DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Diritto Amministrativo

VERSO UNA PUBBLICA AMMINISTRAZIONE INTELLIGENTE: INNOVAZIONE TECNOLOGICA E DIRITTO AMMINISTRATIVO

Chiar.mo Prof. Aristide Police

RELATORE

Chiar.mo Prof. Bernardo Giorgio Mattarella

CORRELATORE

Vittorio Leozappa (Matr. 166993)

CANDIDATO

Anno Accademico 2024-2025

INDICE

INTRODUZIONE

L'evoluzione tecnologica che ha investito la società negli ultimi decenni sta ridefinendo le strutture istituzionali ed amministrative, le modalità di tutela dei diritti fondamentali e la sicurezza nazionale. A tal riguardo, l'intelligenza artificiale rappresenta l'ultima essenziale novità tecnologica capace di superare i confini dell'ambito industriale, interessando il funzionamento di settori fondamentali, tra cui l'amministrazione pubblica. Infatti, lo sviluppo di sistemi intelligenti è stato in grado di generare un acceso dibattito sociale, dottrinale e giurisprudenziale, in particolar modo per la sua implementazione nel settore giuridico ed amministrativo.

Lo sviluppo di algoritmi e tecniche di apprendimento – fino ai più sofisticati *machine learning* e *deep learning* – capaci di processare enormi quantità di dati in breve tempo ha mostrato, da un lato, l'indiscutibile utilità che può derivare dalla loro implementazione anche in settori pubblici e, dall'altro, le problematiche e difficoltà che sorgono in assenza di un'attenta e precisa regolamentazione.

In tal senso, l'Unione europea, con l'adozione del Regolamento 2024/1689/UE, anche noto come AI Act, ha tentato di creare un quadro normativo organico in grado di garantire un utilizzo consapevole ed antropocentrico dell'intelligenza artificiale. In altre parole, imponendo una serie di stringenti obblighi e limitazioni, la disciplina eurounitaria mira a garantire che i sistemi di intelligenza artificiale immessi sul mercato siano sicuri, rispettino i diritti fondamentali, la democrazia e lo Stato di diritto, e promuovano lo sviluppo affidabile e umano-centrico dell'IA.

In questo contesto, la pubblica amministrazione, orientata verso una sempre maggiore digitalizzazione, è chiamata a bilanciare l'implementazione di sistemi "intelligenti" con il rispetto dei principi costituzionali e dei diritti fondamentali. Se, infatti, l'adozione di sistemi di intelligenza artificiale nella pubblica amministrazione, da un lato, garantisce maggiore rapidità, semplificazione ed efficienza, dall'altro, solleva nuove sfide, tra tutte quella della *black box*, e problematiche giuridiche. Invero, l'implementazione di tali strumenti, oltre ad aver suscitato dubbi sul rispetto del fondamentale principio di legalità, si scontra con l'irrinunciabile necessità di garantire l'osservanza dei principi fondamentali formulati dalla normativa comunitaria e ripresi dalla giurisprudenza

amministrativa, tra cui quelli di trasparenza, conoscibilità e comprensibilità nonché di non esclusività della decisione algoritmica e non discriminazione.

Al contempo, la crescente digitalizzazione espone le amministrazioni pubbliche a rischi cibernetici sempre più sofisticati, rendendo la cybersicurezza una componente imprescindibile della *governance* istituzionale ed una condizione necessaria per l'effettività dei diritti e la continuità del servizio pubblico. In altre parole, la sicurezza cibernetica può essere considerata parte integrante del "buon andamento" dell'amministrazione e deve essere garantita attraverso strumenti tecnici, giuridici e organizzativi idonei. A tal fine, l'Unione europea ha adottato numerose direttive – la più recente la Direttiva (UE) 2022/2555, anche nota come NIS 2. Quest'ultima, recepita dal legislatore nazione con il d.lgs. n. 138/2024, con l'obiettivo di rafforzare il livello di sicurezza delle reti e dei sistemi informativi all'interno dell'Unione europea, in modo da garantire la resilienza operativa dei soggetti pubblici e privati che forniscono servizi essenziali o importanti per la società, impone una serie di obblighi stringenti alle pubbliche amministrazioni nazionali.

La crescente importanza delle nuove tecnologie e la loro influenza sulla sicurezza dello spazio cibernetico sono, altresì, dimostrate dall'istituzione di un'apposita agenzia, l'Agenzia per la cybersicurezza nazionale (ACN), che esercita funzioni essenziali non solo nell'ambito della sicurezza cibernetica nazionale e comunitaria, ma anche in materia di intelligenza artificiale, essendo stata designata dal legislatore nazionale come Autorità nazionale per l'intelligenza artificiale.

Obiettivo del presente lavoro, che a tal fine ripercorre il dibattito dottrinale e giurisprudenziale intorno ai principali temi sollevati dall'avvento dell'intelligenza artificiale e dalla sua implementazione nella pubblica amministrazione, è esaminare e comprendere il rapporto tra intelligenza artificiale, legalità algoritmica e sicurezza cibernetica, con particolare attenzione al ruolo, alle funzioni e agli obblighi della pubblica amministrazione, nonché riflettere sulla compatibilità tra innovazione tecnologica e principi fondamentali dello Stato di diritto.

La trattazione è suddivisa in tre capitoli.

Il primo capitolo muove dalla nozione di intelligenza umana, per poi analizzare la nozione tecnica di intelligenza artificiale, ricostruendone l'evoluzione e

illustrando le principali tecniche e strutture computazionali che sostengono i sistemi di IA. Successivamente, approfondisce la nozione normativa di intelligenza artificiale, esaminando la regolamentazione comunitaria del GDPR e dell'AI Act, e concludendo con un riferimento all'intervento normativo italiano in materia (disegno di legge n. 1146).

Una volta delineato il quadro introduttivo con il primo capitolo, il secondo affronta la fondamentale tematica della legalità algoritmica. Più in dettaglio, dopo aver esaminato il principio di legalità alla luce dell'adozione di sistemi algoritmici e la qualificazione giuridica dell'algoritmo, l'analisi si concentra sui fondamentali principi per una pubblica amministrazione automatizzata, anche alla luce dell'articolo 30 del d.lgs. n. 36/2023 (Nuovo Codice dei contratti pubblici). Quindi, facendo riferimento ad importanti sentenze del TAR Lazio e del Consiglio di Stato, si approfondiscono i principi di trasparenza, non esclusività della decisione algoritmica e non discriminazione, evidenziandone criticità e applicazione pratica.

Il terzo ed ultimo capitolo, invece, incentra l'analisi sulla sicurezza cibernetica nazionale. Infatti, dopo aver definito la nozione stessa di cybersicurezza ed aver ripercorso il quadro normativo comunitario e nazionale di riferimento, lo studio si concentra sul ruolo, le funzioni e, in particolar modo, la natura giuridica dell'Agenzia per la cybersicurezza nazionale (ACN). Infine, prima di un attento esame della disciplina della sicurezza cibernetica nel settore dei contratti pubblici, si approfondisce la strategia per la sicurezza cibernetica della pubblica amministrazione.

CAPITOLO I

IL QUADRO TECNICO E NORMATIVO DELL'INTELLIGENZA ARTIFICIALE

SOMMARIO: **1. Intelligenza artificiale, algoritmi e tecnologie correlate** – 1.1. Nozione tecnica di intelligenza artificiale – 1.2. Evoluzione dell'intelligenza artificiale – 1.3. Algoritmi e tecniche di apprendimento nell'intelligenza artificiale – 1.3.1. Algoritmi nell'intelligenza artificiale – 1.3.2. Machine learning – 1.3.2.1. Apprendimento automatico supervisionato – 1.3.2.2. Apprendimento automatico non supervisionato – 1.3.2.3. Apprendimento automatico per rinforzo – 1.3.3. Reti neurali e deep learning – **2. La normativa sull'intelligenza artificiale** – 2.1. Nozione "giuridica" di intelligenza artificiale – 2.2. Dal GDPR… – 2.3. …all'AI Act – 2.3.1. La governance – 2.3.2. AI Act: un'eterogenesi dei fini? – 2.4. GDPR e AI Act: un breve confronto – 2.5. La normativa nazionale: il disegno di legge 1146.

1. Intelligenza artificiale, algoritmi e tecnologie correlate

1.1. Nozione tecnica di intelligenza artificiale

La comprensione dell'attuale nozione di intelligenza artificiale risulta particolarmente complessa, anche alla luce della mancanza di una definizione univoca e condivisa di intelligenza "naturale". Si può, tuttavia, affermare che il concetto di intelligenza concerne le capacità cognitive dell'uomo; più nello specifico, "*l'intelligenza è la capacità complessiva di un individuo di agire in modo propositivo, pensare razionalmente e interagire efficacemente con l'ambiente*".[1] Pertanto, l'intelligenza si rivela nella capacità di svolgere diverse funzioni – l'apprendimento dall'esperienza, la percezione, l'intuizione, il pensiero astratto –, nonché nella capacità di acquisire informazioni dall'ambiente circostante attraverso gli organi di senso, elaborarle ed agire nel modo più efficace ed efficiente.[2]

[1] D. Wechsler, '*The Measurement of Adult Intelligence*', The Williams and Wilkins Company, Baltimore, 1944, p. 3.
[2] G. Sartor, '*L'intelligenza artificiale e il diritto*', Giappichelli, Torino, 2022, p. 1.

L'intelligenza artificiale, come già anticipato da Alan Turing nel 1950 con riferimento ai "*digital computers*", mira a replicare l'intelligenza umana.[3] Infatti, John McCarthy, uno dei pionieri di questa disciplina, ha definito l'intelligenza artificiale come "*la scienza e l'ingegneria del fare macchine intelligenti, specialmente programmi intelligenti per computer. È connessa al compito simile di usare i computer per comprendere l'intelligenza umana, ma l'IA non ha la necessità di limitarsi a metodi che sono biologicamente osservabili*".[4]

L'intelligenza artificiale, quindi, se confrontata con l'essere umano, dovrebbe operare in modo razionale ed essere in grado di: i) agire umanamente, ossia comportarsi in modo indistinguibile da un essere umano; ii) pensare umanamente, risolvendo problemi attraverso processi cognitivi simili a quelli dell'uomo; iii) pensare razionalmente, basandosi sulla logica per elaborare soluzioni; iv) agire razionalmente, adottando un processo che le consenta di ottenere il miglior risultato possibile in base alle informazioni disponibili.[5]

Per raggiungere tali obiettivi, un sistema di IA deve possedere diverse capacità fondamentali. Innanzitutto, deve essere in grado di comprendere, ovvero di correlare dati ed eventi, riconoscendo e interpretando testi, immagini, tabelle, video e voci. Il ragionamento rappresenta un altro aspetto essenziale, poiché l'IA deve elaborare e analizzare simultaneamente un grande volume di informazioni attraverso algoritmi logici. Un ruolo chiave è svolto anche dall'apprendimento, reso possibile dalle tecniche di *machine learning*, che permettono al sistema di acquisire conoscenze dagli esempi forniti e di migliorare progressivamente le proprie prestazioni. Infine, l'interazione uomo-macchina (*Human-Computer Interaction*) consente all'IA di comunicare con gli esseri umani attraverso modalità percettive naturali.[6]

È opportuno, altresì, osservare come il termine "intelligenza artificiale" sia utilizzato in riferimento a due diverse tipologie della stessa: IA debole e IA forte. La prima, anche nota nella comunità scientifica come *narrow AI,* si riferisce a sistemi progettati per simulare alcune capacità cognitive umane, senza tuttavia

[3] A. M. Turing, '*Computing Machinery and Intelligence*', Mind, 59, 1950, pp. 433 e ss.
[4] J. McCarthy, 'What Is Artificial Intelligence', Stanford University, 2007.
[5] R. Marmo, '*Algoritmi per l'intelligenza artificiale – Progettazione, Machine Learning, Neural Network, Deep Learning, ChatGPT, Python*', Hoepli, 2024, p. 7.
[6] *Ibid.*

raggiungere un'intelligenza paragonabile a quella dell'uomo. Questi sistemi eseguono un solo lavoro determinato, replicando alcuni processi logici e decisionali, ma senza una reale comprensione. L'IA forte, invece, ha il fine di imitare l'insieme delle capacità cognitive umane, simulando il cervello umano nei suoi rapporti con l'intero mondo reale, o addirittura di sviluppare una forma di consapevolezza propria, indipendentemente dal fatto che i processi di pensiero siano simili a quelli umani.[7]

1.2. Evoluzione dell'intelligenza artificiale

L'idea di un'intelligenza artificiale regolata da principi etici trova un primo riferimento nelle opere di fantascienza di Isaac Asimov, che nel 1942 formulò le Tre leggi della robotica.[8] Queste regole, concepite per garantire la sicurezza e il controllo dei robot nei suoi racconti, stabiliscono che una macchina non possa nuocere agli esseri umani, debba obbedire ai loro ordini e debba proteggere la propria esistenza, purché ciò non sia in contrasto con le prime due leggi. Sebbene si tratti di un concetto letterario, tali principi hanno anticipato problematiche reali che oggi emergono nell'applicazione dell'IA.

Un passo fondamentale fu compiuto nel 1950 da Alan Turing, che, con il suo celebre Test di Turing[9], propose un criterio per valutare l'intelligenza di una macchina basato sulla sua capacità di imitare il comportamento umano in un gioco di domande e risposte.

L'intelligenza artificiale divenne ufficialmente un'area di ricerca con la Conferenza di Dartmouth del 1956, in occasione della quale John McCarthy, Marvin Minsky e altri studiosi definirono il concetto di *artificial intelligence*. Da quel momento ebbe inizio lo sviluppo di programmi capaci di simulare il ragionamento umano. Tra questi, il sistema ELIZA (1964-1966), progettato da Joseph Weizenbaum, rappresentò uno dei primi esempi di *chatbot* in grado di interagire con gli utenti attraverso il linguaggio naturale.[10]

---

[7] *Ibid*; S. Hénin, '*AI: Intelligenza Artificiale tra incubo e sogno*', Hoepli, 2019, pp. 41 e ss.
[8] I. Asimov, '*Runaround*' in *I, Robot*, Gnome Press, 1942, pp. 3 e ss.
[9] A. M. Turing, '*Computing Machinery and Intelligence*', Mind, 59, *cit.*, pp. 433 e ss.
[10] J. Weizenbaum, '*Computer Power and Human Reason: From Judgment to Calculation*', W. H. Freeman and Company, New York, 1976.

Negli anni successivi, la ricerca si concentrò su sistemi esperti, come il *General Problem Solver*, che utilizzava regole logiche per risolvere semplici problemi specifici.

La fine del XX secolo vide la nascita di IA capaci di competere con l'uomo in giochi complessi, come *Deep Blue* di IBM, che nel 1997 sconfisse il campione mondiale di scacchi Garry Kasparov.[11] Il XXI secolo segnò una svolta con l'accesso a enormi quantità di dati e miglioramenti nell'*hardware*, favorendo il boom dell'apprendimento automatico. Nel 2015, il programma *AlphaGo* di *Google DeepMind*, addestrato su milioni di partite, superò il campione mondiale di Go, dimostrando la potenza delle reti neurali profonde.[12]

Oggi, il *deep learning* consente alle IA di elaborare dati in modo sempre più simile al pensiero umano, grazie alle reti neurali artificiali, che imitano le connessioni cerebrali per affrontare problemi complessi in settori come informatica, elettronica e simulazione. Questi sviluppi rappresentano la frontiera dell'intelligenza artificiale, con applicazioni in continua espansione e nuove sfide etiche e regolatorie.

1.3. Algoritmi e tecniche di apprendimento nell'intelligenza artificiale

L'intelligenza artificiale si basa su un insieme di algoritmi e tecniche di apprendimento che consentono alle macchine di analizzare dati, riconoscere schemi e prendere decisioni in modo autonomo. Questi algoritmi, che variano in complessità e applicazione, rappresentano il cuore dei sistemi intelligenti e sono alla base dei progressi nel settore dell'IA. Tra le principali categorie di tecniche di apprendimento si distinguono il *machine learning* e il *deep learning*, due approcci che hanno rivoluzionato il modo in cui i sistemi informatici elaborano informazioni e acquisiscono conoscenza. Il *machine learning* si concentra sull'addestramento di

[11] D. Yao, '25 Years Ago Today: How Deep Blue vs. Kasparov Changed AI Forever', *AI Business*, 11 maggio 2022, https://aibusiness.com/ml/25-years-ago-today-how-deep-blue-vs-kasparov-changed-ai-forever?

[12] G. Caretto, '*Intelligenza artificiale di Google batte il campione mondiale di Go*', *Start Magazine,* 10 marzo 2016, https://www.startmag.it/innovazione/intelligenza-artificiale-google-batte-campione-mondiale-go/

modelli statistici per estrarre "*pattern*" dai dati, mentre il *deep learning*, attraverso reti neurali artificiali, consente di affrontare problemi complessi con un livello di astrazione più profondo.

1.3.1. Algoritmi nell'intelligenza artificiale

Il termine "algoritmo" ha origine dalla latinizzazione del nome di Al-Khwarizmi, un matematico arabo del IX secolo. In una sua opera del 825 d.C., intitolata *Kitab al-Hisab al-Hindi*, egli illustrò il metodo da seguire per risolvere le principali operazioni matematiche.[13] Sebbene non esista una definizione universalmente accettata di algoritmo, una comune proviene da un libro del 1971 scritto dall'informatico Harold Stone: "*Un algoritmo è un insieme di regole che definiscono con precisione una sequenza di operazioni*".[14] In altri termini, un algoritmo è una procedura di calcolo ben definita che, a partire da determinati valori in ingresso, fornisce determinati valori in uscita.[15] Quindi, lo scopo principale dell'uso degli algoritmi è la risoluzione dei problemi.

In informatica, gli algoritmi sono alla base di ogni programma e processo computazionale, compresi quelli che rientrano nel campo dell'intelligenza artificiale. È opportuno, a tal riguardo, chiarire la differenza tra l'algoritmo e il programma che lo esegue. L'algoritmo, infatti, rappresenta il procedimento logico astratto (ossia la regola) che consente di giungere alla soluzione di un problema, mentre il programma consiste nella sua traduzione in un linguaggio comprensibile e compatibile con la macchina che deve eseguirlo.[16]

Sebbene esistano diverse tipologie di algoritmo, è possibile identificare una serie di caratteristiche comuni che consentono di classificare una sequenza di operazioni come algoritmica.[17] Tali caratteristiche, definite per la prima volta negli anni '60 dal professore Donald Knuth della Stanford University, sono fondamentali per

[13] L. Laura, '*Breve e universale storia degli algoritmi*', Luiss University Press, 2019, p. 15.
[14] H.S. Stone, '*Introduction to Computer Organization and Data Structures*', McGraw-Hill, Inc., 1971.
[15] T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, '*Introduction to Algorithms*', The MIT Press, Fourth edition, 2022.
[16] R. Borruso, S. Russo, C. Tiberi, '*L'informatica per il giurista*', Giuffrè Editore, 2009, p. 210.
[17] *Ibid*, p. 207.

garantire che la sequenza possa effettivamente giungere al termine ed essere compresa. In primo luogo, un algoritmo deve essere finito, ossia composto da un numero determinato di operazioni necessarie per il raggiungimento della soluzione. Ogni algoritmo deve essere poi definito e non ambiguo, in modo che non vi siano incertezze nell'interpretazione della sequenza, né per l'esecutore umano né per la macchina. Inoltre, un algoritmo deve garantire che, a partire da tali dati, venga prodotto un risultato univoco e definito, rispondendo così al criterio di eseguibilità. Infine, un algoritmo deve essere generale, ossia capace di risolvere tutti i problemi appartenenti alla stessa classe, applicandosi quindi a un ampio numero di situazioni simili, piuttosto che limitarsi a casi specifici.

Queste caratteristiche comuni delineano la struttura fondamentale degli algoritmi, i quali, pur variando nella loro complessità e applicazione, costituiscono la base delle operazioni computazionali, inclusi gli avanzamenti nell'ambito dell'intelligenza artificiale.

1.3.2. *Machine learning*

Il concetto di *machine learning* fu introdotto dall'informatico statunitense Arthur Samuel, che, nel 1959, ipotizzò la realizzazione di una macchina capace di apprendere in modo autonomo.[18] L'obiettivo era sviluppare un metodo che permettesse ai sistemi di imparare dall'esperienza, riducendo così il tempo che un programmatore avrebbe dovuto impiegare per scrivere ogni passaggio necessario per giungere a una determinata soluzione. È forse proprio la traduzione italiana – sistema di apprendimento automatico – a chiarire la stessa nozione.

L'idea è, infatti, la seguente: "*un programma per computer R impara dall'esperienza E rispetto al compito T e alla misura di prestazione P, se le sue prestazioni nel compito T, misurate in P, migliorano con l'esperienza*".[19] In altre parole, il *machine learning* consente ai computer di migliorare le proprie capacità di risoluzione di un problema senza che ogni istruzione venga esplicitamente programmata, ma affinando le proprie prestazioni attraverso l'analisi dei dati e

[18] A. L. Samuel, '*Some Studies in Machine Learning Using the Game of Checkers*', IBM Journal of Research and Development 3, no. 3, luglio 1959, pp. 210-229.
[19] T. M. Mitchell, '*Machine learning*', McGraw-Hill Higher Education, New York, 1997, p. 2.

l'esperienza accumulata. Questo approccio permette ai sistemi di adattarsi a nuovi scenari e di ottimizzare le proprie risposte nel tempo, rendendoli più efficienti e versatili nell'elaborazione delle informazioni e nel raggiungimento degli obiettivi prestabiliti.

Risultano, quindi, evidenti i vantaggi di questi sistemi di autoapprendimento, tra cui un ridotto intervento umano, la possibilità di miglioramento continuo, la capacità di gestione di un'enorme quantità di dati di varia natura nonché quella di previsione di determinati comportamenti.[20]

Al contempo, però, è opportuno sottolineare, tra le problematiche principali, quella della trasparenza e interpretabilità. Questo problema, noto come il *black box problem* o *machine learning explainability*[21], si riferisce alla difficoltà di comprendere il funzionamento interno di modelli complessi e si verifica principalmente a causa della non linearità dei modelli di apprendimento automatico. I modelli avanzati, inclusi i sistemi di *deep learning* e le reti neurali profonde, operano su milioni di parametri, rendendo impossibile per un essere umano tracciare in modo diretto il processo decisionale.[22] È, pertanto, il funzionamento di questi sistemi a rendere complessa l'attribuzione precisa del peso di ogni variabile nell'*output* finale del modello.[23] Altresì, le decisioni prese dai modelli sono spesso dipendenti dai dati di addestramento, il che significa che eventuali *bias*[24] nei dati si riflettono nelle previsioni senza un chiaro meccanismo giustificativo.

L'impossibilità di conoscere e comprendere il percorso logico seguito dalla macchina per raggiungere una soluzione rappresenta, infatti, un problema di grande rilievo perché, da un lato, impedisce ai programmatori di sapere dove intervenire per correggere eventuali anomalie[25] e, dall'altro, può portare a decisioni arbitrarie

---

[20] R. Marmo, '*Algoritmi per l'intelligenza artificiale – Progettazione, Machine Learning, Neural Network, Deep Learning, ChatGPT, Python*', *cit.*, p. 134.
[21] Si veda *infra* capitolo 2, paragrafo 4.1.1.
[22] J. Burrell, '*How the machine 'thinks': Understanding opacity in machine learning algorithms*', Big Data & Society, 2016.
[23] C. Molnar, '*Interpretable Machine Learning*', Leanpub, 2020.
[24] *Il bias algoritmico si verifica quando un algoritmo produce risultati sistematicamente distorti a causa dei pregiudizi presenti nei dati di addestramento o nelle scelte di progettazione. Questi pregiudizi possono derivare da vari fattori, tra cui la selezione dei dati, le modalità di raccolta e le ipotesi implicite fatte durante lo sviluppo del modello*. Cfr. L. Di Giacomo, '*Algoritmi e bias: come l'intelligenza artificiale può riprodurre o combattere i pregiudizi*', Diritto.it, 23 agosto 2024, https://www.diritto.it/algoritmi-bias-intelligenza-artificiale-pregiudizi/
[25] R. Marmo, '*Algoritmi per l'intelligenza artificiale – Progettazione, Machine Learning, Neural Network, Deep Learning, ChatGPT, Python*', *cit.*, p. 135.

o discriminatorie, come evidenziato dall'uso degli algoritmi di predizione del rischio nel sistema giudiziario statunitense.[26]

Per affrontare questa problematica sono stati sviluppati diversi approcci, tra cui metodi intrinseci che privilegiano modelli interpretabili per costruzione, metodi *post-hoc* come LIME e SHAP che forniscono spiegazioni locali sulle decisioni del modello, e tecniche basate sulla decomposizione della rete neurale che attribuiscono importanza alle variabili analizzate.[27]

Dal punto di vista normativo, si è cercato di arginare il problema mediante l'adozione di due regolamenti comunitari. Il primo è il Regolamento Generale sulla protezione dei dati (GDPR), che all'articolo 22 stabilisce il diritto degli individui a non essere soggetti a decisioni automatizzate se queste producono effetti giuridici che li riguardano significativamente o li influenzano in modo analogo.[28] Il secondo è l'AI Act che ha introdotto un quadro normativo specifico per i sistemi di intelligenza artificiale, imponendo obblighi di trasparenza. In particolare, l'articolo 13[29] prevede che i sistemi ad alto rischio forniscano informazioni adeguate sul loro funzionamento, mentre l'articolo 14[30] impone, sempre con riferimento ai sistemi ad alto rischio, l'obbligo di sorveglianza umana e prescrive requisiti di interpretabilità per garantire che gli utenti possano comprendere le decisioni dei sistemi.

Sebbene tali interventi normativi abbiano, tra gli altri, l'obiettivo di risolvere il problema della *black box* attraverso meccanismi di trasparenza e supervisione, per comprendere le cause è necessario esaminare il modo in cui i sistemi di IA imparano e prendono decisioni. A tal fine è utile distinguere tre principali forme di apprendimento automatico: apprendimento supervisionato, apprendimento non supervisionato e apprendimento per rinforzo.

[26] *State v. Loomis*, Supreme Court of Wisconsin (881 N.W.2d 749), 2016.
[27] In materia A. Bhattacharya, '*Applied Machine Learning Explainability Techniques*', Packt Publishing, 2022.
[28] Regolamento (UE) 2016/679, art. 22 – *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.*
[29] Regolamento (UE) 2024/1689, art. 13 – *Trasparenza e fornitura di informazioni ai deployer.*
[30] Regolamento (UE) 2024/1689, art. 14 – *Sorveglianza umana.*

1.3.2.1. Apprendimento automatico supervisionato

Per apprendimento automatico supervisionato si intende un metodo in cui alla macchina viene fornito un dataset di esempio (*training set*) per sviluppare diversi algoritmi in grado di associare le caratteristiche dei dati a un'etichetta specifica. Successivamente, questi algoritmi vengono sottoposti a validazione tramite il *validation set*, permettendo di identificare quello con le migliori prestazioni. Infine, l'algoritmo selezionato viene valutato su un ulteriore insieme di dati (*test set*), verificando la sua capacità di effettuare previsioni su dati nuovi e non etichettati.[31]

Più nello specifico, il *training set* è l'insieme iniziale di dati esemplificativi fornito alla macchina, in cui ogni *input* è associato a un *output* atteso. Questo consente al modello di analizzare le correlazioni tra le variabili e individuare schemi ricorrenti che possono essere descritti matematicamente attraverso una funzione. Una volta riconosciute queste relazioni, la macchina sarà in grado di applicarle per prevedere l'*output* di nuovi dati non ancora osservati.

Il *validation set*, estratto dal *dataset* iniziale, ha il compito di valutare le prestazioni dei modelli appresi, aiutando a selezionare quello più efficace nel generalizzare la relazione tra *input* e *output*. Questo passaggio è cruciale per identificare il modello più accurato nel predire risultati su dati non etichettati.

Infine, il *test set* è un insieme di dati distinto da quelli usati in precedenza, utilizzato per misurare l'effettiva capacità predittiva della funzione selezionata. Questa fase permette di verificare le prestazioni del modello su nuovi dati e di valutare la sua robustezza nell'affrontare casi reali.[32]

Gli *step* descritti sono essenziali per evitare il fenomeno dell'*overfitting*, che si verifica quando la funzione appresa si adatta eccessivamente alle peculiarità del *training set*, invece di cogliere le caratteristiche generali del problema da risolvere. In tal caso, il modello mostrerebbe un'elevata accuratezza predittiva sui dati di addestramento, ma le sue prestazioni calerebbero drasticamente quando applicato

[31] O. Colpani, '*Machine Learning: la capacità di prevedere applicata alla ricerca e alla pratica clinica*', Giornale Italiano di Farmacoeconomia e Farmacoutilizzazione, vol. 11, n. 4, 2019, p. 6.
[32] *Ibid*.

al *test set*, compromettendo la sua capacità di generalizzazione su dati non etichettati.[33]

1.3.2.2. Apprendimento automatico non supervisionato

I sistemi di *unsupervised learning* analizzano dati senza ricevere etichette o categorie predefinite. A differenza dell'apprendimento supervisionato, in cui un algoritmo viene addestrato su un *dataset* con *input* e *output* noti, nell'apprendimento non supervisionato l'obiettivo è scoprire strutture nascoste, schemi e relazioni nei dati. Di conseguenza, questi metodi si basano esclusivamente sull'identificazione di *pattern* e strutture nei dati di *input*.[34] Gli scopi principali dell'apprendimento automatico non supervisionato includono l'analisi della distribuzione dei dati, la ricerca di una struttura nascosta in gruppi di dati non etichettati e la loro suddivisione in gruppi omogenei in base a caratteristiche comuni. Un aspetto cruciale di questi metodi è che la valutazione delle loro prestazioni risulta spesso complessa, poiché la qualità dei risultati dipende dal contesto applicativo e può essere soggettiva.

Le tecniche più diffuse comprendono il *clustering* e la riduzione della dimensionalità.

Il *clustering* permette di raggruppare i dati in modo che gli elementi appartenenti a uno stesso *cluster* condividano caratteristiche simili, mentre quelli appartenenti a *cluster* distinti risultino differenti secondo una data metrica. Tra i numerosi algoritmi di *clustering*, due dei più utilizzati sono il *k-means clustering* e il *clustering* gerarchico. Il primo suddivide i dati in k gruppi, determinando un centroide[35] per ciascun *cluster* e assegnando ogni punto al *cluster* il cui centroide è più vicino. Il *clustering* gerarchico, invece, costruisce una gerarchia di *cluster* mediante un processo di ottimizzazione sequenziale, seguendo due strategie principali: l'approccio agglomerativo, che unisce progressivamente *cluster*

[33] *Ibid,* p. 7.
[34] *Ibid,* p. 8.
[35] *Il centroide di ogni cluster, o centro, è la media o la mediana di tutti i punti del cluster a seconda dei dati.* IBM, 'Cos'è il clustering?', 21 febbraio 2024, https://www.ibm.com/it-it/think/topics/clustering#:~:text=Il%20clustering%20%C3%A8%20un%20algoritmo,base%20a%20somiglianze%20o%20modelli.

inizialmente separati, e quello divisivo, che invece suddivide iterativamente i dati in gruppi più piccoli.[36]

La riduzione della dimensionalità, invece, si concentra sulla semplificazione dei dati mantenendone il più possibile la struttura originale. Tra gli strumenti tradizionali rientrano l'analisi delle componenti principali (PCA) e la decomposizione ai valori singolari (SVD).

Infine, gli algoritmi di *unsupervised learning* vengono spesso impiegati per il *pre-processing* dei dati, comprimendoli e rendendoli più gestibili prima della loro elaborazione da parte di reti neurali o altri modelli di apprendimento supervisionato.[37]

1.3.2.3. Apprendimento automatico per rinforzo

L'apprendimento per rinforzo è un paradigma di apprendimento automatico in cui un agente impara a prendere decisioni interagendo con l'ambiente per massimizzare un segnale numerico di ricompensa. Si tratta di una forma di apprendimento per tentativi ed errori: l'agente esplora diverse azioni, osserva le loro conseguenze e affina la sua strategia nel tempo. In particolare, l'apprendimento per rinforzo permette a una macchina di apprendere un comportamento ottimale (*policy*) senza ricevere istruzioni dirette, ma affinando le proprie decisioni attraverso l'esperienza. L'agente, interagendo con l'ambiente, esplora diverse azioni e, in base alle conseguenze che producono, riceve rinforzi positivi (*reward signals*) o negativi (*punishments*) al fine di adattare progressivamente la propria strategia per massimizzare il successo nel lungo termine.[38]

Una caratteristica fondamentale è la sua natura *closed-loop*: le azioni dell'agente influenzano gli *input* futuri, creando un ciclo di *feedback* continuo. Questo processo prevede che l'agente rilevi lo stato attuale dell'ambiente, selezioni un'azione da un insieme di scelte possibili e riceva una risposta dall'ambiente sotto forma di una ricompensa che indica l'efficacia dell'azione. L'agente aggiorna quindi la sua

[36] V. Maini and S. Sabri, '*Machine Learning for Humans*', 2017, pp. 56 e ss.
[37] O. Colpani, '*Machine Learning: la capacità di prevedere applicata alla ricerca e alla pratica clinica*', cit., p. 8.
[38] R.S. Sutton, A. Barto, '*Reinforcement Learning: an Introduction*', The MIT Press, Cambridge, MA, 2018, pp. 1-2.

strategia, bilanciando l'esplorazione – provando nuove azioni per migliorare la conoscenza – e lo sfruttamento – scegliendo le azioni che in precedenza hanno prodotto alte ricompense. Nel corso del tempo, questo processo consente all'agente di apprendere una politica ottimale, una mappatura dagli stati alle azioni che massimizza le ricompense cumulative.[39]

Si tratta di una forma di apprendimento che trova principale applicazione nel campo della robotica. Un esempio proprio in questo campo è utile per comprendere il funzionamento di questo approccio.[40] Immaginiamo un robot che si muove in un ambiente sconosciuto. Il robot può compiere azioni, come avanzare in una determinata direzione, ma non conosce *a priori* quali scelte siano corrette o errate. Ogni volta che esegue un'azione, l'ambiente risponde fornendogli un riscontro: se l'azione lo mantiene sul percorso corretto, riceve una ricompensa; se invece lo porta fuori strada, subisce una penalità. Questo processo si ripete continuamente, creando un ciclo di apprendimento in cui il robot affina progressivamente il proprio comportamento. Quindi, inizialmente esplora il terreno compiendo scelte casuali, ma con il tempo impara a distinguere quali azioni gli permettono di avanzare in sicurezza e quali lo conducono a errori. Il suo obiettivo è "generare una buona *policy*, con il massimo dei premi e il minimo delle punizioni".[41] Alla fine, grazie all'accumulo di esperienza e al meccanismo di rinforzo, il robot sviluppa una strategia ottimale che gli permette di navigare l'ambiente in modo sempre più efficace, senza la necessità di istruzioni predefinite.

1.3.3. Reti neurali e *deep learning*

Le reti neurali artificiali nascono dall'idea di riprodurre, almeno in parte, il funzionamento del cervello umano attraverso sistemi computazionali ispirati ai neuroni biologici.

[39] *Ibid*, pp. 2-9.
[40] R. Marmo, '*Algoritmi per l'intelligenza artificiale – Progettazione, Machine Learning, Neural Network, Deep Learning, ChatGPT, Python*', *cit.*, p. 368.
[41] Ibid, p. 367.

Le basi teoriche delle reti neurali furono poste negli anni ’40 dai ricercatori McCulloch e Pitts, che svilupparono un modello matematico del neurone.[42] Secondo questa rappresentazione, un neurone riceve segnali da più ingressi, li elabora e produce un’uscita, seguendo un principio simile agli operatori logici utilizzati in matematica. Sebbene questo modello fosse una semplificazione estrema del funzionamento reale del cervello, esso rappresentò il primo passo verso lo sviluppo delle neuroscienze computazionali e delle reti neurali artificiali.

Un importante avanzamento si ebbe nel 1958 con la creazione del percettrone, un sistema più evoluto in grado di pesare gli *input* e modificare i propri parametri nel tempo, migliorando così le sue prestazioni.[43]

Per comprendere, quindi, il funzionamento delle reti neurali artificiali, è utile avere una conoscenza elementare del funzionamento del cervello umano. Il nostro cervello è costituito da una vasta rete di neuroni, ognuno dei quali possiede un corpo centrale (soma) e una serie di prolungamenti, i dendriti, che ricevono segnali, e un assone, che trasmette impulsi ad altri neuroni. La comunicazione tra neuroni avviene attraverso le sinapsi, punti di connessione che permettono il passaggio di segnali elettrici o chimici.[44]

Quando un neurone riceve un segnale, elabora l’*input* e lo trasmette ad altri neuroni. Tuttavia, non tutti i neuroni reagiscono allo stesso modo: solo quelli che ricevono un impulso superiore a una determinata soglia si attivano, contribuendo alla propagazione del segnale. Questo meccanismo, ripetuto su una scala enorme, permette al cervello di elaborare informazioni complesse, come riconoscere un oggetto, percepirne la distanza e coordinare un’azione per afferrarlo.[45]

Le reti neurali artificiali si ispirano a questo modello biologico, sostituendo i neuroni con unità computazionali chiamate percettroni. Ogni percettrone riceve degli *input* numerici, ai quali vengono assegnati pesi che determinano la loro rilevanza nel calcolo complessivo. Se la somma pesata degli *input* supera una soglia

[42] W. S. McCulloch, W. Pitts, ‘*A Logical Calculus of the Ideas Immanent in Nervous Activity*’, The Bulletin of Mathematical Biophysics, vol. 5, 1943, pp. 115-116.
[43] G. Roncaglia, ‘*L’architetto e l’oracolo*’, Editori Laterza, 2023, par. 9.
[44] L. Colucci D’Amato, U. Di Porzio, ‘*Introduzione Alla Neurobiologia: Meccanismi Di Sviluppo, Funzione e Malattia Del Sistema Nervoso Centrale*’, Springer, Milano, 2011, pp. 35-36.
[45] G. Roncaglia, ‘*L’architetto e l’oracolo*’, *cit.*, par. 9.

prestabilita, il percettrone si attiva e trasmette il segnale alle unità successive, proprio come un neurone che invia un impulso lungo il suo assone.[46]

Attraverso questa struttura, una rete neurale artificiale è in grado di elaborare informazioni, identificare schemi e generare *output* sulla base dei dati ricevuti. Questo processo consente alla macchina di rappresentare matematicamente un problema e di "ragionare" su di esso, arrivando a una soluzione senza che ogni passaggio debba essere programmato esplicitamente.

Una serie di sviluppi in materia ha permesso di addestrare efficacemente reti neurali con molti strati, eliminando le precedenti limitazioni. Le reti con molti strati sono chiamate reti neurali profonde e il sottocampo dell'apprendimento automatico che si concentra su queste reti è chiamato *deep learning*.[47]

Il *deep learning* rappresenta, quindi, un'evoluzione delle reti neurali artificiali, caratterizzata dall'uso di strutture più complesse e profonde. A differenza delle reti neurali tradizionali, che spesso contano solo pochi strati di neuroni artificiali, il *deep learning* utilizza reti neurali profonde (*deep neural networks*), composte da molteplici livelli di unità computazionali, chiamati strati nascosti.[48]

Questi strati intermedi consentono alla rete di apprendere rappresentazioni gerarchiche dei dati: i livelli più bassi individuano caratteristiche elementari (ad esempio, linee e colori nelle immagini), mentre i livelli più alti elaborano concetti più astratti e complessi (come il riconoscimento di volti o oggetti).

Il funzionamento del *deep learning* si basa su un processo di addestramento in cui la rete neurale viene esposta a grandi quantità di dati. Durante questa fase, i pesi assegnati agli *input* vengono continuamente aggiornati attraverso un algoritmo chiamato *backpropagation*, che minimizza l'errore tra il risultato ottenuto e quello atteso.

A seconda del compito, vengono utilizzate architetture diverse. Le reti neurali convoluzionali (ConvNets) sono specializzate nell'analisi di immagini e video, sfruttando pesi condivisi e gerarchie spaziali per rilevare caratteristiche come bordi, *texture* e oggetti. Le reti neurali ricorrenti (RNN) elaborano dati sequenziali, come

---

[46] F. Sisini, '*Introduzione alle reti neurali con esempi in linguaggio C*', Autopubblicazione, 2020.
[47] C.M. Bishop, H. Bishop, '*Deep Learning – Foundations and Concepts*', Springer Nature, 2024, p. 20.
[48] R. Marmo, '*Algoritmi per l'intelligenza artificiale – Progettazione, Machine Learning, Neural Network, Deep Learning, ChatGPT, Python*', *cit.*, pp. 334 e ss.

il parlato e il testo, mantenendo la memoria degli *input* precedenti, consentendo loro di cogliere le dipendenze temporali.[49]

Nel complesso, quindi, il *deep learning* permette di compiere progressi significativi in ambiti quali il riconoscimento visivo, la comprensione del linguaggio naturale, l'elaborazione del parlato e la ricerca scientifica. Il principale vantaggio di questa metodologia risiede nella capacità del sistema di apprendere rappresentazioni complesse direttamente dai dati, riducendo la dipendenza dalla programmazione manuale delle caratteristiche e favorendo un'elaborazione più efficiente e autonoma delle informazioni.[50]

2. La normativa sull'intelligenza artificiale

L'evoluzione dell'intelligenza artificiale è fonte di rilevanti e complesse questioni normative, la cui risoluzione è necessaria al fine di garantire un utilizzo etico, sicuro e conforme ai diritti fondamentali dei sistemi di IA. In Europa, il Regolamento Generale sulla Protezione dei Dati (GDPR) disciplina in modo organico il trattamento dei dati personali, imponendo principi che, seppur indirettamente, influenzano lo sviluppo e l'implementazione dei sistemi di IA. A completamento di questa disciplina, l'AI Act, approvato dall'Unione europea nel marzo 2024, regolamenta sistematicamente l'IA, introducendo un approccio basato sul rischio – distinguendo tra sistemi a rischio minimo, limitato ed alto – con l'obiettivo di bilanciare innovazione e tutela dei diritti. In tale contesto, anche l'Italia si sta muovendo per recepire il regolamento comunitario attraverso un disegno di legge[51] – approvato il 20 marzo 2025 in Senato e attualmente in discussione alla Camera – finalizzato a stabilire criteri di conformità e meccanismi di vigilanza a livello nazionale.

[49] Y. LeCun, Y. Bengio, G. Hinton, '*Deep learning*', Nature 521, 436-444, 2015.
[50] *Ibid.*
[51] Disegno di legge n. 1146 – Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

2.1. Nozione "giuridica" di intelligenza artificiale

La definizione di intelligenza artificiale è divenuta interessante anche per il giurista nell'anno 2018, quando l'Unione Europea, con un comunicato stampa, ha condiviso l'istituzione di un gruppo di esperti sull'IA con l'obiettivo di elaborare linee guida per lo sviluppo e l'uso etico dell'intelligenza artificiale, nel rispetto dei diritti fondamentali dell'UE.[52] Già nello stesso anno, il Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, ha pubblicato, sulla base della definizione di intelligenza artificiale proposta dalla Commissione europea nella sua comunicazione sull'IA[53], la seguente definizione "aggiornata": "*I sistemi di intelligenza artificiale (IA) sono sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti. Come disciplina scientifica, l'IA include diversi approcci e diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione), e la robotica (che include il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi ciberfisici)*."[54] Si tratta di una definizione che elenca numerose importanti funzioni ed attività dei sistemi di IA e che, al pari di quella di intelligenza "naturale"[55], fa riferimento alla capacità dei

[52] Commissione europea, '*Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards*', (9 Marzo 2018), Comunicato stampa IP/18/1381.
[53] Commissione europea, '*L'intelligenza artificiale per l'Europa*', Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, COM (2018) 237, 25 Aprile 2018.
[54] Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, '*Una definizione di IA: principali capacità e discipline scientifiche*', Bruxelles, aprile 2019.
[55] Si veda *supra* paragrafo 1.1.

sistemi di percepire l'ambiente circostante, acquisire ed interpretare le informazioni ed agire nel modo più opportuno per raggiungere l'obiettivo dato.

La nozione e definizione di IA ha acquisito ancora maggior rilievo dal punto di vista giuridico e normativo in seguito alla presentazione, il 21 aprile 2021, da parte della Commissione europea al Parlamento europeo e al Consiglio di una proposta di regolamento contenente un quadro giuridico unitario sull'IA[56] che ha portato all'adozione, il 13 marzo 2024, del Regolamento 2024/1689 anche noto come AI Act.[57] Quest'ultimo contiene, all'articolo 3, la più recente definizione normativa di "sistema di intelligenza artificiale" come "*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*".[58] Si tratta di una definizione complessa e particolarmente ampia che, da un lato, ha il merito di rimanere attuale nonostante la veloce evoluzione tecnologica, ma che, dall'altro, può comportare difficoltà applicative.[59]

2.2. Dal GDPR…

Nell'anno 2018 è entrato in vigore il Regolamento 2016/679/UE "relativo alla protezione dei dati delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", che ha piena applicazione su tutto il territorio comunitario. L'adozione del Regolamento trova giustificazione nel riconoscimento – operato all'articolo 8, paragrafo 1 della Carta dei diritti fondamentali dell'Unione europea[60] e all'articolo 16 del Trattato sul funzionamento

[56] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 2021/0106, Bruxelles.
[57] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), Bruxelles.
[58] Regolamento (UE) 2024/1689, art. 3 – *Definizioni*.
[59] Si veda *infra* paragrafo 2.3.2.
[60] Carta dei diritti fondamentali dell'Unione Europea (2016/C 202/02), art. 8: *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*

dell'Unione europea[61] – del diritto alla protezione dei dati personali come diritto fondamentale dei cittadini europei.[62] Il GDPR persegue un duplice ed interconnesso obiettivo: da un lato, garantire la tutela dei dati personali delle persone fisiche; dall'altro, assicurare la libera circolazione degli stessi dati. La protezione dei dati, dunque, non è solo un fine in sé, ma anche un mezzo per favorire lo sviluppo dell'economia digitale, garantendo maggiore certezza giuridica e operativa nella normativa applicabile.[63]

Sebbene il Regolamento non disciplini esplicitamente l'intelligenza artificiale, la sua analisi è essenziale perché per lungo tempo ha rappresentato l'unica fonte normativa in grado di fornire principi e tutele applicabili all'uso degli algoritmi e al trattamento automatizzato dei dati. In particolare, il GDPR ha posto le basi per la protezione dei dati personali nell'ambito dei sistemi di IA, introducendo obblighi di trasparenza, *accountability* e limitazioni nell'adozione di decisioni automatizzate. Con l'entrata in vigore dell'AI Act[64], il quadro normativo europeo si è arricchito di una disciplina più specifica che si affianca al GDPR: mentre quest'ultimo tutela i diritti fondamentali legati al trattamento dei dati personali, l'AI Act introduce regole *ad hoc* per garantire la sicurezza, l'affidabilità e il rispetto dei diritti nei sistemi di intelligenza artificiale.

Per comprendere la portata normativa del Regolamento è opportuno, innanzitutto, definire il concetto di "trattamento". Esso consiste in "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione,*

---

[61] Trattato sul funzionamento dell'Unione europea (2012) GU C 326/47, art. 16: *1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.*

[62] F. Pizzetti, '*Intelligenza Artificiale, protezione dei dati personali e regolazione*', Giappichelli, 2018, pp. 5-7.

[63] *Ibid*, p. 13.

[64] Si veda *infra* paragrafo 2.3.

il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".[65] Risulta, quindi, evidente la natura eterogena delle operazioni di trattamento.

Risulta, poi, essenziale approfondire i principi fondamentali su cui si fonda la normativa.[66] Questi principi, infatti, non solo delineano i criteri essenziali per un trattamento lecito e corretto dei dati, ma orientano, altresì, l'interpretazione e l'applicazione delle disposizioni normative, in un'ottica di bilanciamento tra innovazione tecnologica e tutela dei diritti fondamentali.

L'articolo 5, paragrafo 1, lettera a) introduce i principi di liceità, correttezza e trasparenza.[67] Il trattamento dei dati è lecito, ai sensi dell'articolo 6, quando è basato sul consenso dell'interessato o quando ricorre almeno una delle altre cinque condizioni previste, tra cui l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri.[68] Il principio di correttezza è, invece, inerente alla relazione tra il titolare del trattamento e l'interessato. Infatti, i responsabili del trattamento dei dati sono tenuti a garantire che le operazioni di trattamento avvengano nel rispetto dei principi di liceità e trasparenza, informando gli interessati e il pubblico sulle modalità con cui i loro dati vengono trattati nonché della conformità delle proprie attività alle disposizioni del Regolamento.[69] Ancora, il principio di trasparenza richiede che le seguenti informazioni siano messe a disposizione degli interessati: informazioni sull'identità del responsabile del trattamento, informazioni sulle finalità del trattamento dei dati, informazioni relative al diritto dell'interessato di ottenere conferma del trattamento e di accedere ai dati personali che lo riguardano.[70]

Il principio di limitazione della finalità[71] impone che i dati vengano raccolti per scopi specifici, espliciti e legittimi, evitando che siano successivamente trattati in

---

[65] Regolamento (UE) 2016/679, art. 4 – *Definizioni.*
[66] Regolamento (UE) 2016/679, art. 5 – *Principi applicabili al trattamento di dati personali*.
[67] Regolamento (UE) 2016/679, art. 5(1)(a): *I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»).*
[68] Regolamento (UE) 2016/679, art. 6 – Liceità del trattamento.
[69] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, '*Manuale sul diritto europeo in materia di protezione dei dati*' – 2018 edition, p. 132.
[70] Regolamento (UE) 2016/679, cons. (39); P. Voigt, A. von dem Bussche, '*The EU General Data Protection Regulation – A practical guide*', Springer Nature, 2024, p. 136.
[71] Regolamento (UE) 2016/679, art. 5(1)(b): *I dati personali sono: […] b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse,*

modo incompatibile con tali finalità originarie. Questa limitazione garantisce una maggiore protezione della *privacy* degli individui, impedendo un utilizzo eccessivo o imprevedibile delle loro informazioni personali.[72]

Il principio di minimizzazione dei dati[73] prevede che solo i dati strettamente necessari per le finalità dichiarate possano essere raccolti e trattati. Ciò significa che il titolare del trattamento deve valutare con attenzione la quantità e la tipologia di dati richiesti, evitando il trattamento di dati superflui. Questo principio è strettamente legato al concetto di proporzionalità, volto a bilanciare le esigenze operative delle organizzazioni con la tutela della *privacy* degli utenti.[74]

L'esattezza dei dati[75] impone che le informazioni trattate siano corrette, aggiornate e, se necessario, rettificate o cancellate quando risultano inesatte. Esistono circostanze in cui il controllo periodico dell'accuratezza dei dati, incluso il loro aggiornamento, diventa indispensabile per evitare potenziali danni all'interessato derivanti dall'uso di informazioni inesatte.[76]

Il principio di limitazione della conservazione[77] stabilisce che i dati personali debbano essere conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità per le quali sono stati raccolti. Ciò impone ai titolari del trattamento l'implementazione di politiche di gestione dei dati che includano la cancellazione o l'anonimizzazione dopo un certo periodo.

---

di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»).

[72] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, '*Manuale sul diritto europeo in materia di protezione dei dati*' – 2018 edition, *cit.,* p. 137.

[73] Regolamento (UE) 2016/679, art. 5(1)(c): *I dati personali sono: c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»).*

[74] P. Voigt, A. von dem Bussche, '*The EU General Data Protection Regulation – A practical guide*', *cit.*, p. 138.

[75] Regolamento (UE) 2016/679, art. 5(1)(d): *I dati personali sono: d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»).*

[76] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, '*Manuale sul diritto europeo in materia di protezione dei dati*' – 2018 edition, *cit.,* p. 143.

[77] Regolamento (UE) 2016/679, art. 5(1)(e): *I dati personali sono: e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»).*

Il principio di integrità e riservatezza[78] obbliga i titolari del trattamento ad adottare misure tecniche e organizzative adeguate a proteggere i dati da accessi non autorizzati, perdita, distruzione o danno accidentale. A seconda delle specifiche circostanze di ciascun caso, le misure tecniche appropriate potrebbero includere, ad esempio, la pseudonimizzazione e la cifratura dei dati personali.[79]

Infine, il principio di responsabilizzazione[80] richiede ai titolari ed ai responsabili del trattamento di adottare attivamente misure finalizzate a garantire la protezione dei dati. A tal riguardo, ai sensi dell'articolo 24[81], il titolare del trattamento ha l'obbligo di adottare misure idonee a dimostrare, in qualsiasi momento, la conformità al regolamento. Quest'ultima comporta, tra le altre cose, lo svolgimento, da parte del titolare del trattamento, di una valutazione d'impatto sulla protezione dei dati per garantire che i trattamenti di dati personali, soprattutto quelli che presentano un rischio elevato per i diritti e le libertà degli interessati, siano oggetto di un'analisi preventiva.[82] L'obiettivo della valutazione è identificare, valutare e mitigare i rischi associati al trattamento di dati personali, assicurando che quest'ultimo avvenga nel rispetto del Regolamento. Tale processo permette di adottare misure adeguate a garantire la conformità normativa e ridurre la probabilità di violazione della *privacy*.[83] L'articolo 35 stabilisce che una valutazione è necessaria quando un trattamento, a maggior ragione se svolto mediante l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Nel contesto dell'intelligenza artificiale, tale obbligo risulta,

[78] Regolamento (UE) 2016/679, art. 5(1)(f): *I dati personali sono: f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).*

[79] Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, '*Manuale sul diritto europeo in materia di protezione dei dati*' – 2018 edition, *cit.,* p. 147.

[80] Regolamento (UE) 2016/679, art. 5(2): *Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*

[81] Regolamento (UE) 2016/679, art. 24(1): […] *il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.*

[82] Regolamento (UE) 2016/679, art. 35: *Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.* […]

[83] F. Pizzetti, '*Intelligenza Artificiale, protezione dei dati personali e regolazione*', *cit.*, pp. 64 e ss.

quindi, particolarmente rilevante per sistemi che, impiegando tecniche di *machine learning* e *deep learning*, adottano decisioni automatizzate.

È proprio in materia di decisioni automatizzate e profilazione che il Regolamento contiene una norma di fondamentale importanza: l'articolo 22.[84] Quest'ultimo, infatti, stabilisce il diritto, non assoluto[85], degli individui a non essere soggetti a decisioni basate unicamente sul trattamento automatizzato che producano effetti giuridici o incidano significativamente sulla loro persona.[86]

2.3. … all'AI Act

Il primo agosto 2024 è entrato in vigore il Regolamento 2024/1689/UE, anche noto come "AI Act", "che stabilisce regole armonizzate sull'intelligenza artificiale". Il regolamento nasce con l'intento[87], da un lato, di tutelare i diritti e le libertà fondamentali dei cittadini europei nel rispetto della Carta dei diritti fondamentali dell'Unione europea[88] e, dall'altro, di promuovere lo sviluppo e la diffusione di sistemi di intelligenza artificiale stabilendo obblighi omogenei per

[84] Regolamento (UE) 2016/679, art. 22(1): *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*.

[85] Regolamento (UE) 2016/679, art. 22(2): *Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato.*

[86] Si veda *infra* capitolo 2, paragrafo 4.2.

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

[88] Carta dei diritti fondamentali dell'Unione Europea (2016/C 202/02).

tutti gli operatori del territorio comunitario.[89] L'applicabilità delle regole sarà, tuttavia, graduale.[90]

L'articolo 3 limita, dal punto di vista oggettivo, l'ambito di applicazione del Regolamento a sistemi di IA[91] dotati di un certo grado di autonomia, suscettibili di adattamenti dopo la loro attivazione ed in grado di dedurre dall'*input* ricevuto il modo di generare l'*output*, nonché ai "modelli di IA per finalità generali".[92] È, invece, l'articolo 2 a definire l'ambito di applicazione soggettiva che ricomprende tutti gli operatori che, con ruoli e funzioni differenti, intervengono nel ciclo di vita dei sistemi di IA, dalla fase di sviluppo fino all'immissione sul mercato dell'Unione e al loro utilizzo da parte di enti pubblici e privati.[93] A tal riguardo, appare opportuno definire la figura del *deployer – una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA*

---

[89] Regolamento (UE) 2024/1689, cons. (1): *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) nell'Unione, in conformità dei valori dell'Unione, 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.*

[90] Regolamento (UE) 2024/1689, art. 113: […] *Si applica a decorrere dal 2 agosto 2026. Tuttavia: a) I capi I e II si applicano a decorrere dal 2 febbraio 2025; b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101; c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027.*

[91] Si veda *supra* paragrafo 2.1.

[92] Regolamento (UE) 2024/1689, art. 3(63): *«modello di IA per finalità generali»: 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 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.*

[93] Regolamento (UE) 2024/1689, art. 2(1): *Il presente regolamento si applica: a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo; b) ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione; c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione; d) agli importatori e ai distributori di sistemi di IA; e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio; f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione; g) alle persone interessate che si trovano nell'Unione.*

sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.[94] Questa definizione può includere anche la Pubblica Amministrazione qualora impieghi sistemi di IA per l'esecuzione delle proprie funzioni.

Come anticipato, la finalità del Regolamento è assicurare lo sviluppo di tecnologie conformi ai valori, ai diritti ed alle libertà fondamentali dell'Unione europea.[95] A tal fine, l'articolo 5[96] prevede un divieto assoluto per una serie specifica e dettagliata di pratiche ritenute incompatibili con i valori comunitari della dignità umana, libertà, uguaglianza e democrazia.[97] A titolo esemplificativo è vietato l'uso di sistemi di IA progettati per influenzare il comportamento delle persone in modo subliminale se questo può causare danni[98] e di sistemi che sfruttano vulnerabilità di gruppi particolarmente sensibili, come bambini, anziani o

[94] Regolamento (UE) 2024/1689, art. 3(4).
[95] Regolamento (UE) 2024/1689, cons. (6): *In considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani.*
[96] Regolamento (UE) 2024/1689, art. 5 – *Pratiche di IA vietate*.
[97] Regolamento (UE) 2024/1689, art. cons. (28): *L'IA presenta, accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e abusive e dovrebbero essere vietate poiché sono contrarie ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori.*
[98] Regolamento (UE) 2024/1689, art. 5(1)(a): *Sono vietate le pratiche di IA seguenti: a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo.*

persone con disabilità.[99] Tali disposizioni sono divenute applicabili il 2 febbraio 2025.[100]

Le pratiche che invece non sono espressamente vietate sono regolamentate secondo il cosiddetto *risk-based approach*. Tale approccio si fonda sull'idea che l'intensità degli obblighi di vigilanza e di controllo debba essere proporzionata al livello di rischio associato a un determinato sistema di IA. Il regolamento distingue tra sistemi di IA a rischio alto, limitato e minimo, imponendo obblighi differenziati per ciascuna categoria. All'aumentare del rischio, crescono anche gli oneri e le responsabilità a carico di sviluppatori e utilizzatori dei sistemi intelligenti.[101] Appare evidente come la logica sottesa a tale approccio risieda nella necessità di evitare un'applicazione indiscriminata degli obblighi normativi, consentendo invece di adeguare le misure di conformità in funzione dell'esposizione al rischio, anche al fine di non ostacolare l'evoluzione tecnologica.

Il Regolamento, dopo aver disciplinato i sistemi a rischio inaccettabile, dedica il Capo III, la cui applicabilità è posticipata al 2 agosto 2027[102], ai sistemi ad alto rischio. Questi ultimi sono definiti e classificati all'articolo 6, che distingue tra prodotti o componenti di sicurezza[103] e sistemi indipendenti.[104] Il paragrafo 1 prevede due requisiti affinché un sistema possa essere considerato ad alto rischio.

---

[99] Regolamento (UE) 2024/1689, art. 5(1)(b): *Sono vietate le pratiche di IA seguenti: (b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo.*

[100] Regolamento (UE) 2024/1689, art. 113(a): *I capi I e II si applicano a decorrere dal 2 febbraio 2025.*

[101] AIRIA – Associazione Regolazione Intelligenza Artificiale, '*Navigare l'European AI Act*', Wolters Kluwer, Milano, 2024, p. 48.

[102] Regolamento (UE) 2024/1689, art. 113(c): *L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027.*

[103] Regolamento (UE) 2024/1689, art. 6(1): *A prescindere dal fatto che sia immesso sul mercato o messo in servizio indipendentemente dai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.*

[104] Regolamento (UE) 2024/1689, art. 6(2): *Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.*

Innanzitutto, considera ad alto rischio un sistema destinato a essere utilizzato come componente di sicurezza di un prodotto o quando è esso stesso un prodotto disciplinato da uno degli atti normativi elencati nell'Allegato I.[105] Questi atti normativi riguardano settori nei quali la sicurezza è già regolamentata a livello comunitario. Inoltre, per essere qualificato come ad alto rischio, il prodotto o la sua componente di sicurezza, ai fini dell'immissione sul mercato o della sua messa in servizio, devono essere soggetti a una valutazione di conformità da parte di terzi, vale a dire a un processo in cui un organismo notificato verifica il rispetto dei requisiti normativi prima che il prodotto possa essere commercializzato o messo in servizio.[106]

Il paragrafo 2 qualifica, invece, come sistemi di IA ad alto rischio indipendenti[107] quelli di cui all'allegato III.[108] Si tratta di una lista di sistemi utilizzati in determinati settori, come ad esempio, i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto nel settore dell'amministrazione della giustizia.[109] In relazione a questa categoria di sistemi ad alto rischio, il legislatore europeo ha previsto una deroga: il sistema di cui all'allegato III non è ad alto rischio se *"non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale*"[110] e ricorre almeno una delle condizioni di cui al comma 2 del paragrafo 3 dell'articolo 6.[111] Ulteriormente, è bene riconoscere il potere della Commissione di intervenire

[105] Regolamento (UE) 2024/1689, all. I – *Elenco della normativa di armonizzazione dell'Unione.*
[106] Regolamento (UE) 2024/1689, art. 3(20): *«valutazione della conformità»: la procedura atta a dimostrare se i requisiti di cui al capo III, sezione 2, relativi a un sistema di IA ad alto rischio sono stati soddisfatti.*
[107] Regolamento (UE) 2024/1689, cons. (52): *Per quanto riguarda i sistemi di IA indipendenti, ossia i sistemi di IA ad alto rischio diversi da quelli che sono componenti di sicurezza dei prodotti o che sono essi stessi prodotti* […].
[108] Regolamento (UE) 2024/1689, all. III – *Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2.*
[109] Regolamento (UE) 2024/1689, all. III(8)(a).
[110] Regolamento (UE) 2024/1689, art. 6(3).
[111] Regolamento (UE) 2024/1689, art. 6(3): *Il primo comma si applica quando è soddisfatta almeno una qualsiasi delle condizioni seguenti: a) il sistema di IA è destinato a eseguire un compito procedurale limitato; b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata; c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.*

in senso estensivo e restrittivo sull'allegato III al fine di assicurare un periodico aggiornamento dello stesso coerentemente con il contesto tecnologico in rapida evoluzione.[112]

Per i sistemi di IA ad alto rischio, il Regolamento prevede numerosi e rigorosi obblighi di conformità al fine di minimizzare i rischi per la sicurezza e garantire la tutela dei diritti fondamentali della persona. Uno degli obblighi principali per i fornitori di tali sistemi è l'implementazione di un sistema di gestione del rischio, che deve essere attivo per l'intero ciclo di vita del sistema di IA. Tale sistema deve identificare, analizzare e valutare sia i rischi noti sia quelli ragionevolmente prevedibili che il prodotto può comportare per la salute, la sicurezza e i diritti fondamentali, al fine di adottare misure adeguate a prevenirli o mitigarli.[113]

L'articolo 10, invece, disciplina la qualità dei dati utilizzati per l'addestramento, la convalida e il *test* degli algoritmi, imponendo che tali dati siano rilevanti, rappresentativi e privi di distorsioni. In altre parole, i dati devono essere gestiti in modo appropriato, tenendo conto di fattori quali i processi di raccolta, la preparazione, le potenziali distorsioni, le lacune nonché il contesto specifico in cui verrà utilizzato il sistema di IA.[114]

L'AI Act impone, all'articolo 11, l'obbligo di preparare prima dell'avvio di un sistema di IA ad alto rischio e di tenere aggiornata una documentazione tecnica dettagliata. Questa documentazione, i cui contenuti minimi sono elencati nell'allegato IV[115], deve dimostrare che il sistema di IA soddisfa i requisiti di legge e fornire informazioni chiare alle autorità per verificarne la conformità.[116]

Ancora, in continuità con l'articolo 22 del GDPR, l'articolo 13[117] dell'AI Act impone elevati obblighi di trasparenza, affinché chi utilizza i sistemi possa comprenderli e usarli correttamente. I sistemi ad alto rischio devono, infatti, essere corredati da istruzioni chiare, che includano informazioni sul fornitore, sulle capacità e sui limiti del sistema, sui potenziali rischi nonché sulle modalità e i criteri

[112] Regolamento (UE) 2024/1689, art. 7 – *Modifiche dell'allegato III*.
[113] Regolamento (UE) 2024/1689, art. 9 – *Sistema di gestione dei rischi.*
[114] Regolamento (UE) 2024/1689, art. 10 – *Dati e governance dei dati.*
[115] Regolamento (UE) 2024/1689, all. IV – *Documentazione tecnica di cui all'articolo 11, paragrafo 1*.
[116] Regolamento (UE) 2024/1689, art. 11 – *Documentazione tecnica.*
[117] Regolamento (UE) 2024/1689, art. 13 – *Trasparenza e fornitura di informazioni ai deployer*.

di interpretazione degli *output*.[118] Coerentemente con tale obbligo, l'articolo 14[119] prevede che i sistemi ad alto rischio siano progettati in modo da consentire all'uomo di controllarli efficacemente. L'obiettivo della supervisione umana è, infatti, prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono derivare dall'uso di questi sistemi.[120]

Appare, quindi, evidente come la regolamentazione dei sistemi di IA ad alto rischio sia particolarmente dettagliata. Diversamente, i sistemi a rischio limitato o a rischio minimo non sono espressamente definiti, né regolamentati. È l'articolo 50 che contiene una serie di disposizioni applicabili ai sistemi di intelligenza artificiale "*a prescindere dal fatto che siano considerati ad alto rischio o no*".[121] Si tratta di disposizioni che, rafforzando il principio di trasparenza[122], impongono ai fornitori l'obbligo, tra gli altri, di informare gli utenti quando interagiscono con un sistema di IA, a meno che non sia evidente, o di contrassegnare i contenuti creati o manipolati dal sistema come generati artificialmente.[123]

2.3.1. La *governance*

Le istituzioni di *governance*[124] previste dall'AI Act svolgono un ruolo di primaria importanza per garantire l'applicazione e l'osservanza del regolamento, nonché per assicurare che il rispetto delle regole non ostacoli l'innovazione. Il regolamento prevede due livelli di *governance*, uno comunitario[125] ed uno nazionale[126].

L'Ufficio per l'IA (*AI Office*), istituito all'interno della Commissione Europea ai sensi dell'articolo 64 del Regolamento, rappresenta il centro di competenza europeo per la *governance* dell'intelligenza artificiale.[127] Ha il compito di garantire

[118] Si veda *infra* capitolo 2, paragrafo 4.1.
[119] Regolamento (UE) 2024/1689, art. 14 – *Sorveglianza umana.*
[120] Si veda *infra* capitolo 2, paragrafo 4.2.
[121] Regolamento (UE) 2024/1689, cons. (132).
[122] Si veda *infra* capitolo 2, paragrafo 4.1.
[123] Regolamento (UE) 2024/1689, art. 50(1) e (2).
[124] Regolamento (UE) 2024/1689, capo VII – *Governance.*
[125] Regolamento (UE) 2024/1689, capo VII, Sezione 1 – *Governance a livello dell'Unione.*
[126] Regolamento (UE) 2024/1689, capo VII, Sezione 2 – *Autorità nazionali competenti.*
[127] Regolamento (UE) 2024/1689, art. 64(1): *La Commissione sviluppa le competenze e le capacità dell'Unione nel settore dell'IA attraverso l'ufficio per l'IA.*

lo sviluppo e l'uso affidabile dell'IA, monitorando l'applicazione del Regolamento nei vari Stati membri.[128] In particolare, supervisiona i modelli di IA per scopi generali, valuta i rischi sistemici imprevisti e conduce verifiche di conformità. Inoltre, promuove la cooperazione internazionale, coordina i regolatori nazionali e sviluppa *sandbox* regolamentari per testare i sistemi di IA in ambienti controllati, fornendo anche supporto alle PMI.[129]

Accanto all'Ufficio, il Consiglio europeo per l'intelligenza artificiale (*AI Board*), istituito dall'articolo 65, è composto da un rappresentante per ciascun Stato membro con un mandato triennale rinnovabile una volta.[130] Il Consiglio, tra i vari compiti, supporta la Commissione e gli Stati membri nell'attuazione del Regolamento, facilitando il coordinamento tra le autorità nazionali, raccogliendo e diffondendo buone pratiche, fornendo consulenza sull'applicazione del Regolamento e promuovendo l'armonizzazione delle procedure amministrative.[131]

Ulteriori organismi di supporto alla *governance* comunitaria sono il Forum consultivo[132] e il Gruppo di esperti scientifici indipendenti[133]. Il primo, composto da rappresentanti dell'industria, *start-up*, PMI, società civile e mondo accademico, fornisce pareri e raccomandazioni al Consiglio per l'IA e alla Commissione, con particolare attenzione alla competitività europea. Il Gruppo di esperti scientifici indipendenti, invece, selezionato dalla Commissione, offre supporto tecnico e scientifico per l'attuazione del Regolamento, garantendo imparzialità e obiettività nell'analisi dei modelli di IA e nelle attività di vigilanza.

Per quanto concerne, invece, la *governance* nazionale, il Regolamento attribuisce un ruolo centrale alle Autorità nazionali, per garantire efficienza nella gestione della complessità e della vastità dei sistemi di IA operativi.

---

[128] Regolamento (UE) 2024/1689, cons. (148).
[129] IRIA – Associazione Regolazione Intelligenza Artificiale, '*Navigare l'European AI Act*', *cit.*, p. 51.
[130] Regolamento (UE) 2024/1689, art. 65 – *Istituzione e struttura del consiglio per l'IA europeo per l'intelligenza artificiale.*
[131] Regolamento (UE) 2024/1689, art. 66 – *Compiti del consiglio per l'IA.*
[132] Regolamento (UE) 2024/1689, art. 67 – *Forum consultivo.*
[133] Regolamento (UE) 2024/1689, art. 68 – *Gruppo di esperti scientifici indipendenti.*

L'articolo 70 stabilisce che ogni Stato membro deve istituire o designare almeno un'autorità di notifica e un'autorità di vigilanza del mercato.[134] L'autorità di notifica è competente nella gestione e vigilanza della fase di certificazione dei sistemi di IA.[135] L'autorità di vigilanza, invece, ha il compito di verificare il rispetto dell'AI Act da parte di produttori e distributori, con poteri di indagine e sanzione.[136] Gli Stati membri hanno discrezionalità nella scelta delle autorità, che possono essere già esistenti o di nuova istituzione, e che devono operare con indipendenza, imparzialità e competenza tecnica.[137]

Ogni Stato, entro il 2 agosto 2025, deve comunicare alla Commissione l'identità e i compiti delle autorità individuate, aggiornandola su eventuali modifiche.[138]

2.3.2. AI Act: un'eterogenesi dei fini?[139]

L'AI Act, come anticipato, rappresenta il primo tentativo dell'Unione europea di regolamentare in modo organico lo sviluppo e l'utilizzo dell'intelligenza artificiale. Tuttavia, nonostante lo scopo di promuovere un'IA affidabile e rispettosa dei diritti fondamentali, il quadro normativo delineato ha suscitato diverse perplessità.

Innanzitutto, dubbi e criticità sono emersi in relazione all'ampiezza della definizione di "sistema di IA" adottata nel Regolamento.[140] Sebbene questa scelta miri a garantire una regolamentazione che non diventi rapidamente obsoleta, essa comporta difficoltà applicative rilevanti, in quanto amplia significativamente lo spettro delle tecnologie soggette agli stringenti obblighi normativi. Tale scelta

---

[134] Regolamento (UE) 2024/1689, art. 70(1): *Ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato* […].
[135] IRIA – Associazione Regolazione Intelligenza Artificiale, '*Navigare l'European AI Act*', *cit.*, p. 54.
[136] *Ibid.*
[137] Regolamento (UE) 2024/1689, art. 70(1): […] *Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento* […].
[138] Regolamento (UE) 2024/1689, art. 70(2): *Gli Stati membri comunicano alla Commissione l'identità delle autorità di notifica e delle autorità di vigilanza del mercato e i compiti di tali autorità, nonché ogni successiva modifica degli stessi* […].
[139] G. Pesce, '*L'Europa regola i rischi dell'IA. Ma pure troppo'*, L'Espresso, 10 gennaio 2025.
[140] Regolamento (UE) 2024/1689, art. 3.

appare in contrasto con il Considerando 12[141], il quale auspica una definizione chiara e strettamente allineata agli standard internazionali, per garantire certezza giuridica e favorire la convergenza normativa a livello globale.[142]

Un ulteriore aspetto critico concerne la complessità strutturale dell'AI Act che rischia di comprometterne l'efficacia applicativa. Il Regolamento conta 113 articoli, 13 allegati e 180 considerando ed impone obblighi gravosi in termini di conformità e certificazione. Il pericolo di una regolazione unicamente europea, senza un coordinamento globale, è quello di scoraggiare l'innovazione e gli investimenti nel settore dell'IA, portando a una riduzione dell'offerta nel mercato europeo[143] e una divergenza di prodotti o servizi, con il pubblico comunitario che riceverà versioni diverse e meno avanzate.[144] Dal punto di vista economico, è, quindi, opportuno evidenziare come il Regolamento possa configurarsi come un intervento di natura protezionistica, limitando la competitività delle imprese europee rispetto a quelle statunitensi e cinesi, meno vincolate da restrizioni normative.[145]

Quindi, sebbene il Regolamento rappresenti il primo passo verso la regolamentazione dell'intelligenza artificiale nell'Unione europea, le sue criticità sollevano interrogativi sulla sua effettiva capacità di costituire uno standard a livello globale,[146] nonché di bilanciare la protezione dei diritti fondamentali con la promozione dell'innovazione tecnologica.

---

[141] Regolamento (UE) 2024/1689, cons. (12): *La nozione di «sistema di IA» di cui al presente regolamento dovrebbe essere definita 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* […].

[142] IRIA – Associazione Regolazione Intelligenza Artificiale, '*Navigare l'European AI Act*', *cit.*, p. 45.

[143] N. Sousa e Silva, '*The Artificial Intelligence Act: Critical Overview*', Social Science Research Network, 30 luglio 2024.

[144] Ad esempio, Meta non rilascerà il suo modello multimodale Llama AI nell'UE perché il contesto normativo europeo è troppo imprevedibile. Cfr. J. Weatherbed, '*Meta won't release its multimodal Llama AI model in the EU*', The Verge, 18 luglio 2024.

[145] G. Pesce, '*L'Europa regola i rischi dell'IA. Ma pure troppo*', *cit*.

[146] E. Cirone, '*L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*', Quaderni AISDUE - Rivista quadrimestrale, ISSN 2975-2698, fasc. speciale 2, 2024.

2.4. GDPR e AI Act: un breve confronto

Una breve analisi comparativa del GDPR e dell'AI Act può essere utile al fine di comprendere l'interazione tra le due regolamentazioni, evidenziando come la disciplina sulla protezione dei dati personali si integri con le normative specifiche in materia di intelligenza artificiale.

Il diritto alla protezione dei dati personali, come anticipato, è riconosciuto come diritto fondamentale nell'ordinamento europeo.[147] Di conseguenza, le disposizioni sulla protezione dei dati costituiscono un parametro di riferimento per altre normative primarie, soprattutto in settori legati all'evoluzione tecnologica come l'intelligenza artificiale. L'AI Act, infatti, richiama espressamente il GDPR, che, quindi, rimane il riferimento normativo per la legittimità del trattamento dei dati personali nei sistemi di IA.[148] Questo significa che qualsiasi sistema di IA che preveda l'utilizzo di dati personali deve rispettare entrambi i regolamenti, garantendo che i trattamenti effettuati siano conformi ai principi di trasparenza, liceità e correttezza stabiliti dal GDPR, e contestualmente compatibili con le misure di sicurezza, affidabilità e gestione del rischio previste dall'AI Act.

È opportuno, tuttavia, sottolineare come i due regolamenti seguano approcci normativi distinti. L'AI Act adotta un approccio basato sul rischio[149], classificando i sistemi di IA in base al loro potenziale impatto sui diritti fondamentali e imponendo obblighi specifici ai sistemi considerati ad alto rischio. Il GDPR, invece, si basa sul principio di responsabilizzazione (*accountability*), imponendo agli operatori l'obbligo di garantire la legittimità del trattamento dei dati personali attraverso il rispetto di principi fondamentali quali trasparenza, minimizzazione, proporzionalità e riservatezza.[150] Questa differente impostazione si riflette sulle modalità con cui i due regolamenti disciplinano la conformità agli *standard* di sicurezza e protezione dei diritti fondamentali.

---

[147] Carta dei diritti fondamentali dell'Unione Europea (2016/C 202/02), art. 8; Trattato sul funzionamento dell'Unione europea (2012) GU C 326/47, art. 16.

[148] Regolamento (UE) 2024/1689, cons. (10): […] *Il presente regolamento non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti* […].

[149] Si veda *supra* paragrafo 2.3.

[150] Regolamento (UE) 2016/679, art. 5(2).

Invero, l'AI Act stabilisce categorie di rischio per i sistemi di IA, vietando alcune applicazioni e sottoponendone altre a rigorosi requisiti di conformità. La valutazione del rischio non è, quindi, lasciata alla discrezionalità degli operatori, bensì è predefinita dalla legge. I sistemi di IA ad alto rischio, infatti, devono, oltre a rispettare obblighi di gestione del rischio, documentazione tecnica e supervisione umana, ottenere marcature CE e certificazioni di conformità. In assenza di tali requisiti, il sistema è considerato non conforme e non può essere commercializzato.[151]

Il GDPR, invece, adotta un approccio basato sul *self-assesment*, imponendo a titolari e responsabili del trattamento l'obbligo di implementare misure adeguate a garantire un livello di *accountability* proporzionato ai dati trattati, tenendo conto di vari parametri utili a determinare i rischi per i diritti e le libertà degli interessati. Tra gli strumenti previsti vi sono la valutazione d'impatto sulla protezione dei dati (DPIA), il *test* di bilanciamento per il legittimo interesse e la consultazione preventiva con le autorità di controllo in caso di incertezze sulle misure di sicurezza.[152]

2.5. La normativa nazionale: il disegno di legge 1146

Il 20 marzo 2025, il Senato ha approvato il disegno di legge n. 1146 recante disposizioni in materia di intelligenza artificiale presentato, su iniziativa del Presidente del Consiglio, Giorgia Meloni, e del Ministro della Giustizia, Carlo Nordio, dal Governo italiano.

Composto da 28 articoli suddivisi in sei capi, il provvedimento regola l'impiego dell'intelligenza artificiale in Italia, adottando un approccio che, coerentemente con la disciplina comunitaria, coniuga prudenza e innovazione.[153]

---

[151] IRIA – Associazione Regolazione Intelligenza Artificiale, '*Navigare l'European AI Act*', *cit.*, p. 133.
[152] *Ibid*, pp.132-133.
[153] M. T. D'Urso, '*Il d.d.l., di iniziativa governativa, approvato il 23 aprile 2024, sulla Intelligenza artificiale. I principi fondamentali dell'AI per il suo utilizzo in Italia, in linea con "l'AI Act" deliberato dall'UE. Le disposizioni di settore. La Strategia nazionale e le nuove agenzie istituite. La tutela per gli utenti e per il diritto d'autore e le pene per i trasgressori. Il G7 svoltosi il 13-15 giugno 2024 a Borgo Egnazia (BR) con l'intervento di Papa Bergoglio*', in *Quaderni della Rivista della Corte dei Conti*, n. 2/2024, p. 98.

Il disegno di legge italiano non si sovrappone alla normativa europea, ma si pone in un'ottica di integrazione, regolando aspetti specifici del diritto interno nei seguenti settori in cui l'utilizzo di sistemi di intelligenza artificiale potrebbe avere un impatto rilevante: lavoro, pubblica amministrazione, giustizia, sanità, cybersicurezza e tutela dei dati.[154] La sua finalità è quella di assicurare un uso dell'IA che sia etico, trasparente e responsabile, con un'attenzione particolare ai rischi economici e sociali, nonché alla tutela dei diritti fondamentali, in conformità ai principi dell'Unione Europea.[155] Il testo promuove una visione antropocentrica, in cui la tecnologia supporta l'uomo senza sostituirlo nei processi decisionali, specialmente in ambiti con rilevanza etica e sociale.

Nei primi sei articoli vengono definiti i principi fondamentali, ponendo al centro la dignità umana, la sicurezza e la trasparenza nella *governance* algoritmica. L'IA deve, quindi, operare nel rispetto dei diritti costituzionali e delle libertà fondamentali, basandosi su criteri di trasparenza, proporzionalità, sicurezza, protezione dei dati, non discriminazione, parità di genere e sostenibilità.[156] In questo contesto, viene ribadita la centralità della decisione umana, imponendo che le decisioni automatizzate possano essere verificate, contestate e modificate dall'uomo.[157] L'articolo 4, invece, ordina liceità, correttezza e trasparenza nel trattamento dei dati personali garantendo, così, all'utente la conoscibilità e la facoltà di opporsi.[158]

---

[154] Comunicato stampa del Consiglio dei Ministri n. 78, 23 aprile 2024, p. 1.

[155] Disegno di legge n. 1146, art. 1: *1. La presente legge reca princìpi in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e di modelli di intelligenza artificiale. Promuove un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. Garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale. 2. Le disposizioni della presente legge si interpretano e si applicano conformemente al regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024.*

[156] Disegno di legge n. 1146, art. 3(1): *La ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale per finalità generali avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei princìpi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.*

[157] Disegno di legge n. 1146, art. 3(3): *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 spiegabilità e dei princìpi di cui al comma 1, assicurando la sorveglianza e l'intervento umano.*

[158] Disegno di legge n. 1146, art. 4 – *Principi in materia di informazione e di riservatezza dei dati personali.*

Il provvedimento, all'articolo 5[159], promuove un ecosistema innovativo e competitivo, favorendo la creazione di un mercato regolamentato attraverso appalti pubblici mirati e garantendo l'accesso a dati di alta qualità per imprese e comunità scientifica. L'obiettivo è ridurre il divario tra settore pubblico e privato e incentivare nuove opportunità economiche nel rispetto della libera concorrenza.[160] A tal riguardo, infatti, le piattaforme di *e-procurement* della pubblica amministrazione dovranno adeguarsi a regole specifiche per garantire trasparenza nelle procedure di acquisto.

Come anticipato, uno dei settori regolamentati dal disegno di legge è la pubblica amministrazione. L'integrazione dell'IA è finalizzata ad assicurare ed incrementare il buon andamento[161] e l'efficienza dell'azione amministrativa, accelerando i procedimenti e migliorando la qualità e la quantità dei servizi forniti a cittadini e imprese.[162] Tuttavia, l'impiego dell'intelligenza artificiale nel settore pubblico deve garantire, come già sottolineato, la trasparenza e la tracciabilità del suo utilizzo, limitandosi a una funzione di supporto al potere decisionale dell'essere umano[163], che, ai sensi dell'articolo 28 delle Costituzione[164], conserva la responsabilità e l'autodeterminazione.[165]

---

[159] Disegno di legge n. 1146, art. 5 – *Principi in materia di sviluppo economico.*

[160] M. T. D'Urso, '*Il d.d.l., di iniziativa governativa, approvato il 23 aprile 2024, sulla Intelligenza artificiale. I principi fondamentali dell'AI per il suo utilizzo in Italia, in linea con "l'AI Act" deliberato dall'UE. Le disposizioni di settore. La Strategia nazionale e le nuove agenzie istituite. La tutela per gli utenti e per il diritto d'autore e le pene per i trasgressori. Il G7 svoltosi il 13-15 giugno 2024 a Borgo Egnazia (BR) con l'intervento di Papa Bergoglio*', *cit.*, p. 99.

[161] Costituzione, art. 97: […] *I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione.*

[162] Disegno di legge n. 1146, art. 14(1): *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 imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo.*

[163] Disegno di legge n. 1146, art. 14(2): *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.*

[164] Costituzione, art. 28: *I funzionari e i dipendenti dello Stato e degli enti pubblici sono direttamente responsabili, secondo le leggi penali, civili e amministrative, degli atti compiuti in violazione di diritti. In tali casi la responsabilità civile si estende allo Stato e agli enti pubblici*.

[165] M. T. D'Urso, '*Il d.d.l., di iniziativa governativa, approvato il 23 aprile 2024, sulla Intelligenza artificiale. I principi fondamentali dell'AI per il suo utilizzo in Italia, in linea con "l'AI Act" deliberato dall'UE. Le disposizioni di settore. La Strategia nazionale e le nuove agenzie istituite. La tutela per gli utenti e per il diritto d'autore e le pene per i trasgressori. Il G7 svoltosi il 13-15 giugno 2024 a Borgo Egnazia (BR) con l'intervento di Papa Bergoglio*', *cit.*, p. 101.

Il Governo italiano ha inoltre designato l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN) come Autorità nazionali per l'intelligenza artificiale.[166] L'AgID, oltre ad avere il compito di supervisionare e definire linee guida per l'adozione dell'IA nelle amministrazioni pubbliche[167], è responsabile della definizione delle procedure e dell'esercizio delle funzioni relative a notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale.[168] L'ACN, invece, si occupa della protezione dell'infrastruttura digitale nazionale e della prevenzione di attacchi informatici al fine di tutelare la sovranità cibernetica nazionale.[169] All'agenzia sono anche affidati i compiti di vigilanza sull'intelligenza artificiale previsti dalla normativa nazionale e comunitaria.[170]

La presente proposta legislativa si configura, dunque, come un quadro normativo complesso e articolato, volto a coniugare, in coerenza con il panorama regolamentare europeo, l'innovazione tecnologica con la tutela dei diritti fondamentali e la sicurezza nazionale.

---

[166] Disegno di legge n. 1146, art. 20 – *Autorità nazionali per l'intelligenza artificiale*.
[167] AgID, '*Strategia Italiana per l'Intelligenza Artificiale 2024-2026*'.
[168] Disegno di legge n. 1146, art. 20(1)(a): […] *L'AgID provvede, altresì, a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea.*
[169] M. T. D'Urso, '*Il d.d.l., di iniziativa governativa, approvato il 23 aprile 2024, sulla Intelligenza artificiale. I principi fondamentali dell'AI per il suo utilizzo in Italia, in linea con "l'AI Act" deliberato dall'UE. Le disposizioni di settore. La Strategia nazionale e le nuove agenzie istituite. La tutela per gli utenti e per il diritto d'autore e le pene per i trasgressori. Il G7 svoltosi il 13-15 giugno 2024 a Borgo Egnazia (BR) con l'intervento di Papa Bergoglio*', *cit.,* p. 103.
[170] Disegno di legge n. 1146, art. 20(1)(b): *L'ACN* […] *è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea.*

CAPITOLO II

LA LEGALITÀ ALGORITMICA

SOMMARIO: **1. Tecnologia ed amministrazione** – **2. Il principio di legalità** – 2.1. La qualificazione giuridica dell'algoritmo – 2.1.1. Il *software* come atto amministrativo – 2.1.1.1. Critica all'algoritmo come atto amministrativo – 2.1.2. Il *software* come modulo organizzativo – 2.2. Algoritmi e discrezionalità amministrativa – **3. L'articolo 30 del decreto legislativo 31 marzo 2023, n. 36** – 3.1. Spazi di sperimentazione normativa per l'IA – 3.2. La sentenza TAR Lazio n. 4546/2025 – 3.3. Le allucinazioni di intelligenza artificiale e le sue conseguenze processuali – **4. I principi per una pubblica amministrazione automatizzata** – 4.1. Il principio di trasparenza: conoscibilità e comprensibilità – 4.1.1. L'opacità degli algoritmi – 4.1.1.1. Il problema della *black box* – 4.1.1.2. I diritti di proprietà intellettuale sul *software* – 4.2. Il principio di non esclusività della decisione algoritmica – 4.2.1. L'interpretazione giurisprudenziale – 4.3. Il principio di non discriminazione algoritmica – 4.3.1. Il caso *Compas* negli Stati Uniti.

1. Tecnologia ed amministrazione

Negli ultimi decenni, l'implementazione delle tecnologie digitali ha rivoluzionato profondamente le modalità organizzative e decisionali della pubblica amministrazione. L'uso e lo sviluppo delle *information and communication technologies* (ICTs) non si limita più alla solo attività e gestione interna, ma si estende direttamente all'attività amministrativa vera e propria.[171]

Nel tempo, l'amministrazione ha, infatti, compiuto una importante evoluzione fino all'attuale paradigma dell'"*Amministrazione 4.0*"[172], in cui gli strumenti tecnologici sono divenuti anche mezzi per l'assunzione di decisioni. Questa evoluzione è ben sintetizzata nelle nozioni di *street-level bureaucracy e screen-*

[171] Come rilevato, già nel 1979, in M.S. Giannini, '*Rapporto sui principali problemi dell'amministrazione dello* Stato', in *Il Foro italiano*, vol. 102, Parte quinta: monografie e varietà, 1979, p. 298.

[172] D.U. Galetta, J.G. Corvalán, '*Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*', in *federalismi.it*, 2019, fasc. 3, p. 22.

level bureaucracy[173]: se prima le decisioni erano affidate esclusivamente all'uomo, oggi, seppure resti fondamentale l'intervento umano nella programmazione e nella verifica dei risultati, le decisioni vengono mediate da sistemi digitali. Il passaggio ulteriore di questa trasformazione è la cosiddetta *system-level bureaucracy*[174], in cui il ruolo del funzionario è fortemente ridimensionato a vantaggio di un sistema automatizzato, benché sempre sottoposto a una forma di supervisione umana.

A livello europeo, l'ingresso delle tecnologie nell'apparato amministrativo ha portato alla formulazione del concetto di *e-government*, definito come "*l'uso delle tecnologie dell'informazione e della comunicazione nelle Pubbliche Amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche*".[175] In altre parole, si tratta dello strumento necessario a rendere più efficiente ed efficace l'amministrazione e a far fronte all'esigenza – apparentemente contraddittoria – di offrire servizi più numerosi e di migliore qualità con meno risorse.[176] Le istituzioni europee, quindi, promuovendo l'implementazione delle ICTs, favoriscono la diffusione di una pubblica amministrazione più efficiente, trasparente, partecipativa e affidabile.[177]

Nel panorama italiano, il legislatore ha cominciato a occuparsi del rapporto tra tecnologie e pubblica amministrazione a partire dagli anni novanta dello scorso secolo, con l'introduzione della legge 7 agosto 1990, n. 241.[178] Questa, pur non trattando in modo specifico l'innovazione tecnologica, riconosce all'articolo 3-bis che "*per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti*

---

[173] M. D'Angelosante, '*La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*', in S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione*, vol. 4. Firenze, Firenze University Press, 2016, p. 157.
[174] *Ibid.*
[175] Commissione europea, '*Il ruolo dell'eGovernment per il futuro dell'Europa*', Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, COM (2003) 567, 29 marzo 2003, §3, p. 8.
[176] *Ibid.*
[177] Commissione europea, '*Piano d'azione dell'UE per l'eGovernment 2016-2020*', Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, COM (2016) 179, 19 aprile 2016.
[178] Legge 7 agosto 1990, n. 241, 'Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi'.

interni, tra le diverse amministrazioni e tra queste e i privati".[179] Con questa norma, introdotta nel capo dedicato ai principi e risalente ormai a 35 anni fa, si afferma, quindi, la digitalizzazione come principio dell'azione amministrativa[180] e si promuove l'uso della telematica al fine di garantire maggiore efficienza amministrativa.

Successivamente, con il Codice dell'amministrazione digitale (CAD)[181] si è cercato di riordinare l'intero assetto normativo in materia e di definire una disciplina unitaria. A tal riguardo, di particolare importanza è l'articolo 12 che stabilisce: "*le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese*".[182]

Nonostante un'articolazione su diversi livelli, tra cui la carta della cittadinanza digitale, la ripartizione delle competenze, il documento informatico, le firme elettroniche e la gestione dei dati, la capacità del CAD di regolamentare efficacemente un settore in continua evoluzione è stata oggetto di critiche da parte della dottrina. Questa, evidenziandone i limiti, ha riconosciuto che si tratta di un quadro normativo non ancora compiuto, caratterizzato da eterogeneità e lacune[183], e soprattutto carente nel disciplinare in modo specifico il tema della decisione automatizzata.[184] Per questi motivi, di assoluta importanza è l'attività "*di supplenza"* svolta dalla giurisprudenza amministrativa.[185]

---

[179] Legge 241/1990, art. 3-bis – *Uso della telematica.*
[180] A. Sola, '*L'automatizzazione dell'azione amministrativa*', in *Amministrazione in cammino*, 2020, p. 8.
[181] D.lgs. 7 marzo 2005, n. 82, 'Codice dell'amministrazione digitale'.
[182] D.lgs. 82/2005, art. 12 – *Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa.*
[183] E. Carloni, '*La riforma del Codice dell'amministrazione digitale*', in *Giornale di diritto amministrativo*, 2011, fasc. 5, pp. 469-476.
[184] M. Bottari, '*Procedimento amministrativo: evoluzione digitale e i suoi sviluppi nell'era dell'intelligenza artificiale*', in Il diritto amministrativo, anno XVI, n. 03/2023.
[185] *Ibid.*

2. Il principio di legalità

Il principio di legalità, quale carattere essenziale dello stato di diritto, trova applicazione specifica al procedimento amministrativo, come noto, mediante l'articolo 1 della legge n. 241/1990, che stabilisce che "*l'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia, di imparzialità, di pubblicità e di trasparenza secondo le modalità previste dalla presente legge e dalle altre disposizioni che disciplinano singoli procedimenti, nonché dai principi dell'ordinamento comunitario*".[186] Dunque, il principio di legalità necessita, da un lato, che la legge attribuisca espressamente un determinato potere a un ente amministrativo, stabilendo chiaramente la sua competenza e l'ambito in cui tale potere può essere esercitato; dall'altro, che la legge definisca i contesti specifici, le modalità procedurali e i limiti entro cui tale potere può essere utilizzato, garantendo così che l'esercizio dell'autorità pubblica sia sempre conforme a criteri normativi. In altre parole, nei rapporti con i cittadini, le pubbliche amministrazioni esercitano esclusivamente i poteri conferiti dalla legge, entro i limiti da essa stabiliti e perseguendo le finalità previste.[187]

L'evoluzione tecnologica e l'avvento dell'amministrazione algoritmica hanno sollevato dubbi sulla modalità applicativa del principio di legalità. Più nel dettaglio, la dottrina è divisa nel valutare se l'amministrazione debba essere esplicitamente autorizzata da una norma per l'adozione di decisioni amministrative algoritmiche. La risoluzione di questo problema è direttamente connessa ad una questione preliminare fondamentale: determinare se l'utilizzo dell'algoritmo costituisca una semplice modifica negli strumenti a disposizione dell'amministrazione ai fini dell'adozione di una decisione, o, invece, se rappresenti l'esercizio di un vero e proprio nuovo potere amministrativo.[188]

Qualora si abbracci la prima ipotesi – quella attualmente prevalente nei diversi ordinamenti nazionali[189] – il principio di legalità dovrebbe essere applicato

[186] Legge 241/1990, art. 1 – *Principi generali dell'attività amministrativa*.
[187] A. Police, '*La legge, il potere amministrativo e le situazioni giuridiche soggettive*', in G. Della Cananea, M. Dugato, B. Marchetti, A. Police, M. Ramajoli, *Manuale di diritto amministrativo,* Giappichelli, II edizione, 2023, p. 96.
[188] L. Torchia, '*Lo stato digitale – Una introduzione*', Il Mulino, 2023, pp. 114-115.
[189] *Ibid*, p. 117.

all'amministrazione algoritmica allo stesso modo in cui si applica all'amministrazione tradizionale. Infatti, non trattandosi di un nuovo potere amministrativo, ma bensì di un miglioramento strumentale nell'esercizio di un potere già esistente, l'utilizzo di algoritmi o altre tecnologie per assumere decisioni non necessita di una specifica norma abilitante caso per caso, ma è sufficiente una norma di carattere generale che autorizzi l'utilizzo di tecnologie nell'esercizio dei pubblici poteri. E due norme che non solo autorizzino, ma promuovano l'utilizzo di nuove tecnologie sono da tempo già in vigore nel nostro ordinamento. Si tratta, come ricordato[190], dell'articolo 3-bis della legge 241/1990 e dell'articolo 12 del Codice dell'amministrazione digitale.[191]

Qualora, invece, si accolga la seconda ipotesi – quella secondo cui l'algoritmo non è semplicemente uno strumento tecnico, ma configura piuttosto un nuovo potere amministrativo – sarebbe allora necessaria, ai sensi dell'articolo 22 del GDPR, una espressa e specifica norma abilitante caso per caso. Infatti, il diritto di non essere sottoposti ad una decisione unicamente automatizzata non trova protezione qualora la decisione "*sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato*".[192] Quindi, almeno per le decisioni amministrative integralmente automatizzate, una rigorosa applicazione del principio di legalità richiederebbe un'abilitazione normativa riferita a specifici provvedimenti e procedimenti.[193]

2.1. La qualificazione giuridica dell'algoritmo

La posizione adottata in relazione all'applicabilità del principio di legalità all'amministrazione algoritmica è, altresì, determinante per la qualificazione giuridica del *software* utilizzato nella procedura decisionale.

[190] Si veda *supra* paragrafo 1.
[191] L. Torchia, '*Lo stato digitale – Una introduzione*', *cit.*, p. 115.
[192] Regolamento (UE) 2016/679, art. 22(2)(b).
[193] L. Torchia, '*Lo stato digitale – Una introduzione*', *cit.*, p. 116.

Infatti, se, come sostenuto dalla prima posizione dottrinale, l'algoritmo è considerato solo un mezzo per migliorare l'efficacia e l'efficienza della pubblica amministrazione, il *software* non è da considerarsi un atto amministrativo.[194]

Qualora, invece, l'uso dell'algoritmo sia inteso come l'esercizio di un nuovo potere amministrativo, allora il *software* può essere qualificato come atto amministrativo.[195]

2.1.1. Il *software* come atto amministrativo

La posizione dottrinale[196] e giurisprudenziale per cui "*l'algoritmo, ossia il software, deve essere considerato a tutti gli effetti come un "atto amministrativo informatico*"[197], si articola in un processo che inizia con un atto preliminare di carattere generale, con il quale l'amministrazione formalizza la propria intenzione di utilizzare *software* e algoritmi nell'ambito dell'attività amministrativa. Questo atto, qualificabile come atto amministrativo generale, costituisce la base per l'adozione di provvedimenti successivi, prodotti automaticamente dall'algoritmo in una serie indeterminata di casi e destinatari.[198]

Seguirà poi una fase tecnica, in cui l'algoritmo viene effettivamente realizzato dall'amministrazione, o da soggetti terzi incaricati. In questa fase si redigono i codici sorgente, che, pur essendo frutto di una programmazione tecnica, realizzano concretamente la volontà già espressa dall'amministrazione.[199] Dunque, l'algoritmo assume la conformazione di un "*complesso di regole e istruzioni da eseguire in futuro al ricorrere di determinate condizioni mediante le quali si stabilisce ex ante la regolazione di casi futuri non attuali*".[200]

Successivamente, l'algoritmo viene applicato in un procedimento amministrativo in cui l'elaborazione dei dati e l'assunzione delle decisioni è integralmente demandata al *software*. Il provvedimento finale che ne scaturisce è

---

[194] Si veda *infra* paragrafo 2.1.2.
[195] Si veda *infra* paragrafo 2.1.1.
[196] A. Sola, '*Inquadramento giuridico degli algoritmi nell'attività amministrativa*', in *federalismi.it*, 2020, fasc. 16, pp. 351 e ss.
[197] Consiglio di Stato, Sez. VI, 8 aprile 2019, n. 2270.
[198] A. Sola, '*Inquadramento giuridico degli algoritmi nell'attività amministrativa*', *cit.,* p. 351.
[199] *Ibid*, p. 352.
[200] *Ibid*, p. 342.

definito un atto amministrativo elettronico, e rappresenta l'effettiva realizzazione della volontà amministrativa espressa nelle fasi precedenti.[201]

Questa impostazione giuridica porta a sostenere che l'algoritmo, pur non essendo autonomamente impugnabile o considerato un atto amministrativo immediatamente esecutivo, possa essere qualificato come atto amministrativo, in quanto costituisce una manifestazione della volontà dell'amministrazione che condiziona e orienta il contenuto dei provvedimenti amministrativi futuri.[202]

La qualificazione dell'algoritmo come atto amministrativo ha generato una discussione dottrinale sulla sua tipologia. Infatti, da un lato, si può ritenere che il *software* e gli algoritmi possano rappresentare atti amministrativi generali, "*poiché finalizzati all'emanazione di successivi provvedimenti e suscettibili di ripetuta applicazione ad una serie indeterminabile, quantomeno a priori, di casi*".[203] In alternativa, se l'attività di programmazione venisse considerata come una fase del procedimento amministrativo, allora gli algoritmi e il *software* sarebbero qualificati come atti endoprocedimentali.[204]

2.1.1.1. Critica all'algoritmo come atto amministrativo

Una parte della dottrina ha contestato la posizione appena esaminata sulla base di molteplici osservazioni.

In primo luogo, il programma informatico è redatto in un linguaggio di programmazione comprensibile esclusivamente da esperti del settore, ma non dal cittadino destinatario dell'atto, né dall'autorità responsabile della sua adozione. Questo solleva un problema significativo per i principi di pubblicità e trasparenza dell'azione amministrativa, poiché l'impossibilità di comprendere il meccanismo decisionale potrebbe compromettere l'accesso e la conoscibilità delle decisioni prese.[205]

---

[201] *Ibid*, p. 352.
[202] *Ibid*, p. 353.
[203] *Ibid*, p. 354.
[204] *Ibid.*
[205] A.G. Orofino, '*La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*', in *Foro amministrativo CDS*, 2002, fasc. 9, pp. 2269-2270.

Inoltre, qualora si accettasse la qualificazione del *software* come atto amministrativo, sarebbe necessario che tale atto rispetti i requisiti formali previsti dalla legge, inclusa la sottoscrizione. Tuttavia, la firma digitale di un programma informatico comporta difficoltà pratiche, dovute al numero elevato di *files* che compongono il *software*, nonché alla loro mutevolezza.[206]

Ulteriore critica muove dalla nozione stessa di atto amministrativo. Infatti, quest'ultimo si configura come un atto giuridico adottato da un'autorità amministrativa nell'esercizio di una funzione o attività pubblica.[207] Tuttavia, nella quasi totalità dei casi, l'algoritmo impiegato nei procedimenti automatizzati non è frutto dell'attività interna della pubblica amministrazione, bensì realizzato da soggetti ad essa esterni, spesso privati, e talvolta protetto da brevetto o da altri strumenti di proprietà intellettuale.[208] In tali ipotesi, l'acquisizione dello strumento algoritmico da parte dell'amministrazione avviene mediante procedure ad evidenza pubblica, che si concludono con un atto di affidamento, a cui segue, ai sensi dell'articolo 116 del Codice dei contratti pubblici[209], una verifica di conformità o di regolare esecuzione.[210] Nella prassi, quindi, l'amministrazione non partecipa attivamente alla fase di ideazione, progettazione o addestramento del sistema algoritmico, ma si limita, solitamente, a utilizzare la soluzione tecnica acquisita, affidandosi a soggetti terzi.[211]

Infine, non sarebbe contemplata la possibilità di impugnare autonomamente il *software*, essendo la rilevazione di eventuali vizi dell'algoritmo contestabile solo in sede di impugnazione dell'atto finale, in via di illegittimità derivata.[212]

---

[206] *Ibid,* pp. 2270-2271.
[207] N. Durante, '*La discrezionalità amministrativa ed i vizi del procedimento amministrativo, nell'epoca dell'intelligenza artificiale*', rassegna di Diritto pubblico dell'economia, convegno *"Intelligenza artificiale e appalti pubblici, tra capacità predittiva e discrezionalità amministrativa",* Varese, 18-19 aprile 2024, in giustiziamministrativa.it, 2024, p. 4.
[208] *Ibid.*
[209] D.lgs. n. 36/2023, art. 116(1): *I contratti sono soggetti a collaudo per i lavori e a verifica di conformità per i servizi e per le forniture per certificare il rispetto delle caratteristiche tecniche, economiche e qualitative dei lavori e delle prestazioni, nonché degli obiettivi e dei tempi, in conformità delle previsioni e pattuizioni contrattuali.*
[210] N. Durante, '*La discrezionalità amministrativa ed i vizi del procedimento amministrativo, nell'epoca dell'intelligenza artificiale*', *cit.*, p. 4.
[211] *Ibid.*
[212] F. Saitta, '*Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*', in *Rivista di Diritto Amministrativo Elettronico*, 2003, p. 26.

2.1.2. Il *software* come modulo organizzativo

La posizione dottrinale secondo cui il ricorso agli algoritmi da parte della pubblica amministrazione configura l'utilizzo di uno strumento organizzativo e non di un atto amministrativo, ha trovato un'apertura anche nelle pronunce giurisprudenziali. Infatti, il Consiglio di Stato ha affermato che "*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 della legislazione attributiva del potere e delle finalità dalla stessa attribuite all'organo pubblico, titolare del potere*".[213]

Questa pronuncia del massimo Giudice amministrativo appare coerente con la distinzione tra *pre-software* e *software*, secondo cui il primo rappresenta l'atto amministrativo contenente i diversi passaggi procedimentali in linguaggio naturale, mentre il secondo, costituendo la traduzione dei passaggi in linguaggio informatico, si sostanzia in un mezzo attraverso il quale si concretizza l'azione amministrativa.[214] In continuità con tale visione, la dottrina ritiene che il *software* vada qualificato come strumento dell'azione amministrativa e, quindi, come mezzo tecnico che l'amministrazione utilizza nelle fasi centrali del procedimento, in particolare a cavallo tra l'istruttoria e la decisione.[215] Il suo funzionamento si articola, quindi, nell'inserimento dei dati in *input* e, successivamente, nell'elaborazione automatica degli stessi secondo la sequenza di istruzioni prevista dall'algoritmo, fino alla produzione dell'*output*.[216]

L'automazione, in questo contesto, rappresenta una delle modalità possibili di conduzione del procedimento amministrativo, con la conseguenza che l'automazione non può essere qualificata come attività giuridica in senso proprio, né, tantomeno, come espressione di una volontà decisoria.[217]

---

[213] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.
[214] D. Marongiu, '*Gli atti amministrativi ad elaborazione elettronica: la compilazione di un 'pre-software' in lingua italiana*', in *Rivista di Diritto Amministrativo Elettronico*, 2003, pp. 3-4.
[215] A.G. Orofino, '*La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*', *cit.*, p. 2276.
[216] G. Gallone, '*Riserva di umanità e funzioni amministrative*', Wolters Kluwer, 2023, p. 96.
[217] *Ibid,* pp. 96-97.

2.2. Algoritmi e discrezionalità amministrativa

La compatibilità tra strumenti algoritmici e discrezionalità amministrativa rappresenta una delle questioni di maggior rilievo nella riflessione sull'automazione dei procedimenti amministrativi.[218] Se l'ingresso dell'automazione nell'amministrazione pubblica è stato favorito dalla natura rigidamente strutturata degli atti vincolati,[219] per lungo tempo si è ritenuto che la discrezionalità rappresentasse un ostacolo difficilmente superabile all'impiego di tecnologie decisionali automatiche, proprio per la sua natura valutativa e contestuale.[220] In tale prospettiva, l'attività algoritmica è stata tradizionalmente confinata alle ipotesi in cui la norma determina in modo esaustivo i presupposti e gli effetti del provvedimento, mentre l'adozione di scelte discrezionali è stata riservata all'intervento umano, ritenuto insostituibile per la sua capacità di ponderazione qualitativa.[221]

Tuttavia, autorevole dottrina e la giurisprudenza più recente hanno iniziato a superare questo paradigma, ponendo l'attenzione non tanto sul momento esecutivo della decisione, quanto su quello in cui si definiscono le regole generali che guidano l'automatismo.[222] Da questa prospettiva, l'attività discrezionale non sarebbe esclusa dall'automazione, ma verrebbe esercitata in forma anticipata, nella fase di progettazione del sistema.[223] Infatti, sebbene l'algoritmo sia in grado di determinare autonomamente l'esito applicabile a casi singoli, i criteri su cui tale automazione si fonda sono definiti *ex ante* da soggetti umani e costituiscono espressione di una vera e propria scelta discrezionale.[224] In altre parole, la definizione dei criteri decisionali da parte dell'amministrazione, l'attribuzione di un peso agli elementi

---

[218] A. Police, '*Scelta discrezionale e decisione algoritmica*', in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale persona, mercato, amministrazione, giustizia,* Giuffrè, 2022, p. 497.
[219] L. Viola, '*L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*', in *federalismi.it*, 2018, fasc. 21, pp. 5-6.
[220] G. Avanzini, '*Decisioni amministrative e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intelligibilità*', Editoriale scientifica, Napoli, 2019, p. 91.
[221] G. Duni, '*L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto emanato nella forma elettronica*'. Relazione al convegno «L'informatica giuridica al servizio del Paese», Roma, 1-3 giugno 1978, in *Rivista amministrativa della Repubblica italiana*, 1978, fasc. 6, parte 1, p. 409.
[222] A. Police, '*Scelta discrezionale e decisione algoritmica*', *cit*., p. 499.
[223] *Ibid.*
[224] *Ibid.*

rilevanti e la selezione dei parametri che orientano l'esito algoritmico costituiscono, a tutti gli effetti, un esercizio di discrezionalità.[225] Tale schema viene, poi, incorporato nel *software*, che si limita successivamente ad applicarlo in modo automatico.[226] Questa impostazione corrisponde alla teoria dell'autolimite, secondo cui la discrezionalità può essere esercitata mediante un atto che precede logicamente e cronologicamente l'adozione del provvedimento concreto, ponendosi rispetto ad esso come limite esterno.[227] In tale prospettiva, qualora la programmazione dell'algoritmo coincida con questa operazione di autovincolo, anche l'attività discrezionale può ritenersi compatibile con l'automazione, in quanto la componente valutativa è già stata esaurita nella fase di definizione dei parametri decisionali.[228]

Questa impostazione è stata fatta propria anche dal Consiglio di Stato, che ha riconosciuto che non "*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*".[229] Dunque, i Giudici di Palazzo Spada riconoscono la possibilità di impiegare strumenti automatizzati per l'adozione di provvedimenti aventi contenuto discrezionale, collocando l'esercizio della discrezionalità amministrativa al momento dell'elaborazione dell'algoritmo.[230] Tuttavia, devono essere garantite, da un lato, la trasparenza del sistema – intesa come conoscibilità e comprensibilità del funzionamento – e, dall'altro, l'imputabilità della decisione algoritmica all'organo titolare del potere discrezionale.[231]

---

[225] *Ibid.*
[226] *Ibid*.
[227] A. Police, '*La predeterminazione delle decisioni amministrative. Gradualità e trasparenza nell'esercizio del potere discrezionale*', Editoriale scientifica, Napoli, 1997, p. 218.
[228] G. Avanzini, '*Decisioni amministrative e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intelligibilità*', *cit*., pp. 91-92.
[229] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.
[230] Consiglio di Stato, Sez. VI, 8 aprile 2019, n. 2270: *Questa regola algoritmica, quindi:* […] *non può lasciare spazi applicativi discrezionali (di cui l'elaboratore elettronico è privo), ma deve prevedere con ragionevolezza una soluzione definita per tutti i casi possibili, anche i più improbabili (e ciò la rende in parte diversa da molte regole amministrative generali); la discrezionalità amministrativa, se senz'altro non può essere demandata al software, è quindi da rintracciarsi al momento dell'elaborazione dello strumento digitale.*
[231] A. Police, '*Scelta discrezionale e decisione algoritmica*', *cit*., pp. 501-502.

Due ulteriori teorie a sostegno della compatibilità tra automazione e discrezionalità sono quella dell'automazione per fasi e quella dell'automatizzazione della discrezionalità tecnica.[232]

La prima ipotesi prende atto dell'assenza di procedimenti interamente automatizzati e propone, di conseguenza, un modello ibrido in cui l'intervento algoritmico si affianchi a quello umano. Tale impostazione consente di attribuire al *software* funzioni decisionali in relazione sia ad atti vincolati, sia a situazioni caratterizzate da un grado minimo di discrezionalità.[233] Infatti, esiste un ampio insieme di decisioni pubbliche caratterizzate da un elevato grado di standardizzazione, rispetto alle quali l'intervento discrezionale dell'amministrazione risulta marginale o comunque contenuto. Ciò accade nei casi in cui l'attività è vincolata dalla norma di legge, oppure regolata da criteri tecnico-scientifici, o ancora quando la discrezionalità è stata anticipatamente esercitata attraverso la predeterminazione di criteri e regole.[234]

Quanto alla seconda teoria, essa si fonda sull'idea che la discrezionalità tecnica non possa essere assimilata alla discrezionalità in senso proprio, poiché non implica una ponderazione tra interessi contrapposti.[235] In tale prospettiva, una volta formulato il giudizio tecnico secondo parametri oggettivi, l'amministrazione è tenuta ad agire nei limiti predefiniti dall'ordinamento, senza ulteriori margini di scelta.[236] Ne discende che, sul piano giuridico, anche le valutazioni tecniche – per quanto complesse – assumono natura vincolata e, come tali, sono suscettibili di essere oggetto di automazione, al pari delle decisioni basate su norme puntuali e precettive.[237] In questa direzione, la giurisprudenza amministrativa ha osservato che, accanto all'attività vincolata – ambito in cui l'impiego di strumenti algoritmici

[232] L. Viola, '*L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*', *cit.*, p. 30.
[233] *Ibid*, p. 31.
[234] A. Police, '*Scelta discrezionale e decisione algoritmica*', *cit*., p. 498.
[235] A. Masucci, '*L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*', Jovene, Napoli, 1993, p. 24; L. Viola, '*L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*', *cit.*, p. 31.
[236] *Ibid.*
[237] *Ibid.*

risulta già ampiamente diffuso – anche l'esercizio della discrezionalità tecnica può beneficiare delle potenzialità proprie dell'automazione.[238]

3. L'articolo 30 del decreto legislativo 31 marzo 2023, n. 36

Il decreto legislativo 31 marzo 2023, n. 36, generalmente noto come il nuovo codice dei contratti pubblici, rappresenta un ulteriore e significativo passo in avanti nel processo di digitalizzazione della pubblica amministrazione, in particolare nel settore degli appalti pubblici. Entrato in vigore il 1° aprile 2023 con piena efficacia dal 1° luglio 2023, ha sostituito il precedente d.lgs. 50/2016, introducendo importanti novità anche sotto il profilo dell'implementazione di strumenti tecnologici nell'intero ciclo di vita dei contratti pubblici.[239]

Particolare importanza assume a tal riguardo l'articolo 30 del nuovo codice.[240] Quest'ultimo consolida e codifica a livello nazionale una serie di principi che trovavano fondamento principalmente in fonti eurounitarie e nell'elaborazione giurisprudenziale.[241] Con la disposizione in esame, dunque, tali principi trovano una formalizzazione esplicita e sistematica nell'ordinamento nazionale, divenendo direttamente applicabili nell'ambito delle procedure automatizzate della contrattualistica pubblica.

---

[238] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881: "*Piuttosto, se nel caso dell'attività vincolata ben più rilevante, sia in termini quantitativi che qualitativi, potrà essere il ricorso a strumenti di automazione della raccolta e valutazione dei dati, anche l'esercizio di attività discrezionale, in specie tecnica, può in astratto beneficiare delle efficienze e, più in generale, dei vantaggi offerti dagli strumenti stessi.*"

[239] V. Neri, '*AI Act e diritto amministrativo*', in Lavoro Diritti Europa, 2025, fasc. 1, p. 17.

[240] D.lgs. n. 36/2023, art. 30 – *Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici.*

[241] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881: "*A conferma di quanto sin qui rilevato, in termini generali dal diritto sovranazionale emergono tre principi, da tenere in debita considerazione nell'esame e nell'utilizzo degli strumenti informatici. In primo luogo, il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a ricevere informazioni significative sulla logica utilizzata. […] il principio di conoscibilità si completa con il principio di comprensibilità, ovverosia la possibilità, per riprendere l'espressione del Regolamento, di ricevere «informazioni significative sulla logica utilizzata». In secondo luogo, l'altro principio del diritto europeo rilevante in materia (ma di rilievo anche globale in quanto ad esempio utilizzato nella nota decisione Loomis vs. Wisconsin), è definibile come il principio di non esclusività della decisione algoritmica. […] In terzo luogo, dal considerando n. 71 del Regolamento 679/2016 il diritto europeo trae un ulteriore principio fondamentale, di non discriminazione algoritmica.*"

Si tratta, infatti, di una delle disposizioni[242] più innovative del nuovo codice[243] sia per la tematica trattata sia, soprattutto, per il riferimento a tecnologie molto avanzate, tra cui l'intelligenza artificiale. Tale richiamo esplicito permette che l'automatizzazione avvenga non solo mediante l'utilizzo di algoritmi, ma anche attraverso l'implementazione di più complessi sistemi di *machine learning* e *deep learning.*[244] L'impiego di queste tecnologie ha l'obiettivo di rendere effettiva l'automatizzazione delle procedure e di migliorare l'efficienza degli operatori coinvolti, in linea con l'articolo 97 della Costituzione. [245] Tuttavia, il loro utilizzo non è indiscriminato, ma disciplinato da principi che, in un settore in rapida e costante evoluzione, rappresentano lo strumento migliore per una regolamentazione che aspiri ad essere durevole e tecnologicamente adeguata.[246]

I primi principi previsti dall'articolo 30 riguardano la fase di acquisto e sviluppo delle tecnologie utilizzate dalla pubblica amministrazione.[247] Anche se non espressamente qualificati come principi, le regole contenute nel comma 2 mirano a garantire trasparenza e affidabilità degli strumenti tecnologici impiegati. Il comma 2, lett. a), più precisamente, richiede che le amministrazioni abbiano accesso al codice sorgente del *software*, alla documentazione tecnica e a qualsiasi altro elemento utile a comprenderne il funzionamento, al fine di garantire la massima trasparenza agli operatori economici e rafforzare, contestualmente, i principi di buon andamento e imparzialità.[248] Dunque, con il nuovo codice, le soluzioni tecnologiche devono essere *open source* e, a differenza di quanto previsto dal CDA, non sono ammesse deroghe.[249]

---

[242] D.lgs. n. 36/2023, art. 30(1): *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.*

[243] V. Campanile, '*Commento all'art. 30*', in Codice dei contratti pubblici annotato articolo per articolo, C. Contessa, P. Del Vecchio (a cura di), Napoli, 2023, pp. 277.

[244] *Ibid,* p. 279.

[245] A. Iannotti della Valle, '*Codice dei contratti pubblici commentato*', Luca R. Perfetti (a cura di), Wolters Kluwer, 2023, p. 201.

[246] *Ibid.*

[247] D.lgs. n. 36/2023, art. 30(2): *Nell'acquisto o sviluppo delle soluzioni di cui al comma 1 le stazioni appaltanti e gli enti concedenti: a) assicurano la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento.*

[248] S. Del Gatto, '*I sistemi proprietari, l'open source e la pubblica amministrazione*', in *Giornale di diritto amministrativo*, 2021, fasc. 5, pp. 571 e ss.

[249] A. Iannotti della Valle, '*Codice dei contratti pubblici commentato*', *cit*., p. 202.

Il comma 5 rafforza questo principio, stabilendo che tutte le tecnologie usate debbano essere elencate e pubblicate nella sezione "Amministrazione trasparente" dei siti istituzionali al fine di consentire un controllo diffuso da parte dei cittadini e degli operatori economici.[250]

Il comma 3 introduce, invece, tre principi fondamentali per le decisioni automatizzate: *conoscibilità e comprensibilità*, *non esclusività* della decisione algoritmica e *non discriminazione* algoritmica.

Il primo è strettamente connesso alla disponibilità del codice sorgente e mira a garantire ad ogni soggetto interessato il diritto di sapere se una decisione che lo riguarda è stata presa in modo automatizzato nonché il diritto di ricevere informazioni significative sulla logica che la sostiene.[251]

Il secondo, invece, impone che la decisione finale sia comunque assunta da un essere umano. In altre parole, coerentemente con l'articolo 22 del GDPR, l'algoritmo può supportare, ma non sostituire, il ragionamento e il giudizio di un funzionario pubblico.[252]

Infine, il principio di non discriminazione impone che chi gestisce il sistema adotti tutte le misure tecniche e organizzative necessarie a evitare effetti discriminatori nei confronti degli operatori economici.[253] Gli errori nei dati devono essere rettificati affinché i sistemi non producano esiti distorti sulla base dell'etnia, della religione, delle opinioni politiche, della salute o di altri tratti personali.[254]

---

[250] D.lgs. n. 36/2023, art. 30(5): *Le pubbliche amministrazioni pubblicano sul sito istituzionale, nella sezione «Amministrazione trasparente», l'elenco delle soluzioni tecnologiche di cui al comma 1 utilizzate ai fini dello svolgimento della propria attività.*

[251] D.lgs. n. 36/2023, art. 30(3)(a): *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.*

[252] D.lgs. n. 36/2023, art. 30(3)(b): *Le decisioni assunte mediante automazione rispettano i principi di:* […]; *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*

[253] D.lgs. n. 36/2023, art. 30(3)(c): *Le decisioni assunte mediante automazione rispettano i principi di:* […]; *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.*

[254] D.lgs. n. 36/2023, art. 30(4): *Le stazioni appaltanti e gli enti concedenti adottano ogni misura tecnica e organizzativa atta a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, nonché a impedire effetti discriminatori nei confronti di persone fisiche sulla base della nazionalità, dell'origine etnica, delle opinioni politiche, della religione, delle convinzioni personali, dell'appartenenza sindacale, dei caratteri somatici, dello status genetico, dello stato di salute, del genere o dell'orientamento sessuale.*

3.1. Spazi di sperimentazione normativa per l'IA

L'articolo 57[255] dell'AI Act consente ed incentiva, (anche) al fine di "*promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA*"[256], l'istituzione di spazi di sperimentazione normativa dedicati all'intelligenza artificiale.[257] Tali spazi di sperimentazione offrono un ambiente regolato e controllato per sviluppare, addestrare, testare e validare sistemi di intelligenza artificiale innovativi per un periodo di tempo limitato, prima della loro effettiva immissione sul mercato o del loro utilizzo operativo.[258]

Si tratta, quindi, di un'occasione "*per sviluppare analisi e dinamiche innovative, di carattere sperimentale, anche nell'ambito dei pubblici appalti e, comunque, dei procedimenti amministrativi*".[259] L'attivazione di questi spazi consentirebbe un approccio graduale, con la possibilità di testare le soluzioni tecnologiche per fasi o per ambiti, evitando così il rischio di istituire un sistema normativo eccessivamente rigido o già obsoleto.[260] In questo contesto, il settore degli appalti pubblici – già normativamente predisposto all'implementazione di sistemi di intelligenza artificiale ai sensi dell'articolo 30 del D.lgs. n. 36/2023 – si configura come un ambito ideale per avviare sperimentazioni normative.[261]

---

[255] Regolamento (UE) 2024/1689, art. 57 – *Spazi di sperimentazione normativa per l'IA.*
[256] Regolamento (UE) 2024/1689, art. 57(9)(c).
[257] Regolamento (UE) 2024/1689, art. 57(1): *Gli Stati membri provvedono affinché le loro autorità competenti istituiscano almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sia operativo entro il 2 agosto 2026. Tale spazio di sperimentazione può essere inoltre istituito congiuntamente con le autorità competenti di altri Stati membri. La Commissione può fornire assistenza tecnica, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA. L'obbligo di cui al primo comma può essere soddisfatto anche partecipando a uno spazio di sperimentazione esistente nella misura in cui tale partecipazione fornisca un livello equivalente di copertura nazionale per gli Stati membri partecipanti.*
[258] Regolamento (UE) 2024/1689, art. 57(5): *Gli spazi di sperimentazione normativa per l'IA istituiti a norma del paragrafo 1 garantiscono un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e l'autorità competente. Tali spazi di sperimentazione possono comprendere prove in condizioni reali soggette a controllo nei medesimi spazi.*
[259] M. Barberio, '*L'art. 30 del D.L. vo 36/2023 alla prova dell'A.I. Act dell'Unione Europea*', Relazione tenuta al Convegno di Studi presso l'Università degli Studi di Cagliari "*L'intelligenza artificiale nel diritto amministrativo*", in giustiziamministrativa.it, 2023, p. 15.
[260] *Ibid*, p. 16.
[261] *Ibid.*

3.2. La sentenza TAR Lazio n. 4546/2025

Il TAR Lazio, in una recentissima pronuncia, si è espresso in merito all'utilizzo dell'intelligenza artificiale nelle offerte tecniche presentate da operatori economici concorrenti in sede di gara pubblica.[262]

La questione sottoposta all'esame del Tribunale riguarda l'impugnazione, da parte della ricorrente, dell'attribuzione di punteggi elevati a una concorrente aggiudicataria che aveva dichiarato, nella propria offerta tecnica, l'intenzione di avvalersi di strumenti di IA — in particolare, *ChatGPT* — per lo svolgimento di alcune attività a supporto dell'esecuzione del contratto.[263]

La parte ricorrente, classificatasi nella prima posizione non utile ai fini dell'aggiudicazione (terza posizione), sosteneva che l'uso di tale tecnologia fosse inidoneo ai fini indicati e che ciò rendesse illegittima l'attribuzione del punteggio. A fondamento della propria censura, il ricorrente produceva delle interrogazioni rivolte autonomamente a *ChatGPT* dai propri legali, evidenziando che le risposte fornite erano incompatibili con le finalità d'uso prospettate dal concorrente.[264] Conseguentemente, l'assegnazione del punteggio risulterebbe illegittima, in quanto non supportata da alcuna prova circa l'effettiva idoneità dello strumento ad essere impiegato nell'esecuzione del servizio.[265]

Il TAR ha rigettato le censure sollevate dal ricorrente sulla base di varie motivazioni.

In primo luogo, ha escluso la sussistenza di un nesso causale diretto e dimostrabile tra l'indicazione dell'uso dell'intelligenza artificiale nell'offerta tecnica e l'attribuzione del punteggio elevato. Tale attribuzione, infatti, che nel caso di specie è stata effettuata tramite il metodo del confronto a coppie, si basa su un

---

[262] TAR Lazio, Sez. II, 3 marzo 2025, n. 4546.
[263] *Ibid.*
[264] *Ibid*: "*Affermando che Chat GPT (che la ricorrente riferisce di aver interrogato) … ha risposto in maniera incompatibile con l'utilizzo che* [omissis] *intende fare di questo strumento*."
[265] *Ibid:* "*Censura, quindi,* […] *«l'illogicità dell'operato della Stazione appaltante" per aver essa "accolto positivamente, senza alcun approfondimento istruttorio, l'utilizzabilità dell'IA nell'ambito del servizio di cui si discute», «scontando» il contenuto dell'offerta «un problema di indeterminatezza e di genericità, perché – dietro l'uso di un linguaggio estremamente tecnico, talvolta perfino criptico – si nasconde la descrizione di modelli astratti, la cui funzionalità in concreto è tutta da dimostrare».*"

giudizio comparativo delle offerte, che rende inappropriato ogni tentativo di ridurre il risultato ottenuto a un singolo elemento.[266]

Inoltre, "*tale doglianza, prima ancora che infondata, appare del tutto inammissibile, sottintendendo la pretesa della ricorrente di sostituire le proprie unilaterali valutazioni – del tutto opinabili – a quelle tecnico-discrezionali della Commissione, al fine di ottenere una riconsiderazione in peius del punteggio assegnato all'offerta tecnica della controinteressata*".[267] Infatti, il TAR rileva come la giurisprudenza riconosca alla Commissione un ampio margine di apprezzamento comparativo tra le proposte, il cui sindacato giurisdizionale è fortemente limitato. Una volta verificata la correttezza formale e procedurale dell'applicazione del metodo valutativo, non è, infatti, consentito sindacare nel merito i singoli giudizi espressi, se non nei casi di manifesta irrazionalità, illogicità o incongruenza metodologica, che non risultano riscontrabili nel caso di specie.[268]

Il Giudice evidenzia, altresì, come manchi qualunque prova oggettiva dell'asserita inidoneità dello strumento di IA. La censura della ricorrente, infatti, si fonda su una ricostruzione astratta e generalista dell'intelligenza artificiale, senza considerare che, in concreto, l'offerente ne ha dichiarato un utilizzo ben delimitato e specifico, in funzione di supporto all'elaborazione e analisi dei dati. Si tratta, quindi, di un impiego mirato, che non può essere valutato in base alle risposte generiche ottenute da interrogazioni decontestualizzate.[269]

Alla luce di tali considerazioni, "*ben si comprende, dunque, come non sia rinvenibile nel caso di specie*, […], *alcun aspetto di evidente criticità e/o inaffidabilità di tale strumento di ausilio, peraltro ormai di comune e diffuso utilizzo, né conseguentemente alcun motivo che avrebbe dovuto condurre la Commissione a diverse valutazioni*".[270] Dunque, il TAR, in chiusura, pur senza

---

[266] *Ibid*: "*I criteri rispetto ai quali si contestano i punteggi conseguiti da tale aggiudicataria sono nel Capitolato d'oneri molti più articolati e complessi di quanto non voglia far credere la ricorrente, dipendendo l'attribuzione del relativo punteggio da una pluralità di elementi di valutazione, relativi anche a tutta un'altra serie gli altri aspetti ivi richiamati e considerati.*"
[267] *Ibid.*
[268] *Ibid.*
[269] *Ibid*: "*Dall'analisi dell'offerta tecnica di* [omissis] *emerga come tale aggiudicataria abbia proposto un impiego dell'intelligenza artificiale (IA) diverso dall'utilizzo del modello generale descritto nell'atto di motivi aggiunti, a ben vedere mirato e specifico, che ne prevede l'impiego solo come ulteriore strumento di supporto matematico/statistico e di elaborazione di dati, migliorando l'efficienza e la qualità dei servizi offerti*."
[270] *Ibid.*

soffermarsi espressamente sulla questione, lascia intendere che strumenti come *ChatGPT* stiano progressivamente acquisendo la natura di ordinari mezzi di supporto tecnico-operativo, analogamente ai più comuni *software* di produttività.[271]

In sintesi, emergono, in particolare, due statuizioni di rilievo. Anzitutto, gli esiti delle mere interrogazioni svolte autonomamente dalla parte ricorrente su sistemi di IA non costituiscono elemento probatorio sufficiente a confutare la concreta idoneità dell'utilizzo prospettato da un altro concorrente. In secondo luogo, il Giudice chiarisce che le valutazioni relative all'adozione di sistemi di intelligenza artificiale da parte dei concorrenti nell'ambito di una procedura pubblica rientrano nella sfera della discrezionalità tecnica della stazione appaltante.

3.3. Le allucinazioni di intelligenza artificiale[272] e le sue conseguenze processuali

Nel contesto di un giudizio in materia di tutela marchi, il Tribunale di Firenze si è pronunciato in merito alla questione della responsabilità per l'impiego improprio di strumenti di intelligenza artificiale negli atti processuali. Nel procedimento in esame, il ricorrente ha proposto istanza di condanna *ex* articolo 96 c.p.c.[273] (cosiddetta "lite temeraria") nei confronti della parte resistente, contestando l'inserimento di riferimenti giurisprudenziali inesistenti nella comparsa di costituzione. In particolare, "*lo strumento di intelligenza artificiale avrebbe inventato dei numeri asseritamente riferibili a sentenze della Corte di Cassazione inerenti all'aspetto soggettivo dell'acquisto di merce contraffatta il cui contenuto, invece, non ha nulla a che vedere con tale argomento*".[274]

Il Collegio, autorizzando il deposito di note in relazione alla correttezza dei precedenti citati, ha acquisito chiarimenti da parte della difesa della società resistente. Quest'ultima ha spiegato che le sentenze erano state individuate da una

[271] V. Laudani, '*L'intelligenza artificiale negli appalti pubblici: un primo caso applicativo*', in Appalti&Contratti, 6 marzo 2025, https://www.appaltiecontratti.it/lintelligenza-artificiale-negli-appalti-pubblici-un-primo-caso-applicativo/
[272] Tribunale Ordinario di Firenze, Sez. Imprese, ordinanza 14 marzo 2025.
[273] Codice di procedura civile, approvato con R.D. 28 ottobre 1940, n. 1443, e successive modificazioni, art. 96 – *Responsabilità aggravata.*
[274] Tribunale Ordinario di Firenze, Sez. Imprese, ordinanza 14 marzo 2025.

collaboratrice tramite uno strumento di intelligenza artificiale, il cui impiego non era stato preventivamente comunicato al difensore.[275] A causa delle "*allucinazioni di intelligenza artificiale*"[276] – fenomeno che si verifica quando l'IA genera contenuti del tutto inventati, che, pur se sottoposti a una successiva interrogazione, vengono nuovamente confermati come attendibili[277] – la parte resistente ha fatto riferimento a sentenze inesistenti. Quest'ultima, tuttavia, ha riconosciuto l'omissione del controllo e ha chiesto lo stralcio delle sentenze erroneamente citate, ribadendo che la propria difesa era già sufficientemente fondata.

La parte reclamante ha sostenuto che tale condotta avrebbe potuto influenzare impropriamente la decisione del giudice, e ha dunque chiesto l'applicazione dell'articolo 96 c.p.c.[278]

Il Tribunale, tuttavia, ha rilevato come mancasse, da parte del reclamante, qualsiasi allegazione – anche generica – in ordine a danni effettivamente subiti, rendendo inapplicabile la disposizione di cui al primo comma dell'articolo 96 c.p.c. Parimenti, ha escluso la configurabilità della fattispecie di cui al terzo comma, non ravvisando una condotta connotata da dolo o colpa grave, né una strumentalizzazione del processo tale da integrare abuso. Per queste ragioni, la domanda è stata rigettata.[279]

---

[275] *Ibid.*
[276] *Ibid.*
[277] *Ibid.*
[278] Codice di procedura civile, art. 96: *Se risulta che la parte soccombente ha agito o resistito in giudizio con mala fede o colpa grave, il giudice, su istanza dell'altra parte, la condanna, oltre che alle spese, al risarcimento dei danni, che liquida, anche d'ufficio, nella sentenza.*
Il giudice che accerta l'inesistenza del diritto per cui è stato eseguito un provvedimento cautelare, o trascritta domanda giudiziale, o iscritta ipoteca giudiziale, oppure iniziata o compiuta l'esecuzione forzata, su istanza della parte danneggiata condanna al risarcimento dei danni l'attore o il creditore procedente, che ha agito senza la normale prudenza. La liquidazione dei danni è fatta a norma del comma precedente.
In ogni caso, quando pronuncia sulle spese ai sensi dell'articolo 91, il giudice, anche d'ufficio, può altresì condannare la parte soccombente al pagamento, a favore della controparte, di una somma equitativamente determinata.
[279] Tribunale Ordinario di Firenze, Sez. Imprese, ordinanza 14 marzo 2025.

4. I principi per una pubblica amministrazione automatizzata

L'implementazione di strumenti tecnologici nella vita della pubblica amministrazione, come anticipato, è regolamentata per principi che, da un lato, mirano a garantire il rispetto dei diritti del cittadino destinatario di un provvedimento e, dall'altro, perseguono l'efficienza, la trasparenza e la responsabilità nell'operato delle istituzioni pubbliche.

Tra tali principi assumono assoluta importanza il principio di trasparenza e conoscibilità, il principio di non esclusività della decisione algoritmica ed il principio di non discriminazione algoritmica.

4.1. Il principio di trasparenza: conoscibilità e comprensibilità

La trasparenza dell'azione amministrativa rappresenta non solo uno dei principi fondamentali dell'agire pubblico, ma "*un modo di essere dell'amministrazione*".[280] Infatti, "*l'amministrazione al servizio della comunità*"[281] – contrapposta all'amministrazione come apparato dello Stato – deve essere trasparente nei confronti dei cittadini quali destinatari delle decisioni.[282] In altre parole, l'amministrazione deve essere, come da datata ma ancora attuale ed insuperata definizione, una "*casa di vetro*".[283] Appare evidente come tale tensione verso un'amministrazione trasparente, accessibile e comprensibile sia minacciata, nell'ambito dell'automazione del potere decisionale pubblico, dall'opacità degli strumenti tecnologici ed automatizzati adottati dalla pubblica amministrazione.

Nel contesto delle decisioni automatizzate, la trasparenza si declina in due dimensioni essenziali: conoscibilità e comprensibilità.[284] La prima attribuisce al cittadino il diritto fondamentale di essere pienamente informato circa l'eventuale utilizzo di processi decisionali automatizzati, nonché il diritto di accedere alle

[280] G. Arena, '*Il punto sulla trasparenza amministrativa'*, in *Forum PA, Pubblica amministrazione aperta? Diritto di accesso e trasparenza dal 1990 ad oggi*, Roma 11 maggio 2009.
[281] *Ibid.*
[282] *Ibid.*
[283] F. Turati, in '*Atti del Parlamento italiano*', Camera dei deputati, sessione 1904-1908, 17 giugno 1908, 22962.
[284] G. Orsoni, E. D'Orlando, *'Nuove prospettive dell'amministrazione digitale: Open data e algoritmi*', in *Istituzioni del federalismo*, 2019, fasc. 3, p. 608.

informazioni relative al funzionamento dell'algoritmo, incluse le istruzioni, i criteri utilizzati per l'elaborazione delle decisioni e, ove necessario, persino l'accesso al linguaggio informatico in cui l'algoritmo è scritto, ossia al cosiddetto codice sorgente.[285] È, infatti, il Consiglio di Stato a riconoscere che "*il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico. Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato*".[286]

Tuttavia, vista la natura altamente tecnica del linguaggio informatico, il solo accesso all'algoritmo non è sufficiente a soddisfare il principio di trasparenza, se non è, altresì, garantita la possibilità effettiva di comprenderne la logica sottostante.[287] Infatti, come statuito ancora dal Consiglio di Stato, il diritto alla conoscenza deve essere accompagnato da meccanismi che permettano di decifrare la logica della decisione amministrativa.[288] "*In tale ottica, il principio di conoscibilità si completa con il principio di comprensibilità, ovverosia la possibilità,* […]*, di ricevere «informazioni significative sulla logica utilizzata»*."[289]

---

[285] E. Carloni, '*Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*', in Diritto pubblico, 2019, fasc. 2, p. 289.
[286] Consiglio di Stato, Sez. VI, 8 aprile 2019, n. 2270.
[287] F. Nassuato, '*Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*', in Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche (CERIDAP), 2022, fasc. speciale 1, p. 157.
[288] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881: "*Tale diritto alla conoscenza dell'esistenza di decisioni che ci riguardino prese da algoritmi e, correlativamente, come dovere da parte di chi tratta i dati in maniera automatizzata, di porre l'interessato a conoscenza, va accompagnato da meccanismi in grado di decifrarne la logica.*"
[289] *Ibid.*

Insomma, la comprensibilità comporta la traduzione del linguaggio tecnico-informatico in regole giuridiche intelligibili.[290]

Risulta, quindi, evidente come il principio di trasparenza sia intrinsecamente connesso all'obbligo di motivazione del provvedimento amministrativo previsto dall'articolo 3 della legge n. 241/1990.[291] Infatti, come disposto dai Giudici di Palazzo Spada, la fondamentale esigenza di tutela posta dall'utilizzo di strumenti informatici algoritmici è "*la trasparenza nei termini prima evidenziati riconducibili al principio di motivazione e/o giustificazione della decisione*".[292] La dottrina, coerentemente con l'orientamento giurisprudenziale, ritiene inammissibile una motivazione che si limiti a menzionare le componenti tecniche del *software* utilizzato. Una corretta attuazione dei principi di conoscibilità e comprensibilità richiede infatti una spiegazione esaustiva, sia sotto il profilo fattuale che giuridico, della decisione generata dall'algoritmo.[293]

Come evidenziato dalla stessa giurisprudenza[294], il principio di trasparenza nella sua dimensione "evolutiva"[295] appena esaminata, trova fondamento normativo comunitario nel Regolamento generale sulla protezione dei dati. Più precisamente, è l'articolo 12 che impone al titolare del trattamento l'obbligo di fornire all'interessato tutte le informazioni relative ai trattamenti "*in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e*

---

[290] Consiglio di Stato, Sez. VI, 8 aprile 2019, n. 2270: "[…] *la "formula tecnica", che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella «regola giuridica» ad essa sottesa e che la rendano leggibile e comprensibile, sia per i cittadini che per il giudice.*"

[291] Legge n. 241/1990, art. 3: *1. Ogni provvedimento amministrativo, compresi quelli concernenti l'organizzazione amministrativa, lo svolgimento dei pubblici concorsi ed il personale, deve essere motivato, salvo che nelle ipotesi previste dal comma 2. La motivazione deve indicare i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione dell'amministrazione, in relazione alle risultanze dell'istruttoria. 2. La motivazione non è richiesta per gli atti normativi e per quelli a contenuto generale. 3. Se le ragioni della decisione risultano da altro atto dell'amministrazione richiamato dalla decisione stessa, insieme alla comunicazione di quest'ultima deve essere indicato e reso disponibile, a norma della presente legge, anche l'atto cui essa si richiama. 4. In ogni atto notificato al destinatario devono essere indicati il termine e l'autorità cui è possibile ricorrere.*

[292] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881; in termini, Consiglio di Stato, Sez. VI, 8 aprile 2019, n. 2270; Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472.

[293] G. Avanzini, '*Decisioni amministrative e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intelligibilità*', *cit.*, pp. 150-151; A. Di Martino, '*L'amministrazione per algoritmi ed i pericoli del cambiamento in atto*', in *Il diritto dell'economia*, 2020, fasc. 3, pp. 624-625.

[294] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.

[295] G. Orsoni, E. D'Orlando, '*Nuove prospettive dell'amministrazione digitale: Open data e algoritmi*', *cit.*

chiaro".[296] Si tratta, quindi, di un obbligo di trasparenza sostanziale, orientato alla effettiva comprensione da parte del cittadino destinatario del trattamento. Tale obbligo si declina negli articoli 13[297] e 14[298], che disciplinano il contenuto delle informazioni da fornire all'interessato, a seconda che i dati siano raccolti direttamente presso di lui o presso terzi. Entrambe le disposizioni, però, prevedono che l'informativa rivolta all'interessato contenga l'indicazione dell'eventuale impiego di un processo decisionale automatizzato e, in tal caso, che il titolare fornisca "*informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste di tale trattamento per l'interessato*".[299] Inoltre, l'articolo 15, paragrafo 1, lettera h)[300], riconosce all'interessato il diritto di ottenere, su richiesta, l'accesso alle stesse informazioni, assicurando un controllo effettivo "*anche qualora il trattamento abbia avuto inizio, stia trovando esecuzione o abbia addirittura già prodotto una decisione*".[301]

Con l'adozione dell'AI Act, il principio di trasparenza trova un'ulteriore base normativa europea. Infatti, richiamando le linee guida etiche del Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, il regolamento stabilisce che per 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*".[302]

---

[296] Regolamento (UE) 2016/679, art. 12 – *Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato.*
[297] Regolamento (UE) 2016/679, art. 13 – *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato.*
[298] Regolamento (UE) 2016/679, art. 14 – *Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.*
[299] Regolamento (UE) 2016/679, artt. 13 e 14.
[300] Regolamento (UE) 2016/679, art. 15(1): *L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni*: […]; h) *l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*
[301] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.
[302] Regolamento (UE) 2024/1689, cons. (27).

Sono, poi, gli articoli 13[303] e 50[304] del Regolamento ad imporre obblighi positivi di comunicazione e trasparenza, volti a garantire che i sistemi di IA siano comprensibili e utilizzabili consapevolmente dagli operatori e dalle persone coinvolte.

In particolare, l'articolo 13 stabilisce che i sistemi di IA ad alto rischio siano progettati e sviluppati in modo da garantire un adeguato livello di trasparenza, consentendo agli utilizzatori di comprendere il funzionamento del sistema e di utilizzarlo correttamente. I fornitori sono, infatti, tenuti a redigere istruzioni d'uso chiare e complete, che comprendano, tra le altre cose, le modalità di interpretazione degli *output*, nonché i requisiti per il monitoraggio del sistema.[305]

L'articolo 50 introduce, invece, obblighi di trasparenza nei confronti delle persone fisiche che interagiscono con un sistema di intelligenza artificiale. In base a tale disposizione, gli utenti devono essere informati "*in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione"*[306] quando interagiscono con un sistema di IA, a meno che ciò non sia evidente dalle circostanze. L'obbligo informativo è rafforzato nel caso di utilizzo di tecnologie generative (come i *deepfake*), di riconoscimento delle emozioni, o di categorizzazione biometrica, per le quali è richiesta un'esplicita indicazione del carattere artificiale del contenuto o dell'interazione.[307]

---

[303] Regolamento (UE) 2024/1689, art. 13 – *Trasparenza e fornitura di informazioni ai deployer.*

[304] Regolamento (UE) 2024/1689, art. 50 – *Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA.*

[305] Regolamento (UE) 2024/1689, art. 13: *1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del deployer di cui alla sezione 3. 2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso, in un formato appropriato digitale o non digitale, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i deployer.*

[306] Regolamento (UE) 2024/1689, art. 50(5).

[307] Regolamento (UE) 2024/1689, art. 50: 1. *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 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.* […] *4. I deployer di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un «deep fake» rendono noto che il contenuto è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati. Qualora il contenuto*

Infine, come anticipato, i principi di conoscibilità e comprensibilità, quali corollari del principio di trasparenza, trovano fondamento normativo nell'articolo 30 del nuovo codice dei contratti pubblici.[308]

4.1.1. L'opacità degli algoritmi

Due importanti ostacoli alla concreta attuazione del principio di trasparenza sono rappresentati dalla cosiddetta *black box* e dalla tutela dei diritti di proprietà intellettuale sui *software* forniti da soggetti privati alla pubblica amministrazione.

4.1.1.1. Il problema della *black box*

Il concetto di *black box*, come anticipato,[309] descrive un elevato grado di opacità che caratterizza taluni sistemi di intelligenza artificiale (*machine learning* e *deep learning*), al punto da rendere indecifrabili — persino per gli stessi programmatori e sviluppatori — i meccanismi interni di funzionamento e il processo attraverso cui gli *input* vengono elaborati per giungere ad un determinato *output*.[310] Rientra, dunque, nella nozione di *black box* ogni circostanza nella quale risulti impossibile ricostruire l'*iter* logico seguito dall'algoritmo per raggiungere l'obiettivo assegnato.[311]

Da un punto di vista giuridico, la carenza di trasparenza di tali strumenti compromette il diritto alla difesa, poiché in assenza di una chiara spiegazione della decisione algoritmica risulta impossibile contestarne la correttezza o la legittimità, rendendola di fatto insindacabile.[312] Altresì, l'opacità sembrerebbe indicare

---

faccia parte di un'analoga opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera.

[308] D.lgs. n. 36/2023, art. 30(3)(a).

[309] Si veda *supra* Capitolo 1, paragrafo 1.3.2.

[310] G. Lo Sapio, '*La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*', in *federalismi.it*, 2021, fasc. 16, p. 117.

[311] A. Rouvroy, '*Of data and men. Fundamental rights and freedoms in a world of big data*', Council of Europe, Directorate general of Human Rights and Rule of Law, T-PD-BUR(2015)09REV, Strasburgo, 11 gennaio 2016, p. 12.

[312] A. Lirosi, '*L'intelligenza artificiale nel diritto amministrativo – tra riserva di umanità e necessità di garantire una maggiore efficienza amministrativa*', in *Quaderni della Rivista della Corte dei Conti*, n. 2/2024, pp. 128-129.

l'incompatibilità strutturale di questi sistemi con il principio di trasparenza e di motivazione che deve informare l'attività amministrativa.[313]

In questo contesto, la *Explainable Artificial Intelligence* (XAI) si pone come una possibile ed essenziale soluzione per superare l'inaccessibilità logica dei modelli di *machine learning* e *deep learning*, offrendo metodi capaci di rendere comprensibili i meccanismi decisionali delle macchine. La XAI agisce su due fronti: da un lato, fornisce spiegazioni locali o globali delle decisioni, rendendo comprensibili le ragioni per cui un determinato *output* è stato prodotto; dall'altro, interviene in modo strutturale sul processo di addestramento dei modelli, al fine di migliorarne la trasparenza, la robustezza e la capacità di ragionamento.[314] In tal modo, la XAI non si limita ad "*aprire la black box"*[315], ma ne ricostruisce le connessioni interne e, in certi casi, ne permette la correzione mirata.

Un esempio di applicazione avanzata dei principi della XAI è offerto dal recente lavoro del laboratorio di ricerca *Anthropic*. I ricercatori sono riusciti a identificare, all'interno di un modello linguistico, gruppi di neuroni associati a concetti specifici. Attraverso la stimolazione o l'inibizione di questi neuroni, è stato possibile influenzare direttamente il comportamento del modello, inducendolo a evitare la generazione di *output* potenzialmente pericolosi. Questo approccio dimostra come l'interpretabilità possa diventare un mezzo operativo per esercitare un controllo effettivo sui sistemi algoritmici, contribuendo a ridurre – se non eliminare – l'opacità tipica di sistemi avanzati.[316]

4.1.1.2. I diritti di proprietà intellettuale sul *software*

Un ulteriore ostacolo all'attuazione del principio di trasparenza è rappresentato dal conflitto tra la tutela della proprietà intellettuale sul *software* e il diritto di accesso al codice sorgente.

---

[313] G. Lo Sapio, '*La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*', *cit.*, p. 117.
[314] L. Weber, S. Lapuschkin, A. Binder, W. Samek, '*Beyond explaining: Opportunities and challenges of XAI-based model improvement',* in *Information Fusion*, n. 92/2023, pp. 154-176.
[315] *Ibid,* p. 154.
[316] B. Perrigo, '*No One Truly Knows How AI Systems Work. A New Discovery Could Change That*', *Time*, 21 Maggio, 2024, https://time.com/6980210/anthropic-interpretability-ai-safety-research/

La pubblica amministrazione, spesso priva delle competenze tecniche ed economiche necessarie per sviluppare in autonomia i propri strumenti informatici, si rivolge al mercato per acquisire *software.*[317] Tali *software* – comprensivi del codice sorgente – sono protetti dal diritto d'autore ai sensi della legge n. 633/1941[318] e della direttiva 2009/24/CE.[319] In forza di tale normativa, il creatore del programma informatico ha diritto sia allo sfruttamento economico dell'opera sia ai diritti morali.[320] Tuttavia, quando l'amministrazione utilizza un programma all'interno di un procedimento che incide su posizioni giuridiche soggettive, la riservatezza tecnica del *software* può ostacolare la comprensibilità e la sindacabilità della decisione, in contrasto con il fondamentale principio di trasparenza.

La giurisprudenza amministrativa ha affrontato direttamente questa problematica. Il TAR Lazio ha affermato che il codice sorgente dell'algoritmo utilizzato dal Ministero dell'Istruzione per la gestione della mobilità del personale docente costituisce un atto amministrativo informatico accessibile.[321] Successivamente, il Consiglio di Stato ha ribadito che la tutela della proprietà intellettuale non può prevalere in modo assoluto sul diritto alla trasparenza, precisando che l'utilizzo di un algoritmo da parte della pubblica amministrazione comporta l'accettazione delle "*relative conseguenze in termini di necessaria trasparenza*".[322] In questo quadro, quindi, il diritto di accesso al codice sorgente viene riconosciuto come esercitabile ogniqualvolta sia funzionale alla tutela di un interesse giuridicamente rilevante, specialmente in chiave difensiva.

Tale impostazione giurisprudenziale, sebbene innovativa, non risolve il problema in via sistemica. Infatti, manca una esplicita considerazione del principio di proporzionalità, necessario per valutare caso per caso se l'accesso al codice

[317] M. Farina, '*Intellectual property rights in the era of Italian "artificial" public decisions: time to collapse?*', in *Rivista italiana di informatica e diritto,* 2023, fasc. 1, p. 128.
[318] Legge 22 aprile 1941, n. 633, 'Protezione del diritto d'autore e di altri diritti connessi al suo esercizio'.
[319] Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore.
[320] M. Farina, '*Intellectual property rights in the era of Italian "artificial" public decisions: time to collapse?*', *cit.*, p. 131.
[321] TAR Lazio, Sez. III-bis, 22 marzo 2017, n. 3769.
[322] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.

sorgente sia davvero indispensabile o se sia possibile ricorrere a forme alternative di spiegazione, meno invasive per i diritti del titolare.[323]

Una soluzione strutturale richiede un intervento *ex ante*, che abbia luogo nella fase di acquisizione del *software*. Il Codice dell'amministrazione digitale stabilisce, all'articolo 68, l'obbligo per le amministrazioni di effettuare una valutazione comparativa tra le soluzioni *software* disponibili sul mercato – includendo *software* libero, riutilizzabile e proprietario – e di privilegiare, laddove possibile, le soluzioni aperte e riusabili.[324] L'articolo 69, comma 2, specifica che la pubblica amministrazione debba acquisire, ove possibile, la titolarità dei programmi informatici sviluppati per suo conto, salvo che tale scelta risulti eccessivamente onerosa per comprovate ragioni tecnico-economiche.[325] Inoltre, ai sensi del comma 1 del medesimo articolo, qualora venga acquisita la titolarità, la pubblica amministrazione è tenuta a rendere disponibile gratuitamente il codice sorgente al

[323] M. Farina, '*Intellectual property rights in the era of Italian "artificial" public decisions: time to collapse?*', *cit.*, p. 132.

[324] D.lgs. n. 82/2005, art. 68: *1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato: a) software sviluppato per conto della pubblica amministrazione; b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione; c) software libero o a codice sorgente aperto; d) software fruibile in modalità cloud computing; e) software di tipo proprietario mediante ricorso a licenza d'uso; f) software combinazione delle precedenti soluzioni. 1-bis. A tal fine, le pubbliche amministrazioni prima di procedere all'acquisto, secondo le procedure di cui al codice di cui al decreto legislativo n. 50 del 2016, effettuano una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri: a) costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto; b) livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione; c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito. 1-ter. Ove dalla valutazione comparativa di tipo tecnico ed economico, secondo i criteri di cui al comma 1-bis, risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a software liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso. La valutazione di cui al presente comma è effettuata secondo le modalità e i criteri definiti dall'AgID.*

[325] D.lgs. n. 82/2005, art. 69(2): *Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto, salvo che ciò risulti eccessivamente oneroso per comprovate ragioni di carattere tecnico-economico, che l'amministrazione committente sia sempre titolare di tutti i diritti sui programmi e i servizi delle tecnologie dell'informazione e della comunicazione, appositamente sviluppati per essa.*

fine di favorire il riuso del *software* da parte di altre amministrazioni o soggetti giuridici che intendano adattarlo alle proprie esigenze.[326]

Tuttavia, il quadro normativo consente anche il ricorso a soluzioni proprietarie, come licenze d'uso o modalità *cloud*, qualora risultino più convenienti o funzionali. In tali ipotesi, la proprietà del *software* rimane in capo al fornitore, che conserva i diritti esclusivi sul codice sorgente e può legittimamente negarne l'accesso a terzi per tutelare i propri segreti commerciali.[327] La pubblica amministrazione, invece, acquisisce soltanto un diritto d'uso, i cui limiti sono definiti nel bando di gara e, successivamente, nel contratto.[328] Questi ultimi, come affermato dal Consiglio di Stato, costituiscono il parametro normativo vincolante nei rapporti tra amministrazione, operatore economico e terzi eventualmente coinvolti.[329]

Dunque, quando la *lex specialis* e il successivo contratto prevedono che i diritti di proprietà intellettuale restino in capo al fornitore, quest'ultimo mantiene anche il diritto esclusivo alla riservatezza del codice sorgente, con la conseguenza che la pubblica amministrazione non potrà accedervi, nemmeno per finalità di controllo, se non nei limiti previsti contrattualmente.[330] Ciò comporta che, in assenza di clausole specifiche che disciplinino la disponibilità del codice o della documentazione tecnica, ogni successiva richiesta di accesso rischia di risultare inefficace o potenzialmente in conflitto con il regime di protezione del *software*.[331]

La pubblica amministrazione, quindi, dovrebbe superare un approccio meramente passivo all'acquisizione tecnologica, ed assumere un ruolo attivo nella

---

[326] D.lgs. n. 82/2005, art. 69(1): *Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali.*

[327] F. Bravo, '*Access to Source Code of Proprietary Software Used By Public Administrations for Automated Decision-making. What Proprortional balancing of Interests?*', in *European review of digital administration & law – Erdal*, 2020, vol. 1, p. 159.

[328] *Ibid.*

[329] Consiglio di Stato, Sez. V, 5 marzo 2020, n. 1604: "[…] *consolidato principio per cui le prescrizioni stabilite nella lex specialis vincolano non solo i concorrenti, ma anche la stessa amministrazione, che non conserva margini di discrezionalità nella loro concreta attuazione, né può disapplicarle, neppure quando alcune di queste regole risultino inopportune o incongrue o comunque superate, fatta salva naturalmente la possibilità di procedere all'annullamento del bando nell'esercizio del potere di autotutela.*"

[330] F. Bravo, '*Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional balancing of Interests?*', *cit.*, p. 159.

[331] *Ibid.*

definizione delle condizioni contrattuali che regolano l'utilizzo dei *software*, assicurando fin dalla fase di gara l'allineamento con i principi di trasparenza, conoscibilità e comprensibilità.[332]

4.2. Il principio di non esclusività della decisione algoritmica

Il principio di non esclusività della decisione algoritmica, oggi esplicitamente previsto dall'articolo 30 del nuovo codice dei contratti pubblici,[333] è oggetto di analisi e studio dottrinale e giurisprudenziale sin dal 2016, con l'entrata in vigore del GDPR. È, infatti, dall'articolo 22 del Regolamento che muove la nostra analisi. Quest'ultimo riconosce il diritto dell'interessato "*di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*".[334] Appare opportuno, in primo luogo, definire il concetto di profilazione come qualsiasi forma di trattamento automatizzato di dati personali finalizzata a valutare aspetti personali relativi a una persona fisica.[335] Tale definizione include tre elementi essenziali: l'uso di dati personali, la loro elaborazione automatizzata e la finalità valutativa nei confronti della persona fisica.

È importante precisare che il processo decisionale automatizzato non coincide necessariamente con la profilazione: può esservi una decisione automatica senza profilazione o, viceversa, una profilazione non seguita da una decisione.[336] Tuttavia, quando la decisione è fondata esclusivamente sul trattamento

---

[332] *Ibid,* p. 159-160; M. Farina, '*Intellectual property rights in the era of Italian "artificial" public decisions: time to collapse?*', *cit.*, p. 132.
[333] D.lgs. n. 36/2023, art. 30(3)(b).
[334] Regolamento (UE) 2016/679, art. 22(1): *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*.
[335] Regolamento (UE) 2016/679, art. 4(4): *«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.*
[336] A. Caia, '*GDPR e normativa privacy: commentario*', G.M. Riccio, G. Scorza, B. Ernesto (a cura di), Wolters Kluwer, II edizione, Assago, 2022, p. 280.

automatizzato, ed è priva di intervento umano significativo, entra in gioco il divieto previsto dall'articolo 22, paragrafo 1.[337]

L'applicazione della norma dipende dalla cumulativa esistenza di tre condizioni.[338]

In primo luogo, deve sussistere una decisione, intesa come atto che definisce o incide significativamente sulla situazione giuridica o personale dell'interessato, di natura privata o pubblica[339].

In secondo luogo, tale decisione deve essere basata unicamente su un trattamento automatizzato, cioè adottata senza alcun intervento umano significativo nel processo decisionale.[340] Quindi, il divieto sicuramente riguarda decisioni assunte autonomamente da un sistema di IA, mentre dubbi possono sorgere in relazione a decisioni che, a causa di un minimo coinvolgimento finale dell'uomo, non possono formalmente rientrare nella categoria di decisioni "basate unicamente sul trattamento automatizzato".[341] Tuttavia, la dottrina maggioritaria è concorde nel ritenere insufficiente un intervento umano simbolico e acritico per escludere l'applicabilità della disposizione in esame, richiedendo, invece, un intervento sostanziale ed effettivo, successivo alla raccomandazione algoritmica.[342] Infatti, l'avverbio "*unicamente*" copre solamente i processi decisionali automatizzati nei quali l'essere umano non esercita un'influenza reale sull'esito della decisione.[343]

Infine, la terza condizione richiede che la decisione produca effetti giuridici, oppure effetti analoghi a quelli giuridici, che abbiano un impatto significativo sull'individuo, ovvero che, anche senza incidere direttamente sull'esercitabilità di un diritto umano o sullo *status* giuridico, colpiscano comunque interessi rilevanti

---

[337] *Ibid.*
[338] *Ibid*, p. 282.
[339] *Ibid.*
[340] *Ibid,* p. 280.
[341] Ad esempio, si consideri il caso in cui venga respinta una richiesta di finanziamento da parte di un operatore che si sia semplicemente limitato ad attuare la profilazione effettuata dall'IA, senza comprenderne il funzionamento né avere la possibilità di modificarne l'esito. Cfr. B. Parenzo, '*La profilazione algoritmica nel prisma dell'autonomia privata*', Edizioni Scientifiche Italiane, 2024, p. 109.
[342] *Ibid,* p. 110.
[343] UK Information Commissioner's Office, '*Feedback request – profiling and automated decision-making*', 6 aprile 2017, p. 19: *We think it is intended to cover those automated decision-making processes where a human exercises no real influence on the outcome of the decision.*

della persona, come le sue opportunità professionali, condizioni economiche, libertà di scelta o possibilità di accesso a beni e servizi.[344]

L'articolo 22, paragrafo 2, prevede tre eccezioni al divieto: quando la decisione è necessaria per l'esecuzione di un contratto, quando è autorizzata da una previsione normativa dell'Unione o di uno Stato membro, e quando si basa sul consenso esplicito dell'interessato.[345] Tuttavia, l'applicazione delle deroghe è subordinata all'adozione, da parte del titolare del trattamento, di misure appropriate a tutela dei diritti, delle libertà e degli interessi dell'interessato, le quali, nel caso della deroga prevista dalla lettera b), devono essere espressamente indicate nella norma nazionale o dell'Unione che autorizza il trattamento,[346] mentre, nelle ipotesi di deroga fondate su contratto o consenso, devono quantomeno garantire il diritto all'intervento umano, alla possibilità di esprimere la propria opinione e di contestare la decisione.[347]

Infine, per ragioni di completezza, l'articolo 22, paragrafo 4, stabilisce che, qualora la decisione automatizzata riguardi categorie particolari di dati *ex* articolo 9,[348] essa è lecita solo se fondata sul consenso esplicito o su rilevanti motivi di interesse pubblico, a condizione che siano garantite misure adeguate a tutela dei diritti dell'interessato.[349]

Appare opportuno, altresì, soffermarsi sull'articolo 14 dell'AI Act, il quale – pur operando in un diverso contesto normativo – affronta il tema complementare della

---

[344] Article 29 Data Protection Working Party, '*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*', 6 febbraio 2018, p. 21.
[345] Regolamento (UE) 2016/679, art. 22(2): *Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato.*
[346] A. Caia, '*GDPR e normativa privacy: commentario', cit.*, p. 283.
[347] Regolamento (UE) 2016/679, art. 22(3): *Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*
[348] Regolamento (UE) 2016/679, art. 9(1): *È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*
[349] Regolamento (UE) 2016/679, art. 22(4): *Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.*

supervisione umana nei sistemi di intelligenza artificiale ad alto rischio.[350] Infatti, il primo comma impone un obbligo specifico di progettazione e funzionamento che garantisca, durante l'intero ciclo di vita del sistema, la possibilità di intervento umano.[351] La funzione assegnata alla supervisione umana è quella di prevenire o quantomeno ridurre i rischi per la salute, la sicurezza e i diritti e le libertà fondamentali che possono derivare sia da un uso conforme, sia da un utilizzo improprio ma ragionevolmente prevedibile del sistema.[352]

Affinché possa considerarsi conforme, la supervisione umana deve soddisfare alcuni requisiti specifici: l'operatore umano deve essere posto nella condizione di comprendere le capacità e i limiti del sistema, di essere consapevole del rischio di eccessiva fiducia nell'*output* algoritmico, di interpretare in modo corretto i risultati generati, di interrompere o disattivare il funzionamento del sistema in condizioni di sicurezza, nonché di ignorare, modificare o annullare i risultati ottenuti ove ciò si renda necessario.[353]

La disposizione in esame, dunque, incarna un doppio approccio antropocentrico: da un lato, la tecnologia deve essere concepita al servizio dell'essere umano

[350] Regolamento (UE) 2024/1689, art. 14 – *Sorveglianza umana.*
[351] Regolamento (UE) 2024/1689, art. 14(1): *I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.*
[352] Regolamento (UE) 2024/1689, art. 14(2): *La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione.*
[353] Regolamento (UE) 2024/1689, art. 14(4): *Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al deployer in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili; d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.*

(*human-centric technology*); dall'altro, anche la regolazione stessa deve essere orientata a tutela dell'uomo (*human-centric legislation*).[354]

La norma è, altresì, strettamente connessa ai modelli concettuali elaborati dal Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale.[355]. Tali modelli sono: *human-in-the-loop, human-on-the-loop* e *human-in-command.*[356] Il primo riconosce la possibilità di intervento attivo della persona in ogni fase del processo decisionale automatizzato.[357] Il secondo prevede una forma di supervisione umana durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento dello stesso.[358] Il terzo modello, invece, attribuisce all'operatore umano una funzione strategica e sistemica: l'essere umano mantiene la responsabilità generale sull'attivazione, la configurazione, la disattivazione e il monitoraggio del sistema.[359]

4.2.1. L'interpretazione giurisprudenziale

Il Consiglio di Stato, nell'esaminare la portata applicativa del principio in esame, ha affermato che "*deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica*".[360] In altre parole, anche nei procedimenti caratterizzati dall'impiego di sistemi automatizzati, deve essere garantita la presenza di un intervento umano significativo. Tale principio comporta, in linea generale, l'inammissibilità di processi decisionali interamente automatizzati, in quanto solo la partecipazione attiva di un soggetto umano consente di assicurare la piena imputabilità della decisione all'autorità competente, individuata in conformità al principio di legalità, e di garantire l'identificazione di un soggetto responsabile dell'esercizio del potere

[354] A. Panezi, '*The EU Artificial Intelligence (AI) Act: A Commentary*', N. Forgo, C. Necati Pehlivan, P. Valcke (a cura di), Kluwer Law International, 2024, pp. 358-359.
[355] *Ibid*, p. 363.
[356] Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, '*Orientamenti etici per un'IA affidabile*', Bruxelles, aprile 2019.
[357] *Ibid.*
[358] *Ibid.*
[359] *Ibid.*
[360] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.

amministrativo.[361] In quest'ottica, l'automazione decisionale non può mai tradursi in una deresponsabilizzazione dell'amministrazione, la quale rimane titolare e responsabile dell'adozione dell'atto, pur laddove il procedimento sia assistito da strumenti algoritmici.[362] Dunque, utilizzando il linguaggio matematico, "*il modello viene definito come HITL (human in the loop), in cui, per produrre il suo risultato è necessario che la macchina interagisca con l'essere umano*".[363]

Al contempo, nei tribunali amministrativi regionali, si è consolidato un orientamento particolarmente restrittivo, secondo cui, ai sensi degli articoli 3[364], 24[365] e 97[366] della Costituzione e dell'articolo 6 della Convenzione europea dei diritti dell'uomo[367], le procedure informatiche non possono mai sostituire in modo pieno l'attività istruttoria, valutativa e decisionale dell'amministrazione, la quale, per garantire i principi di partecipazione, contraddittorio e tutela degli interessi legittimi, deve restare il soggetto dominante del procedimento.[368] Questa impostazione conduce a ritenere incostituzionale, prima che illegittima, qualsiasi decisione amministrativa assunta in modo esclusivamente automatizzato, con la

---

[361] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881: "*Ciò a garanzia dell'imputabilità della scelta al titolare del potere autoritativo, individuato in base al principio di legalità, nonché della verifica circa la conseguente individuazione del soggetto responsabile, sia nell'interesse della stessa p.a. che dei soggetti coinvolti ed incisi dall'azione amministrativa affidata all'algoritmo.*"

[362] F. Nassuato, '*Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*', *cit.*, p. 159.

[363] Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.

[364] Costituzione, art. 3: *Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese.*

[365] Costituzione, art. 24: *Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi. La difesa è diritto inviolabile in ogni stato e grado del procedimento.*

[366] Costituzione, art. 97: *Le pubbliche amministrazioni, in coerenza con l'ordinamento dell'Unione europea, assicurano l'equilibrio dei bilanci e la sostenibilità del debito pubblico. I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione.*

[367] Convenzione europea dei diritti dell'uomo, art. 6: *Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli 10 11 interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia.*

[368] TAR Lazio, Sez. III-bis, 10 settembre 2018, n. 9224.

conseguenza che un'eventuale violazione non può essere sanata, né dal consenso dell'interessato, né dalla presenza di una clausola contrattuale, né da una specifica previsione legislativa.[369]

Tale orientamento, ha suscitato alcune perplessità in dottrina[370] e non è stato pienamente recepito dal Consiglio di Stato, il quale, come visto, si è limitato ad escludere la legittimità di procedimenti interamente ed esclusivamente automatizzati, senza però precisare quale debba essere il grado di incidenza del contributo umano rispetto al processo algoritmico.[371] Ne consegue che l'intervento umano, purché effettivo, può anche limitarsi a una fase successiva di validazione e controllo dell'*output* algoritmico.[372]

Resta, tuttavia, il rischio che tale forma di controllo si traduca in una mera ratifica acritica degli esiti generati dal sistema, in virtù dell'elevata forza persuasiva attribuita alle valutazioni tecniche dell'algoritmo.[373] Questo fenomeno, definito *automation bias,* si sostanzia nella tendenza psicologica dell'essere umano a ritenere più affidabili le decisioni della macchina rispetto al proprio giudizio, anche in presenza di elementi di incertezza o errore.[374] Ciò può condurre l'operatore a non intervenire, a non contestare o a non annullare decisioni che invece richiederebbero un controllo umano attivo, riducendo l'efficacia delle garanzie previste dalla giurisprudenza amministrativa e della regolamentazione comunitaria.[375] Si è osservato, infatti, che l'introduzione di strumenti decisionali automatizzati in un processo gestito da esseri umani tende progressivamente a orientare e assorbire le scelte dell'amministrazione, tanto per motivi di efficienza pratica quanto per la

[369] A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', in R. Cavallo Perin, D.U. Galetta (a cura di), Il diritto dell'Amministrazione Pubblica digitale, Giappichelli 2025, par. 4.2.
[370] *Ibid,* par. 3.2.
[371] F. Nassuato, '*Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*', *cit.*, p. 160.
[372] *Ibid*, p. 161.
[373] *Ibid.*
[374] Regolamento (UE) 2024/1689, art. 14(4)(b): *Restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche*.
[375] A. Panezi, '*The EU Artificial Intelligence (AI) Act: A Commentary*', *cit*, pp. 366-367.

difficoltà, da parte degli interessati, di dimostrare in giudizio la violazione del principio di non esclusività.[376]

4.3. Il principio di non discriminazione algoritmica

Il principio di non discriminazione algoritmica discende dall'esigenza di assicurare che l'impiego di sistemi di intelligenza artificiale non determini trattamenti differenziati ingiustificati o illegittimi nei confronti degli interessati. Infatti, come affermato dai Giudici di Palazzo Spada, "*è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e 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 tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti.*"[377]

Si tratta di un principio che trova la sua fonte principale, come riconosciuto dalla stessa giurisprudenza amministrativa,[378] nel considerando 71 del GDPR. Quest'ultimo, applicabile ad ogni forma di procedimento predittivo nonostante l'esplicito riferimento alla sola profilazione,[379] impone al titolare del trattamento l'obbligo di adottare misure organizzative adeguate e, se necessario, di rettificare i dati utilizzati nel procedimento, al fine di prevenire effetti discriminatori tra persone

[376] F. Nassuato, '*Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali*', *cit.*, p. 161.
[377] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.
[378] *Ibid*: […] *dal considerando n. 71 del Regolamento 679/2016 il diritto europeo trae un ulteriore principio fondamentale, di non discriminazione algoritmica.*
[379] A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', cit., par. 4.2; A. Simoncini, '*L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*', in *BioLaw Journal – Rivista di BioDiritto*, 2019, fasc. 1, p. 84.

fisiche per ragioni inerenti a razza, origine etnica, opinioni politiche, credo religioso, appartenenza sindacale o altri tratti personali sensibili.[380]

Da tale formulazione si ricavano due corollari fondamentali del principio di non discriminazione: i principi di *privacy by design* e di *data quality by default*, che orientano tanto la fase di predisposizione quanto quella di gestione delle basi di dati pubbliche e dei sistemi decisionali automatizzati.[381]

Il primo, la responsabilità organizzativa e preventiva inerente alla fase di progettazione del trattamento automatizzato, richiede che l'amministrazione configuri i sistemi algoritmici in modo tale da garantire un utilizzo proporzionato e ragionevole degli strumenti tecnologici, assicurando che l'applicazione non determini effetti discriminatori sugli interessati.[382] Le regole algoritmiche utilizzate nell'ambito dei procedimenti amministrativi devono conformarsi non solo ai principi generali di imparzialità e non discriminazione, ma anche a quelli di ragionevolezza e proporzionalità,[383] che trovano espressione anche nel meccanismo di valutazione d'impatto sulla protezione dei dati personali (*Data Protection Impact Assessment*), disciplinato dall'articolo 35 del GDPR.[384] Tale valutazione deve essere obbligatoriamente svolta ogniqualvolta un trattamento di dati personali, specie se basato su nuove tecnologie, comporti un rischio elevato per i diritti e le libertà fondamentali delle persone fisiche.[385] Dunque, i trattamenti decisionali

---

[380] Regolamento (UE) 2016/679, cons. (71): *Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e 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 tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.*

[381] E. Carloni, '*I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*', in *Diritto amministrativo*, 2020, fasc. 2, pp. 298-300.

[382] *Ibid*, p. 298.

[383] *Ibid.*

[384] Regolamento (UE) 2016/679, art. 35 – *Valutazione d'impatto sulla protezione dei dati*.

[385] Regolamento (UE) 2016/679, art. 35(1): *Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei*

automatizzati che si fondano su processi algoritmici suscettibili di produrre esiti discriminatori e che danno luogo a decisioni di impatto rilevante per l'interessato, rientrano tra i casi che l'articolo 35 impone di valutare *ex ante.*[386] Tale valutazione deve contenere almeno una descrizione del trattamento e delle sue finalità; un'analisi della sua necessità e proporzionalità; una valutazione dei rischi per i diritti e le libertà degli interessati; nonché le misure tecniche e organizzative previste per mitigare tali rischi e garantire la conformità al Regolamento.[387]

Il secondo corollario introduce il principio di qualità o correttezza dei dati posti a fondamento della decisione automatizzata. Infatti, la nozione di *data quality by default* richiede che le amministrazioni pubbliche assicurino che i dati utilizzati per addestrare e alimentare gli algoritmi siano aggiornati, rappresentativi e privi di distorsioni sistemiche.[388] A tal riguardo, la giurisprudenza amministrativa, riferendosi al noto principio informatico "*garbage in garbage out"*[389], ha riconosciuto l'esigenza, in capo al titolare del trattamento, di procedere alla rettifica dei dati in *input*, al fine di scongiurare l'insorgenza di effetti discriminatori nel prodotto generato dal sistema algoritmico.[390]

Nonostante la natura interpretativa della disposizione esaminata[391], la stessa è espressiva del principio generale di non discriminazione previsto dall'articolo 3 della Costituzione[392], dall'articolo 14 della Convenzione europea dei diritti

---

trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

[386] E. Carloni, '*I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*', *cit*., pp. 298-299.

[387] Regolamento (UE) 2016/679, art. 35(7): *La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*

[388] E. Carloni, '*I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*', *cit*., pp. 299-300.

[389] A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', cit., par. 4.4: "*È il principio noto tra i data scientists come GIGO – garbage in garbage out – per cui un algoritmo non può che riflettere la qualità dei dati su cui è costruito.*"

[390] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881: "*occorrerebbe rettificare i dati in "ingresso" per evitare effetti discriminatori nell'output decisionale.*"

[391] A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', cit., par. 4.4.

[392] Costituzione, art. 3: *Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni*

dell'uomo[393] e dall'articolo 21 della Carta dei diritti fondamentali dell'Unione europea.[394]

Oggi, anche l'AI Act contiene richiami al principio in esame. Infatti, l'articolo 10[395] stabilisce che i sistemi di intelligenza artificiale ad alto rischio, qualora si basino su tecniche di apprendimento automatico, devono essere sviluppati utilizzando *set* di dati di addestramento, convalida e *test* che rispettino specifici criteri di qualità definiti dal Regolamento.[396] In particolare, tali dati devono essere "*pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista*".[397] Ciò implica che gli algoritmi ad alto rischio debbano essere addestrati su dati privi di distorsioni e pregiudizi che possano generare effetti discriminatori.[398] Inoltre, affinché un *set* di dati possa considerarsi sufficientemente rappresentativo, esso deve riflettere in modo adeguato la diversità presente nella categoria o nello scenario che intende modellare. Tale requisito è fondamentale per garantire che le decisioni algoritmiche siano eque, imparziali e conformi ai principi di uguaglianza e non discriminazione.[399]

---

personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese.

[393] Convenzione europea dei diritti dell'uomo, art. 14: *Il godimento dei diritti e delle libertà riconosciuti nella presente Convenzione deve essere assicurato senza nessuna discriminazione, in particolare quelle fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione.*

[394] Carta dei diritti fondamentali dell'Unione Europea (2016/C 202/02), art. 21: *1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età o le tendenze sessuali. 2. Nell'ambito d'applicazione del trattato che istituisce la Comunità europea e del trattato sull'Unione europea è vietata qualsiasi discriminazione fondata sulla cittadinanza, fatte salve le disposizioni particolari contenute nei trattati stessi.*

[395] Regolamento (UE) 2024/1689, art. 10 – *Dati e governance dei dati*.

[396] Regolamento (UE) 2024/1689, art. 10(1): *I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5 ogniqualvolta siano utilizzati tali set di dati.*

[397] Regolamento (UE) 2024/1689, art. 10(3).

[398] A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', cit., par. 4.4.

[399] K. Yordanova, '*The EU Artificial Intelligence (AI) Act: A Commentary*', *cit*, p. 275.

Infine, come anticipato, e coerentemente con l'orientamento della giurisprudenza amministrativa nonché della normativa comunitaria, l'articolo 30 del d.lgs. n. 36/2023 impone la previsione di misure tecniche ed organizzative idonee ad evitare effetti discriminatori nei confronti degli operatori economici.[400]

4.3.1. Il caso *Compas* negli Stati Uniti

Il dibattito giuridico sul principio di non discriminazione algoritmica trova un esempio emblematico nella caso giurisprudenziale statunitense, deciso dalla Corte Suprema dello Stato del Wisconsin nel 2016, *State v. Loomis*.[401] Al centro della controversia si colloca l'impiego del *software Compas* (*Correctional Offender Management Profiling for Alternative Sanctions*), sviluppato e gestito da una società privata – *Equivant Inc.* – e utilizzato nel sistema giudiziario del Wisconsin per effettuare valutazioni sul rischio di recidiva e di pericolosità sociale degli imputati.[402] Più nel dettaglio, l'algoritmo, elaborando le informazioni contenute nel fascicolo dell'imputato, incluse le precedenti condanne, le condizioni socioeconomiche e altri dati personali, nonché le risposte fornite nel corso dell'intervista individuale, genera una valutazione predittiva del rischio di recidiva, classificandola secondo tre livelli: basso, medio o elevato.[403]

Nel caso in esame, l'imputato Eric Loomis, arrestato e processato nel 2013, ha ricevuto una condanna a sei anni di reclusione anche in ragione del rischio "elevato" di recidiva riconosciuto dal programma *Compas.* Tuttavia, Loomis ha contestato la sua condanna per violazione del diritto al *due process.* In particolare, ha eccepito la lesione del diritto a una condanna fondata su informazioni attendibili, in quanto la natura proprietaria del *software* ha impedito qualsiasi verifica sull'accuratezza del punteggio assegnato; la compromissione del diritto a una valutazione individualizzata, poiché il giudizio si è basato su dati aggregati riferiti a gruppi più

[400] D.lgs. n. 36/2023, art. 30(3)(c): *Le decisioni assunte mediante automazione rispettano i principi di:* […] *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*.
[401] State v. Loomis, Supreme Court of Wisconsin (881 N.W.2d 749), 2016.
[402] F. Lagioia, G. Sartor, '*Il sistema COMPAS: algoritmi, previsioni, iniquità*', in U. Ruffolo (a cura di), '*XXVI Lezioni di diritto dell'Intelligenza Artificiale'*, Giappichelli, Torino 2021, p. 230.
[403] A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', cit., par. 4.4.

ampi, utilizzati per inferire la sua probabilità personale di recidiva; l'impiego improprio di variabili legate al genere nel calcolo del rischio, ritenuto discriminatorio e privo di giustificazione oggettiva.[404]

Il primo nodo giuridico, quindi, riguarda la trasparenza e accessibilità del codice sorgente. *Compas*, infatti, è un *software* proprietario, coperto da segreto industriale, che non consente né all'imputato, né al giudice, né alla difesa, di accedere alla struttura logica con cui i dati vengono trattati e trasformati in una valutazione predittiva. In tal modo, la decisione giudiziaria, seppur formalmente assunta da un essere umano, si fonda in parte su una decisione opaca che impedisce di esercitare un controllo effettivo sulla razionalità e correttezza della valutazione algoritmica.[405]

Il secondo profilo critico è emerso a seguito dell'indagine giornalistica condotta da ProPublica nel 2016, destando particolare preoccupazione sull'affidabilità di *Compas*.[406] Tale inchiesta ha dimostrato che il sistema algoritmico produce valutazioni sistematicamente distorte a danno delle persone afroamericane. In particolare, i soggetti neri venivano classificati con una probabilità doppia di essere etichettati "ad alto rischio" rispetto ai soggetti bianchi, a parità di profili individuali e pregressi. L'algoritmo, dunque, tendeva a generare falsi positivi per le persone nere – valutate ad alto rischio ma in realtà non recidive – e falsi negativi per i bianchi – valutati a basso rischio, ma successivamente recidivi.[407] Tali risultati, pur non imputando una discriminazione diretta – poiché la variabile "*razza*"[408] non è inclusa nei dati – dimostrano che il *dataset* di addestramento incorpora pregiudizi sistemici radicati nella società e nella pratica giudiziaria, riproducendo ed amplificando le diseguaglianze preesistenti.[409]

---

[404] Loomis, 881 N.W.2d, §757.
[405] K. Freeman, '*Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in State v. Loomis*', in North Carolina Journal of Law & Technology, 2016, XVIII, pp. 91-96.
[406] J. Larson, S. Mattu, L. Kirchner, J. Angwin, '*How We Analyzed the COMPAS Recidivism Algorithm*', ProPublic, 23 maggio 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm
[407] *Ibid*; A. Simoncini, '*Amministrazione digitale algoritmica. Il quadro costituzionale*', cit., par. 4.4.
[408] J. Larson, S. Mattu, L. Kirchner, J. Angwin, '*Machine Bias – There's software used across the country to predict future criminals. And it's biased against blacks*', ProPublic, 23 maggio 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
[409] *Ibid.*

Nonostante l'evidenza degli effetti distorsivi generati dall'uso del sistema *Compas*, la Corte Suprema del Wisconsin ha respinto le doglianze sollevate da Loomis, affermando che la decisione giudiziaria sarebbe stata la medesima anche in assenza dello strumento algoritmico.[410] Nondimeno, la Corte ha introdotto una serie di precauzioni interpretative: in primo luogo, ha chiarito che *Compas* può essere utilizzato esclusivamente come strumento ausiliario, privo di efficacia vincolante per il giudice; in secondo luogo, ha stabilito che l'autorità giudiziaria è tenuta a conservare la propria discrezionalità decisoria e a fornire una motivazione autonoma e aggiuntiva rispetto all'*output* generato dal sistema algoritmico.[411]

Dunque, la corte, nonostante la discutibilità della sentenza, stabilisce, come anche sottolineato dal Consiglio di Stato, un diritto a non essere sottoposti ad una decisione esclusivamente automatizzata[412] ed apre le porte al dibattito dottrinale, legislativo e giurisprudenziale sui rischi che derivano dall'implementazione di strumenti algoritmici nei procedimenti decisionali.

[410] Loomis, 881 N.W.2d.
[411] *Ibid.*
[412] Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472, 8473, 8474; Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881: "*In secondo luogo, l'altro principio del diritto europeo rilevante in materia (ma di rilievo anche globale in quanto ad esempio utilizzato nella nota decisione Loomis vs. Wisconsin), è definibile come il principio di non esclusività della decisione algoritmica.*"

CAPITOLO III

LA SICUREZZA CIBERNETICA NAZIONALE

SOMMARIO: **1. La nozione di cybersicurezza** – 1.1. La cybersicurezza come bene pubblico – **2. L'evoluzione della disciplina nazionale ed europea** – **3. L'Agenzia per la cybersicurezza nazionale** – 3.1. La natura giuridica dell'ACN – **4. Sicurezza cibernetica e pubblica amministrazione** – **5. Sicurezza cibernetica e contratti pubblici** – 5.1. La disciplina generale – 5.2. La disciplina per le pubbliche amministrazioni nel Perimetro di sicurezza nazionale cibernetica – 5.3. Gli appalti dell'Agenzia per la cybersicurezza nazionale.

1. La nozione di cybersicurezza

L'evoluzione tecnologica, l'innovazione e l'interconnessione hanno radicalmente modificato il modo di comunicare e il funzionamento della società[413], ridefinendo al contempo la dimensione nella quale vengono svolte attività ed operazioni, fino a identificare il cyberspazio. Alla luce della portata di tali trasformazioni e delle conseguenze sugli interessi fondamentali degli Stati, quali la *privacy*, la sicurezza e l'economia, è imprescindibile conoscere come questo "spazio" sia influenzato e condizionato dalle politiche governative delle nazioni.[414]

Il cyberspazio, infatti, "*è l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete*".[415] È, dunque, possibile identificare tre componenti fondamentali del cyberspazio. La prima è quella fisica, costituita dall'infrastruttura materiale della rete, come gli

[413] A. Karathanasis, '*Cybersecurity and EU Law – Adopting the Network and Information Security Directive*', Routledge Research in EU Law, 2025, par. 1.
[414] F. Mercurio, '*Il cyberspace: la sovranità nel quinto dominio*', in *Cammino Diritto*, 30 ottobre 2024, p. 2.
[415] Presidenza del Consiglio dei Ministri, '*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*', dicembre 2013, p. 10.

hardware, i cavi, i *server* e i computer. La seconda è quella logica, composta dalle connessioni tra i dispositivi di rete, dai dati, i protocolli e le applicazioni che rendono possibile lo scambio di informazioni attraverso la componente fisica. La terza componente è quella sociale che comprende le persone fisiche che interagiscono e svolgono operazioni nel cyberspazio.[416]

Proprio in relazione a questo "spazio" è necessario introdurre la nozione di cybersicurezza. Quest'ultimo è un concetto che si è affermato progressivamente tanto nella riflessione dottrinale quanto nella normativa europea. In dottrina, la cybersicurezza è stata definita come *"un sistema organizzativo finalizzato a proteggere le infrastrutture informatico-digitali di organizzazioni complesse, di natura pubblicistica (o privatistica), in primis lo Stato, attuato tramite la predisposizione di misure tecniche idonee volte alla tutela di diritti e libertà fondamentali*".[417] Tale impostazione evidenzia il superamento di una concezione di *cybersecurity* connessa alla protezione del computer personale, e dimostra il coinvolgimento di interessi ben più rilevanti, quali le infrastrutture degli Stati, la tutela dei diritti e delle libertà fondamentali.[418]

A livello normativo, invece, già nel 2013 la Commissione europea nella Comunicazione su "*Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*" aveva presentato una prima definizione del concetto.[419] Tuttavia, è con il Regolamento 2019/881[420], anche noto come Cybersecurity Act,

---

[416] M. N. Schmitt, '*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*', Cambridge University press, 2017, Part I, General international law and cyberspace, Rule 1, Sovereignty.

[417] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', Contributi di diritto amministrativo, F.G. Scoca, G. Corso, M. D'Orsogna, L. Giani, M. Immordino, A. Police, M.A. Sandulli, M.R. Spasiano (a cura di), Editoriale Scientifica Napoli, 2023, pp. 12-13.

[418] G. Ziccardi, '*La cybersecurity nel quadro tecnologico (e politico) attuale*', in G. Ziccardi, P. Perri, Tecnologia e diritto, Vol. III, Informatica giuridica avanzata, Giuffrè Francis Lefebvre, Milano, 2019, p. 207.

[419] Commissione europea, '*Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*', Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, JOIN (2013), 7 febbraio 2013, p. 3: *La cibersicurezza si riferisce comunemente alle precauzioni e agli interventi che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti. La cibersicurezza si propone di salvaguardare la disponibilità e l'integrità delle reti e dell'infrastruttura e la riservatezza delle informazioni che esse contengono.*

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

e, successivamente con la Direttiva 2022/2555[421], conosciuta come NIS 2 (*Network and Information Security*), che si è giunti a una codificazione formale della nozione. Infatti, la direttiva, rinviando esplicitamente all'articolo 2 del Regolamento[422], definisce la cybersicurezza come "*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*".[423]

1.1. La cybersicurezza come bene pubblico

Sulla base delle definizioni dottrinali e normative appena esaminate, appare evidente come ad essere minacciati da operazioni cibernetiche non siano soltanto individui e imprese, ma, in una prospettiva più ampia, la sicurezza nazionale degli Stati.[424] Ciò ha condotto una parte della dottrina a qualificare, in modo selettivo o sistemico, la cybersicurezza come bene pubblico. Quest'ultimo è dotato di due caratteristiche essenziali: "*la non rivalità e la non escludibilità. La prima indica la circostanza in cui l'uso di un bene da parte di un agente non incide sulla facoltà di goderne completamente da parte di terzi. La seconda rappresenta invece l'impossibilità di estromettere terzi dal consumo di un determinato bene*".[425]

Un primo orientamento dottrinale rigetta l'idea della *cybersecurity* come bene pubblico "*tout court*", poiché non si tratta di un'entità unitaria, bensì di un insieme di pratiche, strumenti e obiettivi eterogenei.[426] In tal senso, la cybersicurezza si articola in tre componenti essenziali: la progettazione di sistemi robusti, capaci di resistere agli attacchi; la definizione di metodi e sistemi per il rilevamento di minacce e anomalie, al fine di garantire la resilienza del sistema; la predisposizione

[421] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
[422] Direttiva (UE) 2022/2555, art. 6(3): *«cibersicurezza»: la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881.*
[423] Regolamento (UE) 2019/881, art. 2(1) – *Definizioni.*
[424] T. Cocchi, '*La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza*', in *Munus – Rivista giuridica dei servizi pubblici*, n. 1/2024, p. 183.
[425] R. Vannini, '*Dizionario di economia e finanza*', Treccani.
[426] M. Taddeo, '*Is Cybersecurity a Public Good?*', in *Minds and Machines – Journal for Artificial Intelligence, Philosophy, and Cognitive Science*, 2019, vol. 29, p. 350.

di risposte agli attacchi.[427] Tra queste, soltanto la robustezza dei sistemi può essere correttamente qualificata come bene pubblico.[428] Infatti, la robustezza – intesa come la capacità di un sistema di mantenere un comportamento stabile e prevedibile anche in presenza di *input* errati – è un prerequisito essenziale per ridurre l'impatto degli attacchi informatici e garantire l'affidabilità dei sistemi.[429] È, quindi, in ragione dell'impatto sull'interesse collettivo e sulla stabilità delle società digitali che la robustezza dovrebbe essere trattata come un bene pubblico.[430] Questa impostazione consentirebbe, tra le altre cose, una condivisione delle responsabilità tra attori pubblici e privati, e un rafforzamento della cooperazione e dello scambio informativo.[431]

Pur riconoscendo la fondatezza e logicità di tale approccio, una parte della dottrina ne ha sottolineato alcune criticità.[432] Infatti, nei testi normativi dell'Unione europea, il concetto di robustezza risulta largamente assente o marginale rispetto a quello di resilienza, ponendo così un limite alla concreta implementazione di un approccio fondato sulla robustezza come bene pubblico.[433] Altresì, l'elevato costo della progettazione di sistemi robusti risulta essere spesso incompatibile con le logiche di mercato.[434] Infine, le forti resistenze, sia da parte degli Stati che degli attori privati, alla condivisione delle vulnerabilità per timori reputazionali, giuridici o legati alla sicurezza nazionale, evidenziano il rischio che tale orientamento rimanga esclusivamente teorico.[435]

Altra parte della dottrina, invece, sostiene che la cybersicurezza, pur nascendo come bene meritorio[436], può e deve essere progressivamente riconosciuta come

---

[427] *Ibid.*
[428] *Ibid.*
[429] *Ibid.*
[430] *Ibid,* p. 351.
[431] *Ibid,* pp. 351-352.
[432] R. Brighi, P.G. Chiara, '*La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*', in *federalismi.it*, 2021, fasc. 21.
[433] *Ibid,* p. 31.
[434] *Ibid*, p. 27.
[435] *Ibid,* p. 30.
[436] M. De Benedetti, '*La cyber sicurezza come nuova dimensione della difesa dello Stato: bene meritorio o bene pubblico?*', in *federalismi.it*, 2018, fasc. 9, p. 6: "*Sono beni meritori quei beni che, pur essendo a domanda individuale, vengono erogati dalle istituzioni a tutti i cittadini i quali corrispondono un prezzo minimo come controprestazione; il motivo risiede nella loro capacità di apportare un vantaggio (esternalità positive) non solo ai soggetti che la consumano ma, indirettamente, a tutta la collettività".*

bene pubblico puro.[437] Infatti, viste l'inadeguatezza del mercato a garantire in modo efficiente la produzione di sicurezza informatica, la diffusione di minacce cibernetiche nonché l'interdipendenza delle reti e l'opacità informativa, la cybersicurezza possiede le caratteristiche fondamentali del bene pubblico: non-rivalità e non-escludibilità.[438] Essa deve dunque essere assunta a oggetto di una politica pubblica strutturata, al pari della difesa nazionale[439], in cui lo Stato agisce come "innovatore".[440] Infatti, solo un intervento pubblico sistemico – capace di creare incentivi, regole, e cooperazione pubblico-privata – può garantire un livello di sicurezza informatica in grado di proteggere l'interesse collettivo.[441]

Insomma, appare evidente come la cybersicurezza non possa più essere ridotta a una questione privata, ma debba essere riqualificata come bene pubblico seppur ancora con incertezze sul ruolo dello Stato nella costruzione di un ecosistema digitale sicuro, equo e sostenibile.

2. L'evoluzione della disciplina nazionale ed europea

L'evoluzione della disciplina in materia di cybersicurezza, tanto a livello europeo quanto nazionale, riflette la crescente consapevolezza circa la centralità della protezione dello spazio cibernetico per la sicurezza collettiva, l'integrità delle infrastrutture critiche e la tenuta dei sistemi democratici.[442]

La regolazione europea prende avvio all'inizio del XXI secolo con una Comunicazione delle Commissione europea del 26 gennaio 2001[443] in cui si sottolinea l'urgenza di rafforzare la sicurezza delle infrastrutture dell'informazione e l'esigenza di contrastare la criminalità informatica. Nello stesso anno, la commissione analizza la *Network and Information Security* (NIS) e propone lo

[437] *Ibid*, pp. 2-15.
[438] *Ibid*.
[439] *Ibid,* p. 14.
[440] *Ibid.*
[441] *Ibid,* pp. 9-10.
[442] A. Pezzuto, '*Evoluzione normativa della sicurezza informatica nell'UE e in Italia*', in *Magistra banca e finanza*, 26 gennaio 2025.
[443] Commissione delle comunità europee, '*Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica*', Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, COM (2000) 890, 26 gennaio 2001.

sviluppo di una politica comunitaria in materia.[444] Nel 2004, con l'approvazione del Regolamento (CE) 460/2004[445] viene istituisce l'Agenzia europea di sicurezza delle reti e dell'informazione – meglio conosciuta come ENISA – "*al fine di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno*."[446] L'Agenzia svolge un ruolo centrale nella promozione di un ecosistema normativo adeguato sia al livello europeo che, soprattutto, nazionale.[447] Infatti, l'attività principale consiste nel coordinare le iniziative degli Stati membri e facilitare il dialogo tra le istituzioni europee, mediante l'elaborazione di linee guida e *best practices*.[448]

Parallelamente, anche in Italia si avviano interventi normativi. Nel 2002, infatti, una direttiva del Presidente del Consiglio individua, per la prima volta[449], nella sicurezza e tutela dei dati e delle informazioni raccolte dalle pubbliche amministrazioni una priorità strategica.[450] Nel 2008, l'Italia, anticipando la direttiva europea 2008/114/CE[451], approva un decreto per stabilire le procedure per la classificazione delle infrastrutture critiche del paese.[452] Tale direttiva, approvata alla fine dello stesso anno, individua e definisce le infrastrutture critiche europee (ECI).[453]

---

[444] Commissione delle comunità europee, '*Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*', Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni COM (2001) 298, 6 giugno 2001.
[445] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.
[446] Regolamento (CE) n. 460/2004, art. 1.1.
[447] C. Cencetti, '*Cybersecurity: Unione europea e Italia Prospettive a confronto*', Quaderni IAI, Edizioni Nuova Cultura, 2014, p. 26.
[448] *Ibid.*
[449] *Ibid,* p. 64.
[450] Direttiva del Presidente del Consiglio dei ministri, Dipartimento per l'Innovazione e le Tecnologie, 'Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni', 16 gennaio 2002, G.U. n. 69 del 22 marzo 2002.
[451] Direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, 8 dicembre 2008.
[452] Decreto del Ministero dell'Interno, 'Individuazione delle infrastrutture critiche informatiche di interesse nazionale', 9 gennaio 2008, G.U. n. 101 del 30 aprile 2008.
[453] Direttiva 2008/114/CE, art. 2(b): *«infrastruttura critica europea» o «ECI» un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri.*

Nel 2013 la Commissione europea adotta una Comunicazione nella quale delinea la strategia comunitaria per la cybersicurezza.[454] Tale comunicazione identifica una serie di principi – "*protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della vita privata; accesso per tutti; governance partecipativa, democratica ed efficiente; responsabilità condivisa per garantire la sicurezza*"[455] – il cui rispetto rappresenta una condizione imprescindibile per l'attuazione delle priorità[456] fissate dalla strategia stessa.[457] Nello stesso anno, in Italia, il DPCM 24 gennaio 2013[458] istituisce due *Computer Emergency Response Team* (CERT) e introduce una prima *governance* nazionale del settore, individuando nella Presidenza del Consiglio dei Ministri il vertice.[459]

Nel 2016 l'Unione europea approva la Direttiva (UE) 2016/1148[460], nota come NIS 1, che rappresenta il primo atto normativo generale sulla cybersicurezza.[461] La direttiva, al fine di incrementare le capacità di cybersicurezza degli Stati membri e di sviluppare un'elevata cooperazione strategica tra Stati, impone l'adozione di strategie nazionale, l'individuazione degli operatori essenziali in settori critici, la designazione di autorità competenti e l'istituzione di gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Team*, CSIRT).[462]

L'Italia, con il d.lgs. 65/2018[463], recepisce la NIS 1 e adempie gli obblighi imposti dalla normativa comunitaria.[464] Nel 2019, invece, con il decreto-legge n.

---

[454] Commissione europea, '*Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*', *cit.*
[455] *Ibid*, p. 4.
[456] *Ibid,* p. 5: *La visione dell'UE delineata nella presente strategia si articola intorno a cinque priorità strategiche per affrontare le sfide sopra descritte: raggiungere la ciberresilienza; ridurre drasticamente il cibercrimine; sviluppare una politica e capacità di ciberdifesa connesse alla Politica di sicurezza e di difesa comune (PSDC); sviluppare le risorse industriali e tecnologiche per la cibersicurezza; creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE.*
[457] C. Cencetti, '*Cybersecurity: Unione europea e Italia Prospettive a confronto*', *cit*., p. 36.
[458] Decreto del Presidente del Consiglio dei ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale', 24 gennaio 2013, G.U. n. 66 del 19 marzo 2013.
[459] C. Cencetti, '*Cybersecurity: Unione europea e Italia Prospettive a confronto*', *cit*., pp. 82-87.
[460] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, 6 luglio 2016.
[461] A. Pezzuto, '*Evoluzione normativa della sicurezza informatica nell'UE e in Italia*', *cit.*, par. 2.
[462] *Ibid.*
[463] Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[464] A. Pezzuto, '*Evoluzione normativa della sicurezza informatica nell'UE e in Italia*', *cit.*, par. 3.

205/2019[465], convertito con modificazioni in legge n. 133/2019[466], istituisce il Perimetro di sicurezza nazionale cibernetica (PSNC).[467] Quest'ultimo rappresenta il quadro normativo entro cui si applicano misure rafforzate di *cybersecurity* nei confronti di soggetti considerati strategici per la sicurezza del Paese, prevedendo un elevato livello di protezione dei sistemi informatici e delle reti la cui compromissione, interruzione o danneggiamento potrebbe arrecare un pregiudizio alla sicurezza nazionale.[468] Infatti, vi rientrano sia i soggetti – comprese le pubbliche amministrazioni – che esercitano funzioni essenziali per lo Stato[469] sia soggetti pubblici o privati che erogano servizi cruciali per il funzionamento di attività civili, sociali o economiche fondamentali[470], entrambi individuati mediante notifica formale.[471] Alcuni anni dopo, con il decreto-legge n. 82/2021[472], convertito

[465] Decreto-legge 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.
[466] Legge 18 novembre 2019, n. 133, Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
[467] Decreto-legge n. 105/2019, art. 1(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*.
[468] S. Poletti, '*La sicurezza cibernetica nazionale ed europea, alla luce della creazione del Perimetro di sicurezza nazionale cibernetica*', in MediaLaws, 2023, fasc. 2, p. 404.
[469] DPCM 30 luglio 2020, n. 131, art. 2: *1. Ai fini di quanto previsto dall'articolo 1, comma 2, lettera a), del decreto-legge: a) un soggetto esercita una funzione essenziale dello Stato, di seguito funzione essenziale, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti.*
[470] DPCM 30 luglio 2020, n. 131, art. 2: 1. *Ai fini di quanto previsto dall'articolo 1, comma 2, lettera a), del decreto-legge: […] b) un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, di seguito servizio essenziale, laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.*
[471] F. Serini, '*La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*', in Rivista italiana di informatica e diritto, 2023, fasc. 2, p. 64.
[472] Decreto-legge 14 giugno 2021, n. 82, 'Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale'.

in legge n. 109/2021[473], viene ridefinita l'organizzazione istituzionale e contestualmente istituita l'Agenzia per la cybersicurezza nazionale[474] (ACN).[475]

L'efficacia applicativa della NIS 1 ha incontrato importanti limiti a causa della forte divergenza attuativa tra gli Stati membri.[476] Per porvi rimedio, l'Unione europea, abrogando la NIS 1, approva la Direttiva (UE) 2022/2555[477], nota come NIS 2. Quest'ultima amplia l'ambito di applicazione della disciplina europea in materia di cybersicurezza, limitando la discrezionalità degli Stati nella designazione degli operatori di servizi essenziali mediante l'individuazione di criteri dimensionali oggettivi, e aggiornando l'elenco dei settori interessati, includendo ambiti strategici come le pubbliche amministrazioni centrali.[478] Tra gli obblighi a carico degli Stati membri, oltre alla conferma degli adempimenti già previsti dalla direttiva NIS 1, vi è l'istituzione di autorità per la gestione delle crisi informatiche, l'adozione di un piano nazionale di risposta agli incidenti e la creazione di una banca dati europea delle vulnerabilità.[479] Inoltre, la NIS 2 rafforza i meccanismi di vigilanza, armonizza il regime sanzionatorio e riconosce crescente importanza agli organi di gestione degli operatori, cercando di superare le frammentarietà generate dalla precedente direttiva.[480] A tal fine, promuove altresì una maggiore condivisione informativa e istituisce formalmente la rete europea *EU-CyCLONE* per la gestione coordinata delle crisi informatiche.[481]

L'Italia recepisce la NIS 2 con il d.lgs. n. 138/2024[482], che abroga il d.lgs. n. 65/2018. Il nuovo decreto, riproducendo sostanzialmente il contenuto della direttiva

---

[473] Legge 4 agosto 2021, n. 109, 'Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale'.
[474] Si veda *infra* paragrafo 3.
[475] A. Pezzuto, '*Evoluzione normativa della sicurezza informatica nell'UE e in Italia*', *cit.*, par. 3.
[476] *Ibid*, par. 2.
[477] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), 14 dicembre 2022.
[478] T. Barzanti, '*La normative dell'Unione europea in materia di cybersicurezza*', in C. Cavaceppi e A. Contaldo (a cura di), *Cybersecurity connect – La disciplina europea della Direttiva NIS2,* tab edizioni, 2024, p. 76.
[479] *Ibid,* p. 77.
[480] *Ibid*, pp. 78-79.
[481] *Ibid,* p. 79.
[482] Decreto legislativo 4 settembre 2024, n. 138, 'Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del

comunitaria, rafforza il controllo e la vigilanza in materia di sicurezza informatica e attribuisce all'Agenzia per la cybersicurezza nazionale funzioni sanzionatorie, di vigilanza e monitoraggio.[483]

Nello stesso anno, l'Italia adotta anche la legge n. 90/2024[484], che integra il quadro con nuove misure in materia di reati informatici, crittografia e obblighi di segnalazione a carico delle PA.[485] Rafforza inoltre il ruolo dell'ACN nel coordinamento delle informazioni e nella verifica della conformità dei *software*, istituendo il Centro nazionale di crittografia.[486]

3. L'Agenzia per la cybersicurezza nazionale

Come anticipato, il decreto-legge n. 82/2021, convertito in legge n. 109/2021, istituisce l'Agenzia per la cybersicurezza nazionale "*a tutela degli interessi nazionali nel campo della cybersicurezza*".[487]

La disciplina è contenuta principalmente negli articoli 5[488], 6[489] e 7[490], dedicati rispettivamente all'istituzione dell'Agenzia, alla sua organizzazione e alle sue funzioni, nonché dai Decreti del Presidente del Consiglio dei Ministri n. 223/2021[491] e n. 224/2021[492] relativi, rispettivamente, all'organizzazione e funzionamento dell'agenzia ed al personale.

Sul piano strutturale, il vertice dell'agenzia è affidato al Direttore generale, al Vice direttore generale e al Collegio dei revisori dei conti.[493] I primi due organi

---

regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148'.

[483] Si veda *infra* paragrafo 3.

[484] Legge 28 giugno 2024, n. 90, 'Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici'.

[485] A. Pezzuto, '*Evoluzione normativa della sicurezza informatica nell'UE e in Italia*', *cit.*, par. 3; si veda *infra* paragrafo 4.

[486] *Ibid.*

[487] Decreto-legge n. 82/2021, art. 5 – *Agenzia per la cybersicurezza nazionale*.

[488] *Ibid.*

[489] *Ibid*, art. 6 – *Organizzazione dell'Agenzia per la cybersicurezza nazionale.*

[490] *Ibid,* art. 7 – *Funzioni dell'Agenzia per la cybersicurezza nazionale*.

[491] Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, 'Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale'.

[492] Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 224, 'Regolamento del personale dell'Agenzia per la cybersicurezza nazionale'.

[493] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', in *federalismi.it*, 2022, fasc. 12, p. 249.

sono nominati dal Presidente del Consiglio dei Ministri[494] tra figure di alta qualificazione – quali magistrati delle giurisdizioni superiori, avvocati dello Stato, dirigenti generali, professori universitari[495] – "*in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione*"[496]. Ai sensi dell'articolo 5 del DPCM n. 223/2021[497], il Direttore generale, tra le altre cose, è gerarchicamente sovraordinato al personale, ha la rappresentanza legale dell'agenzia ed è il referente diretto del Presidente del Consiglio.[498] Il Vice direttore assiste il Direttore nella gestione dell'agenzia e esercita le funzioni attribuitegli con provvedimento dal Direttore.[499] Il Collegio dei revisori dei conti, invece, è composto da 3 membri effettivi e un membro supplente[500] ed esercita ampie funzioni di controllo.[501] L'articolo 12 del DPCM in questione, attuando la previsione dell'articolo 6 del decreto-legge, delinea la macrostruttura interna dell'Agenzia, identificando e disciplinando le funzioni e i poteri di sette servizi.[502]

---

[494] Decreto-legge n. 82/2021, art. 2(1): *Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:* […] *c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, previa deliberazione del Consiglio dei ministri.*

[495] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', *cit.*, pp. 249-250.

[496] Decreto-legge n. 82/2021, art. 5(3).

[497] DPCM n. 223/2021, art. 5: *1. Il direttore generale è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, nella materia della cybersicurezza. 2. Il direttore generale, in particolare: a) è il legale rappresentante dell'Agenzia e ne ha la rappresentanza esterna.*

[498] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', *cit.*, p. 249.

[499] DPCM n. 223/2021, art. 6: *1. Il Vice Direttore generale di cui all'articolo 5, comma 3, del decreto-legge coadiuva il direttore generale nella direzione dell'Agenzia. Sulla base di apposito provvedimento del direttore generale, svolge le funzioni attribuitegli, sovrintende e coordina i Servizi e le altre articolazioni dell'Agenzia, indicate nel medesimo provvedimento. 2. Il Vice Direttore generale svolge altresì le funzioni vicarie per i casi di assenza o impedimento del direttore generale.*

[500] DPCM n. 223/2021, art. 7(1): *Il Collegio dei revisori dei conti è composto da: a) un magistrato della Corte dei conti, in servizio o in quiescenza, che lo presiede; b) un componente effettivo, designato dal Ministero dell'economia e delle finanze ai sensi dell'articolo 16 della legge 31 dicembre 2009, n. 196; c) un ulteriore componente effettivo e un componente supplente, scelti entrambi tra soggetti, in servizio o in quiescenza, appartenenti ai ruoli della magistratura amministrativa, contabile o dell'Avvocatura dello Stato, ovvero tra professori universitari ordinari di contabilità pubblica o discipline similari, ovvero tra alti dirigenti dello Stato.*

[501] DPCM n. 223/2021, art. 7(5): *Il Collegio: a) effettua il riscontro degli atti della gestione finanziaria e formula le proprie osservazioni; b) svolge, almeno una volta ogni tre mesi, verifiche di cassa e di bilancio; c) esprime, in apposita relazione, parere sul progetto di bilancio preventivo, nonché sul rendiconto annuale; d) esercita ogni altra funzione ad esso attribuita dalla normativa vigente.*

[502] DPCM n. 223/2021, art. 12(1): *L'Agenzia, nei limiti stabiliti dall'articolo 6, comma 1, del decreto-legge, e fatto salvo quanto previsto dall'articolo 17, si articola nei seguenti servizi: a)*

Con riferimento alle funzioni, l'Agenzia è investita di una pluralità di compiti che, sebbene analiticamente indicati all'articolo 7 del decreto-legge e nel DPCM attuativo n. 223/2021, possono essere sistematicamente ricondotti, ai sensi dell'articolo 7 del decreto-legge[503], a quattro obiettivi strategici fondamentali: "*l'esercizio di funzioni derivanti dalla qualifica di Autorità nazionale per la cybersicurezza; il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale; la promozione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni; il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore"*.[504] Alla luce di tali obiettivi è possibile analizzare le numerose funzioni attribuite all'Agenzia.[505]

In forza del primo obiettivo l'Agenzia acquisisce un insieme articolato di competenze normative, regolatorie e operative precedentemente distribuite tra più amministrazioni.[506] In tale veste, l'Agenzia è responsabile della predisposizione della strategia nazionale di cybersicurezza e ha la competenza in materia di sicurezza dei dati e delle infrastrutture delle pubbliche amministrazioni, comprese l'adozione e l'aggiornamento delle linee guida tecniche ai sensi del Codice dell'Amministrazione Digitale.[507] A tali funzioni si aggiunge, altresì, il potere di condurre ispezioni, verifiche e accertamenti, imporre prescrizioni e irrogare sanzioni nei confronti di soggetti pubblici e privati inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, nonché un potere consultivo al fine di mantenere "*un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza*"[508].

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.

[503] Decreto-legge n. 82/2021, art. 7 – *Funzioni dell'Agenzia per la cybersicurezza nazionale.*

[504] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', *cit.*, p. 252.

[505] *Ibid.*

[506] *Ibid,* p. 253.

[507] *Ibid,* p. 254.

[508] Decreto-legge n. 82/2021, art. 7(p).

Il secondo obiettivo si sostanzia nella partecipazione attiva dell'ACN agli organi interministeriali e tecnici preposti all'attuazione delle politiche di settore, nonché nei rapporti di cooperazione con le autorità indipendenti, tra cui il Garante per la protezione dei dati personali, con le Forze armate, le forze di polizia, le amministrazioni pubbliche, concorrendo così alla costruzione di una rete nazionale integrata di cybersicurezza.[509]

Il terzo obiettivo include le attività finalizzate allo sviluppo della digitalizzazione del sistema produttivo e delle amministrazioni pubbliche, tra cui la valorizzazione della crittografia come misura di sicurezza, la qualificazione dei servizi *cloud* per la pubblica amministrazione, la partecipazione dell'Italia a progetti e programmi internazionali ed europei, la conclusione di accordi bilaterali e multilaterali in ambito cibernetico, nonché la costituzione o partecipazione, previa autorizzazione del Presidente del Consiglio, a consorzi, fondazioni o società con soggetti italiani e stranieri.[510]

Infine, in esecuzione del quarto obiettivo, l'ACN è designata quale Autorità nazionale di certificazione della cybersicurezza ai sensi del Cybersecurity Act[511], con compiti di supervisione sui processi di qualificazione, valutazione e certificazione di prodotti, servizi e processi ICT, e di accreditamento delle strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità. In aggiunta, l'Agenzia è identificata quale Centro nazionale di coordinamento ai sensi del Regolamento (UE) 2021/887[512], con il compito di supportare il Centro di competenza europeo per la cybersicurezza industriale, tecnologica e di ricerca, e di contribuire allo sviluppo delle capacità europee nel settore.[513]

Con l'entrata in vigore della Direttiva NIS 2 e la conseguente adozione del decreto di recepimento, le funzioni dell'ACN si sono ampliate. Infatti, l'Agenzia è

[509] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', *cit.*, pp. 256-257.
[510] *Ibid,* p. 257.
[511] Regolamento (UE) 2019/881.
[512] Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021 che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.
[513] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', *cit.*, pp. 258-261.

identificata come autorità nazionale competente NIS di cui all'articolo 8 della direttiva (UE) 2022/2555.[514] In quanto tale, l'Agenzia assume un complesso di funzioni di monitoraggio, supporto e vigilanza.[515] Infatti, tra le altre cose, è legittimata a richiedere una rendicontazione sullo stato di attuazione degli obblighi previsti dal decreto e può effettuare controlli mediante esame documentale, ispezioni, nonché attraverso richieste di accesso a dati e informazioni.[516] L'Agenzia può inoltre irrogare sanzioni amministrative, tra le quali è prevista anche la sospensione temporanea dell'attività.[517]

È opportuno, altresì, sottolineare come il disegno di legge n. 1146/2024 recentemente approvato al Senato ed attualmente in discussione alla Camera, designi l'ACN, insieme all'Agenzia per l'Italia digitale, come Autorità nazionali per l'intelligenza artificiale.[518]

Sotto il profilo dell'autonomia[519], l'ACN è dotata di autonomia regolamentare, organizzativa e finanziaria.[520] Infatti, in materia normativa, ai sensi degli articoli 5 e 16 del DPCM n. 223/2021, il Direttore generale esercita tale autonomia mediante l'adozione di provvedimenti (anche) regolamentari per l'esercizio delle funzioni dell'Agenzia.[521] Sul piano organizzativo, il Direttore ha potere di pianificazione strategica, gestione del personale, assegnazione di risorse e adozione degli atti interni necessari all'attuazione delle funzioni.[522] In ambito finanziario, l'Agenzia dispone di entrate proprie, derivanti da servizi resi, sfruttamento di proprietà intellettuale, contributi europei e proventi da sanzioni.[523]

Sebbene dotata di autonomia, l'Agenzia esercita le sue funzioni sotto l'influenza del Presidente del Consiglio dei Ministri, al quale è, infatti, attribuita "*l'alta direzione e la responsabilità generale delle politiche di cybersicurezza*".[524] Al

[514] Decreto legislativo n. 138/2024, art. 10(1) – *Autorità nazionale competente e Punto di contatto unico*.
[515] A. Pezzuto, '*Evoluzione normativa della sicurezza informatica nell'UE e in Italia*', *cit.*, par. 3.
[516] *Ibid.*
[517] *Ibid.*
[518] Disegno di legge n. 1146/2024, art. 20.
[519] Si veda *infra* paragrafo 3.1.
[520] F. Serini, '*La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*', *cit.*, pp. 261-262.
[521] DPCM n. 223/2021, artt. 5(3)(a) e 16.
[522] DPCM n. 223/2021, art. 5(3)(b) e (c).
[523] Decreto-legge n. 82/2021, art. 11.
[524] Decreto-legge n. 82/2021, art. 2(1)(a).

contempo, nonostante una chiara tendenza alla centralizzazione delle competenze in materia di cybersicurezza in capo al Governo, il legislatore ha inteso rafforzare il controllo del Parlamento sull'attività dell'esecutivo.[525] Infatti, mediante il Comitato parlamentare per la sicurezza della Repubblica (c.d. COPASIR), il Parlamento svolge una funzione di controllo sull'attività del Presidente del Consiglio dei Ministri e dell'Agenzia in materia di cybersicurezza.[526] A tal riguardo, il decreto-legge n. 82/2021 prevede, tra le altre cose, il dovere per il Primo ministro di trasmettere al Parlamento e al COPASIR una relazione annuale sull'attività svolta dall'ACN.[527]

Infine, è opportuno evidenziare come, ai sensi dell'articolo 135 del Codice del processo amministrativo, il TAR Lazio, sede di Roma, ha una competenza funzionale inderogabile sulle "*controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale*".[528]

3.1. La natura giuridica dell'ACN

La qualificazione giuridica dell'Agenzia si presenta come una questione complessa, su cui la dottrina ha proposto ricostruzioni eterogenee, accomunate però dalla consapevolezza che ci si trova di fronte a un'entità organizzativa ibrida.

Innanzitutto, appare opportuno comprendere la nozione di agenzia amministrativa. Quest'ultima ha due caratteri distintivi: la specializzazione delle funzioni svolte e l'autonomia gestionale.[529] Infatti, da un lato, l'attività si sostanzia nello svolgimento di compiti e funzioni di natura tecnico-operativa e, dall'altro, le agenzie dispongono di un'ampia libertà nell'impiego delle risorse funzionali al

[525] L. Moroni, '*La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*', in *federalismi.it*, 2024, fasc. 14, p. 191.
[526] *Ibid,* pp. 191-192.
[527] Decreto-legge n. 82/2021, art. 14: *1. Entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri trasmette al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale. 2. Entro il 30 giugno di ogni anno, il Presidente del Consiglio dei ministri trasmette al COPASIR una relazione sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato.*
[528] D.lgs. 2 luglio 2010, n. 104, art. 135(1)(h-bis).
[529] F. Toth, '*La diffusione delle agenzie amministrative in Italia*', in Rivista Italiana di Politiche Pubbliche, 2007, fasc. 1, p. 137.

perseguimento degli obiettivi assegnati.[530] In relazione a quest'ultimo aspetto, nonostante l'autonomia nell'articolazione della struttura organizzativa, la gestione del personale, l'utilizzo delle risorse economiche disponibili e l'organizzazione dei processi operativi, le agenzie sono, a tutti gli effetti, parte dell'apparato amministrativo pubblico.[531] Infatti, come disposto dall'articolo 3 del DPCM n. 223/2021, l'organizzazione ed il funzionamento dell'Agenzia sono ispirati, tra gli altri, dai principi di autonomia, efficienza, imparzialità e trasparenza dell'azione amministrativa.[532]

Per delineare la natura giuridica dell'agenzia in esame, risulta necessario, altresì, identificare e comprendere i tre modelli che esistono attualmente nel panorama amministrativo nazionale: le agenzie istituite precedentemente al d.lgs. n. 300/1999, le agenzie sottoposte alla disciplina generale del d.lgs. n. 300/1999[533] e le agenzie fiscali.[534]

In primo luogo, le agenzie precedenti al d.lgs. n. 300/1999, pur non costituendo un *unicum*, hanno una serie di caratteri comuni.[535] Sul piano strutturale, l'organizzazione interna prevede la presenza di tre organi – presidente, consiglio di

---

[530] *Ibid,* pp. 137-138.
[531] *Ibid,* p. 138.
[532] DPCM n. 223/2021, art. 3(2): *L'organizzazione e il funzionamento dell'Agenzia si ispirano ai seguenti principi: a) autonomia e responsabilizzazione, in relazione al corretto uso delle risorse, al migliore conseguimento dei risultati attesi ed al massimo livello di adesione ai principi, ai valori e alla missione dell'Agenzia stessa; b) efficienza e razionale impiego delle risorse disponibili; c) imparzialità e trasparenza dell'azione amministrativa, nel rispetto della disciplina sulla sicurezza; d) ottimale valorizzazione del capitale umano attraverso la corretta valutazione dei risultati conseguiti, assicurando la formazione e lo sviluppo professionale delle proprie risorse umane e garantendo pari opportunità alle lavoratrici e ai lavoratori; e) contrasto alle situazioni di conflitto di interessi ed ai fenomeni di corruzione e infiltrazione ad opera della criminalità organizzata; f) flessibilità e innovazione tecnologica poste a supporto dei processi gestionali, al fine di garantire nella misura massima l'efficacia e l'efficienza necessarie per la realizzazione degli obiettivi strategici dell'Agenzia; g) semplificazione dei processi di lavoro ed essenzialità dei percorsi amministrativi, chiarezza degli obiettivi assegnati a ciascuna figura professionale ed efficacia delle soluzioni organizzative da adottare, che privilegino il lavoro per processi e di gruppo e la gestione per progetti, specie per le attività a termine di carattere innovativo e di particolare rilevanza e complessità; h) sviluppo dei sistemi informativi a supporto delle decisioni e pieno utilizzo nell'organizzazione delle potenzialità offerte dall'utilizzo delle tecnologie digitali e dei sistemi di comunicazione via web, anche in funzione della promozione dell'innovazione digitale e della facilità di accesso alle attività, all'assistenza e all'informazione da parte delle pubbliche amministrazioni, dei cittadini e delle imprese, secondo principi di cybersicurezza.*
[533] D.lgs. 30 luglio 1999, n. 300, 'Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59'.
[534] L. Casini, '*Le agenzie amministrative*', in Rivista Trimestrale di Diritto Pubblico, 2003, fasc. 2, p. 399.
[535] *Ibid,* p. 413.

amministrazione e collegio dei revisori dei conti – la cui nomina è affidata al Governo tra persone di chiara fama, comprovata capacità tecnica ed esperienza nel settore d'azione dell'agenzia.[536] Sul piano funzionale, seppur con le dovute differenze, tali agenzie svolgono compiti riconducibili ad attività di cooperazione, ricerca, consulenza e programmazione.[537] Inoltre, tutte le agenzie sono dotate di personalità giuridica di diritto pubblico, nonché di autonomia organizzativa, funzionale, contabile e regolamentare.[538] Infine, i poteri di indirizzo e controllo esercitati dal Governo sono riconducibili ad un ordinario rapporto di direzione.[539]

In secondo luogo, le agenzie sottoposte alla disciplina generale degli articoli 8[540] e 9[541] del d.lgs. n. 300/1999, sono dotate di quattro organi fondamentali: il direttore generale – la cui nomina avviene sulla base delle medesime regole previste per i capi dipartimento ministeriali – il comitato direttivo, il collegio dei revisori dei conti ed un organismo interno preposto al controllo di gestione.[542] Sotto il profilo dell'autonomia, tali agenzie sono dotate di autonomia regolamentare, di bilancio e contabile, ma non di autonomia statutaria.[543] Inoltre, con un'eccezione[544], le agenzie sono prive di personalità giuridica, con la conseguenza che non sono da considerarsi soggetti formalmente distinti dalla struttura ministeriale di riferimento.[545] Sul piano funzionale, le agenzie, differentemente dal passato[546], non svolgono più solo attività di natura meramente tecnica, ma esercitano anche funzioni di tipo operativo.[547] Infine, ai rispettivi ministeri sono riconosciuti poteri

[536] *Ibid*; F. Toth, '*La diffusione delle agenzie amministrative in Italia*', *cit.*, p. 149.
[537] L. Casini, '*Le agenzie amministrative*', *cit.*, pp. 414-415; F. Toth, '*La diffusione delle agenzie amministrative in Italia*', *cit.*, p. 149.
[538] L. Casini, '*Le agenzie amministrative*', *cit.*, pp. 413-414; F. Toth, '*La diffusione delle agenzie amministrative in Italia*', *cit.*, p. 149.
[539] L. Casini, '*Le agenzie amministrative*', *cit.*, p. 417.
[540] D.lgs. n. 300/1999, art. 8 – *L'ordinamento.*
[541] D.lgs. n. 300/1999, art. 9 – *Il personale e la dotazione finanziaria.*
[542] L. Casini, '*Le agenzie amministrative*', *cit.*, p. 419; F. Toth, '*La diffusione delle agenzie amministrative in Italia*', *cit.*, p. 150.
[543] L. Casini, '*Le agenzie amministrative*', *cit.*, p. 419-420.
[544] L'Agenzia industrie difesa è dotata di personalità giuridica di diritto pubblico. Cfr. d.lgs. n. 300/1999, art. 22.
[545] F. Toth, '*La diffusione delle agenzie amministrative in Italia*', *cit.*, p. 151.
[546] *Ibid*, p. 150.
[547] D.lgs. n. 300/1999, art. 8(1): *Le agenzie sono strutture che, secondo le previsioni del presente decreto legislativo, svolgono attività a carattere tecnico-operativo di interesse nazionale, in atto esercitate da ministeri ed enti pubblici*.

di controllo e di vigilanza sull'attività delle agenzie, che, in modo innovativo[548], sono regolati da una convenzione stipulata tra il direttore dell'agenzia ed il ministro competente.[549]

La terza ed ultima categoria comprende le agenzie fiscali che ricevono una disciplina apposita all'interno del medesimo d.lgs. n. 300/1999.[550] Tali agenzie, che rappresentano un modello ibrido[551], sono composte da un direttore – nominato con decreto del Presidente della Repubblica previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'economia e delle finanze, sentita la conferenza unificata Stato-regioni-autonomie locali[552] – dal comitato direttivo e dal collegio dei revisori dei conti.[553] Sono, altresì, dotate di personalità giuridica di diritto pubblico e di autonomia patrimoniale, organizzativa, contabile e finanziaria, regolamentare, amministrativa e, a differenza delle altre agenzie regolate dallo statuto in esame, statutaria.[554] Sotto il profilo funzionale, svolgono principalmente attività di carattere tecnico-operativo[555] per la gestione dei compiti del Ministero dell'economia e della finanze.[556] Infine, quest'ultimo, sulla base di una convenzione triennale stipulata con ciascuna agenzia fiscale, esercita poteri di indirizzo, la vigilanza, controllo e coordinamento.[557]

---

[548] L. Casini, '*Le agenzie amministrative*', *cit.*, p. 423; F. Toth, '*La diffusione delle agenzie amministrative in Italia*', *cit.*, p. 151.

[549] D.lgs. n. 300/1999, art. 8(4): *Con regolamenti* […] *sono emanati gli statuti delle agenzie istituite dal presente decreto legislativo, in conformità ai seguenti principi e criteri direttivi*: *e) definizione, tramite una apposita convenzione da stipularsi tra il ministro competente e il direttore generale dell'agenzia, degli obiettivi specificamente attribuiti a questa ultima, nell'ambito della missione ad essa affidata dalla legge; dei risultati attesi in un arco temporale determinato; dell'entità e delle modalità dei finanziamenti da accordare all'agenzia stessa; delle strategie per il miglioramento dei servizi; delle modalità di verifica dei risultati di gestione; delle modalità necessarie ad assicurare al ministero competente la conoscenza dei fattori gestionali interni all'agenzia, quali l'organizzazione, i processi e l'uso delle risorse.*

[550] D.lgs. n. 300/1999, capo II, sezione II – *Le agenzie fiscale.*

[551] F. Toth, '*La diffusione delle agenzie amministrative in Italia'*, *cit.*, p. 152.

[552] D.lgs. n. 300/1999, art. 67(2) – *Organi.*

[553] L. Casini, '*Le agenzie amministrative'*, *cit.*, p. 424; F. Toth, '*La diffusione delle agenzie amministrative in Italia'*, *cit.*, p. 152.

[554] L. Casini, '*Le agenzie amministrative'*, *cit.*, pp. 424-425.

[555] F. Toth, '*La diffusione delle agenzie amministrative in Italia'*, *cit.*, p. 153.

[556] D.lgs. n. 300/1999, art. 57(1): *Per la gestione delle funzioni esercitate dai dipartimenti delle entrate, delle dogane, del territorio e di quelle connesse svolte da altri uffici del ministero sono istituite l'agenzia delle entrate, l'agenzia delle dogane e dei monopoli e l'agenzia del demanio, di seguito denominate agenzie fiscali. Alle agenzie fiscali sono trasferiti i relativi rapporti giuridici, poteri e competenze che vengono esercitate secondo la disciplina dell'organizzazione interna di ciascuna agenzia.*

[557] D.lgs. n. 300/1999, art. 59(2): *Il ministro e ciascuna agenzia, sulla base del documento di indirizzo, stipulano una convenzione triennale, con adeguamento annuale per ciascun esercizio*

Ciascuno dei modelli fino a qui esaminati, connotato da differenti organizzazioni strutturali, funzioni e rapporti con il Governo, ha una natura giuridica differente. Infatti, le agenzie che precedono il decreto esaminato sono riconducibili alla categoria degli enti pubblici, più precisamente degli "*enti non territoriali e non economici, a struttura istituzionale, dotati di autonomia funzionale per lo svolgimento di attività tecniche*".[558] Le agenzie disciplinate dagli articoli 8 e 9 del decreto, invece, poiché prive di personalità giuridica, possono essere inquadrate nella categoria dell'ufficio-agenzia, rappresentando "*un grado di separazione organizzativa dal ministero più accentuato rispetto alle amministrazioni autonome, ma senza il 'salto istituzionale' della costituzione come distinti soggetti, cioè come enti pubblici*".[559] Infine, le agenzie fiscali, alla luce della personalità giuridica di cui sono munite e della natura negoziale della principale fonte di disciplina con il ministero, sono qualificabili come agenzie-ente pubblico.[560]

Una volta delineato il contesto di riferimento, è possibile esaminare la natura dell'Agenzia per la cybersicurezza nazionale, la quale, ai sensi del decreto istitutivo, "*ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal presente decreto*"[561].

Un primo orientamento dottrinale evidenzia come l'ACN non si inserisca nel modello delle agenzie delineato dal d.lgs. n. 300/1999, non richiamandone le disposizioni e non essendo prevista la stipulazione di convenzioni con le amministrazioni di riferimento.[562] In questa prospettiva, l'ACN ha un carattere speciale, essendo dotata di "*una più marcata autonomia rispetto ad altre*

finanziario, con la quale vengono fissati: a) i servizi dovuti e gli obiettivi da raggiungere; b) le direttive generali sui criteri della gestione ed i vincoli da rispettare; c) le strategie per il miglioramento; d) le risorse disponibili; e) gli indicatori ed i parametri in base ai quali misurare l'andamento della gestione.

[558] L. Casini, '*Le agenzie amministrative*', *cit.*, p. 444.

[559] *Ibid*, p. 446.

[560] *Ibid,* pp 448-453.

[561] Decreto-legge n. 82/2021, art. 5(2).

[562] Documentazione parlamentare, Dossier '*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*', 22 giugno 2021, pp. 15-16.

agenzie"[563] e, avendo, al pari delle agenzie fiscali, una personalità giuridica di diritto pubblico.[564]

Una seconda lettura dottrinale, invece, alla luce del rapporto di sovraordinazione della Presidenza del Consiglio dei Ministri[565] e dell'autonomia, nei fatti, fortemente limitata dell'ACN[566], qualifica quest'ultima come *ente strumentale*.[567] Infatti, l'autonomia è largamente ridimensionata da una rete di meccanismi di controllo, esercitati direttamente dalla Presidenza del Consiglio dei Ministri.[568] Più nello specifico, il Presidente del Consiglio, oltre a nominare i vertici dell'Agenzia, impartisce direttive e adotta ogni disposizione necessaria a regolarne l'organizzazione e il funzionamento.[569] In ambito contabile e finanziario, nonostante l'Agenzia disponga di un bilancio autonomo e di proprie entrate, lo stanziamento annuale è stabilito dal Presidente del Consiglio, previa comunicazione al COPASIR.[570] Inoltre, il regolamento di contabilità, proposto dal Direttore generale, è adottato con decreto del Presidente del Consiglio e, sebbene esso possa derogare alle norme generali di contabilità, resta vincolato all'approvazione dei bilanci da parte del Presidente del Consiglio e al controllo della Corte dei conti.[571] L'attività contrattuale e la disciplina del personale sono regolate, anche in forma derogatoria rispetto alla normativa generale, da appositi regolamenti adottati, anch'essi, con decreti del Presidente del Consiglio.[572] Tali "*ipotesi di etero-determinazione, previste dal decreto-legge a favore del Presidente del Consiglio, riducono i margini di autonomia effettivamente spettanti all'Agenzia rispetto a quelli di cui, ad una prima analisi, essa potrebbe apparire dotata*".[573] Pensiero, quest'ultimo, rafforzato dalla carenza di autonomia statutaria e dall'impossibilità di regolare contrattualmente i rapporti con l'amministrazione di riferimento attraverso

[563] *Ibid,* p. 16.
[564] *Ibid.*
[565] L. Parona, '*L'istituzione dell'Agenzia per la cybersicurezza nazionale*', in *Giornale di diritto amministrativo*, 2021, fasc. 6, pp. 714-716.
[566] *Ibid*, p. 714.
[567] *Ibid*, p. 716.
[568] *Ibid*, p. 713-714.
[569] *Ibid,* p. 713.
[570] *Ibid.*
[571] *Ibid.*
[572] *Ibid,* pp. 713-714.
[573] *Ibid,* p. 714.

una convenzione.[574] Tutti questi elementi, uniti al fatto che l'ACN è dotata di personalità giuridica, non permettono di ricondurre l'agenzia in esame nel novero dell'agenzie del modello generale del d.lgs. n. 300/1999[575], bensì porterebbero, come anticipato, a qualificare l'Agenzia come un ente strumentale, "*similarmente alle agenzie di più risalente istituzione*".[576]

A questa linea interpretativa si affianca una terza ricostruzione che propone di qualificare l'Agenzia come un vero e proprio "*tertium genus*".[577] Si tratterebbe, seconda questa prospettiva, di una figura normativa nuova, non assimilabile a quella prevista per le altre agenzie, ma con una struttura organizzativa ispirata al modello delle agenzie[578], istituite con legge n. 124/2007[579], che formano il Sistema di informazione per la sicurezza della Repubblica italiana.[580] Tale impostazione trova conferma nella previsione di una vigilanza specifica da parte del COPASIR – lo stesso Comitato che vigila sull'attività del Sistema di informazione per la sicurezza della Repubblica – che ne riceve la relazione annuale, ne valuta i regolamenti e può convocarne il Direttore generale.[581]

Dunque, pur non essendovi una visione unitaria sulla questione, vi è convergenza su un punto essenziale: l'ACN è un soggetto amministrativo atipico, con una natura giuridica concepita per garantire flessibilità, specializzazione e operatività nelle rilevanti funzioni di tutela della sicurezza nazionale ad essa attribuite.

---

[574] *Ibid.*
[575] *Ibid,* p. 715-716.
[576] *Ibid*, p. 716.
[577] C. Meloni, '*La nuova architettura di cybersicurezza in Italia*', in La Comunicazione – Note Recensioni e Notizie, Pubblicazione della Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica – Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, 2023, vol. 67, p. 216.
[578] Dipartimento delle informazioni per la sicurezza (DIS), Agenzia informazioni e sicurezza esterna (AISE), Agenzia informazioni e sicurezza interna (AISI). Cfr. Legge 3 agosto 2007, n. 124, artt. 4, 6 e 7.
[579] Legge 3 agosto 2007, n. 124, 'Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto'.
[580] C. Meloni, '*La nuova architettura di cybersicurezza in Italia*', *cit*., p. 217.
[581] *Ibid*.

4. Sicurezza cibernetica e pubblica amministrazione

Il processo di digitalizzazione della pubblica amministrazione[582] richiede notevoli sforzi anche sul piano della sicurezza e protezione dei dati trattati e conservati dall'apparato amministrativo, nonché dell'attività esercitata. Infatti, numerosi sono stati gli interventi mirati a definire le strategie per la sicurezza cibernetica della pubblica amministrazione.[583]

In tal senso, il Presidente del Consiglio dei Ministri ha emanato due direttive rivolte alle pubbliche amministrazioni: la prima, del 6 luglio 2023[584], è indirizzata alle pubbliche amministrazioni di cui al d.lgs. 165/2001[585]; la seconda, del 29 dicembre 2023[586], ha come destinatari esclusivi i Ministeri.[587]

La direttiva del luglio 2023 stabilisce, tra le altre cose, l'obbligo in capo alle amministrazioni di collaborare efficacemente e tempestivamente con l'ACN e CSIRT per la gestione di incidenti, minacce e crisi di natura cibernetica, pena l'irrogazione di sanzioni pecuniarie o detentive.[588] Tale obbligo – che si sostanzia anche nel garantire l'accesso ai locali e ai sistemi per l'intera durata delle operazioni – si estende anche a società *in house* o a controllo pubblico che gestiscono i sistemi informativi delle amministrazioni.[589]

La seconda direttiva del 29 dicembre 2023, coinvolgendo il vertice dell'amministrazione e non solo la dirigenza tecnica, impone a ciascun Ministro, d'intesa con il vertice dell'ACN, di sottoscrivere un protocollo in cui si definisce un modello operativo per migliorare la capacità reattiva della pubblica amministrazione in caso di incidente informatico, al fine di contenerne e mitigarne

---

[582] Si veda *supra* capitolo II.
[583] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', in Rivista italiana di informatica e diritto, 2024, fasc. 2, pp. 94-113.
[584] Direttiva del Presidente del Consiglio dei ministri, 'Indirizzi di coordinamento e organizzazione volti a promuovere la gestione adeguata e coordinata delle minacce informatiche, degli incidenti e delle situazioni di crisi di natura cibernetica', 6 luglio 2023, G.U. n.184 del 08 agosto 2023.
[585] D.lgs. 30 marzo 2001, n. 165, 'Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche'.
[586] Direttiva del Presidente del Consiglio dei ministri, 'Resilienza cibernetica del Paese – Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici', 29 dicembre 2023, G.U. n.39 del 16 febbraio 2024.
[587] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 95.
[588] *Ibid*, p. 96.
[589] *Ibid.*

gli effetti.[590] La direttiva, infatti, fornisce istruzioni tecnico-organizzative, riconducibili a quattro punti fondamentali: mappatura degli *asset* digitali e dei flussi informativi, attribuzione formale di ruoli e referenti per la cybersicurezza, pianificazione della gestione del rischio cibernetico e definizione di un piano operativo di risposta agli incidenti.[591]

Ulteriori obblighi sono stati introdotti dalla legge n. 90/2024, il cui ambito di applicazione comprende amministrazioni centrali elencate nella lista S.13 ISTAT[592]; enti locali con popolazione superiore a 100.000 abitanti o capoluoghi di regione; aziende sanitarie locali; società di trasporto urbano o extraurbano operanti nelle città metropolitane; società *in house* che gestiscono servizi informatici, di trasporto, o legati alla gestione dei rifiuti e delle acque reflue.[593]

---

[590] *Ibid,* p. 97.

[591] Direttiva del Presidente del Consiglio dei ministri, 29 dicembre 2023: "*Onde far sì che il meccanismo collaborativo possa esprimere in caso di incidente la massima efficacia, è necessaria la preventiva messa in opera, ovvero implementazione, da parte dei soggetti pubblici interessati, di alcune indispensabili misure che di seguito vengono indicate e, nello specifico, di: un censimento dei sistemi, apparati, piattaforme, applicazioni e flussi di dati utilizzati nello svolgimento delle proprie attività, oltre che dei fornitori e/o partner terzi di sistemi informatici, componenti e servizi utilizzati; un documento in cui siano definiti ruoli e responsabilità inerenti alla cybersicurezza, sia del personale interno, sia di eventuali terze parti che supportano l'amministrazione, comprensivo dell'individuazione, tra il proprio personale, di un incaricato per la cybersicurezza (quale punto di contatto cyber ai fini delle comunicazioni e del necessario raccordo con l'ACN) e di un referente tecnico per la cybersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi IT); piani per la gestione delle vulnerabilità, dei backup dei dati necessari per l'esercizio delle proprie funzioni essenziali, nonché del ciclo di vita dei sistemi, delle identità e dei relativi permessi; un piano di risposta in caso di incidente, nel quale vengano puntualmente definite le articolazioni interne che – in stretto raccordo con l'incaricato per la cybersicurezza (ove non direttamente dipendenti dallo stesso) – sono preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche, onde adeguatamente fronteggiare un incidente cibernetico.*"

[592] La legge n. 90/2024, per quanto riguarda le pubbliche amministrazioni centrali, fa riferimento alla legge n. 196/2009, la quale a sua volta rinvia all'elenco S.13. Cfr. I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 101.

[593] Legge n. 90/2024, art. 1: *1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali* […]. *Tra i soggetti di cui al presente comma sono altresì comprese le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.* […] *3. Per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende*

L'articolo 1[594] introduce importanti obblighi di segnalazione e notifica per le amministrazioni in caso di incidenti informatici.[595] In tal senso, è prevista una procedura, da effettuarsi tramite il portale ACN e seguendo la tassonomia ufficiale degli incidenti definita dalla stessa Agenzia[596], composta da due fasi: una segnalazione iniziale entro 24 ore dall'incidente e la notifica completa entro 72 ore.[597] La mancata segnalazione può comportare ispezioni e sanzioni fino a 125.000 euro, nonché responsabilità disciplinare e contabile per i funzionari e i dirigenti.[598]

Inoltre, al fine di rafforzare ed anticipare la sicurezza cibernetica, la legge, all'articolo 2[599], prevede che l'ACN possa segnalare vulnerabilità a cui le pubbliche amministrazioni sono esposte.[600] In quel caso, le amministrazioni, pena l'irrogazione di sanzioni, hanno 15 giorni per adottare gli interventi risolutivi suggeriti dalla stessa Agenzia.[601]

Sempre la legge n. 90/2024, all'articolo 8[602], impone alle pubbliche amministrazioni di dotarsi, se non già esistente, di una struttura interna dedicata alla cybersicurezza.[603] Quest'ultima provvede, tra le altre cose, alla redazione di un piano di gestione del rischio, alla definizione di ruoli e assetti organizzativi in

---

sanitarie locali e per le società in house che forniscono servizi informatici, i servizi di trasporto di cui al presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008 […].

[594] Legge n. 90/2024, art. 1 – *Obblighi di notifica di incidenti.*

[595] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 100; A. Renzi, '*Proteggere le nuove frontiere del Paese, un'analisi della nuova legge sulla cybersicurezza nazionale italiana*', in Azienditalia, 2024, fasc. 10, p. 1111.

[596] Agenzia per la cybersicurezza nazionale, '*La tassonomia cyber dell'ACN – Definizione della tassonomia cyber dell'Agenzia per la cybersicurezza nazionale*', 31 luglio 2024.

[597] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 100; A. Renzi, '*Proteggere le nuove frontiere del Paese, un'analisi della nuova legge sulla cybersicurezza nazionale italiana*', *cit*., p. 1111.

[598] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 100; A. Renzi, '*Proteggere le nuove frontiere del Paese, un'analisi della nuova legge sulla cybersicurezza nazionale italiana*', *cit*., p. 1112.

[599] Legge n. 90/2024, art. 2 – *Mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale.*

[600] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 104.

[601] *Ibid.*

[602] Legge n. 90/2024, art. 8 – *Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza*.

[603] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, p. 104; A. Renzi, '*Proteggere le nuove frontiere del Paese, un'analisi della nuova legge sulla cybersicurezza nazionale italiana*', *cit*., p. 1112.

materia di sicurezza informatica, all'attuazione delle linee guida ACN e al monitoraggio continuo delle minacce.[604] All'interno di questa struttura deve operare un referente per la cybersicurezza – figura dotata di competenze in materia di cybersicurezza – che funge da punto di contatto unico con l'ACN.[605]

Il d.lgs. n. 138/2024, con cui è stata recepita la direttiva NIS 2, amplia e rafforza gli obblighi della pubblica amministrazione. Innanzitutto, l'ambito di applicazione della disciplina è esteso a tutte le amministrazioni centrali, regionali, locali e di altro tipo elencate nell'allegato III[606] e ad altri soggetti pubblici identificati nell'allegato IV[607]. A tal riguardo, il decreto distingue tra soggetti essenziali – persona fisica o giuridica cruciale per la sicurezza informatica del Paese – e soggetti importanti, riconducendo alla prima categoria, tra gli altri, le amministrazioni centrali di cui all'allegato III (gli organi costituzionali e di rilievo costituzionale, la Presidenza del Consiglio dei ministri e i Ministeri, le Agenzie fiscali e le Autorità amministrative indipendenti)[608] e alla seconda categoria tutte le altre amministrazioni del

---

[604] Legge n. 90/2024, art. 8(1): *I soggetti di cui all'articolo 1, comma 1, individuano, ove non sia già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede: a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni; b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico; c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.*

[605] I. Macrì, '*Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR*', *cit.*, pp. 104-105; A. Renzi, '*Proteggere le nuove frontiere del Paese, un'analisi della nuova legge sulla cybersicurezza nazionale italiana*', *cit*., p. 1113.

[606] D.lgs. n. 138/2024, all. III: *1. Ai fini dell'articolo 3, comma 6, sono individuatele seguenti categorie: a) amministrazioni centrali:1) gli Organi costituzionali e di rilievo costituzionale; 2) la Presidenza del Consiglio dei ministri e i Ministeri; 3) le Agenzie fiscali; 4) le Autorità amministrative indipendenti. b) amministrazioni regionali: 1. le Regioni e le Province autonome. c) amministrazioni locali: 1. le Città metropolitane; 2. i Comuni con popolazione superiore a 100.000 abitanti; 3. i Comuni capoluoghi di regione; 4. le Aziende sanitarie locali. d) altri soggetti pubblici: 1. gli Enti di regolazione dell'attività economica; 2. gli Enti produttori di servizi economici; 3. gli Enti a struttura associativa; 4. gli Enti produttori di servizi assistenziali, ricreativi e culturali; 5. gli Enti e le Istituzioni di ricerca; 6. gli Istituti zooprofilattici sperimentali.*

[607] D.lgs. n. 138/2024, all. IV: *1. Soggetti che forniscono servizi di trasporto pubblico locale; 2. Istituti di istruzione che svolgono attività di ricerca; 3. Soggetti che svolgono attività di interesse culturale: 4. Società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175.*

[608] R. Razzante, P. Spanò, '*La NIS 2 e il decreto cybersicurezza – Le norme e gli adempimenti*', Key Editore, 2025, p. 21.

medesimo allegato[609]. Tali soggetti, al fine di "*consentire alle autorità una visione completa e tempestiva delle infrastrutture digitali e dei servizi essenziali per il funzionamento dello Stato*"[610], sono tenuti, entro il 28 febbraio di ogni anno, a registrarsi, mediante la comunicazione di una serie di dati identificativi e operativi, su una piattaforma messa a disposizione dall'ACN.[611] Quest'ultima, entro il 31 marzo di ogni anno, redige l'elenco dei soggetti essenziali e importanti e ne dà loro comunicazione.[612]

Per quanto riguarda gli obblighi, l'articolo 24[613] impone ai soggetti essenziali e importanti l'obbligo di adottare misure di sicurezza informatica, basate su una valutazione completa dei rischi, che sia in grado di rilevare vulnerabilità e monitorare minacce.[614] Deve essere, altresì, garantito l'aggiornamento costante delle misure in funzione dell'evoluzione tecnologica e normativa "*affinché siano adeguate a fronteggiare minacce in continua evoluzione*".[615] In relazione a tale obbligo, la determinazione ACN 164179 del 14 aprile 2025[616] impone ai soggetti essenziali e importanti di adottare, entro 18 mesi dalla ricezione della comunicazione di inserimento nell'elenco[617], le misure di sicurezza elencate, rispettivamente, negli allegati 2 e 1.[618]

---

[609] D.lgs. n. 138/2024, art. 6(3): *Ai fini del presente decreto, sono considerati soggetti importanti i soggetti di cui all'articolo 3 che non sono considerati essenziali ai sensi dei commi 1 e 2 del presente articolo.*

[610] R. Razzante, P. Spanò, '*La NIS 2 e il decreto cybersicurezza – Le norme e gli adempimenti*', *cit*., p. 23.

[611] *Ibid.*

[612] D.lgs. n. 138/2024, art. 7 – *Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti.*

[613] D.lgs. n. 138/2024, art. 24 – *Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica.*

[614] R. Razzante, P. Spanò, '*La NIS 2 e il decreto cybersicurezza – Le norme e gli adempimenti*', *cit*., p. 54.

[615] *Ibid,* p. 55.

[616] Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

[617] Determinazione ACN 164179 del 14 aprile 2025, art. 3(1): *Il termine per l'adozione delle misure di sicurezza di base di cui agli allegati 1 e 2 è fissato in diciotto mesi dalla ricezione, da parte del soggetto NIS della comunicazione di inserimento nell'elenco dei soggetti NIS.*

[618] Determinazione ACN 164179 del 14 aprile 2025, art. 2(2): *Le misure di sicurezza di base, a carico degli organi di amministrazione e direttivi e in materia di misure di gestione dei rischi per la sicurezza informatica, sono stabiliti: a) per i soggetti importanti, nell'allegato 1; b) per i soggetti essenziali, nell'allegato 2.*

L'articolo 25[619], invece, impone ai soggetti essenziali e importanti l'obbligo di informare tempestivamente il CSIRT Italia in caso di incidenti che abbiano un impatto significativo sulla continuità dei servizi erogati.[620] Tale obbligo deve essere assolto mediante una comunicazione preliminare entro 24 ore dalla conoscenza dell'incidente, a cui segue, entro le successive 72 ore, una notifica più completa, contenente indicazioni sulla gravità dell'incidente, il suo impatto operativo e gli eventuali indicatori di compromissione rilevati.[621] Infine, entro un mese dalla notifica dettagliata, è richiesta la redazione di una relazione conclusiva che riporti in modo articolato la dinamica dell'evento, il tipo di minaccia rilevata, le cause probabili e le misure correttive adottate.[622] In tal senso, la determinazione ACN 164179 del 14 aprile 2025, identifica, agli allegati 3 e 4, gli incidenti significativi che i soggetti importanti ed essenziali rispettivamente[623], devono notificare al CSRIT entro 9 mesi dalla ricezione della comunicazione di inserimento nell'elenco.[624]

5. Sicurezza cibernetica e contratti pubblici

La sicurezza cibernetica, acquisendo una sempre maggiore importanza negli ordinamenti contemporanei, è divenuta un fattore di particolare rilievo anche nel settore dei contratti pubblici. Infatti, il d.lgs. n. 36/2023 (nuovo Codice dei contratti pubblici) introduce due espliciti riferimenti alla cybersicurezza nella sua disciplina.

[619] D.lgs. n. 138/2024, art. 25 – *Obblighi in materia di notifica di incidente.*
[620] L. Previti, '*La nuova legge sulla cybersicurezza, un passo avanti e due indietro*', in Giornale di diritto amministrativo, 2025, fasc. 1, p. 62.
[621] *Ibid,* pp. 62-63.
[622] *Ibid,* p. 63.
[623] Determinazione ACN 164179 del 14 aprile 2025, art. 2(3): *Gli incidenti significativi di base sono stabiliti: a) per i soggetti importanti, nell'allegato 3; b) per i soggetti essenziali, nell'allegato 4.*
[624] Determinazione ACN 164179 del 14 aprile 2025, art. 3(2): *Il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi di base descritti negli allegati 3 e 4 è fissato in nove mesi dalla ricezione, da parte del soggetto NIS, della comunicazione di inserimento nell'elenco dei soggetti NIS.*

In primo luogo, l'articolo 19, comma 5[625], che rappresenta il "*manifesto di politica di cybersicurezza*"[626], prevede che le stazioni appaltanti e gli operatori economici partecipanti alle procedure di gara siano tenuti a implementare misure tecniche e organizzative interne, finalizzate ad assicurare la protezione dei dati personali e la sicurezza informatica.[627]

In secondo luogo, l'articolo 108, comma 4[628], impone che nelle procedure d'appalto di beni e servizi informatici aggiudicate secondo il criterio dell'offerta economicamente più vantaggiosa, la cybersicurezza debba rientrare tra i fattori qualitativi presi in considerazione dalle stazioni appaltanti nella valutazione dell'offerta.[629] Qualora l'impiego sia connesso alla tutela degli interessi nazionali strategici, la stazione appaltante è tenuta ad attribuirvi "*specifico e peculiare rilievo*"[630]. Più in dettaglio, le stazioni appaltanti sono tenute a contenere l'incidenza del punteggio attribuito alla componente economica dell'offerta entro il limite del 10% del totale, con la conseguenza che il peso da attribuire alla componente tecnica, tra cui gli elementi di cybersicurezza, equivale al 90% della valutazione complessiva.[631]

Dunque, da queste due norme emerge chiaramente come il legislatore abbia inteso, da un lato, rendere obbligatoria per tutte le parti coinvolte in una procedura di gara l'adozione di un assetto organizzativo dotato di adeguate misure di sicurezza

---

[625] D.lgs. n. 36/2023, art. 19(5): *Le stazioni appaltanti e gli enti concedenti, nonché gli operatori economici che partecipano alle attività e ai procedimenti di cui al comma 3, adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali. Le stazioni appaltanti e gli enti concedenti assicurano la formazione del personale addetto, garantendone il costante aggiornamento.*

[626] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', in Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche (CERIDAP), 2024, fasc. 2, p. 342.

[627] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., p. 133.

[628] D.lgs. n. 36/2023, art. 108(4): […] *Nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici. Nei casi di cui al quarto periodo, quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento.*

[629] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., p. 133.

[630] D.lgs. n. 36/2023, art. 108(4).

[631] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici', cit*., p. 342.

informatica; dall'altro, ha sancito la necessità di attribuire un ruolo rilevante alla componente di *cybersecurity* nella valutazione delle offerte relative ad appalti nel settore tecnologico.[632] Tuttavia, come sottolineato da parte della dottrina, si tratta di aspetti, nella pratica, preesistenti alla normativa introdotta nel luglio 2023, specialmente per le amministrazioni coinvolte nell'aggiudicazione di appalti in materia tecnologica.[633]

In relazione all'articolo 108 della norma in esame, la dottrina ha sollevato alcune criticità. Infatti, appare difficilmente condivisibile, specialmente trattandosi di appalti connessi alla tutela degli interessi nazionali strategici, la scelta del legislatore di considerare la cybersicurezza come un mero elemento premiale nella valutazione qualitativa dell'offerta, e non come un requisito necessario per la partecipazione alla gara.[634] Inoltre, coerentemente con le prerogative del d.lgs. n. 36/2023[635], la norma attribuisce alle stazioni appaltanti un ampio potere discrezionale nel decidere come valorizzare la cybersicurezza nella valutazione qualitativa.[636] Tuttavia, mancando qualsiasi vincolo, parametro o definizione tecnica, tale discrezionalità può sfociare in un uso arbitrario del criterio, con conseguenze distorsive nelle gare.[637] Infatti, il generico e indeterminato riferimento a concetti quali "*elementi di cybersicurezza*" o "*specifico e peculiare rilievo*" li rende suscettibili di interpretazioni divergenti.[638] Tali criticità assumono ancora maggiore rilievo poiché molte amministrazioni non sono in possesso di competenze tecniche sufficienti per attribuire correttamente un punteggio ai profili di sicurezza cibernetica, rendendo così complessa una valutazione coerente ed efficace delle offerte.[639]

---

[632] *Ibid*, p. 341.
[633] *Ibid.*
[634] T. Cocchi, '*La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza*', *cit.*, p. 197.
[635] *Ibid*, p. 198; F. Cintioli, '*Il principio del risultato nel nuovo codice dei contratti pubblici*', Relazione tenuta al convegno su "I principi nel codice dei contratti pubblici" organizzato dalla Fondazione Cesifin Alberto Predieri, in giustiziamministrativa.it, 2023, pp. 3-5.
[636] T. Cocchi, '*La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza*', *cit.*, p. 198.
[637] *Ibid.*
[638] *Ibid,* p. 197-198.
[639] *Ibid,* p. 199.

Alla luce di tali problematiche, con l'articolo 14 della legge n. 90/2024[640], il legislatore ha tentato, forse invano[641], di garantire un rafforzamento delle tutele connesse alle esigenze di cybersicurezza in materia di contratti pubblici.[642] Infatti, nonostante il riferimento all'"interesse nazionale strategico", la norma in commento non ne fornisce una definizione che permetta di definire chiaramente l'ambito di applicazione sia della disposizione stessa sia dell'art. 108 del Codice dei contratti pubblici.[643] Allo stesso modo, pur definendo "gli elementi essenziali di cybersicurezza" come "*l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo*"[644], rimane ambiguo il confine con i più generici "elementi di cybersicurezza" previsti dal d.lgs. n. 36/2023.[645] Infine, il comma 2 dell'articolo 14[646] – ad eccezione della lettera c), che, nei casi in cui si utilizzi il criterio del minor prezzo, inserisce gli elementi essenziali di cybersicurezza tra i criteri minimi dell'offerta – riproduce i contenuti dell'articolo 108 del d.lgs. n. 36/2023, senza introdurre elementi realmente innovativi.[647]

---

[640] Legge n. 90/2024, art. 14 – *Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.*

[641] L. Nannipieri, '*Cybersicurezza e appalti. Interventi legislativi e prime criticità*', in Rivista italiana di informatica e diritto, 2024, fasc. 2, pp. 74-78.

[642] *Ibid*, p. 74.

[643] *Ibid*, p. 75.

[644] Legge n. 90/2024, art. 14.

[645] L. Nannipieri, '*Cybersicurezza e appalti. Interventi legislativi e prime criticità*', *cit*., p. 76.

[646] Legge n. 90/2024, art. 14(2): *Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza: a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1; b) tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione; c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta; d) nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento.*

[647] L. Nannipieri, '*Cybersicurezza e appalti. Interventi legislativi e prime criticità*', *cit*., pp. 77-78.

Dunque, nonostante la disciplina dell'articolo 14, risulta evidente come le disposizioni del nuovo codice siano "*insufficienti a livello contenutistico*"[648], rendendone necessaria l'integrazione con norme maggiormente operative, tra cui quelle del Codice dell'amministrazione digitale.[649] Ciò permette di identificare tre diversi regimi normativi: una disciplina generale applicabile a tutte le pubbliche amministrazioni, una più specifica applicabile alle pubbliche amministrazioni ricomprese all'interno del Perimetro nazionale di sicurezza cibernetica ed, infine, una speciale relativa alle procedure di appalto aggiudicate dall'Agenzia per la cybersicurezza nazionale.[650]

5.1. La disciplina generale

La disciplina generale, applicabile a tutte le pubbliche amministrazioni, ad eccezione di quelle inserite nel Perimetro nazionale di sicurezza cibernetica, discende dal combinato disposto del nuovo Codice dei contratti pubblici, il Codice dell'amministrazione digitale e il Piano triennale per l'informatica nella pubblica amministrazione 2024–2026.[651]

Secondo il Codice dell'amministrazione digitale, l'Agenzia per l'Italia Digitale (AgID) è incaricata, tra le altre cose, di vigilare, monitorare l'applicazione del Piano triennale per l'informatica nella pubblica amministrazione[652], la cui versione attuale copre gli anni 2024–2026.[653] Tale piano prevede le "gare strategiche per la trasformazione digitale", ossia specifiche procedure di gara, disciplinate sia dal Codice dei contratti pubblici sia dal CAD[654], "*che consentono alle Amministrazioni di acquisire servizi necessari ad implementare le strategie per la trasformazione*

[648] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., p. 133.
[649] *Ibid*, pp. 133-134; S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 343.
[650] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., p. 134; S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 343.
[651] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 344.
[652] Agenzia per l'Italia Digitale, '*Piano triennale per l'informatica nella pubblica amministrazione*', Roma, dicembre 2023.
[653] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 344.
[654] *Ibid.*

digitale della Pubblica Amministrazione".[655] Da un lato, la Concessionaria Servizi Informativi Pubblici (Consip) è responsabile della gestione delle procedure di gara; dall'altro, AgID contribuisce alla definizione dei profili tecnico-informatici delle forniture.[656] In questo contesto, un ruolo particolarmente rilevante è rivestito dagli appalti relativi alla cybersicurezza, che rientrano nell'area merceologica "informatica, elettronica, telecomunicazioni e macchine per ufficio", per i quali le pubbliche amministrazioni sono obbligate a utilizzare gli strumenti messi a disposizione da Consip. Infatti, la normativa, designando Consip quale centrale di committenza nazionale in relazione al Sistema pubblico di connettività, alle reti telematiche e alla rete internazionale delle amministrazioni pubbliche[657], impedisce alle amministrazioni di procedere autonomamente a bandire e gestire gare in materia di cybersicurezza[658]. Dunque, nelle gare strategiche per la trasformazione digitale trovano applicazione gli articoli 62 e seguenti del d.lgs. n. 36/2023 che, disciplinando la centralizzazione delle committenze, prescrivono che le procedure di gara siano gestite dalle centrali di committenza, tra cui Consip[659], ovvero da specifiche stazioni appaltanti che operano per conto di altre amministrazioni aggiudicatrici.[660]

Alla luce di quanto sopra, considerato che gli appalti relativi alla cybersicurezza rientrano a pieno titolo nelle gare strategiche per la trasformazione digitale e che tali gare appartengono a un'area merceologica per la quale vige l'obbligo di utilizzo degli strumenti messi a disposizione da Consip – la quale, peraltro, riveste il ruolo di centrale di committenza nazionale per le reti telematiche delle amministrazioni pubbliche – "*allora risulta spettare proprio a Consip la predisposizione, l'indizione, la gestione e l'aggiudicazione degli appalti di cybersicurezza per l'Amministrazione Pubblica*".[661]

---

[655] Agenzia per l'Italia Digitale, '*Piano triennale per l'informatica nella pubblica amministrazione*', *cit.*, p. 38.
[656] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., p. 136.
[657] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 344.
[658] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., p. 137.
[659] D.lgs. n. 36/2023, art. 63(4).
[660] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 345.
[661] *Ibid.*

Tale attività di centralizzazione è svolta da Consip principalmente attraverso l'accordo quadro, che rappresenta lo strumento più utilizzato per gli appalti in materia di cybersicurezza.[662] Si tratta di uno strumento contrattuale di diritto pubblico che consente a una o più amministrazioni aggiudicatrici di stipulare un'intesa con uno o più operatori economici al fine di fissare, per un arco temporale determinato, le condizioni essenziali – in particolare prezzi e, ove previsto, quantità – degli appalti che saranno successivamente affidati.[663] Dunque, l'accordo quadro non costituisce una procedura di aggiudicazione[664], bensì uno strumento contrattuale, stipulato da Consip in favore di altre pubbliche amministrazioni, la cui attuazione richiede la stipula, da parte delle singole amministrazioni, di appalti specifici conformi ai termini dell'accordo.[665]

5.2. La disciplina per le pubbliche amministrazioni ricomprese nel Perimetro di sicurezza nazionale cibernetica

Le pubbliche amministrazioni ricomprese nel Perimetro di sicurezza nazionale cibernetica[666] sono soggette ad una disciplina particolare finalizzata a garantire un'elevata tutela dei sistemi informatici, imponendo requisiti di sicurezza e affidabilità per ogni strumento o componente ICT che il soggetto intenda integrare nei propri sistemi.[667]

Ai soggetti inclusi nel Perimetro, ai sensi dell'articolo 1, comma 6, del decreto-legge n. 105/2019, è, infatti, imposto l'obbligo di notificare al Centro di valutazione e certificazione nazionale (CVCN) l'intenzione di acquistare, tramite l'accordo quadro stipulato dal Consip, nuove forniture di beni, sistemi o servizi tecnologici da integrare nei propri sistemi.[668] Tale componentistica è sottoposta a specifici *test* di sicurezza e affidabilità, eseguiti dai Laboratori applicativi di prova (LAP)

[662] S. Rossa, '*Cybersicurezza e pubblica amministrazione*', *cit*., pp. 142-143.
[663] *Ibid,* p. 143.
[664] *Ibid,* p. 144.
[665] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 346.
[666] Si veda *supra* paragrafo 2.
[667] S. Poletti, '*La sicurezza cibernetica nazionale ed europea, alla luce della creazione del Perimetro di sicurezza nazionale cibernetica*', *cit.*, p. 407.
[668] *Ibid.*

accreditati presso il CVCN, e i cui esiti costituiscono condizione necessaria all'impiego delle componenti.[669] Se da un lato questa misura risulta essenziale per garantire livelli elevati di sicurezza, dall'altro determina inevitabili rallentamenti nel processo di acquisto, considerati i 45 giorni di tempo previsti per l'attività di verifica.[670] Tuttavia, è bene precisare che trascorso il termine senza che il CVCN si sia pronunciato, le amministrazioni che hanno trasmesso la comunicazione sono autorizzate a proseguire nella procedura di affidamento.[671]

5.3. Gli appalti dell'Agenzia per la cybersicurezza nazionale

La disciplina speciale – DPCM n. 166/2022[672] – prevista per gli appalti dell'Agenzia per la cybersicurezza nazionale introduce una deroga esplicita al Codice dei contratti pubblici.[673]

Il decreto in esame, prevede che, a causa della natura riservata delle attività dell'ACN, i soggetti economici interessati alla partecipazione sono tenuti a rispettare rigorosi obblighi di riservatezza, divieto di divulgazione e limitazione d'uso delle informazioni acquisite.[674] Devono inoltre dimostrare, per tutta la durata della procedura e dell'esecuzione contrattuale, tra gli altri, "*il possesso dei requisiti di idoneità professionale, la capacità economico-finanziaria e quella tecnico-professionale proporzionati all'oggetto dell'appalto*"[675].

Le gare, ai sensi dell'articolo 13, possono essere indette mediante una delle cinque procedure individuate: affidamento diretto, procedura negoziata, accordo quadro, dialogo competitivo o partenariato pubblico-privato.[676] L'affidamento diretto è ammesso per importi inferiori a € 139.000 per servizi e forniture, e a €

[669] *Ibid.*
[670] *Ibid*, pp. 407-408.
[671] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 349.
[672] Decreto del Presidente del Consiglio dei ministri, 1° settembre 2022, n. 166, 'Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico'.
[673] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 350.
[674] *Ibid.*
[675] DPCM n. 166/2022, art. 8(1)(b).
[676] DPCM n. 166/2022, art. 13 – *Procedure di scelta del contraente.*

150.000 per lavori.[677] La procedura negoziata si applica agli appalti di valore superiore, anche senza gara preliminare, purché vengano invitati almeno tre operatori selezionati.[678] Per quanto riguarda il dialogo competitivo e il partenariato pubblico-privato, trova applicazione la disciplina generale del Codice dei contratti pubblici poiché non sono previste condizioni specifiche.[679] Infine, l'accordo quadro, che per l'ACN non può avere durata superiore a nove anni, è utilizzabile solo in presenza di appalti non immediatamente quantificabili.[680] Tuttavia, a differenza del regime generale, che privilegia il ricorso agli strumenti Consip, per l'ACN tale opzione rappresenta un'eccezione. Infatti, "*l'utilizzo degli strumenti di acquisto messi a disposizione dalla società CONSIP S.p.a. è ammesso soltanto quando le condizioni e le modalità dell'appalto risultino compatibili con le esigenze di tutela della sicurezza nazionale nello spazio cibernetico e di tempestività dell'Agenzia*"[681]. Diversamente, l'Agenzia procede autonomamente alla definizione e gestione degli accordi quadro.[682]

[677] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 350.
[678] *Ibid,* pp. 350-351.
[679] *Ibid*, p. 351.
[680] *Ibid.*
[681] DPCM n. 166/2022, art. 13(2).
[682] S. Rossa, '*Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici*', *cit*., p. 351.

CONCLUSIONI

Il lavoro ha inteso dare conto del controverso dibattito in merito all'influenza delle nuove tecnologie sull'attività amministrativa.

Dopo un'attenta analisi della nozione – sia tecnica che giuridica – di intelligenza artificiale, si è esaminato il quadro regolatorio attuale. Quest'ultimo, seppur recentemente arricchito dall'adozione dell'AI Act, risulta particolarmente complesso e di difficile applicazione specialmente nell'ambito della pubblica amministrazione. Infatti, nonostante la legge n. 241/1990 e il decreto legislativo n. 82/2005 assegnino alla digitalizzazione un ruolo essenziale per il progresso organizzativo dell'amministrazione, rimangono dubbi sull'implementazione di nuove tecnologie nell'azione amministrativa.

In tal senso, come analizzato approfonditamente nel capitolo II, la normativa comunitaria e la giurisprudenza amministrativa nazionale giocano un ruolo essenziale nella ricerca di un equilibrio tra certezza del diritto e tutela effettiva degli utenti, nonché nel bilanciamento tra innovazione e regolamentazione. L'introduzione di strumenti di intelligenza artificiale nella pubblica amministrazione, dunque, non deve ridursi ad una mera adozione tecnica, ma è, invece, opportuno che, nel rispetto dei principi fondamentali dell'agire amministrativo, siano definiti i criteri e i limiti entro cui i funzionari pubblici sono legittimati ad utilizzare tali sistemi.

Per garantire un utilizzo consapevole dell'intelligenza artificiale è essenziale che i fondamentali principi di trasparenza, non esclusività della decisione automatizzata e non discriminazione siano concretamente attuati e rispettati. Infatti, nonostante gli innumerevoli vantaggi che derivano dall'implementazione delle nuove tecnologie in esame, è indispensabile che l'uomo rimanga al centro dell'attività amministrativa e che tali sistemi "intelligenti" siano utilizzati come strumenti tecnici utili all'amministrazione nelle fasi centrali del procedimento. In altre parole, è opportuno, almeno in questa fase iniziale, garantire che i provvedimenti amministrativi non siano adottati esclusivamente sulla base di sistemi algoritmici anche al fine di impedire decisioni discriminatorie.

Contestualmente, poiché la pubblica amministrazione ha il potere di adottare decisioni in grado di incidere su diritti ed interessi dei cittadini, è essenziale che il procedimento seguito per giungere a tale decisione sia conoscibile e comprensibile. Infatti, la trasparenza non deve limitarsi ad un requisito di naturale formale, ma, nonostante i problemi della *black box* o dei diritti di proprietà intellettuale sui *software*, deve concretizzarsi in un obbligo stringente per la pubblica amministrazione di motivazione delle decisioni.

Al contempo, però, come si confida di aver illustrato nel capitolo III, l'implementazione di queste nuove tecnologie nell'apparato pubblico nazionale richiede un'attenta e adeguata protezione delle infrastrutture digitali. Infatti, la tutela dello spazio cibernetico appare essenziale al fine di impedire che ogni innovazione si trasformi in una vulnerabilità.

In altre parole, la cybersicurezza non è più da intendersi in un'accezione meramente tecnica, ma come parte integrante del diritto amministrativo. Infatti, non si tratta solo di proteggere dati e reti con strumenti informatici, ma, piuttosto, ai sensi della Direttiva NIS 2 e della relativa legge di recepimento, di adempiere una serie di obblighi di natura tecnica e organizzativa per prevenire, rilevare e gestire gli incidenti informatici. Tale legame con il diritto amministrativo è dimostrato, da un lato, dall'istituzione dell'Agenzia per la cybersicurezza nazionale che, seppur dotata di una natura giuridica atipica, svolge un ruolo essenziale nella tutela della cybersicurezza nazionale e, dall'altro, dalla dettagliata e puntuale disciplina dettata in materia di contratti pubblici.

In conclusione, dunque, il ricorso all'intelligenza artificiale rappresenta una sfida per le pubbliche amministrazioni, specialmente sul piano giuridico ed istituzionale. Infatti, alla luce delle pronunce giurisprudenziali e delle nuove normative di settore, è necessario che i fondamentali principi dell'agire amministrativo siano reinterpretati affinché garantiscano trasparenza, comprensibilità e controllabilità anche in contesti automatizzati. È proprio nella tensione tra esigenza di innovazione e irrinunciabile tutela dei diritti e delle libertà fondamentali, nonché nella capacità della pubblica amministrazione di farsi promotrice di un uso dell'intelligenza artificiale che sia giuridicamente fondato,

tecnicamente sicuro e istituzionalmente responsabile, che si gioca il futuro della pubblica amministrazione “intelligente”.

BIBLIOGRAFIA

LIBRI

AVANZINI G., 'Decisioni amministrative e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intelligibilità', Editoriale scientifica, Napoli, 2019.

ASIMOV I., 'Runaround' in I, Robot, Gnome Press, 1942.

BARZANTI T., 'La normative dell'Unione europea in materia di cybersicurezza', in C. Cavaceppi e A. Contaldo (a cura di), Cybersecurity connect – La disciplina europea della Direttiva NIS2, tab edizioni, 2024.

BHATTACHARYA A., 'Applied Machine Learning Explainability Techniques', Packt Publishing, 2022.

BISHOP C.M., BISHOP H., 'Deep Learning – Foundations and Concepts', Springer Nature, 2024.

BORRUSO R., RUSSO S., TIBERI C., 'L'informatica per il giurista', Giuffrè Editore, 2009.

CENCETTI C., 'Cybersecurity: Unione europea e Italia Prospettive a confronto', Quaderni IAI, Edizioni Nuova Cultura, 2014.

COLUCCI D'AMATO L., DI PORZIO U., 'Introduzione Alla Neurobiologia: Meccanismi Di Sviluppo, Funzione e Malattia Del Sistema Nervoso Centrale', Springer, Milano, 2011.

CORMEN T.H., LEISERSON C.E., RIVEST R.L., STEIN C., 'Introduction to Algorithms', The MIT Press, Fourth edition, 2022.

D'ANGELOSANTE M., 'La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni', in S. Civitarese Matteucci, L. Torchia (a cura di), La tecnificazione, vol. 4. Firenze, Firenze University Press, 2016.

GALLONE G., ‘Riserva di umanità e funzioni amministrative’, Wolters Kluwer, 2023.

HÉNIN S., ‘AI: Intelligenza Artificiale tra incubo e sogno’, Hoepli, 2019.

KARATHANASIS A., ‘Cybersecurity and EU Law – Adopting the Network and Information Security Directive’, Routledge Research in EU Law, 2025.

LAGIOIA F., SARTOR G., ‘Il sistema COMPAS: algoritmi, previsioni, iniquità’, in U. Ruffolo (a cura di), ‘XXVI Lezioni di diritto dell’Intelligenza Artificiale’, Giappichelli, Torino, 2021.

LAURA L., ‘Breve e universale storia degli algoritmi’, Luiss University Press, 2019.

MAINI V., SABRI S., ‘Machine Learning for Humans’, 2017.

MARMO R., ‘Algoritmi per l’intelligenza artificiale – Progettazione, Machine Learning, Neural Network, Deep Learning, ChatGPT, Python’, Hoepli, 2024.

MASUCCI, A., ‘L’atto amministrativo informatico. Primi lineamenti di una ricostruzione’, Jovene, Napoli, 1993.

MITCHELL T.M., ‘Machine learning’, McGraw-Hill Higher Education, New York, 1997.

MOLNAR C., ‘Interpretable Machine Learning’, Leanpub, 2020.

PARENZO B., ‘La profilazione algoritmica nel prisma dell’autonomia privata’, Edizioni Scientifiche Italiane, 2024.

PIZZETTI F., ‘Intelligenza Artificiale, protezione dei dati personali e regolazione’, Giappichelli, 2018.

POLICE A., ‘La legge, il potere amministrativo e le situazioni giuridiche soggettive’, in G. Della Cananea, M. Dugato, B. Marchetti, A. Police, M. Ramajoli, Manuale di diritto amministrativo, Giappichelli, II edizione, 2023.

POLICE A., ‘La predeterminazione delle decisioni amministrative. Gradualità e trasparenza nell’esercizio del potere discrezionale’, Editoriale scientifica, Napoli, 1997.

POLICE A., ‘Scelta discrezionale e decisione algoritmica’, in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), Il diritto nell’era digitale persona, mercato, amministrazione, giustizia. Giuffrè, 2022.

RONCAGLIA G., ‘L’architetto e l’oracolo’, Editori Laterza, 2023.

ROSSA S., ‘Cybersicurezza e pubblica amministrazione’, Contributi di diritto amministrativo, F.G. Scoca, G. Corso, M. D’Orsogna, L. Giani, M. Immordino, A. Police, M.A. Sandulli, M.R. Spasiano (a cura di), Editoriale Scientifica Napoli, 2023.

SARTOR G., ‘L’intelligenza artificiale e il diritto’, Giappichelli, Torino, 2022.

SCHMITT M.N., ‘Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations’, Cambridge University press, 2017.

SIMONCINI A., ‘Amministrazione digitale algoritmica. Il quadro costituzionale’, in R. Cavallo Perin, D.U. Galetta (a cura di), Il diritto dell’Amministrazione Pubblica digitale, Giappichelli 2025.

SISINI F., ‘Introduzione alle reti neurali con esempi in linguaggio C’, Autopubblicazione, 2020.

STONE H.S., ‘Introduction to Computer Organization and Data Structures’, McGraw-Hill, Inc., 1971.

SUTTON R.S., BARTO A., ‘Reinforcement Learning: an Introduction’, The MIT Press, Cambridge, MA, 2018.

TORCHIA L., ‘Lo stato digitale – Una introduzione’, Il Mulino, 2023.

WECHSLER D., ‘The measurement of Adult Intelligence’, The Williams and Wilkins Company, Baltimore, 1944.

WEIZENBAUM J., ‘Computer Power and Human Reason: From Judgment to Calculation’, W. H. Freeman and Company, New York, 1976.

ZICCARDI G., ‘La cybersecurity nel quadro tecnologico (e politico) attuale’, in G. Ziccardi, P. Perri, Tecnologia e diritto, Vol. III, Informatica giuridica avanzata, Giuffrè Francis Lefebvre, Milano, 2019.

ARTICOLI E SAGGI

ARENA G., ‘Il punto sulla trasparenza amministrativa’, in Forum PA, Pubblica amministrazione aperta? Diritto di accesso e trasparenza dal 1990 ad oggi, Roma 11 maggio 2009.

BARBERIO M, ‘L’art. 30 del D.L. vo 36/2023 alla prova dell’A.I. Act dell’Unione Europea’, Relazione tenuta al Convegno di Studi presso l’Università degli Studi di Cagliari “*L’intelligenza artificiale nel diritto amministrativo*”, in giustiziamministrativa.it, 2023.

BOTTARI M., ‘Procedimento amministrativo: evoluzione digitale e i suoi sviluppi nell’era dell’intelligenza artificiale’, in Il diritto amministrativo, anno XVI, n. 03/2023.

BRAVO F., ‘Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional balancing of Interests?’, in European review of digital administration & law – Erdal, 2020, vol. 1.

BRIGHI R., CHIARA P.G., ‘La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell’Unione Europea’, in federalismi.it, 2021, fasc. 21.

BURRELL J., ‘How the machine ‘thinks’: Understanding opacity in machine learning algorithms’, Big Data & Society, 2016.

CARLONI E., ‘Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni’, in Diritto pubblico, 2019, fasc. 2.

CARLONI E., ‘I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo’, in Diritto amministrativo, 2020, fasc. 2.

CARLONI E., ‘La riforma del Codice dell’amministrazione digitale’, in Giornale di diritto amministrativo, 2011, fasc. 5.

CASINI L., ‘Le agenzia amministrative’, in Rivista Trimestrale di Diritto Pubblico, 2023, fasc. 2.

CINTIOLI F., ‘Il principio del risultato nel nuovo codice dei contratti pubblici’, Relazione tenuta al convegno su “I principi nel codice dei contratti pubblici” organizzato dalla Fondazione Cesifin Alberto Predieri, in giustiziamministrativa.it, 2023.

CIRONE E., ‘L’AI Act e l’obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali’, Quaderni AISDUE - Rivista quadrimestrale, ISSN 2975-2698, fasc. speciale 2, 2024.

COCCHI T., ‘La cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza’, in Munus – Rivista giuridica dei servizi pubblici, n.1/2024.

COLPANI O., ‘Machine Learning: la capacità di prevedere applicata alla ricerca e alla pratica clinica’, Giornale Italiano di Farmacoeconomia e Farmacoutilizzazione, vol. 11, n. 4, 2019.

D’URSO M.T., ‘Il d.d.l., di iniziativa governativa, approvato il 23 aprile 2024, sulla Intelligenza artificiale. I principi fondamentali dell’AI per il suo utilizzo in Italia, in linea con “l’AI Act” deliberato dall’UE. Le disposizioni di settore. La Strategia nazionale e le nuove agenzie istituite. La tutela per gli utenti e per il diritto d’autore e le pene per i trasgressori. Il G7 svoltosi il 13-15 giugno 2024 a Borgo Egnazia (BR) con l’intervento di Papa Bergoglio’ in Quaderni della Rivista della Corte dei Conti, n. 2/2024.

DE BENEDETTI M., 'La cybersicurezza come nuova dimensione della difesa dello Stato: bene meritorio o bene pubblico?', in federalismi.it, 2018, fasc. 9.

DEL GATTO S., 'I sistemi proprietari, l'open source e la pubblica amministrazione', in Giornale di diritto amministrativo, 2021, fasc. 5.

DI MARTINO A., 'L'amministrazione per algoritmi ed i pericoli del cambiamento in atto', in Il diritto dell'economia, 2020, fasc. 3.

DUNI G., 'L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto emanato nella forma elettronica', Relazione al convegno «L'informatica giuridica al servizio del Paese», Roma, 1-3 giugno 1978, in Rivista amministrativa della Repubblica italiana, 1978, fasc. 6, parte 1.

DURANTE N., 'La discrezionalità amministrativa ed i vizi del procedimento amministrativo, nell'epoca dell'intelligenza artificiale', rassegna di Diritto pubblico dell'economia, convegno "Intelligenza artificiale e appalti pubblici, tra capacità predittiva e discrezionalità amministrativa", Varese, 18-19 aprile 2024, in giustiziamministrativa.it, 2024.

FARINA M., 'Intellectual Property rights in the era of Italian artificial public decisions: time to collapse?', in Rivista italiana di informatica e diritto, 2023, fasc. 1.

FREEMAN K., 'Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in State v. Loomis', in North Carolina Journal of Law & Technology, 2016, XVIII.

GALETTA D.U., CORVALÁN J.G., 'Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto', in federalismi.it, 2019, fasc. 3.

GIANNINI M.S., 'Rapporto sui principali problemi dell'amministrazione dello Stato', in Il Foro italiano, vol. 102, Parte quinta: monografie e varietà, 1979.

LECUN Y., BENGIO Y., HINTON G., 'Deep learning', Nature 521, 436-444, 2015.

LIROSI A., 'L'intelligenza artificiale nel diritto amministrativo – tra riserva di umanità e necessità di garantire una maggiore efficienza amministrativa', in Quaderni della Rivista della Corte dei Conti, n. 2/2024.

LO SAPIO G., 'La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione', in federalismi.it, 2021, fasc. 16.

MACRÌ I., 'Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del PNRR', in Rivista italiana di informatica e diritto, 2024, fasc. 2.

MARONGIU D., 'Gli atti amministrativi ad elaborazione elettronica: la compilazione di un presoftware in lingua italiana', in Rivista di Diritto Amministrativo Elettronico, 2003.

McCARTHY J., 'What Is Artificial Intelligence', Stanford University, 2007.

McCULLOCH W.S., PITTS W., 'A Logical Calculus of the Ideas Immanent in Nervous Activity', The Bulletin of Mathematical Biophysics, vol. 5, 1943.

MELONI C., 'La nuova architettura di cybersicurezza in Italia', in La Comunicazione – Note Recensioni e Notizie, Pubblicazione della Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica – Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, 2023, vol. 67.

MERCURIO F., 'Il cyberspace: la sovranità nel quinto dominio', in Cammino Diritto, 30 ottobre 2024.

MORONI L., 'La governance della cybersicurezza a livello interno ed europeo: un quadro intricato', in federalismi.it, 2024, fasc. 14.

NANNIPIERI L., ‘Cybersicurezza e appalti. Interventi legislativi e prime criticità’, in Rivista italiana di diritto e informatica, 2024, fasc. 2.

NASSUATO F., ‘Legalità algoritmica nell’azione amministrativa e regime dei vizi procedimentali’, in Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche (CERIDAP), 2022, fasc. speciale 1.

NERI V., ‘AI Act e diritto amministrativo’, in Lavoro Diritti Europa, 2025, fasc. 1.

OROFINO A.G., ‘La patologia dell’atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela’, in Foro amministrativo CDS, 2002, fasc. 9.

ORSONI G., D’ORLANDO E., ‘Nuove prospettive dell’amministrazione digitale: Open data e algoritmi’, in Istituzioni del federalismo, 2019, fasc. 3.

PARONA L., ‘L’istituzione dell’Agenzia per la cybersicurezza nazionale’, in Giornale di diritto amministrativo, 2021, fasc. 6.

PEZZUTO A., ‘Evoluzione normative della sicurezza informatica nell’UE e in Italia’, in Magistra banca e finanza, 26 gennaio 2025.

POLETTI S., ‘La sicurezza cibernetica nazionale ed europea, alla luce della creazione del Perimetro di sicurezza nazionale cibernetica’, in MediaLaws, 2023, fasc. 2.

PREVITI L., ‘La nuova legge sulla cybersicurezza, un passo avanti e due indietro’, in Giornale di diritto amministrativo, 2025, fasc. 1.

RENZI A., ‘Proteggere le nuove frontiere del Paese, un’analisi della nuova legge sulla cybersicurezza nazionale italiana’, in Azienditalia, 2024, fasc. 10.

ROSSA S., ‘Appalti pubblici e cybersecurity, fra (maggior) programmaticità e (minor) operatività nella disciplina del nuovo Codice dei contratti pubblici’, in Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche (CERIDAP), 2024, fasc. 2.

ROUVROY A., ‘Of data and men. Fundamental rights and freedoms in a world of big data’, Council of Europe, Directorate general of Human Rights and Rule of Law, T-PD-BUR(2015)09REV, Strasburgo, 11 gennaio 2016.

SAITTA F., ‘Le patologie dell’atto amministrativo elettronico e il sindacato del giudice amministrativo’, in Rivista di Diritto Amministrativo Elettronico, 2003.

SAMUEL A.L., ‘Some Studies in Machine Learning Using the Game of Checkers’, IBM Journal of Research and Development 3, no. 3, luglio 1959.

SERINI F., ‘La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana’, in Rivista italiana di informatica e diritto, 2023, fasc. 2.

SERINI F., ‘La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021’, in federalismi.it, 2022, fasc. 12.

SIMONCINI A., ‘L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà’, in BioLaw Journal – Rivista di BioDiritto, 2019, fasc. 1.

SOLA A., ‘Inquadramento giuridico degli algoritmi nell’attività amministrativa, in federalismi.it, 2020, fasc. 16.

SOLA A., ‘L’automatizzazione dell’azione amministrativa’, in Amministrazione in cammino, 2020.

SOUSA E SILVA N., ‘The Artificial Intelligence Act: Critical Overview’, Social Science Research Network, 30 luglio 2024.

TADDEO M., ‘Is Cybersecurity a Public Good?’, in Minds and Machines – Journal for Artificial Intelligence, Philosophy, and Cognitive Science, 2019, vol. 29.

TOTH F., ‘La diffusione delle agenzie amministrative in Italia’, in Rivista Italiana di Politiche Pubbliche, 2007, fasc. 1.

TURING A. M., ‘Computing Machinery and Intelligence’, Mind, 59, 1950.

VIOLA L., ‘L’intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell’arte’, in federalismi.it, 2018, fasc. 21.

WEBER L., LAPUSCHKIN S., BINDER A., SAMEK W., ‘Beyond explaining: Opportunities and challenges of XAI-based model improvement’, in Information Fusion, n. 92/2023.

COMMENTO ALLA NORMATIVA

AIRIA – ASSOCIAZIONE REGOLAZIONE INTELLIGENZA ARTIFICIALE, ‘Navigare l’European AI Act’, Wolters Kluwer, Milano, 2024.

CAIA A., ‘GDPR e normativa privacy: commentario’, G.M. Riccio, G. Scorza, B. Ernesto (a cura di), Wolters Kluwer, II edizione, Assago, 2022.

CAMPANILE V., ‘Commento all’articolo 30’, in Codice dei contratti pubblici annotato articolo per articolo, C. Contessa, P. Del Vecchio (a cura di), Napoli, 2023.

IANNOTTI DELLA VALLE A., ‘Codice dei contratti pubblici commentato’, Luca R. Perfetti (a cura di), Wolters Kluwer, 2023.

PANEZI A., ‘The EU Artificial Intelligence (AI) Act: A Commentary’, N. Forgo, C. Necati Pehlivan, P. Valcke (a cura di), Kluwer Law International, 2024.

RAZZANTE R., SPANÒ P., ‘La NIS 2 e il decreto cybersicurezza – Le norme e gli adempimenti’, Key Editore, 2025.

UK Information Commissioner’s Office, ‘Feedback request – profiling and automated decision-making’, 6 aprile 2017.

VOIGT P. VON DEM BUSSCHE A., ‘The EU General Data Protection Regulation – A practical guide’, Springer Nature, 2024.

VARIE

CARETTO G., 'Intelligenza artificiale di Google batte il campione mondiale di Go', Start Magazine, 10 marzo 2016, https://www.startmag.it/innovazione/intelligenza-artificiale-google-batte-campione-mondiale-go/

DI GIACOMO L., 'Algoritmi e bias: come l'intelligenza artificiale può riprodurre o combattere i pregiudizi', Diritto.it, 23 agosto 2024, https://www.diritto.it/algoritmi-bias-intelligenza-artificiale-pregiudizi/

IBM, 'Cos'è il clustering?', 21 febbraio 2024, https://www.ibm.com/it-it/think/topics/clustering#:~:text=Il%20clustering%20%C3%A8%20un%20algoritmo,base%20a%20somiglianze%20o%20modelli.

LARSON J., MATTU S., KIRCHNER L., ANGWIN J., 'How We Analyzed the COMPAS Recidivism Algorithm', ProPublic, 23 maggio 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

LARSON J., MATTU S., KIRCHNER L., ANGWIN J., 'Machine Bias – There's software used across the country to predict future criminals. And it's biased against blacks, ProPublic, 23 maggio 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

LAUDANI V., 'L'intelligenza artificiale negli appalti pubblici: un primo caso applicativo', in Appalti&Contratti, 6 marzo 2025, https://www.appaltiecontratti.it/lintelligenza-artificiale-negli-appalti-pubblici-un-primo-caso-applicativo/

PERRIGO B., 'No One Truly Knows How AI Systems Work. A New Discovery Could Change That', Time, 21 Maggio, 2024, https://time.com/6980210/anthropic-interpretability-ai-safety-research/

PESCE G., ‘L’Europa regola i rischi dell’IA. Ma pure troppo’, L’Espresso, 10 gennaio 2025.

VANNINI R., ‘Dizionario di economia e finanza’, Treccani.

WEATHERBED J., ‘Meta won’t release its multimodal Llama AI model in the EU’, The Verge, 18 luglio 2024.

YAO D., ‘25 Years Ago Today: How Deep Blue vs. Kasparov Changed AI Forever’, AI Business, 11 maggio 2022, https://aibusiness.com/ml/25-years-ago-today-how-deep-blue-vs-kasparov-changed-ai-forever?

NORMATIVA E ATTI UFFICIALI

NORMATIVA

Italia – Leggi ed atti aventi forza di legge

Codice di procedura civile, approvato con R.D. 28 ottobre 1940, n. 1443, e successive modificazioni.

Legge 22 aprile 1941, n. 633, ‘Protezione del diritto d’autore e di altri diritti connessi al suo esercizio’.

Legge 7 agosto 1990, n. 241, ‘Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi’.

Decreto legislativo 30 luglio 1999, n. 300, ‘Riforma dell’organizzazione del Governo, a norma dell’articolo 11 della legge 15 marzo 1997, n. 59’.

Decreto legislativo 30 marzo 2001, n. 165, ‘Norme generali sull’ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche’.

Decreto legislativo 7 marzo 2005, n. 82, ‘Codice dell’amministrazione digitale’.

Legge 3 agosto 2007, n. 124, ‘Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto’.

Decreto legislativo 2 luglio 2010, n. 104, ‘Attuazione dell'articolo 44 della legge 18 giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo’.

Decreto legislativo 18 maggio 2018, n. 65, ‘Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione’.

Decreto-legge 21 settembre 2019, n. 105, ‘Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica’.

Legge 18 novembre 2019, n. 133, ‘Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica’.

Decreto-legge 14 giugno 2021, n. 82, ‘Disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale’.

Legge 4 agosto 2021, n. 109, ‘Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale’.

Decreto legislativo 31 marzo 2023, n. 36, ‘Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici’.

Legge 28 giugno 2024, n. 90, ‘Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici’.

Decreto legislativo 4 settembre 2024, n. 138, ‘Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell’Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148’.

Disegno di legge n. 1146 – Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

Unione europea – Fonti primarie

Trattato sul funzionamento dell’Unione europea (2012) GU C 326/47.

Carta dei diritti fondamentali dell’Unione Europea (2016/C 202/02).

Unione europea – Regolamenti

Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004 che istituisce l’Agenzia europea per la sicurezza delle reti e dell’informazione.

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).

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

Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021 che istituisce il Centro europeo di competenza per la cibersicurezza nell’ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

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

Unione europea – Direttive

Direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, 8 dicembre 2008.

Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore.

Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, 6 luglio 2016.

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

Trattati internazionali

Convenzione europea dei diritti dell'uomo.

ATTI UFFICIALI E DOCUMENTI

Italia

TURATI F., in 'Atti del Parlamento italiano', Camera dei deputati, sessione 1904-1908, 17 giugno 1908, 22962.

Direttiva del Presidente del Consiglio dei ministri, Dipartimento per l'Innovazione e le Tecnologie, 'Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni', 16 gennaio 2002, G.U. n. 69 del 22 marzo 2002.

Decreto del Ministero dell'Interno, 'Individuazione delle infrastrutture critiche informatiche di interesse nazionale', 9 gennaio 2008, G.U. n. 101 del 30 aprile 2008.

Decreto del Presidente del Consiglio dei ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale', 24 gennaio 2013, G.U. n. 66 del 19 marzo 2013.

Presidenza del Consiglio dei Ministri, 'Quadro strategico nazionale per la sicurezza dello spazio cibernetico', dicembre 2013.

Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, 'Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133'.

Documentazione parlamentare, Dossier 'Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale', 22 giugno 2021.

Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, 'Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale'.

Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 224, 'Regolamento del personale dell'Agenzia per la cybersicurezza nazionale'.

Decreto del Presidente del Consiglio dei ministri, 1° settembre 2022, n. 166, 'Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico'.

AgID, ‘Strategia Italiana per l’Intelligenza Artificiale 2024-2026’.

Direttiva del Presidente del Consiglio dei ministri, ‘Indirizzi di coordinamento e organizzazione volti a promuovere la gestione adeguata e coordinata delle minacce informatiche, degli incidenti e delle situazioni di crisi di natura cibernetica’, 6 luglio 2023, G.U. n.184 del 08 agosto 2023.

Agenzia per l’Italia Digitale, ‘Piano triennale per l’informatica nella pubblica amministrazione’, Roma, dicembre 2023.

Direttiva del Presidente del Consiglio dei ministri, ‘Resilienza cibernetica del Paese – Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici’, 29 dicembre 2023, G.U. n.39 del 16 febbraio 2024.

Comunicato stampa del Consiglio dei Ministri n. 78, 23 aprile 2024.

Agenzia per la cybersicurezza nazionale, ‘La tassonomia cyber dell’ACN – Definizione della tassonomia cyber dell’Agenzia per la cybersicurezza nazionale’, 31 luglio 2024.

Determinazione 164179 del Direttore Generale dell’Agenzia per la cybersicurezza nazionale di cui all’articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all’articolo 40, comma 5, lettera l), che, ai sensi dell’articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l’adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo (14 aprile 2025).

Unione europea

Commissione delle comunità europee, ‘Creare una società dell’informazione sicura migliorando la sicurezza delle infrastrutture dell’informazione e mediante la lotta alla criminalità informatica’, Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, COM (2000) 890, 26 gennaio 2001.

Commissione delle comunità europee, 'Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo', Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni COM (2001) 298, 6 giugno 2001.

Commissione europea, 'Il ruolo dell'eGovernment per il futuro dell'Europa', Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, COM (2003) 567, 29 marzo 2003, §3.

Commissione europea, 'Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro', Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, JOIN (2013), 7 febbraio 2013.

Commissione europea, 'Piano d'azione dell'UE per l'eGovernment 2016-2020', Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, COM (2016) 179, 19 aprile 2016.

Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 6 febbraio 2018.

Commissione europea, 'Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards', (9 Marzo 2018), Comunicato stampa IP/18/1381.

Commissione europea, 'L'intelligenza artificiale per l'Europa', Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, COM (2018) 237, 25 Aprile 2018.

Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, 'Manuale sul diritto europeo in materia di protezione dei dati', 2018.

Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, 'Una definizione di IA: principali capacità e discipline scientifiche', Bruxelles, aprile 2019.

Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, 'Orientamenti etici per un'IA affidabile', Bruxelles, aprile 2019.

Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 2021/0106, Bruxelles.

GIURISPRUDENZA

ITALIA

TAR Lazio, Sez. III-bis, 22 marzo 2017, n. 3769.

TAR Lazio, Sez. III-bis, 10 settembre 2018, n. 9224.

Consiglio di Stato, Sez. VI, 8 aprile 2019, n. 2270.

Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8472.

Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8473.

Consiglio di Stato, Sez. VI, 13 dicembre 2019, n. 8474.

Consiglio di Stato, Sez. VI, 4 febbraio 2020, n. 881.

Consiglio di Stato, Sez. V, 5 marzo 2020, n. 1604.

TAR Lazio, Sez. II, 3 marzo 2025, n. 4546.

Tribunale Ordinario di Firenze, Sez. Imprese, ordinanza 14 marzo 2025.

USA

State v. Loomis, Supreme Court of Wisconsin (881 N.W.2d 749), 2016.