parti del documento ove si impiegano termini quali "DEVE", "DEVONO", o gli stessi preceduti dalla negazione.

[138] Fornitori di modelli sono i soggetti che sviluppano e/o forniscono modelli di IA e modelli di IA per finalità generali (GPAI); fornitori di infrastrutture sono i soggetti che sviluppano e/o forniscono componenti infrastrutturali per l'IA quali gestione dei dati, *networking*, *hardware*, servizi *cloud*, piattaforme MLOps. Questi soggetti rappresentano il cuore operativo che supporta l'intero ciclo di vita

di modelli, fornitori di infrastrutture, fornitori di applicazioni e, infine, utilizzatori[139]. Tutti questi soggetti sono chiamati sotto profili diversi a garantire e preservare la sicurezza dei sistemi; i fornitori a secondo dell'impiego della tecnologia (quindi sicurezza dei dati, dell'infrastruttura, del modello), gli utilizzatori adoperando con cautela questi strumenti a seconda del contesto in cui decidono di usarli[140].

Le linee guida richiedono quindi alle pubbliche amministrazioni di determinare e allocare risorse finanziarie, tecnologiche e umane per sviluppare, mantenere e migliorare i sistemi di IA, che devono comprendere non solo i dati e i modelli, ma anche le infrastrutture IT, come *cloud computing, edge computing* e risorse di elaborazione. Il *cloud* viene quindi identificato come una delle risorse indispensabili per l'IA[141], al pari dei dati e degli algoritmi, prospettando l'adozione di un modello federato

---

dell'IA. Fornitori di applicazioni sono i soggetti che sviluppano e/o forniscono applicazioni per scopi specifici adattando i modelli di IA e GPAI. Questi attori possiedono una conoscenza approfondita dei settori e delle esigenze delle organizzazioni utilizzatrici, combinando le capacità dell'IA con competenze di dominio per favorire la personalizzazione delle soluzioni. Gli utilizzatori sono i soggetti che adottano e integrano le tecnologie di IA nei propri sistemi per soddisfare esigenze operative e strategiche. Questi soggetti possono effettuare personalizzazioni o *fine-tuning* dei modelli utilizzando i propri dati al fine di ottimizzare le soluzioni per il contesto operativo specifico.

[139] All'interno della catena del valore una componente fondamentale è rappresentata dai fornitori di infrastrutture, ossia quei soggetti che forniscono servizi *cloud*, ma anche *networking*, *hardware* e MLOps (ovvero Machine learning operations), cfr. sul punto D. Kreuzberger, N. Kühl, S. Hirschl, *Machine Learning Operations (MLOps): Overview, Definition, and Architecture*, in *arXiv,* 2022, che definiscono MLOps (Machine Learning Operations) «[as] *a paradigm, including aspects like best practices, sets of concepts, as well as a development culture when it comes to the end-to-end conceptualization, implementation, monitoring, deployment, and scalability of machine learning products. Most of all, it is an engineering practice that leverages three contributing disciplines: machine learning, software engineering (especially DevOps), and data engineering. MLOps is aimed at productionizing machine learning systems by bridging the gap between development (Dev) and operations (Ops). Essentially, MLOps aims to facilitate the creation of machine learning products by leveraging these principles: CI/CD automation, workflow orchestration, reproducibility; versioning of data, model, and code; collaboration; continuous ML training and evaluation; ML metadata tracking and logging; continuous monitoring; and feedback loops*».

[140] G. Fioriglio, *Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone*, in *Riv. Scienze Giuridiche, Cognitive ed Intelligenza Artificiale*, 2, 2025, p. 8, doi: 10.60923/issn.1825-1927/22648.

[141] L'importanza dell'elemento fisico per lo sviluppo dell'IA è evidenziata anche nella Strategia italiana per l'Intelligenza artificiale 2024-2026 laddove si dice che «La necessità di azioni legate al potenziamento delle infrastrutture è del tutto evidente in un contesto applicativo così fortemente dipendente dalla disponibilità di grandi risorse di calcolo dedicate all'analisi di enormi moli di dati. In effetti, l'ambito infrastrutturale, da una parte, riguarda la necessità di continuare a investire su infrastrutture "fisiche" che consentano di sviluppare soluzioni di Intelligenza Artificiale sempre più all'avanguardia, mantenendo e migliorando il proprio livello di competitività a livello internazionale. Ma ancor più è necessario prendere oggi atto che i repository di dati e informazioni su cui i sistemi di IA possono essere addestrati rappresentano essi stessi una infrastruttura imprescindibile nello sviluppo di queste nuove tecnologie, una nuova dimensione infrastrutturale cui dovremo prestare crescente attenzione».

Nella descrizione del ciclo di vita dell'IA, le linee guida affermano che, nella fase di utilizzazione, la conservazione dei dati deve avvenire in modo sicuro e scalabile, ed è comunemente realizzata tramite

tra pubbliche amministrazioni di gestione delle infrastrutture tecnologiche[142]. Questo approccio, coerente con il Regolamento ACN sul *cloud* pubblico e con la Strategia *Cloud* Italia, consente di realizzare economie di scala e ridurre il rischio di frammentazione[143].

infrastrutture *cloud* che offrano scalabilità elastica, archiviazione distribuita, sicurezza e crittografia dei dati. Il riferimento alla scalabilità elastica e alla crittografia indica che il cloud è considerato la soluzione privilegiata per la gestione di grandi volumi di dati e per garantire resilienza e protezione.

[142] Le Linee guida sottolineano la necessità di superare le iniziative isolate e di promuovere l'implementazione e la gestione centralizzata di infrastrutture e strumenti secondo una logica "*cloud*". Le amministrazioni capofila possono mettere tali infrastrutture a disposizione di ciascun ente, accentrando investimenti e competenze e realizzando economie di scala. Si propone anche la federazione di risorse computazionali tra livello centrale, regionale e inter-regionale, come prospettiva per la condivisione di risorse di *computing* della PA italiana. In tal senso si propone l'adozione di una strategia cooperativa, attraverso una piattaforma comune, che consenta alle pubbliche amministrazioni di accedere a capacità computazionale per IA senza dover costruire infrastrutture proprietarie, cfr. pp. 62-63 delle Linee guida, al seguente link https://www.agid.gov.it/sites/agid/files/2025-02/Linee_Guida_adozione_IA_nella_PA.pdf.

[143] Le linee guida pongono inoltre l'attenzione anche sulla gestione dei dati lungo l'intero ciclo di vita, al fine di garantire che raccolta, archiviazione, elaborazione, analisi, monitoraggio e aggiornamento siano sicuri e conformi alle normative vigenti. Viene quindi fornito un modello di gestione del dato sintetizzando quello fornito dalle linee Guida *Open Data* con le integrazioni derivanti dall'*AI Act* e dagli Standard ISO, articolato in sei fasi: identificazione, analisi, preparazione, validazione, utilizzazione e monitoraggio.

CAPITOLO IV
L'intelligenza artificiale nella Pubblica amministrazione

1. Introduzione.

Il percorso verso la digitalizzazione della pubblica amministrazione interessa diversi ambiti, ma come si è cercato di ricostruire nel precedente capitolo, a fondamento del processo vi sono tre settori diversi (*cloud,* cybersicurezza e intelligenza artificiale), intrinsecamente connessi, sia per ragioni tecniche, sia per scelta del legislatore, specialmente nazionale, che nel definire il quadro delle competenze delle strutture preposte al controllo e alla vigilanza, nonché all'emanazione delle regole tecniche, ha deciso di concentrare in taluni soggetti tali funzioni, su tutti l'Agenzia per la Cybersicurezza Nazionale.

Da questa lettura dell'evoluzione della normativa, si ricava l'intenzione di costruire una sistema di *governance* che tenga conto di questi tre ambiti, inscindibilmente connessi, nella prospettiva della diffusione di nuove tecnologie anche nella pubblica amministrazione, come emerge dalla lettura del rapporto sulla spesa per ICT delle amministrazioni pubbliche[144] e lo studio[145] pubblicato nel 2025 dall'Agenzia per l'Italia Digitale, in cui si analizza, nello specifico, la diffusione dell'intelligenza artificiale negli uffici pubblici[146].

[144] Cfr. Rapporto AgID «La spesa ICT nella P.A. italiana. Percorsi e trend in atto 2022-2025», pubblicato il 29 maggio 2025.

[145] AgID, L'Intelligenza artificiale nella Pubblica amministrazione. Rapporto 202*5*.

[146] In particolare, il rapporto sulla spesa rileva che il 9% dei progetti (per un totale di 73) dedicati al digitale afferisce al macro-ambito 'Dati e Intelligenza Artificiale'. Mentre il risultato dell'indagine pubblicata nel 2025, volta a censire i 120 progetti di intelligenza artificiale (IA) avviati da 45 enti sulle 108 organizzazioni interpellate, restituisce la distribuzione e gli scopi dei progetti relativi all'IA. Nello specifico il 42 % mira a migliorare l'efficienza operativa, il 24 % la gestione e l'analisi dei dati, mentre il 18 % punta a rendere i servizi più accessibili. Le applicazioni più diffuse sono le chatbots e gli assistenti virtuali per l'interazione con i cittadini, utilizzati in oltre il 60 % delle iniziative, seguono i sistemi di supporto alle decisioni, mentre la robotica è marginale. Dal punto di vista infrastrutturale la quasi totalità dei progetti si appoggia a servizi o API cloud, con una quota minore che utilizza piattaforme di cloud computing PaaS, mentre le soluzioni *on-premises* sono residuali. L'indagine ha inoltre verificato che l'addestramento di modelli di Intelligenza Artificiale avviene utilizzando prevalentemente banche dati interne come fonte primaria, ma anche banche dati esterne (banche dati documentali, le banche dati gestionali e le banche dati di tipo statistico) e in alcuni casi sono stati utilizzati anche dati personali. Il rapporto segnala, inoltre, la scarsa attenzione agli standard internazionali ISO/IEC 25012, sulla qualità dei dati, una carenza che rischia di compromettere l'affidabilità degli algoritmi.

In queste considerazioni si inseriscono le Linee guida per l'adozione dell'intelligenza artificiale nella PA e la Strategia italiana per l'intelligenza artificiale redatte dall'AgID, nei quali viene posta particolare attenzione in primo lugo sulla caratteristica distintiva dei sistemi di IA, ossia la capacità inferenziale dei modelli basati sul *machine learning*, che consente al sistema di generare *output*, quali previsioni, contenuti, raccomandazioni o decisioni a partire dai dati ricevuti in *input*, porta con sé il rischio di *bias*[147], con conseguente pericolo di trattamenti ingiusti, discriminazioni o risultati inaffidabili.

Attraverso questi documenti, emerge come l'obiettivo non sia solo definire regole, ruoli e enti controllori, ma anche guidare le pubbliche amministrazioni, segnalando la necessità di analizzare «i fattori esterni e interni che influenzano le capacità dell'ente di conseguire i risultati attesi dall'uso dei sistemi di IA», come le esigenze di cittadini e imprese, nonché i requisiti normativi definiti da CAD, *AI Act*, GDPR e Direttiva NIS2, oltre ai fattori interni riguardanti la struttura organizzativa, il personale dipendente, la capacità tecnologica del territorio (quindi connettività, infrastrutture e servizi *cloud*). In altre parole, l'adozione di strumenti di IA non deve essere lasciata all'iniziativa degli enti, in assenza di una valutazione accurata della capacità di gestirli e dell'effettiva utilità di impiego.

Ma l'adozione di sistemi automatizzati nelle pubbliche amministrazioni comporta un vero e proprio cambiamento culturale[148], non riducibile alla mera idea di semplificazione dei processi ripetitivi, o all'idea di migliorare l'efficienza e l'efficacia[149] dell'azione amministrativa, pur essendo aspetti certamente di rilievo, non superabile dalla semplice adozione di linee guida.

---

[147] V. Linee guida per l'adozione di IA nella pubblica amministrazione, p. 14, in particolare si tratta di *bias* dei dati, *bias* dell'algoritmo o anche dell'essere umano.

[148] Il Codice dell'Amministrazione Digitale tiene in considerazione tale aspetto, con riferimento ai pubblici dipendenti, quando all'art. 13 stabilisce «Le pubbliche amministrazioni, nell'ambito delle risorse finanziarie disponibili, attuano politiche di reclutamento e formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive, ai sensi dell'articolo 8 della legge 9 gennaio 2004, n. 4.
Le politiche di formazione di cui al comma 1 sono altresì volte allo sviluppo delle competenze tecnologiche, di informatica giuridica e manageriali dei dirigenti, per la transizione alla modalità operativa digitale».

[149] European Commission: Joint Research Centre, AI Watch, *Road to the adoption of artificial intelligence by the public sector – A handbook for policymakers, public administrations and relevant stakeholders, Publications Office of the European Union*, 2022, p. 14, https://data.europa.eu/doi/10.2760/288757. Tra i potenziali benefici dell'IA illustrati nel manuale vengono infatti evidenziati quelli sull'efficienza dell'attività interna degli uffici pubblici, liberando i lavorati da attività caratterizzate da un basso livello di specializzazione, incrementando in questo modo il

Le amministrazioni devono adattare, infatti, le proprie strutture interne, in primo luogo conformandosi al quadro regolatorio di riferimento, oltreché alle fonti tecniche che attraverso l'indicazione delle figure necessarie per gestire i processi di digitalizzazione, nonché quelli di acquisto e utilizzo degli strumenti tecnologici, sono tese a responsabilizzare le singole amministrazioni.

Tuttavia, come si è cercato di spiegare attraverso l'analisi degli investimenti per la migrazione al *cloud* dei Comuni, il processo di digitalizzazione non è omogeneo, e dipende molto dalla capacità amministrativa dei singoli enti, oltreché da specifiche scelte normative, quali gli obblighi di cybersicurezza circoscritti a determinati enti. La conseguenza è la disomogenea diffusione di soluzioni di intelligenza artificiale, oltre al rischio di essere priva di reali effetti sulla qualità dei servizi e dell'amministrazione in generale, se non per la mera automatizzazione di taluni processi ripetitivi.

La complessità del fenomeno chiama quindi le pubbliche amministrazioni a ripensarsi dall'interno con un adattamento ai cambiamenti che cominci da quello dal contesto normativo. Una possibile modalità potrebbe avvenire attraverso l'integrazione degli strumenti di automazione nei processi decisionali interni di definizione delle strutture, degli uffici, del personale. In questo capitolo si vuole quindi proporre, quale risposta alla complessità del contesto digitale, un esempio concreto di integrazione dell'algoritmo (in senso lato), quale componente ordinante dell'organizzazione, e non mero strumento.

2. Quale intelligenza artificiale?

2.1. Le diverse soluzioni possibili.

Come già spiegato[150], l'espressione "intelligenza artificiale" abbraccia un insieme di tecnologie in continua evoluzione, dal *machine learning* alla *generative AI*, fino all'intelligenza artificiale agentica.

Esistono infatti differenti livelli o sotto insiemi dell'IA ciascuno dei quali racchiude diverse tecniche, modelli e capacità, e quindi ognuna con le sue peculiarità. Sul punto

tempo per dedicarsi a impieghi a maggiore valore aggiunto, consentendo, in prospettiva, anche un risparmio dei costi operativi.

[150] V. *supra* cap. 1 parr. 4.1 e 4.2.

risulta utile evidenziare, ai fini del discorso, in primo luogo la distinzione tra due grandi categorie che presentano implicazioni profondamente diverse per l'azione amministrativa[151].

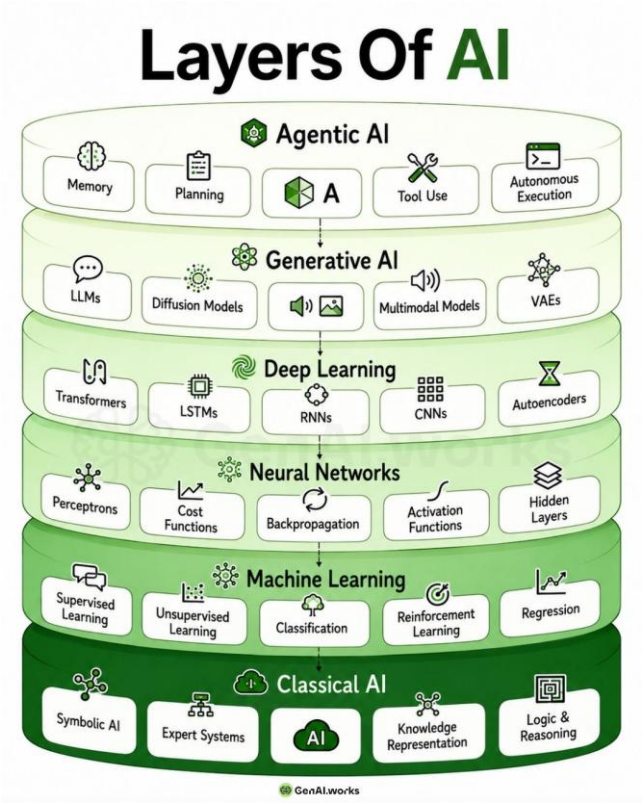


Figura 1 (Immagine presa da genai.works)

La prima è quella degli algoritmi deterministici o condizionali, rientranti nella categoria dell'AI classica (figura 1), formati da un codice contenente serie di regole predeterminate per cui al verificarsi di talune condizioni si produce un risultato[152]. Questa caratteristica rende prevedibile l'*output* e per tali ragioni questi algoritmi non si discostano dal ragionamento giuridico[153] di tipo sillogistico: data una norma, al verificarsi di un presupposto di fatto, si avrà un effetto[154]. La loro elasticità di impiego

[151] E. Buoso, *Disruptive technologies and public administration: rethinking administrative law for the brave new world?*, in V. Faggiani, F. J. Garrido Carrillo (a cura di), *Avances en el desarrollo de la inteligencia artificial. Principios éticos y democràticos, concreciones normativas en la uniòn europea, y limites para las administraciones pùblicas*, Aranzadi, 2025, p. 228.
[152] Questo gruppo di algoritmi è stato infatti impiegato dal MIUR nella procedura di assegnazione delle sedi di lavoro per i vincitori.
[153] Questa è la definizione classica di algoritmo, cfr. capitolo 1 par. 4.2.
[154] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. inform*., 3, 2021, p. 435.

ne consente un uso anche in procedure ripetitive, ad esempio per verificare in maniera automatica il contenuto di un'istanza e i requisiti di essa.

Più complessa è invece la seconda categoria, quella degli algoritmi di *machine learning*[155]. Questi algoritmi, basati su tecniche di apprendimento automatico, si addestrano su basi di dati e individuano *pattern* senza una codifica esplicita; sono impiegati per attività più complesse (come la valutazione di rischio o l'analisi di scenari) ma generano un effetto "black box", con conseguente scarsa trasparenza del procedimento. In questi casi, la decisione può sfuggire al controllo umano e richiede specifiche misure di supervisione.

Vi è quindi l'IA generativa basata sui modelli linguistici di grandi dimensioni e sistemi conversazionali (*Large Language Models*, LLM), modelli addestrati su enormi *corpus* testuali in grado di generare risposte in linguaggio naturale a partire da istruzioni fornite in linguaggio naturale.

L'ultimo livello è rappresentato dalla *agentic AI*, un'evoluzione significativa rispetto ai precedenti modelli di *machine learning*, in quanto dotata di autonomia, memoria, ragionamento e pianificazione che permettono a questi sistemi di auto adattarsi e di essere semi indipendenti, richiedendo quindi un minimo intervento umano[156], essendo capaci di apprendere continuamente e adeguare le proprie azioni in risposta ai cambiamenti ambientali[157]. Gli strumenti agentici infatti si connotano per la proattività intesa come «*the extent to which it actively works on tasks as opposed to simply reacting*»[158] che consente loro di prendere decisioni senza la necessità di istruzioni, anticipando quelli che possono essere gli eventi futuri o i bisogni che devono essere soddisfatti[159], modificando le decisioni al mutare del contesto in cui agiscono[160]. In tali caratteristiche risiede la differenza rispetto ai *Large Language Models* per così dire tradizionali, che sono principalmente modelli predittivi di tipo probabilistico.

---

[155] V. *supra* cap. 1, par. 4.2.

[156] I. Adabara, B.O. Sadiq, et. al., *Trustworthy agentic AI systems: a cross-layer review of architectures, threat models, and governance strategies for real-world deployment*, in *F1000Research*, 2025, p. 7 doi.org/10.12688/f1000research.169927.1. Vi è inoltre un'ulteriore categoria che rappresenta un passo ulteriore nell'evoluzione tecnologica chiamata "intelligenza organoide", la frontiera della ricerca nel settore del *biocomputing*, che combina biologia e tecnologia; sul punto A. Crismani, *La frontiera dell'IO (Intelligenza Organoide)*, in *Ceridap*, 4, 2024.

[157] I. Adabara, B.O. Sadiq, et. al, *op. cit.*, p. 8.

[158] S.T. Erukude, S.R. Veluru, et al., *Agentic ai - the rise of autonomous intelligent agents in the era of LLMS*, in *Indian Journal of Computer Science and Engineering*, 1, 2025, p. 10.

[159] U. Nisa, M. Shirazi, et al., *Agentic AI: The age of reasoning-A review*, in *Journal of Automation and Intelligence*, 2025, p. 7, doi.org/10.1016/j.jai.2025.08.003.

[160] A. Plaat, M. van Duijn, et al., *Agentic Large Language Models, a survey*, in *arXiv*, 2025, p. 4.

Proprio la capacità dell'*Agentic AI* di ragionare secondo procedimento di inferenza, analizzando, pianificando e risolvendo un compito, attraverso la validazione e il raffinamento della risposta, differenzia quest'ultima dal modo di funzionamento tipico della GAI (basata sulle correlazioni trovate nei dati di addestramento) rendendo possibile l'esecuzione di compiti complessi e multi-task [161].

2.2. Un confronto tra *generative AI* e *knowledge-based system*.

A fronte delle molteplici soluzioni tecniche adottabili e relative applicazioni, nel solco del ragionamento su quali possano essere i vantaggi per una pubblica amministrazione nell'adozione di strumenti di IA, nella prospettiva che si propone nel presente capitolo, ovvero di un possibile ricorso a tali strumenti nella definizione o comunque nell'ausilio alla definizione dell'organizzazione degli uffici pubblici, sembra opportuno limitare il ragionamento a due categorie la *generative AI* e i *knowledge-based systems*, strutturalmente differenti e conseguentemente impiegabili in maniera diversa.

Premessi i confini del ragionamento, occorre muovere dalla definizione di queste due espressioni.

Quanto all'IA generativa, manca a livello normativo una definizione. L'*Artificial Intelligence Act* si limita infatti a definire i modelli di AI a finalità generale[162] facendo unicamente un riferimento[163] all'IA generativa nel considerando 99, secondo cui «i grandi modelli di IA generativi sono un tipico esempio di modello di IA per finalità generali, dato che consentono una generazione flessibile di contenuti, ad esempio sotto forma di testo, audio, immagini o video, che possono prontamente rispondere a un'ampia gamma di compiti distinti» e stabilendo alcuni obblighi, tra cui quello di

[161] J. Schneider, *Generative to Agentic AI: Survey, Conceptualization, and Challenges*, in *arXiv*, 2025, p. 14.

[162] Art. 3, n. 63: «un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato».

[163] B. Adsuara Varela, *Articulo 3*, in M. Barrio Andrés (a cura di), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, La Ley, 2024, p. 171.

assicurare la trasparenza[164]. Si trova, infine, un riferimento esplicito a questa categoria nell'art. della l. 132/2025, laddove indica allo Stato e alle autorità pubbliche il compito di indirizzare le piattaforme di *e-procurement* delle pubbliche amministrazioni nella scelta dei fornitori e dei sistemi di intelligenza artificiale, privilegiando i «modelli in grado di assicurare elevati standard in termini di sicurezza e trasparenza nelle modalità di addestramento e di sviluppo di applicazioni basate sull'intelligenza artificiale generativa». Sembra quindi opportuno chiarirne la nozione.

L'IA generative viene definita dal *National Institute of Standard and Technologies*: «*The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content*»[165]; mentre l'*Organisation for Economic Co-operation and Development*[166] la definisce «*a category of AI that can create new content such as text, images, videos, and music*».

Muovendo da questa definizione descrittiva, ovvero indicante cosa è in grado di fare, è possibile affermare dunque che con intelligenza artificiale generativa (anche GAI dall'inglese *generative artificial intelligence*) si fa riferimento a tecniche computazionali in grado di generare contenuti apparentemente nuovi e significativi, come testi, immagini o audio, a partire da dati di addestramento[167]. Vi sono quindi alcuni elementi caratterizzanti, come la presenza di dati di addestramento, da cui è possibile generare contenuti simili ad essi, ma originali, di diverse tipologie, dai testi alle immagini, attraverso l'azione dell'utente che inserisce un comando[168].

Si tratta di un segmento dell'intelligenza artificiale, in cui l'algoritmo non classifica i dati, ma inferisce[169] una probabile distribuzione di essi per generare nuovi *output*[170]. Per

---

[164] Intesa quale obbligo di informare le persone che stanno interagendo con un sistema di IA (v. art. 50 *AI Act*).

[165] Definizione ripresa anche nell'*Executive Order* 14110 del Presidente degli Stati Uniti J. Biden, successivamente abrogato dall'*Executive Order* del Presidente D. Trump.

[166] Responsabile della redazione di numerosi report sull'intelligenza artificiale, tra cui il «*G7 Toolkit for Artificial Intelligence in the Public Sector*».

[167] S. Feuerriegel, J. Hartmann, et al., *Generative AI*, in *arXiv*, 2023, p. 2.

[168] A. Tewari, *If generative AI is the answer, what is the question?*, in *arXiv*, 2025, p. 3.

[169] Cfr. W. Ertel, *Introduction to Artificial Intelligence*, Springer, 2017, p. 275 che spiega le «*Inference rules are patterns of sound inference that can be used to find proofs. The resolution rule yields a complete inference algorithm for knowledge bases that are expressed in conjunctive normal form. Forward chaining and backward chaining are very natural reasoning algorithms for knowledge bases Horn form*». Peraltro, anche l'*AI Act* contiene un richiamo a questa caratteristica, estendendola in generale ai sistemi di intelligenza artificiale, laddove al considerando 12 dice: «Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che

fare ciò, viene utilizzata una particolare tipologia di algoritmi definiti di *deep learning*, una sottocategoria del *machine learning*[171], costruiti sulla base di regole matematiche di tipo probabilistico (la cui iniziale elaborazione si colloca negli anni Ottanta del secolo scorso) per poter operare con grandi quantità di variabili, in cui è presente un margine di incertezza, ed essere in tal modo più efficienti nel fornire risultati[172]. Per tali ragioni quando si parla di GAI, ci si riferisce anche al modello costruito con un'architettura di *machine learning*[173].

I modelli generativi più recenti e diffusi[174] sono tutti accomunati dal fatto che si basano sul principio della maggiore probabilità[175] e sono distinti in: *generative adversarial networks*[176], *diffusion models*, *variational autoencoders* e *transformer-based model*[177]. Quest'ultima tipologia è quella che ha permesso la creazione di *generative pre-trained transformer* (GPT)[178], ossia un modello di *deep learning* che, grazie ai miglioramenti architetturali, basati sull'architettura *transformer*, dotata di meccanismo chiamato *self-attention*, che permette di svolgere in parallelo più processi, valutando l'importanza di ogni parola[179], per generare testi simili a quelli scritti da un essere umano, sono diventati sempre più grandi e performanti. Questi progressi hanno ampliato la loro

possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati consentendo l'apprendimento, il ragionamento o la modellizzazione.»

[170] S. Feuerriegel, J. Hartmann, et al., *op. cit.*, p. 3. M. Trigka, E. Dritsas, *The Evolution of Generative AI: Trends and Applications*, in *IEEE Access*, vol.13, 2025, p. 1.

[171] Un algoritmo di *machine learning* è un algoritmo in grado di apprendere dai dati, al fine di «affrontare compiti troppo difficili da risolvere con programmi scritti e progettati dagli esseri umani», così I. J, Goodfellow, Y. Bengio, A. Courville, *Deep learning*, MIT Press, 2016, p. 97.

[172] I. Goodfellow, Y. Bengio, A. Courville, *op. cit.*, p. 52.

[173] S. Feuerriegel, J. Hartmann, et al., *op. cit.*, p. 3.

[174] S.S. Sengar, A.B. Hasan, et al. *Generative artificial intelligence: a systematic review and applications*, in Multimed Tools Appl 84, 23661–23700, 2025, doi.org/10.1007/s11042-024-20016-1.

[175] Per una spiegazione in dettaglio di ciascun modello v. A. Tewari, *op. cit.*, p. 10.

[176] Concepite da Ian J. Goodfellow et al., *Generative Adversarial Nets*, in *arXiv*, 2014.

[177] Concepiti da A. Waswani, N. Shazeer et al., *Attention is all you need*, in *arXiv*, 2017.

[178] Tale modello è stato creato da OpenAI, la società ideatrice di *chatGPT*, così S. Bengesi, et al. *Advancements in Generative AI: A Comprehensive Review of GANs, GPT, Autoencoders, Diffusion Model, and Transformers*, in *IEEE Access*, vol. 12, 2024, p. 69817. Y. Gokul Y., M. Ramalingam, et al., *GPT (Generative Pre-trained Transformer) – A Comprehensive Review on Enabling Technologies, Potential Applications, Emerging Challenges, and Future Directions*, in *arXiv*, 2023.

[179] A. Waswani, N. Shazeer, *op. cit.*, p. 3-4.

capacità di svolgere compiti di *natural language processing* consentendo lo sviluppo dei *large language model*[180].

Il processo di costruzione avviene in due fasi, la prima denominata di *pre-training* non supervisionato su grandi quantità di dati, alla quale segue, per allinearlo a specifici compiti, una fase di *fine-tuning*, tramite apprendimento supervisionato[181] o anche *reinforcement learning*, una tecnica con cui si istruisce il modello a comprendere, attraverso tentativi ed errori, quale azione sia giusta in una determinata situazione e quale no, imitando la modalità di apprendimento dell'essere umano[182].

Per queste sue caratteristiche prodotti basati su questi modelli, ossia ChatGPT, Claude, Gemini, si sono diffusi molto velocemente, al pari di tutte le altre categorie di modelli ascrivibili alla GAI, ossia anche quelli capaci di generare video, immagini o musica, e trovano applicazione già in alcuni uffici pubblici, in particolare nelle chatbot e negli assistenti virtuali per l'interazione con i cittadini. Si tratta sicuramente della categoria più diffusa, in quanto presente in oltre il 60% delle iniziative di IA censite da AgID.

Diversi invece sono i sistemi basati sulla conoscenza (*knowledge-based systems* o KBS), una categoria tradizionale dell'intelligenza artificiale, in quanto, incorporando la conoscenza in un determinato campo, similmente a quella umana, sono in grado eseguire un compito solitamente svolto da un essere umano esperto[183]. Tali sistemi funzionano su una base di conoscenza[184], ossia un archivio di informazioni contenute in un *database*[185]. Viene quindi costruito un modello di ragionamento utilizzando regole di inferenza logiche, quali ad esempio "*if-then*",[186] rese quindi eseguibili attraverso un *software* che applicandole è in grado di interrogare il *database* per fornire una risposta,

---

[180] Cfr. *supra* capitolo 1, nota 77.

[181] T. Wang, Y. Wang et al., *Deep Learning and Machine Learning – Generative Models: Foundations, Techniques, and Applications*, 2024, p. 101, disponibile in SSRN: ssrn.com/abstract=5211980 o dx.doi.org/10.2139/ssrn.5211980. V. sul punto capitolo 1, par. 4.

[182] W. Ertel, *op. cit.*, p. 289.

[183] P. Szolovits, *Knowledge-Based Systems: A Survey*, in M.L. Brodie, J. Mylopoulos (eds.), *On Knowledge Base Management Systems. Topics in Information Systems*, Springer, 1986, p. 339. V. anche C. Tasso, *Attori, processi, meriti e responsabilità nell'utilizzo di algoritmi di Intelligenza Artificiale: il caso del Machine Learning*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino, 2021, pp. 19 – 48.

[184] Russell, Norvig, *Artificial intelligence: a modern approach*, 2017, p. 234.

[185] Russell, Norvig, *op. cit.*, p. 235.

[186] Con riferimento allo schema *if-then* è opportuno precisare che trattasi di uno schema logico comune a tutti i programmi, in cui l'elaboratore riceve le istruzioni ed esegue uno o più compiti. Cfr. sul punto S. Orlando, *Linguaggi di programmazione e responsabilità*, in S. Orlando, G. Capaldo (a cura di), *Annuario 2022. Osservatorio Giuridico sulla Innovazione Digitale*, Sapienza Università Editrice, 2022, p. 272.

secondo un linguaggio formale che consente di rappresentare la conoscenza[187]. La base di conoscenza viene dunque impiegata per raccogliere e organizzare le informazioni, consentendo un facile recupero, ed ha come obiettivo quello di rappresentare le conoscenze usate dagli esseri umani per svolgere determinati compiti[188]. Un KBS è in particolare un modello computerizzato finalizzato a risolvere problemi con capacità di risoluzione dei problemi paragonabili a quelle di un esperto del settore[189].

2.3. *Generative AI* o *Knowledge-based systems* nel dominio legale.

Per come sinteticamente descritti i due sistemi mostrano evidenti differenze. Da un lato la GAI genera *output* attraverso modelli che inferiscono dai dati su cui sono addestrati possibili soluzioni (ovvero nel caso degli LLM, la capacità di predire la parola successiva[190]). Viceversa i *knowledge-based systems* operano secondo regole logiche dichiarative, ossia relazioni esplicite. Da questa distinzione discende la più significativa differenza; l'opacità dei modelli di IA generativa, poiché è difficile comprendere come arrivino a generare un determinato *output*, a cui si aggiunge il rischio di *bias* causato dai dati di addestramento[191]. Se i dati presentano *bias* il modello produrrà risultati distorti[192]. Viceversa, i KBS consentono una maggiore comprensione e verifica del ragionamento, così da rendere comprensibile l'*output* generato[193].

Se da un lato i *knowledge-based systems* consentono una valutazione tanto delle informazioni immesse nel modello quanto del meccanismo di ragionamento, e quindi

[187] W. Ertel, *op. cit.*, p. 20.
[188] S. Ferilli, E. Girardi et al. (a cura di), *L'Intelligenza artificiale per lo sviluppo sostenibile*, Cnr edizioni, 2021, p. 176.
[189] R. Studer, V. R. Benjamins and D. Fensel, *Knowledge Engineering: Principles and Methods*, in *Data & Knowledge Engineering*, Vol. 25, Issues 1–2, 1998, p. 163.
[190] A.R. Doshi, J.J. Bell, et al., *Generative Artificial intelligence and evaluating strategic decisionsi*, in *Strategic Management Journal*, vol. 46, 3, 2025, disponibile in SSRN: ssrn.com/abstract=4714776 oppure dx.doi.org/10.1002/smj.3677.
[191] P. Traverso, *Breve introduzione tecnica all'Intelligenza Artificiale*, in *DPCE*, 1, 2022, p. 164.
[192] T. Wang, Y. Wang, et al, *op. cit.*, p. 164, ssrn.com/abstract=5211980 oppure dx.doi.org/10.2139/ssrn.5211980.
[193] M. Umar, A. Mehmood, H. Song, *A Survey on State-of-the-Art Knowledge-based System Development and Issues*, in *The Smart Computing Review*, p. 501. V. anche J. Giarratano, G. Riley, *Expert Systems Principles and Programming*, PWS, 3rd Edition, 2020, p. 8.

del risultato, i *generative models* permettono unicamente una valutazione del risultato[194], a fronte di una maggiore capacità computazionale.

Premessa questa sintetica differenza, è possibile allora riflettere come un impiego dei sistemi di intelligenza artificiale nella pubblica amministrazione debba tenere in considerazione il loro effettivo funzionamento, al fine di operare una scelta sulla soluzione preferibile a seconda del fine perseguito, deflattivo dell'attività ordinaria oppure di ausilio all'azione amministrativa, con funzioni predittive, o ancora di automatizzazione dei processi decisionali[195]. Con particolare riferimento alla possibilità di automazione dell'azione amministrativa (entro limiti che verranno analizzati nel successivo paragrafo), bisogna altresì considerare il significativo divario tra il ragionamento probabilistico dei *large language models* e quello giuridico[196], caratterizzato dall'interpretazione dei principi dell'ordinamento e delle norme di diritto positivo[197], spesso aventi un significato oscuro o ambiguo, che richiedono la capacità di eliminare i significati improbabili per calare nel contesto concreto il precetto normativo[198]. Per mitigare questi problemi rispetto all'uso dell'IA generativa sono possibili alcune soluzioni, come ad esempio il *fine-tuning* specificamente finalizzato a adattare il modello agli usi legali oppure la *retrieval-augmented generation*, che consente di ottenere le risposte fornendo una base documentale al modello[199]. Entrambi questi approcci consentono di mitigare il rischio di "allucinazioni", fenomeno che si verifica quando il sistema fornisce risposte non basate sulla realtà o documenti ufficiali.

Una ulteriore problematica relativa all'utilizzo dell'IA, in particolare nel procedimento amministrativo, attiene all'onere di motivazione del provvedimento amministrativo. Se, infatti, per quanto riguarda gli atti vincolati, tale onere può essere assicurato dall'esplicitazione dei presupposti sulla base del quale sono stati emanati (che potrebbe avvenire secondo lo schema *if-then*), altrettanto non può dirsi nel caso degli atti discrezionali[200].

---

[194] H. Prakken, *On Evaluating Legal-Reasoning Capabilities of Generative AI*, in *CEUR WS*, 2024, p. 101.
[195] M. Macchia, *Pubblica amministrazione e tecniche algoritmiche*, in *DPCE*, 1, 2022, p. 314.
[196] Cfr. sul punto E. Linna, T. Linna, *Judicial Requirements for Generative AI in Legal Reasoning*, in *arXiv*, 2025.
[197] V. la disamina sulla questione da parte di A. Schiavello, *Osservazioni in margine a Legal Reasoning and Legal Theory di Neil MacCormick a venti anni dalla pubblicazione*, in *Foro It.*, 1999, p. 245.
[198] G. Terranova, *Il ragionamento giuridico*, Giuffrè, 2021, p. 28.
[199] E. Linna, T. Linna, *op. cit.*
[200] M. Macchia, *op. cit.*, p. 322.

Sulla base delle caratteristiche descritte i KBS risultano maggiormente compatibili con il procedimento amministrativo, potendo consentire la verifica automatica di requisiti ad esempio di un'istanza, la valutazione di conformità giuridica, o la formalizzazione di regole di scelta, tenendo altresì traccia del ragionamento seguito. Viceversa, i modelli generativi permettono di snellire il lavoro, semplificando quelle attività che esulano da una manifestazione di volontà della pubblica amministrazione, ossia la semplificazione linguistica di atti, il supporto alla comunicazione con il cittadino e l'analisi semantica di grandi archivi testuali[201].

In ogni caso entrambe le tipologie di sistema necessitano di una supervisione umana. Infatti, anche i KBS, pur essendo apparentemente più affidabili, possono condurre a risultati errati, se l'*input* inserito non è corretto, oppure produrre effetti non conformi alla legge, se l'*output* viene letto in maniera erronea dal funzionario umano[202]. Per queste ragioni risulta necessaria una *governance* che è in concreto quella in costruzione[203] ad opera del legislatore europeo e nazionale.

3. L'automazione dall'attività amministrativa: considerazioni sul procedimento algoritmico.

Le considerazioni fino a qui svolte assumono rilievo in riferimento al procedimento amministrativo algoritmico quale momento di interazione tra l'innovazione tecnologica descritta nel paragrafo precedente e il diritto amministrativo.

La l. n. 241/1990 stabilisce un modello ispirato alla trasparenza, alla partecipazione e alla motivazione, ponendo norme precise volte a regolare il procedimento

[201] Cfr. sul punto OECD Report, *cit.*, p. 26, con riferimento all'utilizzo dell'IA generativa da parte del Governo del Regno Unito.

[202] Su tali questioni v. H. de Bruin, H. Prakken, J. Svensson, *The Use of Legal Knowledge-Based Systems in Public Administration: What Can Go Wrong?*, in T.J.M. Bench-Capon, A. Daskalopulu and R.G.F. Winkels (eds.), *Legal Knowledge and Information Systems*. Jurix 2002: The Fifteenth Annual Conference. Amsterdam: IOS Press, 2002, pp. 123-132.

[203] L'*AI Act* è entrato parzialmente in vigore nel 2024, ma, come accennato in precedenza, il legislatore europeo ha previsto un differimento per alcune disposizioni onde consentire ai soggetti di adeguarsi. Similmente il legislatore nazionale con la l. 132/2025 ha conferito delega al Governo per adottare testi normativi dedicati alla regolamentazione dell'IA nei vari ambiti della società, dal settore della giustizia a quello del lavoro.

amministrativo, che non è solo una sequenza di atti finalizzata all'emanazione di un provvedimento[204], ma è il modo in cui la funzione amministrativa viene esercitata[205].

Nel corso del tempo il procedimento si è progressivamente trasformato, a partire dall'informatizzazione guidata dal Codice dell'Amministrazione Digitale, il quale ha sancito da un lato il diritto dei cittadini a interagire con le amministrazioni mediante strumenti informatici, e dall'altro l'obbligo per queste ultime di adoperarli, dimostrando come fosse possibile adattare l'ordinamento al mutato contesto delle tecnologie strumentali per l'assolvimento dei compiti attribuiti dalla legge alla pubblica amministrazione.

L'utilizzo dell'intelligenza artificiale ha invece sollevato questioni di particolare rilievo sul modo in cui i principi del diritto amministrativo necessitano una reinterpretazione, alla luce della possibilità di automatizzare tutte o alcune fasi del procedimento, segnando quindi un punto di rottura nel rapporto tra tecnologia ed azione amministrativa, in considerazione della possibilità non tanto di cambiare il modo in cui la pubblica amministrazione gestisce i processi interni ed esterni[206], quanto piuttosto il modo in cui decide. Si tratta di una trasformazione che segna il passaggio verso il procedimento amministrativo algoritmico[207], che è cosa diversa dalla digitalizzazione. Quest'ultima rappresenta un processo di conversione verso l'informatica, mentre l'intelligenza artificiale incide sulla dimensione cognitiva e decisionale del potere amministrativo[208].

Una ulteriore considerazione attiene al tipo di attività della pubblica amministrazione. Nel caso dell'attività vincolata, essendo la legge a predeterminare i presupposti e gli effetti del provvedimento, come evidenziato dalla giurisprudenza già da molto tempo[209], l'utilizzo dell'IA non crea problemi ed è lecito concludere che possano essere impiegati

[204] A.M. Sandulli, *Il procedimento amministrativo*, Milano, 1940.
[205] M.S. Giannini, *Lezioni di diritto amministrativo*, Milano, 1950, p. 259.
[206] A. Corrado, *La trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, in *Federalismi.it*, p. 197.
[207] F. Nassuato, *Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*, in *Ceridap*, 1, 2022, p. 152.
[208] A.L. Rum, *Il provvedimento amministrativo adottato mediante algoritmo: il ruolo dell'intelligenza artificiale nel processo decisionale della P.A.*, in www.ildirittoamministrativo.it; B. Raganelli, *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenze diverse nell'assunzione di decisioni amministrative*, in *Federalismi.it*, 22, 2020, p. 252.
[209] Cfr. Cons. St. nn. 2270/2019 e 8472/2019.

algoritmi di tipo deterministico[210]. Mentre se si tratta di attività discrezionale, stante il potere conferito all'amministrazione di bilanciamento degli interessi rilevanti nel procedimento, saranno gli algoritmi non deterministici ad essere utilizzati, ponendo rilevanti questioni rispetto all'osservanza delle regole e delle garanzie procedimentali[211]. Nel procedimento amministrativo l'algoritmo può certamente trovare spazio nell'attività istruttoria[212], ma può trovare anche impiego nell'attività di valutazione e decisione tipicamente assolta dal funzionario. Ed è proprio questa delega di funzioni al sistema automatizzato il centro del dibattito teorico-giuridico su cui, inizialmente la giurisprudenza[213], e successivamente il legislatore, hanno definito dei principi e delle regole, nell'intento di determinare i confini dell'utilizzo intelligenza artificiale.

I temi centrali attorno ai quali ruota il dibattito in dottrina[214] attiene ai principi di legalità, di trasparenza, di imputazione della decisione algoritmica e di responsabilità[215]. In altri termini, occorre chiedersi se e in che misura un atto amministrativo che sia il risultato di un algoritmo possa rispettare questi criteri, e quindi in definitiva quale sia la legittimazione delle decisioni automatizzate.

Risulta possibile sostenere che sotto il profilo del principio di legalità non vi siano problemi, a fronte dell'approvazione della legge italiana sull'intelligenza artificiale[216], a

---

[210] G.C. di San Lucia, M. Paladino, *Decisioni amministrative e intelligenza artificiale*, in *Federalismi.it*, 4, 2025, p. 135.

[211] F. Conte, *La trasformazione digitale della pubblica amministrazione : il processo di transizione verso l'amministrazione algoritmica,* in *Federalismi.it,* 11, 2023 p. 73. V. Tar. Napoli, sez. VII, 14 novembre 2022, n. 7003, in cui viene ribadito che «Il ricorso all'algoritmo, in funzione integrativa e servente della decisione umana, ovvero anche in funzione parzialmente decisionale nei procedimenti a basso tasso di discrezionalità, non può mai comportare un abbassamento del livello delle tutele garantite dalla legge sul procedimento amministrativo, ed in particolare di quelle sulla individuazione del responsabile del procedimento, sull'obbligo di motivazione, sulle garanzie partecipative, e sulla cd. non esclusività della decisione algoritmica».

[212] D.U. Galetta, J.C. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 2, 2019, p. 19.

[213] V. cap. 1, par. 4.3.

[214] Sull'argomento vi sono diversi contributi, tra cui E. Carloni, *Dalla legalità algoritmica alla legalità (dell'amministrazione) artificiale. Premesse ad uno studio*, in *Riv. it. infor. dir.*, 2, 2024; I. Alberti, *op. cit.*, p. 285. P. Otranto, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in *Federalismi.it*, 7, 2021; A.G. Orofino, *L'attuazione del principio di trasparenza nello svolgimento dell'amministrazione elettronica*, in *www.judicium.it*, 2020; D.U. Galetta, J.C. Corvalàn, *op. cit.*; S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità,* in *Dir. pubbl.*, 1, 2019; I.M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Ist. feder*., 3, 2019, p. 650.

[215] I.M. Delgado, *op. cit*., p. 650.

[216] L'art. 14, comma 1 della l. 132/2025 infatti recita: «Le pubbliche amministrazioni utilizzano l'intelligenza artificiale allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle

cui si si aggiunge l'art. 30 del Nuovo codice degli appalti pubblici[217], che unitamente letti portano a concludere per l'ammissibilità dell'utilizzo dell'intelligenza artificiale nel procedimento amministrativo, nella misura in cui è la legge stessa ad autorizzare la pubblica amministrazione ad avvalersi di questa tecnologia, quale modalità dell'esercizio dell'azione amministrativa[218]. Tale aspetto vien statuito al comma 2 dell'art. 14 della l. 132/2025, ove si sancisce che «L'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale», così affermando non solo la strumentalità di questi sistemi, ma evidenziando il criterio di imputazione della decisione, che rimane in capo del funzionario persona fisica, anche in caso di utilizzo di sistemi automatizzati.

Tale disposizione forse non era necessaria[219], a meno di non mettere in crisi la teoria dell'organo[220], che persiste come finzione normativa per spiegare la riferibilità degli atti e degli effetti dell'attività posta in essere dal funzionario alla pubblica amministrazione[221], implicando la riferibilità e quindi la responsabilità dello stesso per l'atto della macchina[222]. Ad ogni modo il legislatore ha voluto sancire espressamente l'imputabilità degli atti posti in essere con l'uso dell'IA, avente contributo strumentale all'attività amministrativa, ribadendo il principio che l'unico ad assumere e fare proprie

---

imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo».

[217] L'art. 30, comma 1 stabilisce infatti che «Per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti, nel rispetto delle specifiche disposizioni in materia».

[218] *Ex multis*, Cons. St., sez. VI, 13 dicembre 2019 n. 8472.

[219] G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Dir. info. informatica*, 3, 2021, p. 437, il quale osserva che «ove l'organo competente ad adottare la decisione assuma la responsabilità di questa facendola propria, non pare potersi mettere in dubbio 'la riferibilità della decisione finale all'autorità ed all'organo competente in base alla legge attributiva del potere'».

[220] Sulla teoria dell'organo v. *supra* capitolo 3. Cfr. M. C. Cavallaro, *Immedesimazione organica e criteri di imputazione della responsabilità,* in *P.A. persona e amministrazione*, 1, 2019.

[221] I.M. Delgado, *op. cit.*, p. 653, secondo cui «il fatto che la decisione sia stata adottata in maniera automatizzata senza l'intervento diretto di una persona, non implica che l'attività venga imputata alla macchina, ma la paternità dell'atto ricadrà sull'organo amministrativo che detiene la potestà ed esercita la competenza avvalendosi del sistema».

[222] S. Civitarese Matteucci, *op. cit.*, p. 21, il quale ragionando sull'imputabilità e responsabilità delle decisioni automatizzate osserva come «sia implicito nel suddetto argomento letterale che se si affidasse a una 'macchina' l'assunzione di una decisione si interromperebbe il nesso di imputazione tra la norma che conferisce il potere e il soggetto umano cui tale potere è conferito. Questo aspetto chiama in causa la questione della responsabilità connessa al potere decisionale. È certo da escludere che la macchina cui viene delegato il potere decisionale sia 'personalmente' responsabile degli atti che pone in essere».

le decisioni finali è il funzionario persona fisica, con le connesse conseguenze sotto il profilo della responsabilità della pubblica amministrazione per il provvedimento emanato[223]. Tale principio si salda, inoltre, con la disciplina dettata dall'*AI Act*, il cui art. 14 impone la supervisione umana dei sistemi ad alto rischio.

L'aspetto forse più dibattuto connesso all'uso dell'IA nel procedimento amministrativo attiene alla trasparenza della decisione e quindi alla spiegabilità del percorso logico-giuridico seguito dalla pubblica amministrazione che si sia avvalsa di sistemi automatizzati al fine di decidere. Questo tema è stato già affrontato dalla giurisprudenza amministrativa[224] e il legislatore europeo vi ha dedicato particolare attenzione nel regolamento, laddove già nei considerando richiama più volte tale principio, precisando che «Con 'trasparenza' si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i *deployer* delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti»[225]. Il regolamento, quindi, individua tra i propri scopi anche quello di dettare regole armonizzate in materia di trasparenza (art. 1, comma 2 lett. d), imponendo specialmente per i sistemi di IA così detti ad alto rischio, una progettazione ed uno sviluppo «tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai *deployer* di interpretare l'*output* del sistema e utilizzarlo adeguatamente», assicurando «un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del *deployer*»[226] previsti alla sezione 3 dal regolamento, in cui viene normata la gestione del ciclo di vita dei sistemi di IA ad alto rischio, in modo da garantire la costante verifica e controllo della conformità dei sistemi alla legge. A tali obblighi si aggiungono anche quelli previsti in particolare al capo IV, art. 50 [227], laddove si declina la trasparenza nel

[223] Sulle diverse ipotesi di responsabilità correlate alla decisione algoritmica cfr. P. Del Vecchio, V. Bignoli, *le responsabilità amministrative da algoritmo e intelligenza artificiale Lla responsabilità da provvedimento algoritmico sia ai fini del risarcimento del danno in sede civilistica che in sede contabile come responsabilità erariale*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?, Vol. 2, Amministrazione, responsabilità, giurisdizione*, Il mulino, 2022, p. 321.

[224] Cfr. Cons. St. nn. 8472, 8473, 8474 del 2019.

[225] Considerando 27.

[226] Così l'art. 13 del regolamento.

[227] Rubricato «Obblighi di trasparenza per i fornitori e i *deployers* di determinati sistemi di IA», il cui comma 1 recita: «I fornitori garantiscono che i sistemi di IA destinati a interagire direttamente con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista

senso di rendere edotti gli utenti che stanno interagendo con un sistema automatizzato, cui correlativamente si prevede, all'art. 86, un diritto alla spiegazione sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata[228].

La duplice accezione di trasparenza emergente dall'*AI Act*, intesa sia come comprensibilità[229] dell'*output* sia come informazione agli utenti, si giustifica in ragione delle peculiarità del funzionamento degli algoritmi, nello specifico non deterministici, come sono quelli su cui si basa l'intelligenza artificiale generativa. Tali modelli e in generale quelli basati su tecniche di apprendimento automatico sono caratterizzati infatti da opacità, ossia dall'impossibilità di comprendere le logiche interne del sistema impiegate per generare un risultato. È questo il problema, di cui si è già accennato, della *black box*[230] e quindi della possibilità di spiegare come il sistema abbia generato un determinato risultato, rendendo complesso[231] per le pubbliche amministrazioni ricorrere a questi strumenti nei processi decisionali[232]. Se, infatti, la decisione è assunta con l'ausilio di un algoritmo, il destinatario del provvedimento (e i controinteressati) devono essere posti in condizione di comprendere almeno le logiche generali del sistema, i parametri, le basi di dati utilizzate e le modalità con cui queste hanno inciso sul provvedimento[233].

Il problema della spiegabilità non si pone poi in maniera uniforme rispetto a tutti i sistemi di intelligenza artificiale. Ad esempio, con riferimento ai due esempi descritti

---

di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato».

[228] L'art. 86, rubricato «Diritto alla spiegazione dei singoli processi decisionali», al comma 1 statuisce infatti che «Qualsiasi persona interessata oggetto di una decisione adottata dal *deployer* sulla base dell'output di un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi elencati al punto 2 dello stesso, e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali ha il diritto di ottenere dal *deployer* spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata».

[229] A.G. Orofino, *op. cit.*, p. 8.

[230] Tra gli altri v. G. Lo Sapio, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi.it*, 16, 2021, A. Cerillo i Martinez, *How can we open the black box of public administration? Transparency and accountability in the use of algorithms*, in *Rivista catalana de dret pùblic*, 58, 2019.

[231] D.U. Galetta, J.C. Corvalàn, *op. cit.*, p. 16.

[232] O.M. Puigpelat, *The impact of the AI Act on public authorities and on administrative procedures*, in *Ceridap*, 4, 2023, p. 247.

[233] A. Corrado, *op. cit.*, p. 198. Il già menzionato art. 14, co. 1 della l. 132/2025 prescrive infatti che le pubbliche amministrazioni quando utilizzano l'intelligenza assicurano agli interessati la conoscibilità del suo funzionamento, nonché la tracciabilità del suo utilizzo.

nel paragrafo precedente, ossia i *knowledge-based systems* e i *generative AI models*, tale questione assume dimensioni diverse, sotto il profilo tecnico, ma anche giuridico. Come già spiegato, i KBS possono adoperare regole condizionali del tipo "*if-then*", ossia meccanismi di inferenza basati su condizioni, al soddisfacimento delle quali si produce un determinato risultato. Sotto questo profilo, pur considerando il fatto che ben possono essere adoperati altri meccanismi di inferenza, il loro impiego da parte della pubblica amministrazione non risulta problematico[234]. Discorso diverso deve farsi per i sistemi di IA generativa, sia per quanto si è detto nel precedente paragrafo, sia per l'attenzione dedicatavi dal legislatore europeo. Come si è avuto modo di esporre nel capitolo 2, il Regolamento UE 2024/1689 dedica una disciplina a parte per questi sistemi, prevedendo altresì una *governance* apposita, in ragione dei peculiari aspetti che li caratterizzano, implicando, per un'amministrazione che voglia impiegarli, da un lato un'attività di adeguamento alla normativa europea, dall'altro la salvaguardia delle garanzie procedimentali rispetto ad una tecnologia i cui processi non si prestano a una effettiva intelligibilità.

Similmente, il legislatore nazionale ha introdotto una norma di principio all'art. 3, co. 3 della l. 132/2025 in base al quale «I sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità e dei principi di cui al comma 1, assicurando la sorveglianza e l'intervento umano».

L'altra faccia della questione relativa alla spiegabilità attiene alla possibilità da parte dell'interessato di accedere all'algoritmo, alla stregua degli altri documenti amministrativi del procedimento, al fine di tutelare le proprie ragioni[235]. Di tale principio il giudice amministrativo ha già specificato il perimetro, chiarendo come non debba trattarsi di mera ostensione del codice sorgente[236], ma anche di spiegazione della decisione algoritmica, ossia delle logiche di funzionamento del sistema[237].

---

[234] H. de Bruin, H. Prakken, J. Svensson, *op. cit.*, p. 129, in cui gli autori prendo come esempio un caso di impiego di un KBS da parte di un Comune olandese per la gestione delle misure di sostegno al reddito per le famiglie in difficoltà.

[235] M. Palma, *Gli algoritmi dell'amministrazione pubblica e l'amministrazione pubblica degli algoritmi*, in *Riv. it. informatica dir.*, 2, 2022, p. 41.

[236] Ossia l'insieme delle istruzioni che determinano il funzionamento del sistema informatico.

[237] Cons. St., n. 8472/2019, Cons. St. n. 881/2020; F. Nassuato, *op. cit.*, p. 157-158.

4. Una nuova prospettiva dell'algoritmo nella pubblica amministrazione.

4.1. L'algoritmo come atto di organizzazione.

La possibilità di utilizzare l'intelligenza artificiale nel procedimento amministrativo, pur con le considerazioni svolte nel precedente paragrafo, risulta certamente acquisita nell'ordinamento, in tanto in quanto vi è una legge che lo prevede, autorizzando l'impiego di tali soluzioni tecniche[238], nel rispetto dei principi dell'ordinamento, oltreché degli obblighi previsti, nello specifico, dal Regolamento UE 2024/1689, e dei principi elaborati dalla giurisprudenza. Secondo la ricostruzione teorica offerta dalla dottrina tale possibilità si ammette anche in tanto in quanto gli strumenti di intelligenza artificiale rappresentano un modulo organizzativo[239], e sono quindi esercizio della potestà di auto organizzazione della pubblica amministrazione[240], che sceglie quali strumenti utilizzare nel procedimento amministrativo.

Muovendo da queste considerazioni, si può allora aggiungere un ragionamento al tema del governo o della *governance*.

Definito il tema del governo del digitale, nelle numerose sfaccettature, che, come si è visto, rappresenta una dimensione complessa in cui il potere pubblico si trova ad agire e a fare i conti, tra definizione delle regole e attribuzione delle responsabilità, nonché dei ruoli, si può allora ragionare sull'organizzazione sotto una prospettiva differente. Nel momento in cui si introducono strumenti in grado non solo di automatizzare processi, ma anche di analizzare dati e individuare *pattern*, prendendo quindi una decisione, intesa nel senso di produrre un *output* non atteso o previsto, allora la struttura stessa dell'organizzazione può essere costruita con essi, ovvero definita dalla macchina.

Sulla base di quanto analizzato anche nei precedenti capitoli, si può già sostenere che l'IA ha ridefinito o comunque sta ridefinendo le organizzazioni, sia per esigenze tecniche sia per esigenze normative. Il passo ulteriore è la modificazione dell'organizzazione attraverso la "macchina", anziché a causa di essa.

L'organizzazione è infatti un sistema in cui devono trovano traduzione in termini concreti quell'insieme di regole astratte, che devono essere eseguite perché possano

[238] Il riferimento è all'art. 30 d.lgs. 36/2023, all'art. 9 del d.lgs. 12 luglio 2024, n. 103, nonché in termini più ampi la l. n. 132/2025.

[239] I. Forgione, *La prospettiva dell'intelligenza artificiale nel procedimento e nell'attività amministrativa*, *Riv. it. informatica dir.*, 2, 2024, p. 510.

[240] In senso critico rispetto a questa tesi cfr. T.A.R. Veneto, sez. III, 21 ottobre 2025 n. 1845.

dispiegare i propri effetti all'interno dell'organizzazione stessa, prima ancora che all'esterno. Da questa premessa risulta allora postulabile un parallelismo tra algoritmi e organizzazioni[241], intese come sistemi complessi e strutturati in cui ogni componente deve eseguire un compito sulla base di un *input* ricevuto (dalla legge, dal cittadino, dall'amministrazione stessa o da un'altra), per generare un *output* (che è astrattamente identificabile nell'atto volto a perseguire il fine pubblico stabilito dalla legge) mediante procedure e regole. Questo concetto permette di considerare come processi decisionali e strutture operative proprie di un'organizzazione abbiano in effetti la struttura di un algoritmo, seppur con alcune precisazioni.

L'organizzazione amministrativa trova fondamento nell'art. 97 Cost., ove viene sancito il principio della riserva di legge, e nel d.lgs. 165/2001, in base ai quali «la determinazione delle linee fondamentali di organizzazione degli uffici pubblici […] è rimessa – sulla base di 'principi generali' fissati dalla legge – a ciascuna amministrazione pubblica, che vi provvede mediante 'atti organizzativi' (cfr. artt. 2 e 5 d.lgs. n. 165/2001), complessivamente ispirati a criteri di funzionalità, flessibilità, trasparenza ed imparzialità, idonei a tradurre e compendiare, in prospettiva programmatica, i principi costituzionali di buon andamento ed imparzialità (art. 97 Cost.) e a perseguire la complessiva efficacia ed efficienza dell'azione amministrativa (art. 1 l. n. 241/1990)»[242]. Nell'ordinamento la distinzione in materia di atti organizzativi è tra atti di macro organizzazione e atti di micro organizzazione, laddove i primi costituiscono esercizio di un potere autoritativo per la definizione delle linee fondamentali della struttura amministrativa e le competenze degli uffici[243], mentre gli altri sono esercizio del potere di organizzazione interna ai singoli uffici pubblici, nonché dei rapporti di lavoro[244]. Tramite questi atti gli organi di vertice delle amministrazioni implementano il sistema di regole esaminato, per darvi attuazione all'interno degli uffici, a partire dalla definizione dei ruoli.

---

[241] V. L. Glasera, J. Sloana, J. Gehman, *Organizations as Algorithms: A New Metaphor for Advancing Management Theory*, in *Journal of Management Studies*, 61, 2024, gli autori propongono un nuovo concetto "*organizations as algorithms*" con cui spiegare il mutamento delle organizzazioni a causa degli algoritmi verso una capacità di agire distribuita e come la programmazione e il *prompting* stiano mutano le relazioni interne con le tecnologie.

[242] Cons. St., 3 settembre 2018 n. 5143.

[243] T.A.R. Campania, sez. V, 25 marzo 2022 n. 2017, Cons. St., sez. III, 3 aprile 2019 n. 2210.

[244] T.A.R. Lazio, sez. V, 5 dicembre 2023, n. 18189.

Nella prospettiva ipotizzata, suffragata dalla dottrina e dalla giurisprudenza, che vedono nell'algoritmo uno strumento, allora è possibile dire che esso è in grado di definire i ruoli e i processi decisionali, di ordinare, strutturare e regolare le organizzazioni[245], in quanto parte dell'insieme dell'organizzazione composta dalle persone fisiche[246] e dalle risorse strumentali, ovvero con efficacia ordinante, oltre la prospettiva condizionante esterna, bensì con efficacia ordinatrice interna.

4.2. L'atto organizzativo come insieme di istruzioni: un esperimento.

Se l'organizzazione è descrivibile come un sistema strutturato per processare informazioni e coordinare decisioni[247], allora l'adozione di un atto organizzativo algoritmico non introduce un elemento estraneo, ma può costituisce la formalizzazione in codice degli elementi fondamentali della pubblica amministrazione: il fine pubblico, la persona giuridica, l'organizzazione, l'organo[248]. La legge stabilisce quindi il fine che deve essere perseguito dall'amministrazione, ovvero l'interesse pubblico la cui tutela viene ad essa affidata, nonché i principi generali dell'organizzazione amministrativa, la cui concreta determinazione viene demandata alle singole amministrazioni[249], attribuendo all'organo di indirizzo politico e ai dirigenti il potere di determinare le

[245] M. Schuilenburg, R. Peeters, *Algorithmic Governance: Technology, Power, and Knowledge*, in *The SAGE Handbook of Digital Society*, 2023, p. 440, doi.org/10.4135/9781529783193, i quali descrivono l'uso dell'algoritmo «*as a form of 'ordering society'*». Gli Autori riassumono le diverse tendenze emerse negli studi sull'influenza degli algoritmi nel settore pubblico. Ai fini del discorso che qui si svolge emerge un concetto interessante, quello di "algocrazia", secondo cui, muovendo dalla Teoria Weberiana della burocrazia quale autorità attraverso la conoscenza per governare le persone, è possibile vedere uno spostamento dell'autorità dalla persona alla tecnologia, capace di condizionare il comportamento delle persone.

[246] V.L. Glasera, J. Sloana, J. Gehman, *op. cit.*, p. 2755.

[247] V. M. A. Valentine, A.L. Pratt, et al., *The Algorithm and the Org Chart: how algorithms can conflict with organizational structures*, in *Proceedings of the ACM on Human-Computer Interaction,* Volume 8, Issue CSCW2, 2024, p. 364:4.

[248] Tale schematizzazione vuole essere una sintesi della sequenza concettuale proposta da L.R. Perfetti, *Organizzazione amministrativa e sovranità popolare. L'organizzazione pubblica come problema teorico, dogmatico e politico*, in *Il dir. economia*, 98, 2019, p. 50 il quale individua gli elementi concettuali che compongono l'amministrazione sotto il profilo soggettivo, ossia [fine pubblico] ⊢ [persona giuridica pubblica] ⊢ [organizzazione] ⊢ [organo] ⊢[funzionario] e in senso oggettivo, ovvero [fine pubblico] ⊢ [procedimento] ⊢ [competenza] ⊢ [organo] ⊢ [decisione/volontà].

[249] L'art. 2 del d.lgs. 165/2001 (Testo Unico del Pubblico Impiego) dispone, infatti, che «Le amministrazioni pubbliche definiscono, secondo principi generali fissati da disposizioni di legge e, sulla base dei medesimi, mediante atti organizzativi secondo i rispettivi ordinamenti, le linee fondamentali di organizzazione degli uffici; individuano gli uffici di maggiore rilevanza e i modi di conferimento della titolarità dei medesimi; determinano le dotazioni organiche complessive».

scelte organizzative. Se questi concetti fondamentali possono trovare traduzione in linguaggio comprensibile dalla macchina, allora risulta possibile costruire un atto organizzativo in termini algoritmici e, astraendo, leggere l'amministrazione come sistema informatico di cui l'algoritmo sono le istruzioni per fare funzionare il sistema.

A titolo esplicativo si prenda come esempio l'obbligo introdotto nel 2024 di individuazione di un responsabile per la cybersicurezza, di cui si è discusso nel terzo capitolo. I presupposti sono stabiliti dalla l. 90/2024 e i compiti sono ivi individuati, unitamente a quelli dettagliati nel d.lgs. 138/2024. In particolare, vi sono due elementi che assumono rilievo ai fini del presente discorso: l'ambito di applicazione, ossia i soggetti destinatari di questi obblighi, e le modalità di assolvimento degli stessi a cominciare dall'individuazione di un responsabile per la cybersicurezza. Sotto tale profilo, la l. 90/2024 limita l'applicazione degli obblighi di cybersicurezza, tra gli altri soggetti, agli enti territoriali, nello specifico i Comuni, aventi popolazione superiore ai 100.000 abitanti. In secondo luogo, la legge stessa consente di individuare il referente tra i dipendenti dotati delle competenze necessarie e di comunicare tale nominativo all'Agenzia per la Cybersicurezza Nazionale[250], disponendo altresì che sia designato quale punto di contatto unico con cui questa si interfaccerà per le questioni relative alla sicurezza cibernetica, ossia segnalazione di incidenti informatici e comunicazione relative all'adempimento delle indicazioni fornite dall'Agenzia. Il d.lgs. n. 138/2024, invece, elenca i compiti del referente[251] in relazione alla gestione dei rischi per la sicurezza informatica. Per le pubbliche amministrazioni tali obblighi hanno quindi imposto all'organo politico, quale vertice dell'amministrazione, di provvedere con proprio atto al fine di assicurare la conformità dell'organizzazione alle regole stabilite dal legislatore, al ricorrere per l'ente di appartenenza delle condizioni previste dalla legge. Tale adempimento è un atto di organizzazione attribuito nello specifico dall'art. 50, comma 10 del Testo Unico del Pubblico Impiego[252] al Sindaco.

Sulla base di questo esempio, si può allora ipotizzare la traducibilità di questo atto in linguaggio eseguibile dalla macchina, per cui, definite le condizioni, essa verifichi se in

[250] Art. 8 l. 90/2024.
[251] In particolare, agli artt. 24 e 25.
[252] Ai sensi del quale «Il sindaco e il presidente della provincia nominano i responsabili degli uffici e dei servizi, attribuiscono e definiscono gli incarichi dirigenziali e quelli di collaborazione esterna secondo le modalità ed i criteri stabiliti dagli articoli 109 e 110, nonché dai rispettivi statuti e regolamenti comunali e provinciali».

concreto l'ente rientra tra i destinatari della legge e quindi produca come *output* l'atto in linguaggio naturale, consistente nella individuazione e designazione del dirigente quale referente per la cybersicurezza.
Tale algoritmo può essere strutturato nel modo seguente:

Condizioni preimpostate sulla base delle quali l'algoritmo deve fornire l'output:

- Normativa vigente: Legge 90/2024; D.Lgs. 138/2024 (NIS2)
- Obblighi di designazione imposti agli enti con >100.000 abitanti
- Il Comune di X ha popolazione superiore ai 100.000 abitanti
- Profilo professionale del personale dirigente
- Verifica RTD ex art. 17 CAD
- Piano Triennale Prevenzione Corruzione e Trasparenza
- Parere di regolarità amministrativa ex art. 147bis TUEL

Input: Determina dell'organo politico per la designazione di un responsabile per la cybersicurezza

Step 1: Estrazione dati dal dominio (informazioni ente e personale dipendente)

Step 2: Identificare gli obblighi normativi

1) Legge 90/2024 → obbligo di individuare:
   a) struttura di cybersicurezza
   b) referente per la cybersicurezza
2) D.Lgs. 138/2024 → obbligo di:
   a) nominare punto di contatto NIS2
   b) registrarsi annualmente sulla piattaforma ACN
   c) comunicare dati (art. 7) e adottare misure di sicurezza (artt. 23–25)
3) Verificare l'applicabilità delle norme sulla cybersicurezza
   a) Se Comune di X rientra tra i soggetti obbligati (popolazione > 100.000):
      → procedere con la designazione del referente e del punto di contatto
   b) Altrimenti:
      → terminare (nessun obbligo)

Step 3: Verificare i requisiti del personale disponibile

Se un dirigente possiede 'specifiche e comprovate professionalità' in cybersicurezza:

→ candidato eleggibile

Altrimenti:

→ selezionare altro profilo o attivare percorso formativo

Step 4: Valutare il dirigente individuato:

Se NC

- è Dirigente Servizio Trasformazione Digitale
- è già nominato
- ha competenze adeguate

Allora:

→ condizione per la nomina soddisfatta

Altrimenti:

→ tornare allo Step 3

Output (atto finale)

Output 1: Nomina di NC come Referente Cybersicurezza ex Legge 90/2024

Output 2: Designazione dello stesso quale Punto di Contatto NIS2 ex D.Lgs. 138/2024

Output 3: Attribuzione delle funzioni operative:

- registrazione piattaforma ACN
- adempimenti annuali (art. 7)
- attuazione misure di sicurezza
- gestione obblighi informativi verso ACN

La macchina quindi deve seguire questi passaggi nell'esecuzioni delle istruzioni ricevute, affinché venga generato il risultato atteso, in termini positivi, con conseguente nomina del dirigente, oppure in termini negativi, se l'ente è escluso tra i soggetti destinatari della legge.

In termini concreti il primo passaggio è la definizione del *domain model*, ossia la rappresentazione concettuale delle entità, delle relazioni e delle regole, che costituisce il livello del *software* che riunisce gli oggetti e la logica di dominio. Al centro del modello si trovano le classi concettuali, che rappresentano le idee o gli elementi fondamentali del vocabolario del dominio, ciascuna definibile attraverso il suo nome, la sua descrizione e

l'insieme dei casi a cui si applica[253]. Nell'esempio proposto devono quindi essere definite le condizioni e le regole sulla base delle quali il sistema deve operare, e le informazioni a cui il sistema deve accedere, secondo la seguente rappresentazione[254]:

```python
"""
ASSISTENTE NIS2 — Generatore di bozza di determina di nomina del Referente
                  per la Cybersicurezza e del Punto di Contatto NIS2
"""

from __future__ import annotations
from dataclasses import dataclass, field
from pathlib import Path
from typing import Optional
from datetime import date
import yaml


# ============================================================================
# 1. STRUTTURE DATI DI INPUT
# ============================================================================

@dataclass
class Comune:
    """Dati anagrafici dell'ente."""
    nome: str
    popolazione: int
    capoluogo_regione: bool = False
    citta_metropolitana: bool = False
    indicato_nel_dpcm_nis2: bool = False


@dataclass
class Dirigente:
    """Dati del dirigente da nominare."""
    nome: str
    ruolo: str
    competenze: set[str] = field(default_factory=set)
    # esempio: {"competenze_cyber", "esperienza_pa"}


@dataclass
class EsitiVerifiche:
    """Esiti delle verifiche procedurali. Le chiavi devono corrispondere
    ai codici definiti nel file di policy YAML."""
    esiti: dict[str, bool] = field(default_factory=dict)
```

Figura 2

Il passaggio successivo è la realizzazione di un algoritmo decisionale che, sulla base del *domain model*, ricevuto un *input*, ossia la richiesta di redigere un atto organizzativo, segua i vari passaggi di verifica, ossia se il soggetto, l'ente pubblico, sia obbligato ai sensi per legge, quale personale dipendente disponga della qualifica necessaria, oltre a verificare se il soggetto individuato sia effettivamente qualificato. Per fare ciò al

[253] C. Larman, *Applying UML And Patterns: An Introduction to object-oriented analysis and design and iterative development*, Prentice Hall, 2004, p. 136.
[254] L'algoritmo è stato realizzato col linguaggio utilizzato da Google Colab, applicativo in *cloud* di Alphabet che consente di creare ed eseguire codice Python per compiere principalmente analisi dei dati e realizzare algoritmi di *machine learning*.

modello devono essere quindi fornite informazioni ulteriori, ossia le fonti normative, nonché le policy, ovvero i regolamenti e gli atti di indirizzo. Per consentire un controllo effettivo non solo da parte del programmatore, ma anche *ex post* dall'utilizzatore, l'esempio proposto è stato implementato in linguaggio Python e si compone di un modulo principale, nonché da un insieme di file (fonti normative e policy) di configurazione utilizzando il formato YAML. Questo è un linguaggio di serializzazione per rappresentare dati strutturati in un modo facilmente comprensibile dall'uomo e interpretabile dalle macchine, consentendo agli sviluppatori e agli utenti di esprimere strutture di dati complesse in un formato simile al linguaggio naturale.

Tali istruzioni sono così riprodotte:

```python
# ============================================================================
# 2. CARICAMENTO DELLE FONTI NORMATIVE E DELLE POLICY
# ============================================================================

@dataclass
class FonteNormativa:
    """Rappresentazione strutturata di una fonte normativa caricata da YAML."""
    id: str
    denominazione: str
    titolo_breve: str
    data_vigore: str
    in_vigore: bool
    ambito_applicazione: dict
    articoli_rilevanti: list[dict]
    formula_richiamo: str

    @classmethod
    def da_yaml(cls, path: Path) -> "FonteNormativa":
        with open(path, "r", encoding="utf-8") as f:
            d = yaml.safe_load(f)
        return cls(
            id=d["id"],
            denominazione=d["denominazione"],
            titolo_breve=d["titolo_breve"],
            data_vigore=d["data_vigore"],
            in_vigore=d.get("in_vigore", True),
            ambito_applicazione=d.get("ambito_applicazione", {}),
            articoli_rilevanti=d.get("articoli_rilevanti", []),
            formula_richiamo=d.get("formula_richiamo", "").strip(),
        )

    def is_applicabile_a(self, comune: Comune) -> bool:
        """Verifica se la fonte normativa è applicabile al Comune indicato,
        in base ai criteri definiti nel file YAML."""
        if not self.in_vigore:
            return False
        criteri = self.ambito_applicazione.get("criteri_soggetto_obbligato", [])
        if not criteri:
            return True
        for criterio in criteri:
            if _soddisfa_criterio(comune, criterio):
                return True
        return False


def _soddisfa_criterio(comune: Comune, criterio: dict) -> bool:
    """Valuta un singolo criterio di applicabilità.
    Estendibile aggiungendo nuovi tipi di criterio."""
    tipo = criterio.get("tipo")

    if tipo == "soglia_popolazione":
        valore = criterio["valore"]
        operatore = criterio.get("operatore", "maggiore")
        if operatore == "maggiore":
            return comune.popolazione > valore
        if operatore == "maggiore_uguale":
            return comune.popolazione >= valore
        if operatore == "minore":
            return comune.popolazione < valore
        return False

    if tipo == "qualifica_ente":
        valore = criterio["valore"]
        if valore == "capoluogo_regione":
            return comune.capoluogo_regione
        if valore == "citta_metropolitana":
            return comune.citta_metropolitana
        if valore == "comune_obbligato_nis2":
            return comune.indicato_nel_dpcm_nis2
        return False

    if tipo == "settore":
        return False

    return False
```

Figura 3

```python
@dataclass
class PolicyInterne:
    """Policy interne dell'ente caricate da YAML."""
    id: str
    descrizione: str
    verifiche_procedurali: list[dict]
    competenze_dirigente: list[dict]
    documenti_da_allegare: list[str]

    @classmethod
    def da_yaml(cls, path: Path) -> "PolicyInterne":
        with open(path, "r", encoding="utf-8") as f:
            d = yaml.safe_load(f)
        return cls(
            id=d["id"],
            descrizione=d.get("descrizione", ""),
            verifiche_procedurali=d.get("verifiche_procedurali_richieste", []),
            competenze_dirigente=d.get("competenze_dirigente_richieste", []),
            documenti_da_allegare=d.get("documenti_da_allegare", []),
        )


def carica_fonti_normative(cartella: Path) -> list[FonteNormativa]:
    """Carica tutte le fonti normative dalla cartella indicata.
    Ogni file .yaml o .yml è interpretato come una fonte."""
    cartella = Path(cartella)
    fonti = []
    for path in sorted(cartella.glob("*.y*ml")):
        try:
            fonti.append(FonteNormativa.da_yaml(path))
        except Exception as e:
            print(f"Errore nel caricamento di {path.name}: {e}")
    return fonti
```

Figura 4

L'ulteriore passaggio è far compiere i controlli alla macchina, affinché verifichi se la normativa si applica all'amministrazione prima di generare un *output* secondo un percorso logico verificabile dall'essere umano.

```python
# ═══════════════════════════════════════════════════════════════════
# 3. ESITI DEL RAGIONAMENTO (per tracciabilità)
# ═══════════════════════════════════════════════════════════════════

@dataclass
class EsitoApplicabilita:
    """Risultato della valutazione di applicabilità delle fonti normative
    al caso concreto. Il funzionario può ispezionare questo oggetto per
    verificare il ragionamento dell'assistente."""
    fonti_applicabili: list[FonteNormativa]
    fonti_non_applicabili: list[FonteNormativa]
    motivo_non_obbligo: Optional[str] = None

    @property
    def comune_soggetto_obbligato(self) -> bool:
        fonti_settoriali = [
            f for f in self.fonti_applicabili
            if f.ambito_applicazione.get("criteri_soggetto_obbligato")
        ]
        return len(fonti_settoriali) > 0


def valuta_applicabilita(
    comune: Comune,
    fonti: list[FonteNormativa],
) -> EsitoApplicabilita:
    """Determina quali fonti normative si applicano al Comune."""
    applicabili = [f for f in fonti if f.is_applicabile_a(comune)]
    non_applicabili = [f for f in fonti if not f.is_applicabile_a(comune)]
    return EsitoApplicabilita(
        fonti_applicabili=applicabili,
        fonti_non_applicabili=non_applicabili,
    )


@dataclass
class EsitoVerificheProcedurali:
    """Risultato del controllo sulle verifiche procedurali richieste
    dalle policy interne."""
    tutte_le_obbligatorie_ok: bool
    verifiche_mancanti: list[str]
    verifiche_completate: list[str]

```

Figura 5

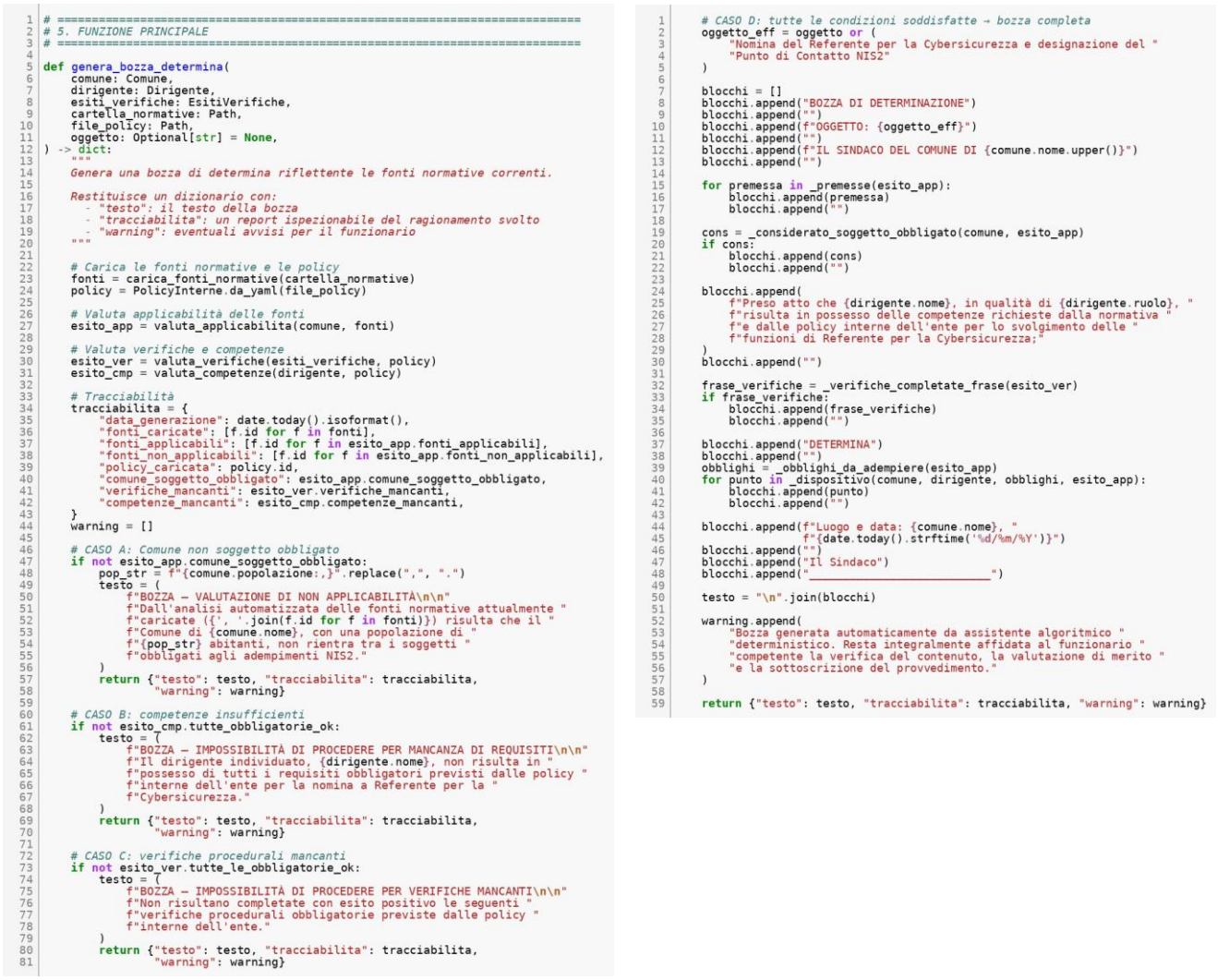
```python
def valuta_verifiche(
    esiti: EsitiVerifiche,
    policy: PolicyInterne,
) -> EsitoVerificheProcedurali:
    """Controlla gli esiti delle verifiche rispetto alle policy."""
    mancanti = []
    completate = []
    for v in policy.verifiche_procedurali:
        codice = v["codice"]
        if v.get("obbligatoria", False):
            if not esiti.esiti.get(codice, False):
                mancanti.append(v["descrizione"])
            else:
                completate.append(v["formula_richiamo"])
        else:
            if esiti.esiti.get(codice, False):
                completate.append(v["formula_richiamo"])
    return EsitoVerificheProcedurali(
        tutte_le_obbligatorie_ok=(len(mancanti) == 0),
        verifiche_mancanti=mancanti,
        verifiche_completate=completate,
    )


@dataclass
class EsitoCompetenze:
    """Risultato della verifica delle competenze del dirigente."""
    tutte_obbligatorie_ok: bool
    competenze_mancanti: list[str]


def valuta_competenze(
    dirigente: Dirigente,
    policy: PolicyInterne,
) -> EsitoCompetenze:
    mancanti = []
    for c in policy.competenze_dirigente:
        codice = c["codice"]
        if c.get("obbligatoria", False) and codice not in dirigente.competenze:
            mancanti.append(c["descrizione"])
    return EsitoCompetenze(
        tutte_obbligatorie_ok=(len(mancanti) == 0),
        competenze_mancanti=mancanti,
    )
```

Figura 6

L'ulteriore passaggio necessario è la produzione di un testo in linguaggio naturale contenente un atto organizzativo che venga adottato dall'organo politico. Pertanto devono essere fornite precise istruzioni alla macchina, affinché l'*output* rispetti la struttura di questo tipo di atti; per farlo alla macchina deve essere data l'istruzione corretta, ossia fornire il codice che indichi la struttura di base di questo tipo di provvedimento, prima dell'esecuzione.



```python
# ============================================================================
# 5. FUNZIONE PRINCIPALE
# ============================================================================

def genera_bozza_determina(
    comune: Comune,
    dirigente: Dirigente,
    esiti_verifiche: EsitiVerifiche,
    cartella_normative: Path,
    file_policy: Path,
    oggetto: Optional[str] = None,
) -> dict:
    """
    Genera una bozza di determina riflettente le fonti normative correnti.

    Restituisce un dizionario con:
      - "testo": il testo della bozza
      - "tracciabilita": un report ispezionabile del ragionamento svolto
      - "warning": eventuali avvisi per il funzionario
    """

    # Carica le fonti normative e le policy
    fonti = carica_fonti_normative(cartella_normative)
    policy = PolicyInterne.da_yaml(file_policy)

    # Valuta applicabilità delle fonti
    esito_app = valuta_applicabilita(comune, fonti)

    # Valuta verifiche e competenze
    esito_ver = valuta_verifiche(esiti_verifiche, policy)
    esito_cmp = valuta_competenze(dirigente, policy)

    # Tracciabilità
    tracciabilita = {
        "data_generazione": date.today().isoformat(),
        "fonti_caricate": [f.id for f in fonti],
        "fonti_applicabili": [f.id for f in esito_app.fonti_applicabili],
        "fonti_non_applicabili": [f.id for f in esito_app.fonti_non_applicabili],
        "policy_caricata": policy.id,
        "comune_soggetto_obbligato": esito_app.comune_soggetto_obbligato,
        "verifiche_mancanti": esito_ver.verifiche_mancanti,
        "competenze_mancanti": esito_cmp.competenze_mancanti,
    }
    warning = []

    # CASO A: Comune non soggetto obbligato
    if not esito_app.comune_soggetto_obbligato:
        pop_str = f"{comune.popolazione:,}".replace(",", ".")
        testo = (
            f"BOZZA – VALUTAZIONE DI NON APPLICABILITÀ\n\n"
            f"Dall'analisi automatizzata delle fonti normative attualmente "
            f"caricate ({', '.join(f.id for f in fonti)}) risulta che il "
            f"Comune di {comune.nome}, con una popolazione di "
            f"{pop_str} abitanti, non rientra tra i soggetti "
            f"obbligati agli adempimenti NIS2."
        )
        return {"testo": testo, "tracciabilita": tracciabilita,
                "warning": warning}

    # CASO B: competenze insufficienti
    if not esito_cmp.tutte_obbligatorie_ok:
        testo = (
            f"BOZZA – IMPOSSIBILITÀ DI PROCEDERE PER MANCANZA DI REQUISITI\n\n"
            f"Il dirigente individuato, {dirigente.nome}, non risulta in "
            f"possesso di tutti i requisiti obbligatori previsti dalle policy "
            f"interne dell'ente per la nomina a Referente per la "
            f"Cybersicurezza."
        )
        return {"testo": testo, "tracciabilita": tracciabilita,
                "warning": warning}

    # CASO C: verifiche procedurali mancanti
    if not esito_ver.tutte_le_obbligatorie_ok:
        testo = (
            f"BOZZA – IMPOSSIBILITÀ DI PROCEDERE PER VERIFICHE MANCANTI\n\n"
            f"Non risultano completate con esito positivo le seguenti "
            f"verifiche procedurali obbligatorie previste dalle policy "
            f"interne dell'ente."
        )
        return {"testo": testo, "tracciabilita": tracciabilita,
                "warning": warning}
```

```python
    # CASO D: tutte le condizioni soddisfatte → bozza completa
    oggetto_eff = oggetto or (
        "Nomina del Referente per la Cybersicurezza e designazione del "
        "Punto di Contatto NIS2"
    )

    blocchi = []
    blocchi.append("BOZZA DI DETERMINAZIONE")
    blocchi.append("")
    blocchi.append(f"OGGETTO: {oggetto_eff}")
    blocchi.append("")
    blocchi.append(f"IL SINDACO DEL COMUNE DI {comune.nome.upper()}")
    blocchi.append("")

    for premessa in _premesse(esito_app):
        blocchi.append(premessa)
        blocchi.append("")

    cons = _considerato_soggetto_obbligato(comune, esito_app)
    if cons:
        blocchi.append(cons)
        blocchi.append("")

    blocchi.append(
        f"Preso atto che {dirigente.nome}, in qualità di {dirigente.ruolo}, "
        f"risulta in possesso delle competenze richieste dalla normativa "
        f"e dalle policy interne dell'ente per lo svolgimento delle "
        f"funzioni di Referente per la Cybersicurezza;"
    )
    blocchi.append("")

    frase_verifiche = _verifiche_completate_frase(esito_ver)
    if frase_verifiche:
        blocchi.append(frase_verifiche)
        blocchi.append("")

    blocchi.append("DETERMINA")
    blocchi.append("")
    obblighi = _obblighi_da_adempiere(esito_app)
    for punto in _dispositivo(comune, dirigente, obblighi, esito_app):
        blocchi.append(punto)
        blocchi.append("")

    blocchi.append(f"Luogo e data: {comune.nome}, "
                   f"{date.today().strftime('%d/%m/%Y')}")
    blocchi.append("")
    blocchi.append("Il Sindaco")
    blocchi.append("_____")

    testo = "\n".join(blocchi)

    warning.append(
        "Bozza generata automaticamente da assistente algoritmico "
        "deterministico. Resta integralmente affidata al funzionario "
        "competente la verifica del contenuto, la valutazione di merito "
        "e la sottoscrizione del provvedimento."
    )

    return {"testo": testo, "tracciabilita": tracciabilita, "warning": warning}
```

Figura 7

Sulla base dell'esempio proposto, il risultato sarà quindi un testo in linguaggio naturale contenente una determina del Sindaco con cui viene nominato il referente della cybersicurezza e punto di contatto NIS per il Comune destinatario di tale obbligo ai sensi della l. 90/2024. E un algoritmo con questa struttura risulta essere potenzialmente utilizzabile per la redazione di altri atti simili, adattandolo al quadro normativo di volta in volta rilevante e modificando i dati di riferimento su cui deve lavorare.

L'esempio qui riportato può essere ricondotto alla categoria degli algoritmi deterministici o condizionali. Il sistema opera infatti sulla base di regole predeterminate, per cui dato un determinato *input*, ossia i dati del Comune, quelli del dirigente designato, gli esiti delle verifiche procedurali e, specialmente le fonti normative caricate nei file di configurazione, viene prodotta una bozza di provvedimento, ovvero un

risultato verificabile in quanto è possibile controllare la sequenza del ragionamento seguito dalla macchina.

Sotto questo profilo non si tratta quindi di un algoritmo in grado di apprendere, ma alla modifica dei parametri normativi, ossia ad esempio in caso di novella normativa, il sistema leggerà le nuove regole applicandole.

L'esempio presentato rivela come la predisposizione di atti organizzativi possa essere formalizzata in termini di codice, la cui struttura rimane immutata, cambiando le fonti di riferimento, ovvero la normativa rilevante, a seconda delle circostanze; come farebbe un dirigente o l'organo politico. In questi termini, l'automazione può inserirsi nel processo decisionale dell'ente, in conformità ai richiamati principi specialmente in materia di IA nella pubblica amministrazione, e quindi il principio della riserva di umanità e di imputabilità della decisione.

In una prospettiva futura, simili strumenti potrebbero essere implementati anche per apprendere dal contesto in cui operano individuando le soluzioni migliori per l'organizzazione, ed in questi termini può essere immaginata la macchina che si inserisce nel processo decisionale, determinando la struttura organizzativa, attraverso la ridefinizione dei ruoli e dei compiti o anche semplicemente dei processi interni e la composizione degli uffici a seconda delle esigenze emergenti al mutare del contesto normativo. In ogni caso l'effettiva decisione organizzativa dovrà comunque essere fatta propria dall'essere umano.

Sulla base dell'esperimento proposto è possibile ritenere il potere ordinante dell'algoritmo all'interno di un'organizzazione. Esso seleziona quali siano i dati ovvero le informazioni rilevanti, rispetto al compito richiesto, stabilisce quindi, sulla base di regole, più o meno rigide, quale risposta o decisione generare. In questi termini ha il potenziale di ordinare flussi o distribuzione del lavoro in maniera efficiente, in tanto in quanto dispone in via immediata di un maggiore numero di informazioni.

Nell'esperimento si è proposto un algoritmo deterministico poiché risulta maggiormente applicabile nei termini descritti, tuttavia in una prospettiva evolutiva, è certamente immaginabile una versione basata su tecniche di *machine learning*, ad esempio mediante l'affinamento di un *Large Language Model* su precedenti atti organizzativi, che quindi apprenda dalle scelte eseguite in passato e adattare la risposta al contesto.

In questi termini allora può essere vista la forza ordinante dell'intelligenza artificiale, come capacità di incidere non sull'azione dell'organizzazione, ma sulla sua struttura e funzionamento interni.

5. L'organizzazione e la necessità di nuove figure professionali per la pubblica amministrazione.

L'esperimento illustrato nel precedente paragrafo offre una prospettiva su un possibile impiego di strumenti tecnici in una prospettiva differente, ovvero tesa a migliorare prima di tutto l'amministrazione al suo interno, al fine di affrontare, in primo luogo, le numerose prescrizioni e obblighi richiesti dalla legge proprio nel settore della digitalizzazione, ma anche gestire i processi evolutivi della società, che riguardano e incidono anche sulla pubblica amministrazione, nella prospettiva di una trasformazione con (o grazie a) l'intelligenza artificiale.

L'ipotesi è di un connubio tra capitale umano e tecnologia, anche se è innegabile il carico di adempimenti a cui deve far fronte un'amministrazione, che intenda adottare strumenti di IA anche solamente per l'organizzazione interna. Infatti, anche l'impiego interno di essi, sono comunque necessarie valutazioni d'impatto interne e formazione del personale, nonché trasparenza, con ruolo attivo e continuo del DPO nell'intero processo decisionale[255].

Un tanto è ancora più necessario in ragione degli obblighi previsti, in particolare, dall'art. 27, par. 1 dell'*AI Act*, per cui «i *deployer* che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i *deployer* di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre». Gli enti pubblici sono nello specifico chiamati a svolgere una valutazione d'impatto sui diritti fondamentali (per i sistemi ad alto rischio) che comprenda contesto d'uso, durata, soggetti coinvolti, rischi, sorveglianza umana, misure correttive e *governance* in ambito operativo, similmente a quanto già previsto dall'art. 35 del GDPR.

[255] Cfr. Bollettino n. 12, *Pillole di innovazione. Intelligenza artificiale e pubblica amministrazione, dicembre 2025*, pubblicato nell'ambito del progetto "Province&Comuni".

Conseguentemente le organizzazioni interessate ad implementare sistemi di IA al proprio interno sono onerate anche dall'assolvimento del *fundamental rights impact assessment* (o FRIA), oltre a quello già previsto in materia di protezione dei dati personali, il DPIA (*data protection impact assessment*), in tanto in quanto trattasi pur sempre di strumenti che vanno ad incidere sulla vita degli individui, e, nel presente ragionamento, sui dipendenti dell'ente. Poiché si tratterebbe comunque di produrre un provvedimento con effetti sulle persone, nello specifico dipendenti dell'amministrazione. Conseguentemente, sarebbero necessarie quelle figure e quegli adempimenti di cui l'amministrazione si deve dotare, adeguando la struttura al quadro normativo, ovvero esattamente quello che il prototipo proposto mira a fare.

È vero, tuttavia, come sia auspicabile una diffusione di questi strumenti, anche attraverso il miglioramento degli stessi, come proposto in alcuni studi incentrati sull'incremento della qualità dei risultati dei *large language models*, perché possano operare in ambiti specifici, definiti *domain specific large language models*, ovvero modelli linguistici addestrati sulla base di uno specifico dominio della conoscenza[256]. Questo tipo di approccio consente di adattare la potenza di questi modelli agli specifici contesti in cui sono chiamati ad operare per produrre risultati qualitativamente superiori[257]. Nell'esempio fatto, la base della conoscenza è costituita non solo dalla legge, ma dalle informazioni relative al personale, le risorse strumentali ed economiche dell'ente, nonché gli atti di programmazione che costituiscono i documenti fondamentali per l'attività dell'ente, sulla quale è possibile addestrare un modello, affinché tratte le informazioni fondamentali possa determinare quali scelte gli organi di vertice devono adottare[258].

---

[256] Z. Song, R. Zhao, et. al., *Injecting Domain-Specific Knowledge into Large Language Models: A Comprehensive Survey*, in *arXiv*, 2025, p. 2-3. Gli autori descrivono il dominio specifico della conoscenza come «*[a] specialized information or expertise pertinent to a specific field or application, distinguishing it from general knowledge that spans across multiple domains. While general knowledge enables models to understand broad contexts, domain-specific knowledge is essential for addressing specialized tasks where precise, field-specific understanding is required»,* distinguendo due momenti in cui questo miglioramento del modello possa avvenire: «*Static Knowledge Injection and Modular Knowledge Adapters integrate knowledge prior to inference and involve parameter updates—through either full fine-tuning or adapter-based tuning. In contrast, Dynamic Knowledge Injection and Prompt Optimization inject knowledge at inference time without altering model parameters: the former retrieves external information, while the latter leverages internal knowledge through designed prompts*».

[257] Cfr. C. Ling, Z. Zhao, et al., *Domain Specialization as the Key to Make Large Language Models Disruptive: A Comprehensive Survey*, in *ACM Computing Surveys*, 2025, consultabile al seguente link dl.acm.org/doi/10.1145/3764579.

[258] In base alla distinzione sancita dalla legge tra politica e amministrazione, per cui l'organo politico è titolare del potere di indirizzo, ovvero di definizione degli obiettivi, di programmazione e di

Invero, tale impiego sarebbe comunque astrattamente conforme ai principi ordinanti dell'organizzazione amministrativa[259]. Parimenti il potere organizzativo non verrebbe sottratto al soggetto titolare, il quale assumerebbe comunque la paternità della decisione e ne rimarrebbe comunque responsabile.

Un ulteriore aspetto da considerare è ovviamente quello tecnico. Poiché infatti un problema molto discusso sono i *bias*, è necessario prevedere una *governance* del sistema, dalla progettazione al suo impiego.

Sotto questo profilo è interessante lo standard proposto dal *National Institute of Standard Technologies* che ho delineato un modello di gestione del ciclo di vita dei sistemi di IA diviso in quattro fasi: *pre-design*, *design and development*, *deployment stage*, *test and evaluation*[260]. Nella proposta, il ciclo di vita dei sistemi di IA è concepito come un processo iterativo, in cui decisioni iniziali, selezione dei dati, progettazione, test continui, monitoraggio e coinvolgimento di più *stakeholder* sono determinanti per individuare e mitigare i *bias*, prevenendo effetti indesiderati lungo l'intero sviluppo e utilizzo del modello.

Per queste ragioni, appare certamente necessario il ricorso a nuove figure di esperti al servizio della pubblica amministrazione che si voglia dotare di strumenti di automazione, con relativa perdita dei lavori considerati non più necessari perché sostituiti dalla tecnologia[261]. Sul punto le Linee guida elencano una serie di figure tecniche ritenute rilevanti per la gestione del ciclo di vita dei sistemi di IA, non solo

---

monitoraggio/verifica dei risultati raggiunti, attraverso atti quali regolamenti, atti programmatori e finanziari. Mentre spetta alla dirigenza l'adozione di atti amministrativi e di gestione interna ed esterna all'ente, compresa l'organizzazione e la gestione delle risorse umane e strumentali (artt. 16 e 17, d.lgs. n. 165/2001).

[259] Invero, tale impiego degli algoritmi sembra comunque poter astrattamente rispettare i criteri cui deve conformarsi l'organizzazione amministrativa, ossia buon andamento, imparzialità ed efficienza, a mente del fatto che ben si può affermare sulla base della rigida logica su cui vengono eseguiti, che garantiscano una maggiore imparzialità e un buon andamento.
Tuttavia, le problematicità rilevate nella letteratura, circa l'importanza della qualità dei dati immessi e gli accorgimenti stessi adottati nella costruzione del codice al fine di evitare *bias* possono determinare il replicarsi di situazioni discriminatorie verificatesi in passato; sul punto cfr. B. Ponti, *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in *Riv. it. infor. dir.*, 2, 2024, p. 522.

[260] R. Schwartz, A. Vassilev, et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, *NIST special publication 1270*, *National Institute of Standard Technologies*, 2022, p. 13, https://doi.org/10.6028/NIST.SP.1270, in cui si aggiunge «Le organizzazioni sono incoraggiate a svolgere attività continue di test e valutazione di tutti i componenti e delle funzionalità dei sistemi di IA in cui i bias possano contribuire a impatti dannosi. Ad esempio, se durante il deployment il modello viene riaddestrato con nuovi dati per uno specifico contesto, il *deployer* dovrebbe collaborare con il produttore del modello per valutare le prestazioni effettive ai fini dell'analisi dei *bias*».

[261] Cfr. OECD Report, *G7 Toolkit for Artificial intelligence in the Public sector*, p. 54

ingegneristiche ma anche di giuristi esperti del settore[262]. Alcune di queste figure sono state individuate ufficialmente con la pubblicazione della norma UNI[263] 11621-8:2026, con la quale vengono descritti i profili professionali nell'ambito dell'intelligenza artificiale, definendo i ruoli e i compiti di ciascuna figura al fine di offrire un quadro di riferimento condiviso da tutti gli operatori del settore.

Accanto ai professionisti specificamente preposti al funzionamento del sistema di IA, la norma UNI indentifica quelli necessari per il suo impiego effettivo, tra cui l'esperto di sicurezza, in grado non solo di analizzare e prevenire le possibili minacce informatiche ma capace anche di coniugare il tema della *cyber security* all'intelligenza artificiale, garantendo difese sempre più efficienti ed in grado di adattarsi autonomamente alle minacce esterne.

L'innesto di nuove figure professionali e la possibilità di adottare soluzioni di intelligenza artificiale aprono certamente nuovi scenari per la Pubblica amministrazione, poiché l'autonomia operativa e, in prospettiva, la capacità di adattamento del sistema alle esigenze dell'ente, permettono un livello di automazione non limitato a singoli compiti o attività specifiche, incidendo profondamente sull'organizzazione del settore pubblico. Il ruolo di personale esperto permetterebbe quindi non solo di pensare un

[262] Il documento richiama lo standard ISO/IEC 42001 secondo cui servono figure professionali diversificate per competenze in funzione delle diverse fasi ciclo di vita dell'AI, così come per garantire l'adeguata rappresentatività con riferimento ai dati usati per l'addestramento dei modelli di *machine learning*, e menziona tra quelle ritenute più critiche il *data engineer*, un esperto nella progettazione, nello sviluppo e nella gestione dei dati che si occuperà di garantire che i dati vengano raccolti, raffinati e resi disponibili in maniera efficiente e affidabile, il *machine learning engineer*, un esperto in algoritmi di machine learning e di programmazione in grado di progettare, implementare e ottimizzare algoritmi di machine learning fondamentali per il corretto funzionamento dei servizi digitali sviluppati con questa tecnologia; il *prompt engineer*, l'esperto che istruisce l'IA generativa alla produzione di output efficaci, secondo le indicazioni ricevute. Ma vi è anche l'*AI architect*, un esperto in grado di valutare e progettare l'architettura dei sistemi di intelligenza artificiale assicurando che siano scalabili, sicuri e performanti. All'occorrenza, questo esperto collabora nell'integrazione dell'IA nelle infrastrutture esistenti. La scelta dell'architettura influenza la realizzazione della soluzione *software* incidendo su tempi, costi e prestazioni. Altre figure individuate sono l'*AI ethics expert* e quella del giurista esperto di sistemi di IA.
Cfr. sul punto M. C. Pollicino, *Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa*, in *Riv. it. infor. dir*., 1, 2025, p. 25, la quale evidenzia che «Allo stesso tempo, l'art. 35 GDPR prevede che quando il trattamento di dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, soprattutto allorquando il rischio sia connesso all'uso di nuova tecnologia, è obbligatorio effettuare la valutazione di impatto dei diritti fondamentali (in inglese *Data Protection Impact Assessment*, in breve DPIA). […] Tra i trattamenti, che necessitano della DPIA, […] vi sono: (i) trattamenti valutativi o di scoring, compresa la profilazione; (ii) decisioni automatizzate che producono significativi effetti giuridici (es.: assunzioni, concessione di prestiti, stipula di assicurazioni); (iii) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative».

[263] Una norma UNI non ha forza di legge, ma è uno standard tecnico elaborato e pubblicato dall'Ente Italiano di Normazione, un'associazione senza scopo di lucro riconosciuta dall'Italia e dall'Unione europea che pubblica standard tecnici di ausilio agli operatori di diversi settori.

sistema adatto alle esigenze dell'ente, ma garantire un costante monitoraggio dello stesso, assicurando la tracciabilità delle azioni, oltre ad un costante *auditing*,[264].

Dei fattori considerati fino a qui, quello maggiormente rilevante risulta infatti essere l'acquisizione di nuove competenze all'interno dell'organizzazione anche attraverso il reclutamento di figure professionali[265].

6. La responsabilità amministrativo-contabile del dipendente pubblico tra protezione dei dati personali e intelligenza artificiale.

La questione delle competenze del personale dipendente, anche nella prospettiva dell'adozione di atti elaborati dall'intelligenza artificiale, emerge anche sotto un'altra prospettiva, ossia quella della responsabilità amministrativo-contabile del funzionario[266], che utilizza strumenti di IA.

Il tema emerge a partire dalla lettura del Regolamento (UE) 2024/1689 ove viene indicato ai *deployer* gli obblighi cui devono conformarsi, includendo tra essi anche le pubbliche amministrazioni intenzionate ad usare sistemi di IA, con conseguente responsabilità dei funzionari[267]. Lo stesso risulta dalla legge n. 132/2025, in cui viene sancito l'utilizzo dell'intelligenza artificiale in termini di ausilio all'attività provvedimentale, senza che essa possa mai sostituire il potere decisionale e la responsabilità della persona fisica preposta (art. 14, co. 3)[268].

La volontà di responsabilizzare le pubbliche amministrazioni emerge anche nelle Linee guida per l'adozione dell'intelligenza artificiale nella pubblica amministrazione AgID ha indicato l'assolvimento dell'obbligo di Valutazione d'impatto sulla protezione dei

[264] C. Schmitz, J. Rystrøm, J. Batzne, *Oversight structures for agentic ai in public-sector organizations*, in *arXiv*, 2025, p. 4.

[265] M. Falcone, *La data science come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni*, in *Riv. it. infor. dir.*, p. 538.

[266] L. Schavello, *Responsabilità contabile formale e amministrativa*, Jovene, Napoli, 1987; F.G. Scoca (a cura di), *La responsabilità amministrativa ed il suo processo*, CEDAM, Padova, 1997; P. Maddalen, *La sistemazione dogmatica della responsabilità amministrativa*, in *Lexitalia*, 1, 2022; E.F. Schlitzer, C. Mirabelli (a cura di), *Trattato sulla nuova configurazione della giustizia contabile, Editoriale scientifica*, Napoli, 2018.

[267] Cfr. *supra* capitolo 2 par. 3.

[268] Così all'art. 3 comma 3 si stabilisce che i sistemi e i modelli di intelligenza artificiale per finalità generali devono essere applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità. Cfr. S. Ariota, *L'intelligenza artificiale: la nuova frontiera del controllo amministrativo-contabile*, in *Quad. Corte Conti*, 6, 2025, p. 121.

dati (DPIA dall'inglese *Data Protection Impact Assessment*) per i sistemi ad alto rischio e la formazione continua del personale quale condizione imprescindibile per un utilizzo responsabile[269].

Il tema è di rilevante centralità poiché, dall'utilizzo di strumenti di automazione possono, in primo luogo, derivare conseguenze dirette sulle casse pubbliche, come ad esempio in caso di erogazione di contributi decisa dall'IA[270], ma anche, in caso di inosservanza della normativa menzionata, possono scaturire conseguenze per le amministrazioni, in termini di provvedimenti sanzionatori irrogate dalle autorità di vigilanza preposte[271] In entrambi i casi ne discende la responsabilità amministrativo-contabile del dipendente pubblico.

Questa seconda ipotesi di origine della responsabilità può trovare riscontro nel concreto, prendendo in considerazione la giurisprudenza della Corte dei Conti che riconduce alla responsabilità contabile le condotte dei dipendenti pubblici che abbiano determinato l'irrogazione di sanzioni da parte del Garante per la protezione dei dati personali a carico dell'amministrazione di appartenenza. In tal senso si pongono le sentenze della Corte dei Conti, Sezione giurisdizionale di Bolzano, 9 gennaio 2024 n. 1 della Corte dei Conti, Sezione giurisdizionale per la Regione Valle d'Aosta, 12 agosto 2025 n. 36 e della Corte dei Conti, Sezione giurisdizionale per la Regione Emilia-Romagna 18 febbraio 2026 n. 29. In tutti questi casi funzionari e dirigenti pubblici sono stati chiamati a rispondere del danno erariale indiretto conseguente al pagamento di sanzioni inflitte per illecita diffusione di dati personali sulla pagina web istituzionale o per inosservanza delle prescrizioni del Garante o per illecito trattamento dei dati dei dipendenti[272]. Si tratta di vicende con profili diversi, ma tutte incentrate sulla mancata osservanza del GDPR, da cui è derivata una sanzione per le amministrazioni.

In particolare, nel caso sottoposto al giudizio della Corte dei Conti di Bolzano trae origine dalla sanzione pecuniaria inflitta dal Garante per la protezione dei dati personali al Comune di Bolzano per violazioni sistematiche della disciplina sulla tutela dei dati

[269] S. Ariota, *op. cit.*, p. 122.

[270] Sul punto v. N.M. Tritto, *Il danno erariale da intelligenza artificiale*, in *Federalismi.it*, 2, 2024, p. 296, il quale, in considerazione della atipicità della fattispecie, enuncia le varie ipotesi in cui potrebbe verificarsi un danno erariale per la pubblica amministrazione nel caso di impiego di sistemi di IA.

[271] A titolo esemplificativo, le sanzioni irrogabili dall'ACN alle amministrazioni che non si conformano agli obblighi in materia di cybersicurezza.

[272] Corte Conti, sez. giurisdiz., Valle d'Aosta 12 agosto 2025 n. 36; Corte Conti, sez. giurisdiz., Emilia-Romagna 18 febbraio 2026 n. 29.

personali (ossia Reg. UE 2016/679 e Codice della *privacy*). Le violazioni riguardavano, da un lato, la raccolta e conservazione dei dati di navigazione Internet dei dipendenti, effettuata in assenza di idonea informativa, e, dall'altro, l'utilizzo di modulistica per l'accesso a servizi di assistenza psicologica che comportava la conoscenza indebita di dati sensibili da parte dei dirigenti responsabili.

Sul piano della responsabilità, il Collegio in capo alla funzionaria dirigente ha riconosciuto l'esistenza di obblighi specifici di vigilanza e di coordinamento in materia di protezione dei dati, discendenti dagli atti di nomina, che le attribuivano compiti di predisposizione, approvazione e aggiornamento della regolamentazione interna. Le omissioni contestate, riguardanti trattamenti di carattere massivo e di evidente impatto sui diritti dei dipendenti, sono state ritenute causalmente collegate alla sanzione comminata dal Garante.

Invece, nella vicenda portata all'attenzione Corte dei Conti della Valle d'Aosta, il Collegio ha ravvisato la colpa grave nel comportamento del dirigente competente alla pubblicazione delle deliberazioni di Giunta, il quale non solo aveva omesso di adempiere alle prescrizioni del Garante, ma aveva reiteratamente insistito sulla legittimità di modalità di pubblicazione, senza anonimizzazione, espressamente censurate dall'autorità di controllo, opponendosi alle indicazioni ricevute e contestando in sede di giudizio di responsabilità l'indeterminatezza delle stesse[273].

Queste pronunce risultano di particolare interesse, in particolare ai fini della presente ricerca, in quanto, rivelano come l'orientamento giurisprudenziale si rivolga per una struttura della responsabilità erariale che, nei casi di violazione della normativa sulla *privacy*, prescinda dalla complessità tecnica della condotta e si appunta sull'elemento della consapevolezza, ovvero richiama il dipendente alla conoscenza e corretta applicazione della normativa sulla protezione dei dati personali, senza poter invocare la frammentazione delle competenze organizzative interne. In particolare, la vicenda decisa dalla Corte dei Conti di Bolzano rileva altresì come è il dirigente o comunque il capo dell'ufficio il soggetto chiamato ad esprimere maggiore competenza e vigilanza.

Sembra, allora, corretto ritenere che qualora l'ente utilizzi sistemi di IA, il funzionario soggiace ai diversi obblighi, dalla selezione dei dati, al controllo su tutto il ciclo di vita del sistema, alla trasparenza della decisione, sino alla verifica del risultato prodotto (che

[273] V. Corte dei Conti, sez. giurisdiz. Regione Valle d'Aosta, n. 36/2025.

come visto si complica nel momento in cui vengono impiegati algoritmi di *machine learning*). Se dunque al funzionario sono attribuiti determinati obblighi similmente a quanto visto nelle richiamate vertenze decise da diverse sezioni giurisdizionali della Corte dei Conti, può configurarsi una responsabilità dell'amministrazione per i danni cagionati da provvedimenti adottati tramite questi strumenti e correlativamente una responsabilità amministrativa da danno erariale[274].

In tale senso, la decisione della Corte dei Conti di Bolzano risulta particolarmente interessante, poiché la violazione del GDPR era avvenuta nei confronti dei dipendenti dell'ente. Pertanto, qualora l'amministrazione intenda impiegare l'intelligenza artificiale con finalità interna, come nel caso dell'atto organizzativo di cui all'esperimento fatto nel presente capitolo, la violazione delle norme dell'*AI Act* potrebbe portare a sanzioni da parte delle autorità di vigilanza, con conseguente danno per l'ente.

Quanto detto trova conferma nell' «Ipotesi di Contratto Collettivo Nazionale di Lavoro[275] relativo al personale del comparto funzioni centrali, triennio 2025 – 2027» in cui per la prima volta viene inserito un titolo apposito dedicato all'impiego di sistemi di IA in ambito lavorativo, prevedendo norme a tutela del lavoratore dipendente, tra cui il diritto di conoscere in forma comprensibile i criteri di funzionamento dei sistemi di IA incidenti sulla valutazione della prestazione e sull'assegnazione dei compiti. Inoltre viene prevista l'istituzione di un Organismo paritetico per l'innovazione che monitori l'impatto dell'IA sull'organizzazione del lavoro e sulle professionalità.

Nel solco della giurisprudenza contabile richiamata, emerge inoltre un ulteriore potenziale fonte di responsabilità, derivante dal nesso tra dati personali e intelligenza artificiale, atteso che l'acquisizione di dati tramite strumenti di IA in maniera non conforme al GDPR dà luogo a violazione delle norme sulla *privacy*, e può determinare *output* viziati. Tale profilo di rischio è reso ancor più evidente dalla circostanza che le linee guida AgID impongono espressamente l'integrazione tra sistemi di IA e normativa sulla protezione dei dati, incluso il GDPR, riconoscendo che la violazione di tali prescrizioni da parte del funzionario responsabile può costituire condotta gravemente negligente idonea a fondare la responsabilità erariale.

[274] S. Cimini, *La responsabilità civile e amministrativa di fronte alle sfide dell'intelligenza artificiale*, in *Ceridap*, 1, 2026, p. 38.
[275] Pubblicata da ARAN il 9 giugno 2026.

Nondimeno, come è stato osservato[276], risulta particolarmente complessa la configurabilità della responsabilità contabile del dipendente, specialmente nel caso di impiego di sistemi come quelli di IA generativa, connotati dall'opacità algoritmica, che richiederebbe una verifica del percorso logico seguito dalla macchina (cosa non possibile), e parimenti imporrebbe di imputare la condotta lesiva in capo al funzionario solo in caso di comportamento negligente, potenzialmente privo di competenze tecniche adeguate, diversamente risulta arduo l'accertamento della sussistenza dell'elemento soggettivo della colpa grave, specie alla luce della recente riforma della Corte dei Conti, introdotta dalla l. 7 gennaio 2026, n. 1, con cui è stata modificata la nozione di colpa grave[277].

La prospettiva dunque è quella secondo cui, alla luce del principio dello *human in the loop* sancito dall'*AI Act* e quello di responsabilità delle decisioni algoritmiche[278], il funzionario dovrà prestare particolare attenzione in fase di scelta del sistema di IA da utilizzare, assicurando il rispetto degli obblighi per i *deployer* (tra cui trasparenza e sicurezza cibernetica) atteso che in caso di violazione degli stessi, si avrebbe quella violazione manifesta di norme di diritto che la legge n. 1/2026 individua come nucleo tipizzato della colpa grave.

La responsabilità amministrativo-contabile tende allora a concentrarsi sulle fasi endoprocedimentali che precedono la decisione algoritmica, a partire dalla scelta del sistema di IA, ovvero come è stato costruito a partire dalla selezione dei dati di addestramento, fino alla realizzazione del modello[279] assicurando il controllo umano effettivo[280] nonché il principio di trasparenza.

Appare quindi evidente come si aprano ulteriori ipotesi di responsabilità di cui il funzionario deve tenere conto. Parimenti l'amministrazione nel suo complesso si espone a rischi di responsabilità, che come già visto abbracciano numerosi aspetti, dalla protezione dei dati alla cybersicurezza.

---

[276] P. Evangelista, *Intelligenza artificiale e responsabilità amministrativo-contabile*, in *Quad. Corte conti*, 2, 2024, p. 141; S. Cimini, *op. cit.*, p. 51.

[277] L'art. 1 modificando l'art. 1 della legge 14 gennaio 1994, n. 20 prevede che «Costituisce colpa grave la violazione manifesta delle norme di diritto applicabili, il travisamento del fatto, l'affermazione di un fatto la cui esistenza è incontrastabilmente esclusa dagli atti del procedimento o la negazione di un fatto la cui esistenza risulta incontrastabilmente dagli atti del procedimento».

[278] P. Evangelista, *op. cit*., 142.

[279] Cfr. M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 16, 2019, p. 19.

[280] S. Cimini, *op. cit.*, pp. 54 – 55.

La gestione e la sicurezza degli strumenti informatici e dei dati[281] (che costituiscono la base del funzionamento di qualunque sistema di intelligenza artificiale) diviene per queste ragioni una competenza necessaria anche per i pubblici dipendenti. Diverso è il discorso dell'impiego di sistemi di IA, in tal caso starà alle singole amministrazioni dotarsi delle figure professionali come informatici e *data analyst*, per le competenze tecniche divenute fondamentali[282] di cui sono in possesso, senza trascurare che la competenza tecnica si riverbera sul funzionario, il quale oltre all'esercizio delle funzioni pubbliche previste dalla legge, deve assumere anche il ruolo di controllore e garante della correttezza del funzionamento degli strumenti algoritmici, nella misura in cui questi assistono e agevolano l'azione amministrativa.

Proprio la questione della responsabilità della persona potrebbe essere l'elemento maggiormente incidente sull'adozione dell'intelligenza artificiale nella pubblica amministrazione. In altre parole, il timore del dipendente di essere chiamato a rispondere per il danno erariale indiretto, nel caso di soccombenza delle amministrazioni nei giudizi relativi a lesioni di interessi legittimi o diritti soggettivi, così come nel caso in cui le stesse venissero sanzionate dalle autorità di vigilanza preposte, nonché per danno erariale diretto, derivante da provvedimento pregiudizievole nei confronti di terzi, qualora non venissero rispettati quei criteri sanciti dalla legge (trasparenza, riserva di umanità), o qualora venga adottata senza un controllo effettivo il risultato fornito dal sistema di IA, sono fattori potenzialmente limitanti.

[281] Tale aspetto viene preso in considerazione dal legislatore quando, nel 2023, intervenendo sul Codice di comportamento dei pubblici dipendenti introduce due nuove disposizioni l'art. 11 *bis* e 11 *ter* al d.P.R. 16 aprile 2013 n. 62, i quali oltre ad introdurre obblighi a carico dei dipendenti al fine di tutelare l'immagine della pubblica amministrazione nell'ambiente digitale, autorizza l'amministrazione a svolgere gli accertamenti necessari a garantire la sicurezza dei sistemi informatici e la protezione delle informazioni e dei dati, con le modalità previste dalle linee guida AgID; cfr. sull'argomento F. Midiri, *La correttezza dei dipendenti pubblici in ambiente digitale*, in *Gior. dir. amm.,* 4, 2023.

[282] J.B. Auby, *Il diritto amministrativo di fronte alle sfide digitali*, in *Ist. federalismo*, 3, 2019, p. 624. Il Piano triennale per l'informatica 2024-2026 rileva la necessità di esperti ICT per le amministrazioni pubbliche soprattutto in materia di sicurezza per potenziare gli Uffici per la transizione digitale.

CONCLUSIONI

La ricerca condotta nel presente lavoro ha permesso di spiegare, a partire dalle origini storico-culturali, come stia venendo costruita l'architettura di *governance* dell'intelligenza artificiale nella pubblica amministrazione, e come questa tecnologia possa avere reale possibilità di diffusione a partire dai fattori condizionanti l'adozione.

Il processo di riforma avviato alla fine del secolo scorso, che aveva inaugurato un modello basato sul decentramento[283], con il coinvolgimento di una pluralità di attori implicati nella definizione delle politiche pubbliche, anche attraverso l'istituzione delle agenzie indipendenti specializzate per settori, con la giustificazione dell'efficienza, ha determinato lo svuotamento di competenze elevate nelle pubbliche amministrazioni[284].

Le strutture di controllo concepite negli anni Novanta, caratterizzate da specializzazione in ambiti definiti e dotate di indipendenza dal potere politico, paiono essere superate anche in quanto inadeguate a governare sistemi di intelligenza artificiale che richiedono supervisioni trasversali e integrate[285], poiché ampio è l'ambito interessato, dalla protezione dei dati, alla sicurezza informatica, alla tutela dei diritti delle persone e diverso è l'approccio richiesto, ossia un controllo *ex ante* e non solo *ex post*.

L'indagine condotta rivela come il legislatore sembri aver risposto a queste problematiche definendo un modello di *governance* costituito da strutture centrali di vigilanza e controllo, dotate di ampie competenze e funzioni, ma anche responsabilizzazione dei singoli enti pubblici attraverso la creazione di referenti per ciascuna amministrazione, deputati all'implementazione delle politiche pubbliche in materia digitale, nonché al dialogo costante con queste agenzie e, tramite esse, con gli organismi istituiti dall'Unione europea.

---

[283] E. D'Orlando, *Algoritmi e organizzazione dell'amministrazione locale: come declinare il principio di adeguatezza affrontando la complessità*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Quaderni del dipartimento di giurisprudenza dell'Università di Torino, 2021, p. 197.

[284] A. Grassi, A. Sanetti, S. Campostrini, *La governance dell'intelligenza artificiale nella pubblica amministrazione: il ruolo dei dati e dell'organizzazione alla luce dell'AI Act. Oltre il punto di vista giuridico*, p. 157, consultato al seguente link https://doc989.consiglioveneto.it/dirreg/resources/Articolo_Grassi_Sanetti_Campostrini_per_sito.pdf .

[285] C C. Schmitz, J. Rystrøm, J. Batzne, *Oversight structures for agentic ai in public-sector organizations*, in *arXiv*, 2025., p. 3.

Nondimeno, alla concentrazione di funzioni in capo a organismi tecnici già esistenti (come l'ACN e AgID) corrisponde un tendenziale accentramento del controllo del Governo, e nello specifico del Presidente del Consiglio dei Ministri, in ragione del potere di direzione esercitato sugli stessi, con riflesso sullo sviluppo tecnologico del Paese. In altre parole, in contraddizione con quanto previsto dall'*AI Act*, come si è sostenuto nel capitolo 2, a fronte della velocità dello sviluppo dell'IA e dei rischi posti in tema di sovranità e quindi di democrazia, vi è una precisa scelta di esercitare un certo grado di controllo su un settore divenuto centrale, a cui si aggiunge un parallelo controllo negli altri ambiti necessari per la digitalizzazione, ovvero *cloud*, cybersicurezza.

La scelta del legislatore nazionale per come analizzata nel secondo capitolo (che peraltro come si è visto risulta simile a quella del modello spagnolo) trova in parte una giustificazione nella mancanza di difesa effettiva della sovranità da parte della disciplina europea (*AI Act,* NIS2, eccetera) tanto da rendere necessaria l'implementazione a livello nazionale per colmare questo aspetto. Invero, anche l'Unione europea sembra aver preso contezza del vuoto normativo sul punto, dato che il 3 giugno 2026 la Commissione ha presentato una proposta di Regolamento per stabilire un quadro giuridico volto a rafforza gli ecosistemi *cloud* e IA, denominato *Cloud and AI Development Act.* L'UE non vuole più considerare il *cloud* e l'IA come due mercati separati, ma intrinsecamente connessi, poiché senza autonomia dai fornitori di servizi di *cloud* non può esserci autonomia di sviluppo dell'intelligenza artificiale. Con questa consapevolezza, la proposta di regolamento si propone quindi di porre al centro della normativa la sovranità digitale e, nel passaggio al momento maggiormente interessante, lo introduce quale criterio di scelta del contraente nelle gare pubbliche per l'aggiudicazione di servizi di *cloud computing*. In base alla tipologia di servizio e di dati della pubblica amministrazione si potranno scegliere fornitori unicamente europei o di paesi extra-UE.

Il tema fondamentale emergente è dunque la sovranità, ma in una prospettiva diversa, ossia del controllo. Quello esercitato dalla politica sugli enti tecnici, quello delle autorità di vigilanza sugli strumenti tecnologici, quello sullo sviluppo tecnologico.

Tutto questo si traduce per le pubbliche amministrazioni, sotto il profilo della *governance* esterna, in un confronto costante con le autorità nazionali di vigilanza e

controllo. Mentre, per altro verso, sotto il profilo della *governance* interna, le singole amministrazioni si vedono costrette ad adeguare le loro strutture e processi interni per conformarsi non solo al mutare del contesto tecnologico, ma anche normativo.

Quella che con la ricerca si è voluto mettere in evidenza è la presenza di tre forze ordinatrice che stanno modificando la pubblica amministrazione: la legge, l'organizzazione, l'intelligenza artificiale, la cui interazione e integrazione produce una modificazione delle strutture organizzative[286].

La prima stabilisce, infatti, i limiti entro cui le pubbliche amministrazioni possono agire e attribuisce le funzioni, determinando, specialmente con riferimento al digitale, quali obblighi devono essere adempiuti. La seconda è caratterizzata dalle scelte interne all'ente (pur condizionate dall'ordinamento) e ne definisce la struttura operativa al fine di coordinarne le attività. Infine, l'IA in quanto in grado di condizionare i processi decisionali in ragione di un dominio della conoscenza (relativa ai dati) più ampio di quello del funzionario, può influire sui rapporti interni.

Le prime due costituiscono certamente forza ordinante, mentre la portata della terza si comprende nella misura in cui si considera che l'organizzazione è l'unione di più persone che si propongono di risolvere compiti in vista del raggiungimento di fini prefissati, dividendosi il lavoro e coordinandosi, la cui unità di azione finalistica viene assicurata dal coordinamento attraverso un principio di autorità, e quindi di gerarchia[287].

In relazione a queste caratteristiche, l'ingresso dell'intelligenza artificiale ha il potenziale di modificare tali caratteristiche essenziali dell'organizzazione formale dell'amministrazione, ossia la divisione del lavoro (per cui le varie funzioni vengono ripartite secondo il principio di specializzazione), la delega di potere, un sistema di comunicazione delle informazioni all'interno della struttura e un sistema di coordinamento[288]. Proprio perché «*an organization chart is designed to support human decision-making given humans' limited information processing and coordination*

[286] G. von Krogh, *Artificial Intelligence in Organizations: New Opportunities for Phenomenon-Based Theorizing*, in *Academy of Management*, 2018, p. 405, https://doi.org/10.3929/ethz-b-000320207.
[287] S. Cimmino, *L'organizzazione amministrativa nel suo contesto sociale*, Casa Editrice Prof. Riccardo Patron, Bologna, 1962, p. 130-131.
[288] S. Cimmino, *op. cit.*, p. 134.

capacities, whereas an algorithm is designed to maximize its objective regardless of those information processing and coordination needs – for better or for worse»[289].

Possono allora essere formulate due prospettazioni sull'evoluzione della tecnificazione pubblica. La prima vede l'integrazione dei processi decisionali artificiali e umani attraverso la combinazione di differenti strumenti di IA, dagli algoritmi deterministici a quelli predittivi, intersecando la decisione logico-causale del funzionario pubblico con quella statistico-probabilistica della macchina, superando la gerarchizzazione interna dell'organizzazione e la rigida divisione dei ruoli e dei compiti, integrata con figure specializzate trasversali. La seconda ipotesi, invero quella che l'*AI Act* e la legislazione nazionale sembrano esprimere, vede un utilizzo dell'IA a meri fini ausiliari, neutralizzando la decisione algoritmica attraverso l'imputazione umana della decisione o il ricorso a sistemi con funzioni meramente di controllo o *checklist*[290].

In entrambe le ipotesi l'integrazione dei sistemi di intelligenza artificiale può portare indubbi vantaggi all'organizzazione amministrativa, non solo in termini di servizi ma anche di gestione interna. Basti pensare all'automazione delle procedure di inquadramento o di progressione di carriera, ma anche alla valutazione del personale dipendente o come si è ipotizzato nel capitolo 4 l'attribuzione di funzioni o il conferimento di incarichi. Questo garantisce infatti non solo equità e certezza, ma anche efficienza e celerità nella gestione interna del personale[291], con conseguenti riflessi positivi nel funzionamento della macchina pubblica.

I limiti risiedono nei fattori individuati nel corso della presente dissertazione, ovvero i quelli infrastrutturali e di sicurezza, con la prospettiva di un divario tra le amministrazioni nell'adozione di nuove tecnologie e conseguente disomogenea diffusione dell'innovazione, creando o acuendo disparità nella transizione verso l'amministrazione algoritmica.

Se a questo si aggiunge la considerazione che la necessità di mantenere il controllo sull'algoritmo, comporta l'aumento delle responsabilità per il funzionario preposto,

---

[289] M. A. Valentine, A.L. Pratt, et al., *The Algorithm and the Org Chart: how algorithms can conflict with organizational structures*, in *Proceedings of the ACM on Human-Computer Interaction*, Volume 8, Issue CSCW2, 2024, p. 364:3.

[290] Tale considerazione prende spunto dal convegno «Intelligenza Artificiale: progetti pilota e stato dell'arte per le applicazioni nella Pubblica Amministrazione» tenutosi il 17 dicembre 2025 a Firenze, nell'ambito del quale sono stati presentati i risultati del progetto GAIPS *Generative AI for Public procurement compliance System*, consistente in un *proof of concept* dell'utilizzo di un *tool* per la *compliance* amministrativa in modalità semiautomatica.

[291] P. Miele, *Intelligenza artificiale e pubblica amministrazione*, in *Quad. Corte conti*, 2, 2024, p. 152

nonché della pubblica amministrazione, allora è evidente che il problema sull'utilizzo dei sistemi automatizzati si traduce nell'adozione di un adeguato modello organizzativo[292] volto a prevenire l'adozione di decisioni che danneggino i destinatari. Il problema allora non è soltanto tecnico, o regolatorio, ma anche e forse prima di tutto organizzativo e culturale[293].

In definitiva il fattore umano sia che si esplichi nelle forme del controllo sia che lo si intenda quale posse delle capacità, e quindi competenze all'interno dell'organizzazione attraverso il reclutamento di nuove figure[294], risulta essere centrale per la *governance* e per l'effettiva implementazione dell'IA all'interno delle amministrazioni. È un percorso in divenire, in cui le scelte verso l'innovazione sono e saranno condizionate anche in base al mutamento del contesto complessivo.

[292] Sul punto v. S. Cimini, *Modello organizzativo e responsabilità della p.a.*, in *P.A. persona e amministrazione*, 1, 2019, p. 103. L'autore in particolare facendo un confronto con la responsabilità degli enti *ex* l. 231/2001 ritiene che «un appropriato modello organizzativo teso a prevenire abusi e illegittimità nell'esercizio della funzione provvedimentale, richiederebbe una serie di azioni, molte delle quali riguardano il profilo dell'organizzazione, come quelle di predeterminare le regole in modo da evitare arbitri interpretativi da parte dei funzionari». Estendendo questo ragionamento è allora ipotizzabile la necessità di un appropriato modello organizzativo per stabilire a priori il contesto e i compiti in cui possono essere impiegati i sistemi di IA.

[293] N. Tomaževič, E. Murko, A. Aristovnik, *Organisational Enablers of Artificial Intelligence Adoption in Public Institutions: A Systematic Literature Review*, in *Central European Public Administration Review*, 1, 2024, p. 128.

[294] M. Falcone, *La data science come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni*, in *Riv. it. infor. dir.*, 6, 2024, p. 538.

BIBLIOGRAFIA

AA.VV., *The Global Risks Report 2017. 12th Edition*, in www3.weforum.org/docs/GRR17_Report_web.pdf

Adabara I., Sadiq B.O., et. al., *Trustworthy agentic AI systems: a cross-layer review of architectures, threat models, and governance strategies for real-world deployment*, in F1000Research 2025, doi.org/10.12688/f1000research.169927.1

Adsuara Varela B., *Articulo 3*, in M. Barrio Andrés (a cura di), *Comentarios al Reglamento Europeo de Inteligencia Artificial*, La Ley, 2024

Alberti I., *La partecipazione procedimentale per legittimare gli algoritmi nel procedimento amministrativo*, in R. Cavallo Perin, *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Rubettino Editore, 2021

Albertini L., *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. civ.*, 6, 1998

Allegri M.R., *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Riv. it. infor. dir.*, 2, 2021

Almada M., Radu A., *Brussels Effect*, in A. Parrish, C. Ryngaert, D. Ireland-Piper, *Elgar Concise Encyclopedia on Extraterritoriality and the Law*, 2025, disponibile in SSRN: https://ssrn.com/abstract=5123680 or http://dx.doi.org/10.2139/ssrn.5123680

Amato G., *Le autorità indipendenti nella Costituzione economica*, in AA.VV., *Regolazione e garanzia del pluralismo. Le Autorità amministrative indipendenti*, Milano, 1997

Ariota S., *L'intelligenza artificiale: la nuova frontiera del controllo amministrativo-contabile*, in *Quad. Corte Conti*, 6, 2025

Armiento M.B., *Prove di regolazione dell'intelligenza artificiale: il Regolamento della Banca d'Italia sulla gestione degli esposti*, in *Giornale di diritto amministrativo*, 1, 2023

Auby J.B., *Il diritto amministrativo di fronte alle sfide digitali*, in *Ist. federalismo*, 3, 2019

Barone G., *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Dir. pen. proc.*, 8, 2024

Barzelay M., *The New Public Management: Improving Research and Policy Dialogue*, University of California Press, Berkeley, 2001

Bassanini F., *Lo stato delle riforme amministrative, il "perimetro" della Pubblica Amministrazione, e i problemi del public procurement*, in L. Fiorentino, *Lo stato compratore. L'acquisto di beni e servizi nelle pubbliche amministrazioni*, Il Mulino, Bologna, 2007

Bassanini F., *Vent'anni di riforme del sistema amministrativo italiano (1990-2010)*, in *The Journal of European economic History*, 1, 2010, www.astrid.it

Bassi N., *Principio di legalità e poteri impliciti*, Milano 2001

Benanti P., *Human in the loop. Decisioni umane e intelligenze artificiali*, Mondadori, Milano, 2022

Bengesi S., et al. *Advancements in Generative AI: A Comprehensive Review of GANs, GPT, Autoencoders, Diffusion Model, and Transformers*, in *IEEE Access*, vol. 12, 2024

Bergé J.S., Grumbach S., Zeno-Zencovich V., *The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance*, in *Eur. Journal Comparative Law and Governance*, 2, 2018, disponibile in SSRN: https://ssrn.com/abstract=3185943

Bertola V., *La sovranità digitale e il futuro di Internet,* in *Riv. it. infor. dir.*, 1, 2022

Betzu M., *I poteri privati nella società digitale: oligopoli e antitrust*, in *Dir. pubbl.*, 3, 2021

Bluemke E., Collins T., et al., *Exploring the Relevance of Data Privacy-Enhancing Technologies for AI Governance Use Cases,* disponibile in https://arxiv.org/abs/2303.08956

Bommasani R., Hudson D.H. et. al., *On the opportunities and risks of foundation models*, disponibile in https://crfm.stanford.edu/report.html

Borruso R., *Il documento informatico, la firma elettronica e la firma digitale alla luce delle ultime norme (d. lgs. 23 gennaio 2002 n. 10, d.P.R. 7 aprile 2003 n. 137 e l. 29 luglio 2003 n. 229)*, in *Giust. civ.*, 3, 2004

Boto A., *La agencia como forma organizativa de optimización de servicios públicos. Pasado, presente y futuro en una España en crisis*, in *Revista digital de Derecho Administrativo*, 13, 2015

Bovetti R., Broccardo L., Materzanin G., *Shadow automation: l'automazione robotica dei processi come strumento di efficienza per le aziende*, in *Controllo gestione*, 5, 2023

Bradford A., *The Brussels Effect*, in *Northwestern University Law Review*, 1, 2012, disponibile in https://scholarship.law.columbia.edu/faculty_scholarship/271

Bravo F., *Le cooperative di dati*, in *Contratto impresa*, 3, 2023

Bruti Liberati E., *Poteri privati e nuova regolazione pubblica*, in *Dir. pubbl*, 1, 2023

Buoso E., *Disruptive technologies and public administration: rethinking administrative law for the brave new world?*, in V. Faggiani, F. J. Garrido Carrillo (a cura di), *Avances en el desarrollo de la inteligencia artificial*. *Principios éticos y democràticos, concreciones normativas en la uniòn europea, y limites para las administraciones pùblicas*, Aranzadi, 2025

Burelli C., *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?*, in *Quad. AISDUE - Rivista quadrimestrale*, *Fasc. speciale*, 2, 2024

Burri M., Zihlmann Z., *The EU Cyber Resilience Act – An Appraisal and Contextualization*, in *Zeitschrift für Europarecht*, 2, 2023

Caballero Sanchez R., *Téoria general de la organizaciòn administrativa*, in F. Velasco Caballero, M. M. Darnaculleta Gardella (a cura di), *Manual de Derecho administrativo*, 2024

Cappiello B., Carullo G., *Blockchain, Law and Governance*, Springer, 2020

Carloni E., *Dalla legalità algoritmica alla legalità (dell'amministrazione) artificiale. Premesse ad uno studio,* in *Riv. it. infor. dir.*, 2, 2024

Carloni E., *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm*. 2, 2020

Carlotti G., *I principi nel Codice dei contratti pubblici: la digitalizzazione*, in www.giustizia-amministrativa.it., 2023

Carotti B., *Algoritmi e poteri pubblici: un rapporto incendiario*, in *Gior. dir. amm.*, 1, 2020

Carotti B., *Le finzioni dell'intelligenza senza corpo, o dell'AI Act*, in *Giorn. dir. amm*., 1, 2025

Carotti B., *Sicurezza cibernetica e Stato-nazione*, in *Giornale di diritto amministrativo*, 5, 2020

Carullo G., *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in *Ceridap*, 3, 2024

Carullo G., *Decisione amministrativa e intelligenza artificiale*, in *Dir. inform.*, 3, 2021

Carullo G., *L'amministrazione quale piattaforma di servizi digitali*, Editoriale Scientifica, 2022

Casetta E., *Manuale di diritto amministrativo*, Milano, 2017

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

Casonato C., *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in *DPCE*, 1, 2021

Cavallaro M.C., *Immedesimazione organica e criteri di imputazione della responsabilità,* in *P.A. persona e amministrazione*, 1, 2019

Cavallaro M.C., Smorto G., *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 16, 2019

Cavallo Perin R., Alberti I., *Atti e procedimenti amministrativi digitali*, in R. Cavallo Perin, D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020

Cavallo Perin R., *Ragionando come se la digitalizzazione fosse data*, in *Dir. amm.*, 2, 2020

Cepiku D., *Governance: riferimento concettuale o ambiguità terminologica nei processi di innovazione della PA*, in *Azienda pubbl*., 1, 2005

Cereda S., *Il concetto di algoritmo in una recente sentenza del Consiglio di Stato*, in *Medialaws*, 3, 2022

Cerrillo i Martínez A., *How can we open the black box of public administration? Transparency and accountability in the use of algorithms*, in *Revista Catalana de Dret Públic*, 58, 2019, doi.org/10.2436/rcdp.i58.2019.3277

Cerulli Irelli V., *La tecnificazione*, in L. Ferrara, D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana*, Vol. IV, S. C. Matteucci, L. Torchia (a cura di), *La tecnificazione*, Firenze University Press, 2016

Cerulli Irelli V., *Principi del diritto amministrativo*, *vol. II*, Giappichelli, Torino, 2005

Chessa O., *Sul rapporto tra Stato e capitalismo. Riflessioni a partire da Hobbes, Schmitt e Mortati*, in *Cosituzionalismo.it*, 3, 2024

Chiti E., Marchetti B., *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, 1, 2020

Chiti E., Marchetti B., Rangone N., *L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali*, in *BioLaw Journal*, 2, 2022

Chun J., Schroeder de Witt C., Elkins K., *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US*, in *arXiv*, 2025

Cimini S., *Modello organizzativo e responsabilità della p.a.*, in *P.A. persona e amministrazione*, 1, 2019

Cimini S., *La responsabilità civile e amministrativa di fronte alle sfide dell'intelligenza artificiale*, in *Ceridap*, 1, 2026

Cimmino S., *L'organizzazione amministrativa nel suo contesto sociale*, Casa Editrice Prof. Riccardo Patron, Bologna, 1962

Cingolani R., Andresciani D., *Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020

Civitarese Matteucci S., *Il significato formale dell'ideale del «governo delle leggi» (rule of law)*, in *Dir. amm.*, 1, 2011

Civitarese Matteucci S., *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl.*, 1, 2019

Conte F., *La trasformazione digitale della pubblica amministrazione: il processo di transizione verso l'amministrazione algoritmica*, in *Federalismi.it*, 11, 2023

Contessa C., *Il potere pubblico al tempo dei Big Data*, disponibile in www.giustizia-amministrativa.it

Cormen T. H., Leiserson C. E., et al., *Introduction to Algorithms*, MIT Press, 2009

Corrado A., *La trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, in *Federalismi.it*

Corso G., *Il principio di legalità*, in M.A. Sandulli (a cura di), *Codice dell'azione amministrativa*, Giuffrè, Milano, 2010

Crialesi G., *Verso un'intelligenza artificiale UE antropocentrica e affidabile che garantirà la sicurezza e i diritti di imprese e cittadini* in *Pratica Fiscale e Professionale*, 14, 2024

Crismani A., *La frontiera dell'IO (Intelligenza Organoide)*, in *Ceridap*, 4, 2024

D'Angelosante M., *La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in L. Ferrara, D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana*, Vol. IV, S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione*, Firenze University Press, 2016

D'Orsogna M., *Programmazione strategica e attività decisionale della Pubblica amministrazione*, Torino, 2001

Daniell K.A., Kay A., *Multi-Level Governance: Conceptual Challenges and Case Studies from Australia*, ANU Press, 2017

de Bruin H., Prakken H., Svensson J., *The Use of Legal Knowledge-Based Systems in Public Administration: What Can Go Wrong?*, in T.J.M. Bench-Capon, A. Daskalopulu and R.G.F. Winkels (a cura di), *Legal Knowledge and Information Systems*, Jurix 2002: The Fifteenth Annual Conference. Amsterdam: IOS Press, 2002

Del Vecchio P., Bignoli V., *Le responsabilità amministrative da algoritmo e intelligenza artificiale. La responsabilità da provvedimento algoritmico sia ai fini del risarcimento del danno in sede civilistica che in sede contabile come responsabilità*

erariale, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?, Vol. 2, Amministrazione, responsabilità, giurisdizione*, Il mulino, 2022

Delgado I.M., *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Ist. feder*., 3, 2019

Della Valle S., *Crisi e ridefinizione della sovranità nel contesto plurilivellare*, in *Costituzionalismo.it*, 3, 2016

Deng Z., Guo Y., et al., *AI agents under threat: A survey of key security challenges and future pathways*, in *ACM Computing Surveys*, 2025

di San Lucia G.C., Paladino M., *Decisioni amministrative e intelligenza artificiale*, in *Federalismi.it*, 4, 2025

Diaco D., *Brevi riflessioni sulla natura giuridica del software (a partire da TAR Lazio, sez. III-bis, n. 8384/2023),* in www.giustiziainsieme.it

Di Martino A., *Tecnica e potere nell'amministrazione per algoritmi*, Ed. Scientifica, Napoli, 2023

D'Orlando E., *Innovazione tecnologica e fonti del diritto*, in J.B. Auby, G. De Minico, G. Orsoni (a cura di), *L'amministrazione digitale. Quotidiana efficienza e intelligenza delle scelte. Atti del Convegno 9-10 maggio 2022*, *Federico II, Napoli*, Napoli, 2023

D'Orlando E., *Algoritmi e organizzazione dell'amministrazione locale: come declinare il principio di adeguatezza affrontando la complessità*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Quad. Dipartimento di giurisprudenza dell'Università di Torino, 2021

Doshi A.R., Bell J.J., et al., *Generative Artificial intelligence and evaluating strategic decisionsi*, in *Strategic Management Journal*, vol. 46, 3, 2025, disponibile in SSRN: ssrn.com/abstract=4714776 oppure dx.doi.org/10.1002/smj.3677

Ebers M., *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. Di Matteo, M. Cannarsa, C. Poncibò (a cura di), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, 2022

Engin Z., Crowcroft J., et al., *The Algorithmic State Architecture (ASA): An Integrated Framework for AI-Enabled Government*, in *arXiv*, 2025

Entsiea E., Frempong Aidoo F.K., Vaz A., *Systematic review of cloud computing adoption in the public sector: Insights from the TOE framework and DOI theory*, in *Multidisciplinary Reviews*, 9(2), 2025, https://doi.org/10.31893/multirev.2026091

Ertel W., *Introduction to Artificial Intelligence*, Springer, 2017

Erukude S.T., Veluru S.R., et al., *Agentic AI - The rise of autonomous intelligent agents in the era of LLMS*, in *Indian Journal of Computer Science and Engineering*, 1, 2025

Evangelista P., *Intelligenza artificiale e responsabilità amministrativo-contabile*, in *Riv. Corte conti*, 2, 2024

Fabbrini F., *Il diritto dell'UE e l'indipendenza delle autorità nazionali garanti della protezione dei dati*, in *Gior. dir. amm*., 10, 2010

Faini F., *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *Federalismi.it*, 2, 2023

Falcone M., *La data science come nuovo sapere per governare le intelligenze artificiali nelle pubbliche amministrazioni*, in *Riv. it. infor.dir.*, 6, 2024

Faletti E., *Mai accettare caramelle né atti amministrativi da sconosciuti, ancorché algoritmi (Nota a T.A.R. Napoli, 14 novembre 2022, n.7003, sez. III),* in *Dir. inform.*, 17, 2023

Ferilli S., Girardi E. et al. (a cura di), *L'Intelligenza artificiale per lo sviluppo sostenibile*, Cnr edizioni, 2021

Ferrajoli L., *La sovranità nel mondo moderno. Nascita e crisi dello Stato nazionale*, Roma-Bari, 1997

Feuerriegel S., Hartmann J., et al., *Generative AI*, in *arXiv*, 2023

Fierro Rodriguez D., *Luces y sombras en el panorama de la Agencia Española de Supervisión de Inteligencia Artificial*, in *eXtoikos*, 26, 2023

Filice M., *Il sindacato giurisdizionale sull'attività delle Autorità indipendenti*, in *Giorn. dir. amm.*, 4, 2015

Filicetti C., *Sulla definizione di algoritmo (nota a Consiglio di Stato, Sezione Terza, 25 novembre 2021 numero 7891)*, in www.giustiziainsieme.it

Finocchiaro G., *La sovranità digitale*, in *Dir. pubbl.*, 3, 2022

Fioriglio G., *Intelligenza artificiale e cibersicurezza: profili informatico-giuridici, fra vulnerabilità delle macchine e delle persone*, in *Riv. Scienze Giuridiche, Cognitive ed Intelligenza Artificiale*, 2, 2025

Floridi L., *Etica dell'intelligenza artificiale. Sviluppo, opportunità, sfide*, Raffaello Cortina Editore, Milano, 2022

Forgione I., *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 *Dir. amm.*, 4, 2022

Forgione I., *La prospettiva dell'intelligenza artificiale nel procedimento e nell'attività amministrativa*, in. *Riv. it. infor. dir.*, 2, 2024

Franchini C., *Autonomia e indipendenza nell'amministrazione europea*, in *Dir. amm*., 1, 2008

Frosinini V., *Cibernetica diritto e società*, RomaTre Press, 2023

G'sell F., *An Overview of the European Union Framework Governing Generative AI Models and Systems*, 2024, disponibile in ssrn.com/abstract=4762804

Galetta D.U., Corvalàn J.G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019

Gallone G., *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, CEDAM, 2023

Gallone G*., Riserva di umanità, intelligenza artificiale e funzione giurisdizionale alla luce dell'IA Act. Considerazioni (e qualche proposta) attorno al processo amministrativo che verrà*, in *Judicium*, 2024

Garlassi A., *Il* cloud*: opportunità di crescita per i sistemi di controllo digitali*, in *Controllo gestione,* 3, 2022

Garofoli R., Ferrari G., *Manuale di diritto amministrativo*, Molfetta, 2020

Gatti A., *Istituzioni e anarchia nella rete. i paradigmi tradizionali della sovranità alla prova di internet*, in *Dir. inform.,* 3, 2019

Gentili A., *Regole per l'intelligenza artificiale*, in *Contratto impresa*, 4, 2024

Giannini M.S., *Diritto amministrativo*, Giuffré, Milano, 1993

Giannini M.S., *In principio sono le funzioni*, disponibile al seguente link https://www.eticapa.it/eticapa/wp-content/uploads/2017/08/M-S-GIANNINI-In-principio-sono-le-funzioni.pdf

Giannini M.S., *Lezioni di diritto amministrativo*, Milano 1950

Giannini M. S., *Parlamento e amministrazione*, in *Amm. civ.*, 1961

Giannini M.S., *Rapporto sui principali problem dell'amministrazione dello Stato*, 1979

Giarratano J., Riley G., *Expert Systems Principles and Programming*, PWS, 3rd Edition, 2020

Giglioni F., *La composizione dei sistemi amministrativi comuni*, in Del Gatto S., Vesperini G. (a cura di), *Manuale di diritto amministrativo europeo*, Giappichelli, 2024

Giovagnoli R., *Compendio di diritto amministrativo*, ita ed., Torino, 2022

Giupponi T. F., *Il governo nazionale della cybersicurezza*, in *Quad. cost.*, 2, 2024

Glasera V.L., Sloana J., Gehman J., *Organizations as Algorithms: A New Metaphor for Advancing Management Theory*, in *Journal of Management Studies*, 61, 2024

Y. Gokul, M. Ramalingam, et al*., GPT (Generative Pre-trained Transformer) – A Comprehensive Review on Enabling Technologies, Potential Applications, Emerging Challenges, and Future Directions*, in *arXiv*, 2023

Golisano L., *Il governo del digitale: strutture di governo e innovazione digitale*, in *Gior. dir. amm.*, 6, 2022

Gomez Moreno J.B., *Agencias estatales: el modelo consolidado en sistemas jurídicos de tradición anglosajona que fracasó en españa,* in *Revista Aragonesa de Administración Pública*, 58, 2022

Goodfellow I. J, Bengio Y., Courville A., *Deep learning*, MIT Press, 2016

Goodfellow J. et al., *Generative Adversarial Nets*, in *arXiv*, 2014

Grasso G., *L'anomalia di un «modello»: le autorità (amministrative) indipendenti nei paesi membri dell'unione europea*. *Prime ipotesi per un «inventario»*, in *Il Politico*, 2000

Gruening G., *Origin and theoretical basis of New Public Management,* in *International Public Management Journal*, 4, 2001

Gstrein O.J., *European AI Regulation: Brussels Effect versus Human Dignity?*, in *Zeitschrift für Europarechtliche Studien (ZEuS)*, 4, 2022, p. 758, disponibile in ssrn.com/abstract=4214358

Gstrein O.J., Haleem N., Zwitter A., G*eneral-purpose AI regulation and the European Union AI Act*, in *Internet Policy Review*, 13, 2024, doi.org/10.14763/2024.3.1790

Gualtiero Blancato F., *The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem*, in *Policy & internet*, 2023

Hammerschmid G., Van de Walle S., Andrews R. et al., *New Public Management Reforms in Europe and their Effects: Findings from a 20-Country Top Executive Survey*, in *International Review of Administrative Sciences*, 3, 2019

Hanisch M., Goldsby C., et al., *Digital Governance: A Conceptual Framework and Research Agenda*, in *Journal of Business Research*, 162, 2023

Hassija V., Chamola V. et al., *Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence*, in *Cognitive Computation*, Springer, 2024

Hofmann H., *European Administration - Nature and Developments of a Legal and Political Space*, C. Harlow, G. della Cananea, L. Sandberg (Eds.), *Research Handbook in EU Administrative Law*, Cheltenham, 2016

Hoffmann J., Katzenbach C., Gollatz K., *Between coordination and regulation: Finding the governance in Internet governance*, in *New Media & Society*, 2016, disponibile in SSRN: https://ssrn.com/abstract=2836068

Hood V, *A Public Management for all seasons?*, in *Public adm.*, 1, 1991

Janiesch C., Zschech P., Heinrich K., *Machine learning and deep learning*, in *Electronic markets*, 4, 2021

Kop M., *EU Artificial Intelligence Act: The European Approach to AI*, in *Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments*, Stanford University, 2, 2021, disponibile in ssrn.com/abstract=3930959

Kozak M., Batura O., *Study on the NRA independence Final Report*, 2022

Kreuzberger D., Kühl N., Hirschl S., *Machine Learning Operations (MLOps): Overview, Definition, and Architecture*, in *arXiv*, 2022

Kumar I., Manning S., *Trends in Frontier AI Model Count: A Forecast to 2028*, in *arXiv*, 2025

Kwentoa I. K., *Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology*, in *Journal of Next-Generation Research 5.0*, 2025

Larman C., *Applying UML And Patterns: An Introduction to object-oriented analysis and design and iterative development*, Prentice Hall, 2004

Lestari M., Wijaya A. F., Chandra M., *Enterprise Architecture Model for Smart Government Implementation*, in *Journal of Information Systems and Informatics*, 1, 2025

Leucci V.S., Girella S., Beccara J.L., *Pubblica amministrazione e protezione dei dati personali nelle "nuvole": criticità e soluzioni*, in *Inf. dir.*, 2, 2014

Limiti C., *La governance del processo di digitalizzazione della pubblica amministrazione*, in *www.iusinitinere.it*

Ling C., Zhao Z., et al., *Domain Specialization as the Key to Make Large Language Models Disruptive: A Comprehensive Survey*, in *ACM Computing Surveys*, 2025, consultabile al seguente link dl.acm.org/doi/10.1145/3764579

Linna E., Linna T., *Judicial Requirements for Generative AI in Legal Reasoning*, in *arXiv*, 2025

Lonero G., *Relazione sul Regolamento UE 241 del 2021. Una panoramica comprensiva delle disposizioni e delle implicazioni,* in *Il Diritto Amministrativo*, disponibile al seguente link https://www.ildirittoamministrativo.it/Relazione-sul-Regolamento-UE-

241-del-2021-Una-panoramica-comprensiva-delle-disposizioni-delle-implicazioni/gamm1090

Lòpez-Jurado F. B., *Administracòn y sector pùblico estatal,* in F. Velasco Caballero, M. M. Darnaculleta Gardella (a cura di), *Manual de Derecho administrativo*, 2024

Lo Sapio G., *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi.it*, 16, 2021

Maas M.M., *AI, Governance Displacement, and the (De)Fragmentation of International Law*, 2021, disponibile in ssrn.com/abstract=3806624

Maas M.M., Villalobos J.J., *International AI institutions. A literature review of models, examples, and proposals*, *Institute for Law & AI, AI Foundations Report*, 1, 2023, disponibile in www.law-ai.org/international-ai-institutions

Macchia M., Figliolia C., *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, in *Gior. dir. amm*., 4, 2018

Macchia M., Mascolo A., *Intelligenza artificiale e regolazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022

Macchia M., *Pubblica amministrazione e tecniche algoritmiche*, in *DPCE*, 1, 2022

Macrì I., *Cloud della Pubblica Amministrazione: una casa moderna per i dati degli italiani*, in *Azienditalia*, 11, 2021

Macrì I., *Cybersicurezza, le novità per il 2024*, in *Azienditalia*, 1, 2024

Macrì I., *Dalle infrastrutture digitali delle amministrazioni al cloud, il nuovo regolamento per la sicurezza dei dati e dei servizi pubblici*, in *Azienditalia*, 3, 2022

Macrì I., *Il cloud per le pubbliche amministrazioni*, in *Azienditalia*, 1, 2021

Macrì I., *Cybersicurezza, le novità per il 2024*, in *Azienditalia*, 1, 2024

Macrì I., *Polo Strategico Nazionale*, in *Azienditalia*, 3, 2023

Maddalena P., *La sistemazione dogmatica della responsabilità amministrativa*, in *Lexitalia*, 1, 2022

Maglia S., Balossi M.V., *Le ordinanze contingibili e urgenti dopo le modifiche operate dal d.l. n. 90/2008*, in *Ambiente & sviluppo*, 8, 2008

Magliari A., *L'indipendenza delle autorità di vigilanza finanziaria: le esigenze di uniformazione e l'uso (improprio) della soft law*, in *Gior. dir. amm*., 3, 2024

Manetti M., *Sull'autonomia e indipendenza delle autorità*, in *Rivista AIC*, 2, 2023

Manfredi G., *Legalità procedurale*, in *Dir. amm.*, 4, 2021

Mangiameli S., *La sovranità digitale*, in *dirittifondamentali.it*, 3, 2023

Mäntymäki M., Minkkinen M., et al., *Defining organizational AI governance*, in *AI and Ethics*, 2022

Marchetti B., *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in *Biodiritto*, 2, 2021

Marinică E., *Digitalization – The Key for Adapting Good Administration to a Better Governance*, in *Academic Journal of Law and Governance*, 2, 2020

Martire D., *Intelligenza artificiale e Stato costituzionale*, in *Dir. pubbl.*, 2, 2022

Mascolo A., *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giorn. dir. amm.*, 3, 2020

Massa C., *L'indipendenza delle autorità nazionali di regolamentazione dal potere politico: recenti sviluppi nel settore dei media in Italia*, in *Quaderni AISDUE - Rivista quadrimestrale*, 1, 2024

Massarotto G., *What Is Algorithmic Bias and Why Antitrust Agencies Should Care*, in *CPI Antitrust Chronicle*, University of Pennsilvania, Inst. for Law & Econ, paper No. 23-39, 2023, disponibile in SSRN: https://ssrn.com/abstract=4625894

Masucci A., *L'atto amministrativo informatico: primi lineamenti di una ricostruzione*, Napoli, 1993

Mayntz R., *La teoria della governance. Sfide e prospettive*, in *Riv. it. scienza pol*., 1, 1999

Mazzucato M., *Lo Stato innovatore*, Laterza, Bari, 2014

Midiri F., *La correttezza dei dipendenti pubblici in ambiente digitale*, in *Gior. dir. amm.,* 4, 2023

Miele P., *Intelligenza artificiale e pubblica amministrazione*, in *Quad. Corte conti*, 2, 2024

Minerva M., *Verso l'integrazione dei sistemi informativi pubblici: la rete unitaria della pubblica amministrazione*, *Dir. infor.*, 3, 1998

Montagnani E., *Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali*, in *Riv. it. inform. dir.,* 1, 2022

Montagnani E., *Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e le comunità digitali*, in *Riv. it. infor. dir.,* 1, 2022

Montero Pascual J.J., *Articulo 70*, in M. Barrio Andrés (dir.), *Comentarios al Reglamento Europeo de Inligencia Artificial*, Madrid, 2024

Morace Pinelli A., *Dalla Data Protection alla Data Governance: il Regolamento UE 2022/868*, in *Nuova giur. civ. comm.* 2, 2024

Morace Pinelli A., *La circolazione dei dati personali tra tutela della persona, contratto e mercato,* in *Nuova giur. civ. comm.*, 6, 2022

Moroni L., *La governance della Cyber sicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*

Napolitano G., *Autorità amministrative indipendenti e agenzie amministrative*, voce in M. Clarich, F. Fonderico (a cura di), *Dizionario di diritto amministrativo*, Milano, 2007

Napolitano G., *Il partenariato pubblico-privato per la realizzazione del Polo strategico nazionale*, in *Gior. dir. amm.*, 6, 2021

Nassuato F., *Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*, in *Ceridap*, 1, 2022

Neri A., *Uso di un algoritmo discriminatorio nella contrattazione privata*, in *Nuova giur. civ. comm.*, 4, 2021

Neri V., *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urb. app.*, 5, 2021

Nigro M., *La pubblica amministrazione fra costituzione formale e costituzione materiale*, in *Riv. trim. dir. proc. civ.*, 1985, ora in Scritti giuridici, III, Milano, Giuffrè, 1996

Nisa U., Shirazi M., et al., *Agentic AI: The age of reasoning – A review*, in *Journal of Automation and Intelligence*, 2025, doi.org/10.1016/j.jai.2025.08.003

Notari F., *Il percorso della digitalizzazione delle amministrazioni pubbliche: ambiti normativi mobili e nuovi modelli di governance*, in *Giorn. dir. amm.*, 1, 2020

Notarmuzi C., *DigitPA: la terza riorganizzazione dell'informatica pubblica*, in *Giorn. dir. amm.*, 10, 2010

Novelli C., Floridi L., Sartor G., *AI as legal persons: past, patterns, and prospects*, in *Journal of law and society*, 2024, disponibile in ssrn.com/abstract=5032265

Novelli C., Hacker P., et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *Eur. J. Risk Reg.*, 2024, doi:10.1017/err.2024.57

Ntalampiras S., Misuraca G., Rossel P., *Artificial Intelligence and Cybersecurity Research*, 2022

Ongaro E., *The Napoleonic Administrative Tradition and Public Management Reform in France, Greece, Italy, Portugal and Spain*, in M. Painter, B.G. Peters (Eds.), *Tradition and Public administration*, London, 2010

Orlando S., *Linguaggi di programmazione e responsabilità*, in S. Orlando, G. Capaldo (a cura di), *Annuario 2022. Osservatorio Giuridico sulla Innovazione Digitale*, Sapienza Università Editrice, 2022

Orofino A.G., Gallone G., *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giur. it*, 2020

Orofino A.G., *L'attuazione del principio di trasparenza nello svolgimento dell'amministrazione elettronica*, in *www.judicium.it*, 2020

Orsoni G., D'Orlando E., *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Ist. Federalismo*, 3, 2019

Oswald M., Paul A., *'Bias'*, in Kaufmann M., H. M. Lomell, *De Gruyter Handbook of Digital Criminology*, De Gruyter, 2025, p. 101, disponibile in SSRN: https://ssrn.com/abstract=4738337

Otranto P., *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, in *Federalismi.it*, 7, 2021

Pagnanelli V., *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Riv. it. infor. dir.*, 1, 2021

Palma M., *Gli algoritmi dell'amministrazione pubblica e l'amministrazione pubblica degli algoritmi*, in *Riv. it. informatica diritto*, 2, 2022

Papyshev G., Chan K.J.D., *AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities*, in Electron Markets, 36, 8, 2026, doi.org/10.1007/s12525-025-00870-z.

Petroni A.M., *Le riforme della Pubblica Amministrazione in Italia: una valutazione*, in *Giorn. dir. amm*., 2013

Petruso R., Smorto G., *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *Nuova giur. civ. com*., 4, 2024

Picozza E., *Intelligenza artificiale e diritto. Politica, diritto amministrativo and artificial intelligence*, in *Giur. it*., 7, 2019

Picozza E., *Politica, diritto amministrativo e Artificial Intelligence*, in *Giur. it.*, 7, 2019

Pirelli C., *L'AI Act: gestione del rischio e tutela dei diritti*, in *Giur. it.*, 2, 2025

Plaat A., van Duijn M., et al., *Agentic Large Language Models, a survey*, in *arXiv*, 2025

Poletti D., *Il quadro normativo del Data Governance Act: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Nuove leggi civ.*, 3, 2024

Polisetty S.M., Pendyala S.K., Prabhakaran S.P., *Strengthening data integrity and security via cloud administration and access control strategies*, in *International Journal of Computer Engineering and Technology*, 3, 2023

Pollicino M. C., *Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa*, in *Riv. it. infor. dir.*, 1, 2025

Ponte D., *Serve conoscenza e comprensione della decisione "automatizzata" (nota a Tar Campania, Sez. III, 14 novembre 2022, n. 7003)*, in *Guida dir.*, 46, 2022

Ponti B., *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in *Riv. it. infor. dir.*, 2, 2024

Prakken H., *On Evaluating Legal-Reasoning Capabilities of Generative AI*, in *CEUR WS*, 2024

Proietti G., *Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico*, in *Contratto e impresa*, 3, 2024

Prosperetti E., *Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del Tar Lazio*, in *Dir. inform*, 4, 2019

Puigpelat O.M., *The impact of the AI Act on public authorities and on administrative procedures*, in *Ceridap*, 4, 2023

Puzzanghera A., *La sfida tecnologica alla legalità amministrativa*, in *Riv. it. infor. dir.*, 2, 2022

Rallo Lombarte A., *Las administraciones independientes: una aproximaciòn constitucional*, in C. P. Chuvi, B.T. Mallén (Eds.), *Las administraciones independientes*, Valencia, 11, 2009

Raganelli B., *Decisioni pubbliche e algoritmi: modelli alternativi di dialogo tra forme di intelligenze diverse nell'assunzione di decisioni amministrative*, in *federalismi.it*, 22, 2020

Rebora G., *Public Management: una prospettiva di scienza dell'organizzazione*, in *Riv. it. public management*, 1, 2018

Renzi A., *La sicurezza cibernetica: lo stato dell'arte*, in *Giornale di diritto amministrativo*, 4, 2021

Resta F., *Articolo 70*, in A. Mantelero, G. Resta, G.M. Riccio (a cura di), *Intelligenza artificiale. Commentario*, Milano, 2025

Řezníková S., *Regulating AI – borders of freedom and sovereignty*, in *Ceridap*, 2026

Rhodes R.A.W., *Foreword: Governance and Networks, in G. Stoker, The New Management of British Local Governance*, Macmillan, Londra, 1999

Rhodes R.A.W., *The New Governance: Governing without Government*, in *Pol. Studies*, 1996

Rhodes R.A.W., *Understanding Governance: policy networks, governance, reflexivity and accountability*, Open University Press, Philadelphia, 1997

Ricci A., *Introduzione al Regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *Nuove leggi civ.*, 4, 2024

Rich E., *Artificial Intelligence,* New York, 1983

Ricolfi M., *L'impiego di opere protette come input e come output dell'intelligenza artificiale*, in *Dir. ind.*, 5, 2024

Ridolfi M., *Servizi di informazione e cybersicurezza*, in *Giorn. dir. amm.*, 2, 2023

Rizzi M.A., Serini F., *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Riv. it. infor. dir.*, 2, 2024

Romano A., *Amministrazione, principio di legalità e ordinamenti giuridici*, in *Dir. amm*. 1, 1999

Romano S., *Organi*, in M. Croce, M. Goldoni (a cura di), *Frammenti di un dizionario giuridico*, Quodlibet, 2019

Rossa S., *Cyber attacchi e incidenti nella pubblica amministrazione, tra organizzazione amministrativa e condotta del funzionario*, in *Vergentis. Revista de Investigación de la Cátedra Internacional Conjunta Inocencio III*, 17, 2023

Rossa S., *Cybersecurity e pubblica amministrazione*, Ed. scientifica, Napoli, 2023

Rotondo F., *Principi di public governance nei sistemi integrati di offerta turistica*, Giappichelli, Torino, 2011

Rugolo A., *Intelligenza Artificiale: la rivoluzione della Cybersecurity*, in *Difesa online,* https://www.difesaonline.it/evidenza/cyber/intelligenza-artificiale-la-rivoluzione-della-cybersecurity

Rum A.L., *Il provvedimento amministrativo adottato mediante algoritmo: il ruolo dell'intelligenza artificiale nel processo decisionale della P.A.*, in www.ildirittoamministrativo.it

Ruohonen J., Mickelsson S., *Reflections on the Data Governance Act*, in *Digital Society*, 2, 2023, doi.org/10.1007/s44206-023-00041-7

Russell S.J., Norvig P., *Artificial intelligence: a modern approach*, 2017

Russell S.J., Norvig P., *Artificial Intelligence. A modern approach*, Pearson Ed., 2010

Rustichelli R., *L'autorità garante della concorrenza e del mercato: origini e prospettive*, in *Riv. Corte conti*, 1, 2022

Saito-Jensen M., *Multilevel Governance Theory*, in *Theories and Methods for the Study of Multilevel Environmental Governance*, Center for International Forestry Research, 2015, http://www.jstor.org/stable/resrep02152.5

Sala G., *Potere amministrativo e principi dell'ordinamento*, Milano, 1993

Salanitro U., *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. civ.*, 6, 2020

Sandulli A.M., *Il procedimento amministrativo*, Milano, 1940

Santaniello M., *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics*, 3, 2021

Saporito A., V*erso una "nuova" amministrazione digitale*, in *Ambientediritto.it*, 2, 2023

Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996

Sartor G., *L'intelligenza artificiale e il diritto*, Torino, 2022

Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, Milano, 2020

Sartoretti C., *Le* authorities *al tempo del covid-19. Riflessioni sul ruolo delle autorità indipendenti: modello in declino o consolidato?*, in *DPCE*, 2, 2021

Satta F., *Principio di legalità e pubblica amministrazione nello Stato democratico*, Padova 1969

Scarciglia R., *Artificial intelligence and the state from a comparative perspective*, in *IJPL*, 2, 2025

Scarselli G., *Autorità amministrative indipendenti: appunti per una possibile riforma*, in *Il Foro Italiano*, 126(11), 231/232-249/250. http://www.jstor.org/stable/23197926

Schiavello A., *Osservazioni in margine a Legal Reasoning and Legal Theory di Neil MacCormick a venti anni dalla pubblicazione*, in *Foro It*., 1999

Schmitz C., Rystrøm J., Batzne J., *Oversight structures for agentic ai in public-sector organizations*, in *arXiv*, 2025

Schneider J., *Generative to Agentic AI: Survey, Conceptualization, and Challenges*, in *arXiv*, 2025

Schroeder de Witt C., Elkins K., *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US*, in *arXiv*, 2025

Schuilenburg M., Peeters R., *Algorithmic Governance: Technology, Power, and Knowledge*, in *The SAGE Handbook of Digital Society*, 2023

Schwartz R., Vassilev A., et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, *NIST special publication 1270*, *National Institute of Standard Technologies*, 2022

Schiavello L., *Responsabilità contabile formale e amministrativa*, Jovene, Napoli, 1987

Schlitzer E.F., Mirabelli C. (a cura di), *Trattato sulla nuova configurazione della giustizia contabile, Editoriale scientifica*, Napoli, 2018

Scoca F. G., *La pubblica amministrazione come organizzazione*, in L. Mazzarolli, G. Pericu, A. Romano, F.A. Roversi Monaco, F.G. Scoca (a cura di), *Diritto amministrativo*, Bologna, 1998

Scoca F.G. (a cura di), *La responsabilità amministrativa ed il suo processo*, CEDAM, Padova, 1997

Scognamiglio A., *Rileggendo la voce "interesse" di Cannada Bartoli, qualche riflessione sul metodo*, in *Dir. amm.*, 4, 2022

Sengar S.S., Hasan A.B., et al. *Generative artificial intelligence: a systematic review and applications*, in *Multimed Tools Appl,* 84, 2025

Sforna M., *Le garanzie di conoscibilità degli algoritmi e l'esigenza di assicurare un controllo umano del procedimento amministrativo (c.d. human in the loop). (Nota a Tar Campania, Sez. III, 14 novembre 2022, n. 7003)*, in www.giustiziainsieme.it

Sgueo G., *Governare le macchine. Governare con le macchine*, in *Rivista dello Stato digitale*, 1, 2025

Sgueo G., *La transizione digitale*, in *Gior. dir. amm.*, 6, 2021

Sgueo G., *Le autorità amministrative indipendenti: genesi, funzioni e ruolo*, in *www.diritto.it*, 14 giugno 2007

Sharma G. D., Yadav A., Chopra R., *Artificial intelligence and effective governance: A review, critique and research agenda*, in *Sustainable Futures*, 2, 2020, doi.org/10.1016/j.sftr.2019.100004

Simoncini A., *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin, D.U. Galetta, *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020

Song Z., Zhao R., et. al., *Injecting Domain-Specific Knowledge into Large Language Models: A Comprehensive Survey*, in *arXiv*, 2025

Sordi B., *Il principio di legalità nel diritto amministrativo che cambia. La prospettiva storica*, in *Dir. amm*., 1, 2008

Sousa e Silva N., *The Artificial Intelligence Act: Critical Overview*, 2024, disponibile in ssrn.com/abstract=4937150

Spagnuolo Vigorita R., *Potere amministrativo, poteri e interessi privati*, in *Ceridap*, 2, 2024

Studer R., Benjamins V. R., Fensel D., *Knowledge Engineering: Principles and Methods*, in *Data & Knowledge Engineering*, Vol. 25, issues 1–2, 1998

Szolovits P., *Knowledge-Based Systems: A Survey*, in M.L. Brodie, J. Mylopoulos (a cura di), *On Knowledge Base Management Systems. Topics in Information Systems*, Springer, 1986

Tallaro F., *La digitalizzazione del ciclo di vita dei contratti pubblici*, in *giustizia-amministrativa.it*, 2023

Tasso C., *Attori, processi, meriti e responsabilità nell'utilizzo di algoritmi di Intelligenza Artificiale: il caso del Machine Learning*, in R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino, 2021

Terranova F., *Il ragionamento giuridico*, Giuffrè, 2021

Tewari A., *If generative AI is the answer, what is the question?*, in *arXiv*, 2025

Tomaževič N., Murko E., Aristovnik A., *Organisational Enablers of Artificial Intelligence Adoption in Public Institutions: A Systematic Literature Review*, in *Central European Public Administration Review*, 1, 2024

Tornatzky L.G., Fleischer M., *The process of technological innovation*, Lexington Book. Massachussets/Toronto, 1990

Torchia L., *Lo stato digitale. Una introduzione*, Il Mulino, Bologna, 2023

Torchia L., *Pubblica amministrazione e transizione digitale*, in *Gior. dir. amm.*, 6, 2024

Toschei S., Puzzanghera A., *La crisi del principio di legalità amministrativa*, in *Dir. pubbl. comp. eur.*, 4, 2022

Traverso P., *Breve introduzione tecnica all'Intelligenza Artificiale*, in *DPCE online*, 1, 2022

Trigka M., Dritsas E., *The Evolution of Generative AI: Trends and Applications*, in *IEEE Access*, vol.13, 2025

Tritto N.M., *Il danno erariale da intelligenza artificiale*, in *Federalismi.it*, 2, 2024

Tronca L., *Verso un'analisi strutturale delle forme di governance*, in *Studi sociologia*, 3, 2007

Turchini V., *Le autorità amministrative indipendenti oggi. La necessità di un approccio storico e comparato*, in *Quad. Corte conti*, 1, 2022

Umar M., Mehmood A., Song H., *A Survey on State-of-the-Art Knowledge-based System Development and Issues*, in *The Smart Computing Review*

Valentine M. A., Pratt A.L., et al., *The Algorithm and the Org Chart: how algorithms can conflict with organizational structures*, in *Proceedings of the ACM on Human-Computer Interaction,* Volume 8, Issue CSCW2, 2024

Vercelli A., *United Nations, artificial intelligences and regulations: analysis of the General Assembly AI Resolutions and the Final Report of the Advisory Body on AI*, in *3rd Workshop on Bias, Ethical AI, Explainability and the Role of Logic and Logic Programming (BEWARE24), co-located with AIxIA 2024, November 25-28, 2024, Bolzano, Italy*, https://ceur-ws.org/Vol-3881/paper11.pdf

Vesperini G., *Il diritto amministrativo europeo e le trasformazioni istituzionali dell'Unione europea*, in *Gior. dir. amm.*, 6, 2024

Vioque R. G., *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público [BOE n.o 236, de 2-X-2015]*, in *Ars Iuris Salmanticensis*, 1, 2016

von Krogh G., *Artificial Intelligence in Organizations: New Opportunities for Phenomenon-Based Theorizing*, in *Academy of Management*, 2018

Voss E., *EU Agencies, Common Approach and Parliamentary Scrutiny*, *European Parliamentary Research Service*, 2018

Wang T., Wang Y., et al., *Deep Learning and Machine Learning – Generative Models: Foundations, Techniques, and Applications*, 2024, p. 164, disponibile in ssrn.com/abstract=5211980 oppure dx.doi.org/10.2139/ssrn.5211980

Waswani A., Shazeer N. et al., *Attention is all you need*, in *arXiv*, 2017

Zoppoli L., *A dieci anni dalla riforma Bassanini: dirigenza e personale*, in www.astrid.it

Zorzi Galgano N., *Il Regolamento UE 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contratto impresa.*, 1, 2025

UNIVERSITÀ
DEGLI STUDI
DI TRIESTE

La borsa di dottorato è cofinanziata con risorse dell'Unione europea, NextGeneration EU - Piano Nazionale di Ripresa e Resilienza, Missione 4 – Componente 1 – Investimento 4.1 CUP J92B22000900007