RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0283 • articolo sottoposto a peer review • pubblicato in anteprima il 15 lug. 2026

Benedetto Ponti

Il tool ACOI per lo screening del conflitto d'interessi e il *gap* italiano da colmare nei sistemi AI di prevenzione della corruzione

Il saggio, attraverso lo studio di caso del progetto PNRR "ACOI-*Assessing Conflicts of Interest*", esamina le condizioni che renderebbero un sistema AI anticorruzione operativo nell'ordinamento italiano. ACOI — sviluppato in partnership dall'Università di Perugia e da Transcrime (Università Cattolica del Sacro Cuore), in collaborazione con il Ministero dell'Interno — ha verificato empiricamente la praticabilità tecnica di uno strumento di screening automatizzato del conflitto d'interessi su un campione di 485 dirigenti pubblici, incrociando dati di ANPR, Registro delle Imprese, Catasto e Orbis, confermando la fattibilità del modello. L'analisi individua tuttavia le condizioni abilitanti necessarie per il passaggio dalla sperimentazione all'operatività sistematica: sul piano normativo, la designazione legislativa delle banche dati autorizzate e la specificazione del trattamento AI secondo il requisito di legalità funzionale (art. 2-*ter* Codice privacy); sul piano giuridico-infrastrutturale, l'accesso strutturato attraverso la PDND; sul piano tecnico, la conformità ai requisiti AI Act per i sistemi ad alto rischio, pseudonimizzazione embedded e supervisione umana degli alert. La conclusione – anche in prospettiva comparata internazionale – è che il gap italiano non è tecnologico ma normativo e organizzativo, e che colmarlo costituisce oramai un dovere imposto dalla Direttiva (UE) 2026/1021 sulla prevenzione e il contrasto della corruzione.

Anticorruzione – Intelligenza artificiale – Conflitto d'interessi – Screening automatizzato – ACOI

The ACOI tool for conflict-of-interest screening and the Italian gap to be closed in AI-based corruption prevention systems

This article examines, through the case study of the PNRR project "ACOI – Assessing Conflicts of Interest", the conditions that would make an AI-based conflict-of-interest prevention system operationally viable in Italy. ACOI — developed in partnership by the University of Perugia and Transcrime (Università Cattolica del Sacro Cuore), in collaboration with the Ministry of the Interior — empirically tested an automated screening tool on 485 public managers, cross-referencing data from the National Population Register, the Companies Register, the Land Registry, and Orbis, confirming the model's feasibility. The analysis identifies the enabling conditions still required for the transition to systematic operation: legislative designation of authorised data sources and specification of AI-based processing under the functional legality standard (Art. 2-ter Privacy Code); structured access through the National Digital Data Platform (PDND); and compliance with AI Act requirements for high-risk systems, including embedded pseudonymisation and meaningful human oversight. The conclusion — also from a comparative perspective — is that Italy's gap is not technological but normative and organisational, and that closing it is an obligation imposed by Directive (EU) 2026/1021 on the prevention and combating of corruption.

Anti-corruption – Artificial intelligence – Conflict of interest – Automated screening – ACOI

L'Autore è professore associato di Diritto amministrativo nell'Università degli studi di Perugia

Introduzione

La governance dei dati[1] si configura come uno degli snodi fondamentali affinché il patrimonio informativo pubblico possa essere pienamente sfruttato, entro il nuovo paradigma abilitato dalle intelligenze artificiali. La letteratura internazionale documenta con crescente sistematicità l'impiego di sistemi algoritmici nella prevenzione della corruzione: sistemi di machine learning analizzano in tempo reale le procedure di affidamento dei contratti pubblici in Brasile, in Ucraina e in Portogallo; modelli predittivi stimano la probabilità di manipolazione delle gare prima che queste vengano aggiudicate; strumenti di elaborazione del linguaggio naturale processano decine di migliaia di segnalazioni di operazioni sospette nell'arco di settimane che un ufficio tradizionale impiegherebbe anni a gestire; immagini satellitari elaborate con algoritmi di computer vision rilevano il disboscamento illegale con mesi di anticipo e con un'accuratezza che non ha precedenti nella storia del monitoraggio ambientale[2].

Eppure l'Italia – che dispone di un'architettura normativa anticorruzione tra le più articolate d'Europa, di patrimoni informativi pubblici di straordinaria ricchezza e di infrastrutture di interoperabilità in fase di implementazione, grazie agli investimenti del PNRR – sconta un ritardo

1. Il presente contributo è stato realizzato anche sulla scorta dei risultati del progetto di ricerca "Assessing conflict of interest – ACOI", finanziato dall'Unione europea – NextGenerationEU, Missione 4 "Istruzione e ricerca", Componente 2 "Dalla ricerca all'impresa", Investimento 1.1 – PRIN 2022 PNRR, progetto P2022JSLZW, CUP J53D23018880001. Università degli Studi di Perugia (resp. Benedetto Ponti, PI di progetto) e Università Cattolica del Sacro Cuore di Milano (resp. Francesco Calderoni).

2. Resimić 2025.

sistematico nell'integrazione degli strumenti digitali avanzati a supporto dei meccanismi di prevenzione. Questo ritardo non si spiega (solo) con l'assenza di risorse o con una carenza di competenze tecniche disponibili nel sistema pubblico: si spiega, anche, se non soprattutto, con l'assenza di un'architettura normativa e istituzionale che definisca con sufficiente chiarezza le condizioni alle quali i dati pubblici e, tra questi i dati personali, detenuti dalle diverse amministrazioni possono essere integrati, messi in relazione e analizzati con strumenti AI a fini di prevenzione della corruzione[3].

Il presente saggio si propone un obiettivo duplice. Sul primo versante, intende offrire una ricognizione sistematica delle applicazioni internazionali dell'AI nell'anticorruzione, organizzata lungo due assi analitici: quello della maturità delle applicazioni – distinguendo tra sistemi già operativi in contesti reali con risultati misurabili e sistemi ancora sperimentali con significative incertezze non risolte – e quello del tipo di contributo epistemico offerto, poiché non tutte le applicazioni AI producono lo stesso tipo di conoscenza e le implicazioni istituzionali, giuridiche e di governance cambiano notevolmente a seconda del contributo in gioco. Tale ricognizione è utile per verificare il gap accumulato in sede nazionale riguardo alle applicazioni di AI dedicate all'anticorruzione, anche con riferimento alle soluzioni più mature e consolidate. Sul secondo versante, il saggio intende analizzare il sistema italiano di governance dei dati nelle sue articolazioni di forza e di debolezza rispetto alle esigenze che l'impiego dell'AI nella prevenzione della corruzione pone: i vincoli derivanti dalla tutela dei dati personali alla loro circolazione integrata tra banche dati pubbliche; le opportunità aperte dall'infrastruttura di interoperabilità abilitata dagli investimenti del PNRR attraverso la Piattaforma Digitale Nazionale dei Dati (PDND); i rischi connessi all'impiego dell'AI nell'azione pubblica, anche alla luce del Regolamento (UE) 2024/1689 (AI Act) e della legge 9 luglio 2025, n. 132.

La chiave di lettura che permea il saggio muove dalla constatazione che il nodo problematico principale non è tecnologico ma giuridico-istituzionale: l'Italia dispone delle infrastrutture informatiche e del patrimonio di dati necessari per costruire sistemi AI anticorruzione di alto profilo, ma non dispone ancora dell'architettura normativa di governance che renderebbe questi sistemi praticabili a regime. Colmare questo gap non è soltanto un'opportunità di policy: è una necessità imposta dal diritto sovranazionale ed eurounitario, tenuto conto in particolare degli impegni derivanti dalla recente direttiva Ue sulla prevenzione e il contrasto della corruzione che richiede agli Stati membri di dotarsi di misure efficaci di prevenzione, presidiate da organismi dotati delle risorse finanziarie, di staff e tecnologiche necessarie a renderle effettive[4].

Il saggio si è articolato in tre parti. La prima parte offre la mappa comparata: una tassonomia dei contributi epistemici dell'AI all'anticorruzione (§1) e una ricognizione delle applicazioni mature (§2) e sperimentali (§3). La seconda parte analizza la governance dei dati in Italia: i vincoli della tutela dei dati personali (§4), le opportunità della PDND (§5) e il quadro regolatorio dell'AI (§6). La terza parte traduce la ricognizione comparata in analisi del gap italiano su un piano generale (§7) e attraverso uno studio di caso specifico – il progetto di ricerca ACOI sullo screening automatizzato dei conflitti di interesse (§8) – che consente di apprezzare in termini concreti le condizioni giuridiche per l'implementazione sistematica di un sistema AI anticorruzione nell'ordinamento italiano.

Parte prima. L'AI nell'anticorruzione: una mappa comparata

1. I contributi epistemici dell'AI alla prevenzione della corruzione

Prima di analizzare settori e gradi di maturità, è necessario comprendere che cosa fa l'intelligenza artificiale in termini di produzione di conoscenza. Le applicazioni AI di anticorruzione non sono tutte epistemicamente equivalenti, e distinguerle tra loro secondo questo parametro è importante. Infatti, i rischi, i requisiti istituzionali e le implicazioni giuridiche cambiano radicalmente a seconda del tipo di contributo epistemico in gioco. Si identificano di seguito sette tipologie, che attraversano

3. APEC 2025; v. anche la tassonomia "prevention, detection, sanction" adottata come framework di riferimento.
4. Direttiva (UE) 2026/1021, del 29 aprile 2026, sulla lotta contro la corruzione. Per il profilo della verifica del conflitto di interessi nel testo della direttiva, cfr. Ponti 2026.

trasversalmente i vari settori interessati e i diversi livelli di maturità, e costituiscono una chiave di lettura preliminare all'analisi svolta nel saggio[5].

1.1. L'estensione volumetrica

Il contributo più accessibile e al tempo stesso più diffuso è quello che potremmo definire di estensione volumetrica: l'AI processa volumi di dati – documenti, transazioni, segnalazioni, dichiarazioni, atti amministrativi – che nessuna struttura di controllo umana potrebbe gestire con le risorse ordinarie. La quantità, in questo contesto, genera qualità: un sistema di controllo che esamina il 100% delle gare, anziché un campione del 3%, non è semplicemente più efficiente, ma produce un tipo diverso di evidenza, statisticamente e giuridicamente più robusta[6].

I casi documentati sono significativi. Transparency International UK ha classificato con strumenti di machine learning oltre 140.000 voci del registro del lobbying britannico, costruendo per la prima volta una mappa sistematica delle reti di influenza sui processi legislativi. In Perù, il sistema Inspector AI elabora in un anno circa 23.000 segnalazioni di operazioni sospette (SARs), un volume che i revisori umani dell'UIF peruviana non avrebbero mai potuto processare con tempi comparabili. Nel procedimento contro Rolls-Royce condotto dallo Serious Fraud Office britannico (SFO), strumenti AI hanno esaminato un corpus documentale di milioni di pagine, consentendo di ridurre i tempi di analisi preliminare da anni a mesi[7].

Il limite epistemico di questo tipo di contributo è tuttavia altrettanto preciso quanto la sua forza. L'estensione volumetrica replica e amplifica il giudizio umano: se i criteri di classificazione sono sbagliati – se il modello ha imparato a riconoscere le forme di corruzione già identificate nel passato, anziché la corruzione effettiva – li applica a milioni di casi invece che a mille, moltiplicando l'errore sistematico anziché correggerlo. Il problema, che la letteratura specialistica denomina *selective labelling problem*, non è tecnico ma epistemologico: riguarda la qualità della conoscenza di partenza su cui il sistema viene addestrato, non la potenza computazionale con cui viene applicato[8].

1.2. Il rilevamento di anomalie statistiche

Il secondo tipo di contributo è quello del rilevamento di anomalie statistiche: il sistema apprende la distribuzione statistica di un fenomeno – gare d'appalto, rimborsi spese, concessioni, pratiche edilizie – e segnala le deviazioni significative rispetto alla norma. A differenza di un sistema basato su regole scritte da esperti, che i soggetti corrotti imparano rapidamente ad aggirare modificando i comportamenti che attivano gli alert, il modello statistico non ha una teoria della corruzione: ha una teoria della normalità, e segnala tutto ciò che si discosta da essa in modo statisticamente rilevante. Questa neutralità statistica costituisce al tempo stesso il punto di forza e il punto di debolezza del contributo[9].

In Brasile, il sistema Rosie – sviluppato dall'organizzazione civica Operação Serenata de Amor – applica algoritmi di machine learning alle note spese dei parlamentari: il solo effetto di pubblicazione degli alert ha prodotto una riduzione del 10% nelle richieste di rimborso per pasti, senza che

5. L'impianto analitico basato sulle sette tipologie di contributo epistemico è sviluppato, nella letteratura internazionale, a partire dalla distinzione tra usi "banali" e usi qualitativamente caratterizzati dell'AI proposta in Resimić 2025; e Zinnbauer 2025. Cfr. anche APEC 2025; OECD 2025-a.
6. Resimić 2025, dove l'Autore utilizza l'espressione "mundane uses of AI" per designare le applicazioni di estensione volumetrica, avvertendo tuttavia che la denominazione è fuorviante: "the quality of evidence changes when you achieve 100% coverage instead of sampling".
7. Il sistema Inspector AI è documentato in GIZ 2024; cfr. anche Resimić 2025. Per il caso Rolls-Royce/SFO e il ricorso a strumenti AI per l'e-discovery su corpus documentali di milioni di pagine, cfr. OpenText 2018; APEC 2025.
8. Sul selective labelling problem come limite epistemologico strutturale delle applicazioni ML anticorruzione cfr. Ash–Galletta–Giommoni 2025; Gallego–Rivero–Martínez 2021; v. anche Gerli 2026.
9. I dati sul sistema Rosie (riduzione del 10% nelle richieste di rimborso per pasti) sono documentati in Odilla 2023; cfr. anche Odilla–Mattoni 2023. Per DOZORRO e il risparmio stimato di 133 milioni di UAH nel primo semestre 2025, cfr. Resimić 2025.

fosse necessario alcun procedimento sanzionatorio. In Ucraina, il sistema DOZORRO – integrato nella piattaforma di e-procurement Prozorro – ha prevenuto nel primo semestre del 2025 sprechi stimati in 133 milioni di UAH, rilevando pattern anomali nelle procedure di affidamento. In Ungheria, modelli di machine learning applicati alle gare pubbliche hanno raggiunto un'accuratezza dell'82% nella previsione delle offerte singole prima della loro pubblicazione, partendo dall'accuratezza di base del 77% dei sistemi a regole fisse.

Il tratto epistemico specifico di questo contributo – la neutralità statistica – si traduce in un deficit di interpretabilità che pone questioni di legittimità giuridica non trascurabili: il sistema non spiega perché qualcosa è anomalo, ma solo che lo è. Questa opacità è meno grave quando il modello viene usato per selezionare fascicoli da approfondire, ma diventa molto problematica quando l'alert produce effetti diretti su soggetti specifici, perché priva il destinatario della possibilità di comprendere e contestare le ragioni della segnalazione. I modelli più interpretabili tendono a essere meno accurati, e i più accurati meno interpretabili, generando un trade-off che non è tecnico ma politico: riguarda quanto rischio di opacità si è disposti ad accettare in cambio di prestazioni migliori, e la risposta a questa domanda non può essere delegata alla tecnologia[10].

1.3. La sintesi di conoscenza eterogenea

Il terzo tipo di contributo è forse il più potente sul piano epistemico: la sintesi di conoscenza eterogenea, ossia la capacità di mettere in connessione archivi separati – registro delle imprese, catasto, dati fiscali, banche dati dei contratti pubblici, anagrafi degli eletti, registri del credito – e di generare, dall'incrocio, conoscenza che non preesisteva in nessuna delle fonti originali. Si tratta di un contributo qualitativamente diverso dall'amplificazione: non si tratta di fare più velocemente ciò che un funzionario potrebbe fare in linea di principio, ma di produrre connessioni che, per ragioni strutturali di complessità cognitiva e di organizzazione per silos dei sistemi informativi pubblici, sarebbero impossibili da ottenere altrimenti. Il fatto che il titolare formale di un'impresa aggiudicataria sia il cognato di un funzionario che ha presieduto la commissione, che un immobile non dichiarato nelle disclosure patrimoniali appaia nel catasto, che una società offshore sia la stessa già oggetto di un'indagine penale in un'altra giurisdizione: nessuna di queste informazioni è segreta, ma tutte rimangono invisibili finché non vengono messe in relazione.

I casi documentati illustrano la portata di questo contributo. Il sistema cinese Zero Trust – che suscita comprensibili perplessità sul piano della governance e dei diritti fondamentali – incrocia più di 150 banche dati per monitorare oltre 8.700 funzionari pubblici, producendo connessioni che nessun ufficio ispettivo tradizionale potrebbe costruire. Secondo il final report del progetto DATACROS, coordinato da Transcrime e cofinanziato dalla Commissione europea nell'ambito dell'Internal Security Fund – Police, l'analisi ha riguardato le strutture proprietarie di oltre 56 milioni di imprese in 29 Paesi europei e il prototipo sviluppato è stato in grado di identificare correttamente fino all'83% delle imprese collegate a persone soggette a sanzioni o con precedenti penali[11].

Sul piano tecnico, questo tipo di contributo richiede un'infrastruttura che nella maggior parte dei sistemi pubblici non è ancora disponibile nella forma necessaria: data lake integrati, API interoperabili, standard tecnici comuni per la rappresentazione dei dati, regole di data governance che definiscano chi può accedere a quali dati e in quale forma. Il problema non è computazionale ma istituzionale e politico: i sistemi informativi delle amministrazioni pubbliche sono stati costruiti nel tempo per servire la singola amministrazione, non il sistema nel suo complesso, e la loro integrazione richiede non solo investimenti tecnologici ma una revisione profonda delle logiche organizzative che li governano. È

10. Sul trade-off tra interpretabilità e accuratezza dei modelli ML in ambito anticorruzione, e sulla natura politica (non meramente tecnica) di questa scelta, cfr. Köbis–Starke–Rahwan 2022; Gerli 2026. Per la letteratura sull'Explainable AI (XAI), si rinvia alla rassegna citata in Resimić 2025.

11. Sulla sintesi di conoscenza eterogenea come contributo epistemico e sull'uso di approcci data-driven per la valutazione del rischio di corruzione, cfr. OECD 2019; Parvanova 2025. Per il sistema DATACROS (I, II e III) cfr. https://www.transcrime.it/. Per il sistema cinese Zero Trust, cfr. South China Morning Post 2019 e U4 Anti-Corruption Resource Centre 2023.

precisamente questo il nodo che il sistema italiano di governance dei dati deve sciogliere.

1.4. La topologia delle reti corruttive

Il quarto tipo di contributo va oltre la sintesi eterogenea: non si limita a identificare singole connessioni anomale, ma rivela la struttura – la topologia – di reti corruttive. Chi occupa posizioni centrali, quali nodi fungono da intermediari obbligati, dove si concentra il controllo sull'intera rete, quali sono i legami più vulnerabili la cui rimozione comporta la disgregazione del sistema: si tratta di conoscenza che non riguarda singoli episodi o singole transazioni, ma l'architettura complessiva del fenomeno corruttivo. Per ragioni strutturali di complessità cognitiva, una rete di migliaia di entità con relazioni di secondo e terzo grado è semplicemente inaccessibile all'analisi umana, anche con risorse investigative illimitate: l'AI non amplifica la capacità umana di vedere, ma la sostituisce in un dominio in cui essa non opera affatto[12].

Un caso paradigmatico è ContÁgil, sviluppato dalla Controladoria-Geral da União brasiliana nell'ambito dell'Operação Lava Jato: basato su machine learning e analisi delle reti, ha ridotto da una settimana a un'ora il tempo necessario per mappare le reti di intermediari corruttivi, consentendo agli investigatori di identificare i nodi strategici del sistema e di concentrare le risorse nei punti di massima vulnerabilità. La letteratura accademica sulla *network analysis* applicata alla corruzione documenta con rigore come colpire nodi centrali di una rete corruttiva sia sistematicamente più efficace, in termini di risorse impiegate e di effetti sulla capacità operativa del sistema, di smantellarne un numero equivalente di nodi periferici[13].

1.5. La conoscenza anticipatoria

Il quinto tipo di contributo epistemico rompe con la logica fondamentale del controllo anticorruzione tradizionale, che è sempre stato reattivo: si interviene dopo che la corruzione è avvenuta, spesso molto tempo dopo. I sistemi di *predictive analytics* producono invece conoscenza sul futuro: la probabilità che una gara non ancora aggiudicata sia soggetta a manipolazione, che un funzionario in una certa posizione sia a rischio di comportamenti scorretti, che un'area geografica con certe caratteristiche strutturali sia vulnerabile a specifiche forme di corruzione. Si tratta del tipo di contributo epistemicamente più originale – e al tempo stesso del più problematico dal punto di vista giuridico e istituzionale.

Il sistema Forest Foresight, sviluppato dall'organizzazione WWF-Paesi Bassi, predice con sei mesi di anticipo e 80% di accuratezza dove avverrà disboscamento illegale su aree pilota in Gabon e nel Borneo. In Ungheria, il modello ML per la previsione delle offerte singole stima la probabilità di manipolazione prima dell'aggiudicazione, consentendo all'autorità di controllo di intervenire quando il costo dell'intervento è minimo e l'effetto massimo. In Colombia, un sistema di early warning basato su algoritmi di LASSO e gradient boosting assegna a ciascun contratto pubblico un punteggio di rischio prima che l'esecuzione inizi, permettendo di concentrare le risorse ispettive sulle situazioni più vulnerabili[14].

Il problema epistemico e giuridico centrale è che la conoscenza anticipatoria opera su probabilità, non su evidenze. Un sistema che assegna a una gara un punteggio di rischio del 90% non afferma che quella gara è corrotta: stima che gare con caratteristiche simili lo siano state nel 90% dei casi passati. L'uso di questa informazione per prendere decisioni che incidono su soggetti specifici – intensificare i controlli, sospendere un'aggiudicazione, avviare un'indagine – pone questioni delicate su quale garanzia procedurale si applica al soggetto trattato diversamente sulla base di una stima probabilistica, e come si gestisce il rischio

12. Sulla capacità dell'analisi delle reti di far emergere la topologia dei fenomeni corruttivi, cfr. Gerli 2026; OECD 2025-a; Rusinov 2025. Per ContÁgil e la riduzione da una settimana a un'ora nel mapping delle reti corruttive, cfr. Odilla 2023; OECD 2025-b.
13. Tello Arista–Fazekas–Volkotrub 2026, dove si documenta il matching di 8 milioni di contratti pubblici con 11 milioni di record di beneficial ownership in sei paesi europei.
14. Per il sistema Forest Foresight (80% di accuratezza a sei mesi, aree pilota in Gabon e nel Borneo), cfr. WWF Netherlands 2022; FAO 2024. Per il modello colombiano di early warning basato su LASSO e gradient boosting, cfr. Gallego–Rivero–Martínez 2021; cfr. anche Resimić 2025.

strutturale di self-fulfilling prophecy, per cui l'alert porta a più controlli, i controlli trovano più irregolarità, e le irregolarità trovate confermano l'accuratezza dell'alert, producendo un circolo che tende ad amplificare le asimmetrie di enforcement già esistenti[15].

1.6. La percezione sensoriale estesa

Il sesto tipo di contributo può essere definito in termini di percezione sensoriale estesa: l'AI come organo di senso artificiale per monitorare realtà fisiche inaccessibili o troppo vaste per l'osservazione diretta. Non si tratta di amplificare il giudizio umano né di mettere in connessione archivi esistenti: si tratta di percepire ciò che l'umano non può fisicamente vedere, sia per ragioni geografiche (aree remote), sia per ragioni di scala (estensioni territoriali enormi), sia per ragioni tecniche (bande spettrali invisibili all'occhio umano). Computer vision e remote sensing applicati alla governance delle risorse naturali rappresentano il caso più maturo di questo tipo di contributo. Il sistema Global Fishing Watch – che monitora il comportamento delle imbarcazioni industriali attraverso i segnali AIS e l'analisi di immagini satellitari radar – ha documentato come il 72-76% delle imbarcazioni sfugga al monitoraggio pubblico attraverso la disattivazione deliberata dei transponder: dati invisibili a qualsiasi sistema di controllo tradizionale[16].

Il limite strutturale di questo tipo di contributo è diverso dagli altri: la percezione estesa genera alert su eventi fisici, ma la traduzione di questi alert in azione anticorruzione richiede capacità di risposta sul campo – personale, mezzi, coordinamento istituzionale, volontà politica – che in molti dei contesti più vulnerabili alla corruzione nella governance delle risorse naturali semplicemente non esistono. Il divario tra capacità di rilevamento e capacità di risposta rischia di trasformare gli alert in documenti di monitoraggio senza conseguenze operative.

1.7. La democratizzazione dell'accesso all'analisi anticorruzione

Il settimo tipo di contributo è epistemicamente diverso dagli altri: non si tratta di produrre conoscenza nuova per esperti istituzionali, ma di rendere accessibile la conoscenza esistente a soggetti che non avrebbero altrimenti la capacità cognitiva o tecnica di elaborarla – cittadini, giornalisti, organizzazioni della società civile, ricercatori, piccole e medie imprese. Il sistema Rosie in Brasile non solo elabora le note spese parlamentari, ma pubblica gli alert in formato comprensibile ai cittadini, permettendo un monitoraggio diffuso che l'architettura istituzionale tradizionale non avrebbe mai consentito. DOZORRO in Ucraina trasforma i dati grezzi della piattaforma Prozorro in alert leggibili dalla società civile e dai media, costruendo un secondo livello di controllo che integra e in certi casi supplisce alle carenze del primo[17].

Il tratto epistemico specifico di questa tipologia è la riduzione delle asimmetrie informative tra chi detiene il potere e chi ne è governato. La corruzione prospera nell'opacità; la trasparenza è una delle sue principali contromisure. Ma la trasparenza formale – la pubblicazione di dati in formato PDF su siti istituzionali – produce informazione che resta largamente inaccessibile a chi non dispone di competenze tecniche per elaborarla. L'AI che trasforma questa informazione in segnali comprensibili e azionabili da attori non specializzati realizza una forma di empowerment cognitivo con effetti anticorruzione strutturali: non perché l'AI scopra la corruzione, ma perché aiuta gli umani a scoprirla, redistribuendo la

15. La self-fulfilling prophecy come rischio strutturale dei sistemi di predictive analytics anticorruzione è analizzata in Gallego–Rivero–Martínez 2021; cfr. anche Resimić 2025, che parla di "feedback loops that can reinforce existing enforcement biases".

16. Per Global Fishing Watch e il dato che il 72-76% delle imbarcazioni industriali sfugge al monitoraggio pubblico attraverso la disattivazione deliberata dei transponder AIS, cfr. Paolo–Kroodsma–Raynor et al. 2024; Global Fishing Watch 2022. Per una panoramica dei sistemi di remote sensing applicati alla governance ambientale, cfr. APEC 2025.

17. Sul potenziale delle applicazioni AI per la democratizzazione del controllo civico e la riduzione delle asimmetrie informative, cfr. Odilla–Mattoni 2023; Odilla 2025; Zinnbauer 2025. Per l'esperienza italiana si rinvia ai progetti Monithon (OpenCoesione), IrpiMedia e Openpolis, con le relative documentazioni istituzionali.

capacità cognitiva anziché concentrarla ulteriormente negli organi di controllo istituzionale[18].

2. Le applicazioni mature: settori e casi

La distinzione tra applicazioni mature e sperimentali va intesa come gradiente, e non come una soglia netta. Si propone di qualificare come "mature" le applicazioni che dispongono di sistemi operativi in contesti reali, di risultati misurabili pubblicati e verificabili, e di un numero sufficiente di casi indipendenti da consentire comparazioni significative. La maturità non implica assenza di problemi: anche le applicazioni più avanzate presentano vulnerabilità strutturali che si analizzeranno a seguire. Significa, però, che vi è sufficiente evidenza empirica per valutarne l'efficacia, identificarne i limiti ricorrenti e trarne indicazioni per le politiche pubbliche[19].

2.1. I contratti pubblici

I contratti pubblici costituiscono il settore più avanzato nell'applicazione dell'AI anticorruzione, con il maggior numero di implementazioni reali, i dati di impatto più verificabili e i modelli più trasferibili. La ragione strutturale di questa maturità è duplice: per un verso, le procedure di affidamento producono dati strutturati in formato digitale – bandi, offerte, aggiudicazioni, prezzi – che si prestano naturalmente all'analisi algoritmica; per altro verso, la corruzione negli appalti è sistematicamente documentata come tra le più pervasive e costose, il che ha concentrato su questo settore l'attenzione istituzionale e le risorse di ricerca in via prioritaria. Le applicazioni operative si articolano su tre livelli distinti.

Al primo livello si collocano i sistemi di monitoraggio in tempo reale, che analizzano le procedure durante il loro svolgimento, prima dell'aggiudicazione. Il caso più documentato è Alice (Achados e Licitações), sviluppato dalla Controladoria-Geral da União brasiliana: applica algoritmi di ML alle gare nell'istante in cui vengono pubblicate, producendo alert che possono portare alla sospensione della procedura prima che il contratto sia stipulato. Tra il 2019 e il 2022, Alice ha portato alla sospensione o alla cancellazione di procedure per un valore complessivo superiore a 9,7 miliardi di reais brasiliani, mantenendo la stessa efficacia di rilevamento a fronte di una riduzione del 28% del personale della CGU impegnato nei controlli preventivi. In Cile, il sistema VigIA della Contraloría General de la República utilizza modelli di ML per calcolare indici di rischio sulle procedure in corso, generando red flag automatiche in presenza di tempi di sottomissione anormalmente brevi, requisiti tecnici eccessivamente restrittivi o criteri di selezione insoliti[2021].

Al secondo livello si collocano i sistemi di risk scoring pre-aggiudicazione, che assegnano a ciascuna gara un punteggio di rischio prima dell'aggiudicazione, consentendo alle autorità di controllo di concentrare le risorse ispettive sui casi statisticamente più vulnerabili. In Spagna, il sistema ML dell'Intervención General de la Administración del Estado (IGAE) applicato ai contributi pubblici ha identificato 42.152 casi ad alto rischio su 1,05 milioni di contratti analizzati, ottimizzando l'allocazione delle risorse ispettive in modo che non sarebbe stato possibile con metodi tradizionali. In Ungheria, modelli ML hanno raggiunto un'accuratezza dell'82% nella previsione delle offerte singole. In Colombia, il sistema di early warning integra variabili sulla stazione appaltante, il settore merceologico e il contesto territoriale per produrre stime di rischio che guidano l'allocazione delle ispezioni[22].

18. L'AI si configura, in questo modo, come un mediatore della trasparenza; cfr. Ponti 2019-a.
19. Per la distinzione tra applicazioni mature e sperimentali nell'AI anticorruzione, cfr. Resimić 2025; Zinnbauer 2025; APEC 2025, che adotta il framework tripartito "prevention, detection, sanction" come griglia di classificazione.
20. Sul sistema Alice (Achados e Licitações) della Controladoria-Geral da União e i risultati documentati nel periodo 2019-2022, cfr. Controladoria-Geral da União 2022; Odilla 2023.
21. Per il sistema VigIA (Contraloría General de la República de Chile) e la sua metodologia di risk scoring basata su ML, cfr. APEC 2025; Resimić 2025.
22. Per il sistema ML dell'IGAE spagnola applicato ai contributi pubblici e il dato di 42.152 casi ad alto rischio su 1,05 milioni di contratti analizzati, cfr. Gerli 2026, come uno dei benchmark europei più avanzati; Katona–Fazekas 2024.

Al terzo livello si collocano i sistemi di audit post-aggiudicazione, che analizzano la documentazione dei contratti già conclusi per identificare irregolarità nell'esecuzione. Il Tribunal de Contas portoghese ha sviluppato, con il supporto dell'OCSE e della NOVA University Lisbon, un modello di risk assessment basato su ML e 37 indicatori per rafforzare il controllo degli appalti pubblici, migliorando l'efficienza dell'analisi e l'individuazione precoce di irregolarità[23].

Gli indicatori di rischio più utilizzati nei sistemi ML per i contratti pubblici – sistematizzati dalla guida Open Contracting Partnership del 2024 – comprendono: single bidding (procedure con un solo offerente, indicatore di mercati ristretti o accordi collusivi); winner rotation (alternanza regolare tra vincitori, indicativa di accordi orizzontali tra imprese); pricing anomalies (prezzi unitari che si discostano significativamente dai prezzi di mercato di riferimento); vendor concentration (elevata concentrazione delle aggiudicazioni su un numero ristretto di imprese); timeline compression (tempi di pubblicazione e aggiudicazione anormalmente compressi, che impediscono una competizione effettiva). La ricerca più avanzata non usa questi indicatori singolarmente ma in combinazione, sfruttando la capacità degli algoritmi ML di rilevare pattern complessi che coinvolgono più variabili simultaneamente[24].

Nel contesto italiano, il sistema di monitoraggio degli appalti è tra i più articolati per architettura normativa: il d.lgs. 31 marzo 2023, n. 36 ha disegnato un ciclo di vita interamente digitale dei contratti pubblici, la Banca Dati Nazionale dei Contratti Pubblici (BDNCP) gestita da ANAC costituisce uno degli archivi di dati sugli appalti più ricchi d'Europa per ampiezza della copertura, e la delibera ANAC n. 148 dell'aprile 2026 e il Bando Tipo n. 2/2026 hanno introdotto per la prima volta l'obbligo per gli operatori economici di dichiarare l'eventuale utilizzo di sistemi di intelligenza artificiale nella predisposizione delle offerte e nell'esecuzione dei contratti, in attuazione dell'art. 13 della l. 132/2025 e del Regolamento (UE) 2024/1689. Il passaggio a sistemi ML automatizzati di risk scoring è tuttavia ancora in fase sperimentale, e il confronto con i sistemi spagnolo e portoghese – entrambi costruiti su basi normative e istituzionali comparabili – suggerisce che il gap da colmare è più organizzativo che tecnologico[25].

2.2. L'antiriciclaggio e l'intelligence finanziaria

L'antiriciclaggio e l'intelligence finanziaria costituiscono il secondo settore per maturità nell'applicazione dell'AI anticorruzione, con una storia di adozione algoritmica che precede cronologicamente quella degli appalti. Le unità di intelligence finanziaria (UIF) e le istituzioni bancarie sono state tra i primi ad adottare sistemi di machine learning per la detection di operazioni anomale, spinte da una combinazione di incentivi che non ha equivalenti in altri settori: obblighi normativi sempre più stringenti in materia di antiriciclaggio; risorse private consistenti e forte orientamento all'innovazione nel settore bancario; disponibilità di dataset strutturati e completi – le transazioni finanziarie – che si prestano naturalmente all'analisi algoritmica.

Il sistema Inspector AI, sviluppato dall'Unità di Intelligence Finanziaria peruviana con il supporto della GIZ, utilizza NLP e reti neurali per elaborare le SARs ricevute dalle istituzioni finanziarie, classificandole automaticamente per livello di rischio e producendo report strutturati per i revisori umani: a parità di personale, il numero di casi trasmessi alle procure si è più che raddoppiato, non perché il sistema abbia abbassato le soglie di segnalazione, ma perché ha liberato i revisori dall'onere di analisi preliminare. Nel settore bancario privato, il caso più citato è quello della partnership tra HSBC e Google: l'adozione di algoritmi ML per il rilevamento di operazioni sospette ha prodotto una riduzione del

23. Per il Tribunal de Contas portoghese e il modello di risk assessment basato su ML e 37 indicatori, cfr. OECD 2024-a; OECD 2025-b; cfr. anche Longobucco–Ferwerda 2025.

24. Open Contracting Partnership 2024. Gli indicatori sistematizzati dalla guida comprendono: single bidding, winner rotation, pricing anomalies, vendor concentration, timeline compression.

25. Il d.lgs. 31 marzo 2023, n. 36 ha disegnato un ciclo di vita interamente digitale dei contratti pubblici. Per un'analisi del "paradigma digitale dell'evidenza pubblica", cfr. Mancini Palamoni 2024.

75% nei falsi positivi, con un risparmio significativo in termini di costi di analisi manuale[26].

Nel contesto italiano, l'UIF della Banca d'Italia ha registrato nel 2025 il record storico di 162.058 segnalazioni di operazioni sospette, con un incremento dell'11,5% rispetto all'anno precedente, in una dinamica di crescita strutturale che ha reso non più differibile il ricorso a strumenti automatizzati di triage e classificazione. L'infrastruttura applicativa integrata RADAR incorpora un modello di risk scoring composto da tre componenti algoritmiche distinte: il ranking finanziario (valutazione automatica del peso di ciascun soggetto in proporzione ai volumi dell'operatività segnalata); il link rating (mapping attraverso algoritmi di analisi dei grafi dei collegamenti latenti tra SARs diverse sulla base di soggetti comuni e flussi finanziari incrociati); la classificazione automatica dei soggetti neutri, realizzata con modelli NLP. Si tratta di un'architettura che integra simultaneamente tre dei contributi epistemici identificati nella sezione precedente – rilevamento di anomalie statistiche, analisi topologica delle reti e sintesi di conoscenza eterogenea – in un sistema operativo unitario[27].

2.3. Le dichiarazioni patrimoniali e i conflitti di interesse

Le dichiarazioni patrimoniali dei funzionari pubblici e la verifica dei conflitti di interesse costituiscono un settore relativamente maturo, con implementazioni operative in diversi contesti nazionali, ma ancora lontano dalla piena maturità osservabile negli appalti. Le applicazioni ML in questo settore si articolano su due modalità distinte. La prima è quella del cross-referencing automatico: il sistema verifica sistematicamente la coerenza tra quanto dichiarato e i dati in possesso di altre amministrazioni – catasto, registro delle imprese, dati fiscali, anagrafi degli eletti – rilevando incongruenze che l'analisi manuale lascerebbe invisibili, sia per ragioni di volume sia per ragioni di frammentazione istituzionale delle banche dati. La seconda modalità è quella del rilevamento di pattern temporali: il sistema analizza l'evoluzione nel tempo delle dichiarazioni, identificando variazioni patrimoniali anomale rispetto al profilo del dichiarante o strutture di detenzione di beni insolite per la categoria professionale di appartenenza.

Il sistema armeno di verifica automatica delle dichiarazioni patrimoniali integra i dati dichiarati dai funzionari con i dati del catasto, del registro delle imprese e dell'amministrazione fiscale, producendo alert automatici sulle incongruenze rilevate. Il progetto DATACROS applica algoritmi di ML e NLP alle strutture proprietarie di 56 milioni di imprese europee, individuando catene anomale riconducibili a soggetti politicamente esposti. Sistemi di verifica automatica sono altresì operativi in diversi paesi dell'Europa centrale e orientale – Romania, Georgia, Moldavia – dove le riforme anticorruzione degli ultimi anni hanno prodotto investimenti significativi in questo settore[28].

Nel contesto italiano, il sistema delle dichiarazioni patrimoniali è frammentato tra diversi regimi normativi e i formati di raccolta non sono standardizzati, con pubblicazione spesso in formati non machine-readable che rende l'analisi algoritmica sistematica tecnicamente impraticabile senza un intervento preliminare di normalizzazione. Il sistema ARACHNE della Commissione europea – parzialmente utilizzato in Italia per il monitoraggio dei beneficiari dei fondi strutturali e del PNRR – rappresenta il modello più vicino a un sistema di cross-referencing automatizzato già operativo nel nostro ordinamento. Più di recente, il progetto ACOI – Assessing Conflict of Interest, finanziato con fondi PNRR e condotto da Transcrime-Università Cattolica in collaborazione con l'Università di Perugia, ha testato uno strumento sperimentale per lo screening

26. Per il caso HSBC/Google (riduzione del 75% nei falsi positivi con l'adozione di algoritmi ML per il rilevamento di operazioni sospette), cfr. Resimić 2025; GIZ 2024.
27. Per il sistema RADAR (UIF) e le sue tre componenti algoritmiche (ranking finanziario, link rating, classificazione dei soggetti neutri mediante NLP), cfr. Banca d'Italia 2025; Banca d'Italia 2026. Dati 2025: 162.058 segnalazioni di operazioni sospette ricevute, con incremento dell'11,5% rispetto all'anno precedente.
28. Il progetto DATACROSS è documentato in *Report on AI-driven service*, nel sito transcrime.it. Sull'impiego di ML per il monitoraggio delle strutture societarie opache e per l'identificazione dei beneficiari effettivi di contratti pubblici, cfr. Parvanova 2025; OECD 2019. Per le applicazioni in Romania, Georgia e Moldavia, cfr. Resimić 2025; APEC 2025.

automatizzato del rischio di conflitto di interessi, che costituisce lo studio di caso analizzato nella terza parte del presente saggio[29].

2.4. Il monitoraggio della spesa pubblica

Il monitoraggio della spesa pubblica discrezionale – rimborsi, indennità, contributi, agevolazioni – costituisce un settore in cui le applicazioni ML mostrano risultati misurabili ma anche, in alcuni casi documentati, effetti collaterali gravi che richiedono attenzione specifica. I casi di fallimento più noti – il sistema SyRi nei Paesi Bassi, annullato dalla Corte distrettuale dell'Aia nel 2020 come violazione della CEDU per l'impossibilità dei soggetti interessati di comprendere e contestare le ragioni del profilo di rischio; il sistema automatizzato del Michigan per l'assicurazione contro la disoccupazione, che ha prodotto circa 40.000 false accuse di frode; lo scandalo olandese del childcare benefit, che ha colpito decine di migliaia di famiglie innocenti portando alle dimissioni del governo Rutte nel 2021 – condividono tre caratteristiche: opacità algoritmica; assenza di supervisione umana effettiva; concentrazione degli errori sui soggetti più vulnerabili[30].

Questi casi dimostrano che il rischio di un'applicazione ML nel monitoraggio della spesa pubblica non è simmetrico: i danni da falsi positivi ricadono sistematicamente sulle fasce più deboli della popolazione. Si tratta del retroterra casistico da cui si è poi attivata l'esigenza di regolazione che ha trovato concretizzazione – nel contesto europeo – nell'adozione dell'AI Act.

2.5. L'amministrazione fiscale

L'amministrazione fiscale è il settore dove i sistemi ML hanno la storia più lunga e i risultati più robusti. Il confine tra evasione fiscale e corruzione amministrativa è mobile e spesso incerto: la collusione tra funzionari fiscali e contribuenti – che permette a questi ultimi di ridurre arbitrariamente il proprio carico tributario in cambio di compensi illegali – è una forma di corruzione amministrativa con impatti enormi sul gettito pubblico e sulla fiducia istituzionale. Le applicazioni più mature riguardano tre aree: il risk scoring delle dichiarazioni fiscali; il rilevamento delle frodi carosello IVA, in cui sistemi che incrociano i dati del sistema VIES con quelli delle dichiarazioni fiscali nazionali identificano le catene di imprese utilizzate per generare crediti IVA inesistenti; e il monitoring of the monitors, ossia l'analisi comportamentale degli ispettori fiscali per rilevare pattern anomali nelle loro decisioni.

In Italia, l'obbligo di fatturazione elettronica, introdotto per tutte le partite IVA a partire dal 2019, ha prodotto un dataset di straordinaria ricchezza per l'analisi ML delle frodi IVA e delle incongruenze tra flussi economici dichiarati e reali. L'Agenzia delle Entrate gestisce il sistema VeRa (Verifica dei Rapporti Finanziari), che incrocia i dati dell'Anagrafe tributaria, dell'Archivio dei rapporti finanziari comunicato dagli operatori bancari e dei flussi dei pagamenti digitali, producendo liste di contribuenti a rischio per orientare l'attività di controllo. Il recupero complessivo dell'evasione ha raggiunto 18,1 miliardi di euro nel 2023, con l'Atto di indirizzo per la politica fiscale del febbraio 2026 che ha fissato la traiettoria evolutiva verso l'impiego di "nuovi strumenti di analisi avanzata dei dati, favoriti dall'applicazione di tecniche di intelligenza artificiale, quali il machine learning, il text mining e il network analysis", utilizzando i dati "in chiave predittiva"[31].

3. Le applicazioni sperimentali: promesse e limiti

Le applicazioni qualificate come sperimentali non lo sono necessariamente per ragioni tecniche: alcune tecnologie in questa categoria sono mature

29. Calderoni–Pollicino–Ponti–Valle 2026.

30. Sul sistema SyRi (Paesi Bassi) e il suo annullamento da parte della Corte distrettuale dell'Aia nel 2020 per violazione della CEDU, cfr. Rechtbank Den Haag, 5 febbraio 2020; Appelman–Ó Fathaigh–Van Hoboken 2021; Rachovitsa–Johann 2022. Per lo scandalo olandese del childcare benefit e le dimissioni del governo Rutte nel 2021, cfr. Resimić 2025; APEC 2025.

31. Per il sistema VeRa (Verifica dei Rapporti Finanziari, Agenzia delle Entrate) e i risultati del recupero dell'evasione (18,1 miliardi di euro nel 2023), cfr. OECD 2026; OECD 2025-a. L'Atto di indirizzo per la politica fiscale del febbraio 2026 ha fissato l'obiettivo di impiegare "nuovi strumenti di analisi avanzata dei dati, favoriti dall'applicazione di tecniche di intelligenza artificiale, quali il machine learning, il text mining e il network analysis", utilizzando i dati "in chiave predittiva".

sul piano computazionale ma non lo sono sul piano istituzionale, giuridico o della governance. La distinzione rilevante non è dunque tra ciò che funziona e ciò che non funziona in laboratorio, ma tra ciò che ha maturato un'evidenza empirica sufficiente in contesti istituzionali reali e ciò che non ha ancora raggiunto questo stadio di sviluppo. In alcuni casi l'assenza di maturità si spiega con la novità della tecnologia; in altri con la complessità dei requisiti istituzionali necessari per la sua implementazione; in altri ancora con il fatto che i fallimenti documentati hanno raffreddato l'entusiasmo e rallentato la diffusione.

3.1. L'AI nelle indagini giudiziarie sulla corruzione

Le indagini giudiziarie anticorruzione costituiscono il fronte meno sviluppato della catena del valore, paradossalmente il più strategico in termini di deterrenza. La deterrenza dipende dalla probabilità percepita di sanzione, non solo dalla qualità della prevenzione; e la probabilità percepita di sanzione dipende, in larga misura, dalla capacità investigativa. Il caso ContÁgil costituisce l'esempio più citato: la capacità di mappare reti di intermediari corruttivi in un'ora anziché in una settimana ha effettivamente modificato le strategie investigative dell'Operação Lava Jato. Va però detto che lo stesso sistema ha prodotto anche problemi significativi: un numero elevato di alert – a fronte di una capacità di risposta investigativa limitata – ha generato un effetto di alert overflow; la presenza di falsi positivi in una fase così delicata del procedimento penale ha esposto l'indagine a contestazioni sulla correttezza del metodo; e la scarsa adattabilità del sistema a tipologie di rete diverse da quelle su cui era stato addestrato ne ha limitato la trasferibilità ad altri contesti investigativi[32].

Il caso del Serious Fraud Office britannico è ancora più istruttivo. Il sistema Axcelerate, utilizzato in decine di casi compreso quello contro Rolls-Royce, ha omesso documenti rilevanti dal corpus analizzato per problemi di codifica dei file – un tipo di errore tecnico ordinario, gestibile nell'analisi documentale commerciale, ma con conseguenze potenzialmente molto rilevanti nella fase di disclosure probatoria del processo penale. Il caso ha aperto contestazioni su condanne già definitive e ha costretto lo SFO a riconsiderare le proprie procedure di gestione dei sistemi AI nelle indagini penali. Questi episodi mostrano che i requisiti di qualità e tracciabilità necessari per l'uso dell'AI in un contesto giuridicamente rilevante sono significativamente più elevati rispetto a quelli sufficienti per l'uso in contesti di analisi gestionale[33].

3.2. La governance delle risorse naturali

Le applicazioni di computer vision e remote sensing alla governance delle risorse naturali rappresentano il caso più avanzato di percezione sensoriale estesa applicata all'anticorruzione. Il sistema Forest Foresight prevede con sei mesi di anticipo e 80% di accuratezza dove avverrà disboscamento illegale su aree pilota; il sistema Global Fishing Watch ha documentato come il 72-76% delle imbarcazioni industriali sfugga al monitoraggio pubblico attraverso la disattivazione deliberata dei transponder AIS. La ragione del carattere ancora sperimentale di queste applicazioni non sta nella tecnologia di rilevamento – che è matura – ma nella difficoltà di tradurre le evidenze visive in azione istituzionale efficace. In molti dei contesti più vulnerabili alla corruzione nella governance ambientale, la capacità di risposta sul campo è insufficiente per trasformare gli alert in interventi[34].

32. Sul caso ContÁgil nella fase investigativa dell'Operação Lava Jato e sui suoi limiti (alert overflow, falsi positivi, scarsa trasferibilità), cfr. la documentazione sul sistema disponibile nel sito istituzionale della Controladoria-Geral da União e Odilla 2023. Per l'inquadramento metodologico della network analysis nelle indagini anticorruzione, cfr. OECD 2025-a.

33. Per il sistema Axcelerate (SFO britannico) e le contestazioni processuali derivanti dall'omissione di documenti per problemi di codifica, cfr. OpenText 2018; BBC News 2018; GOV.UK 2025; Resimić 2025. Il caso ha aperto la questione dei "quality and traceability requirements" necessari per l'uso dell'AI in contesti giuridicamente rilevanti.

34. Per Forest Foresight (previsione del disboscamento illegale con 80% di accuratezza a sei mesi) cfr. WWF Netherlands 2022; FAO 2024. Per Global Fishing Watch (rilevamento del 72-76% di imbarcazioni non monitorate), cfr. Paolo–Kroodsma–Raynor et al. 2024; APEC 2025.

3.3. L'AI generativa e i Large Language Models

L'applicazione di Large Language Models (LLM) all'anticorruzione rappresenta la frontiera tecnologicamente più avanzata e al tempo stesso la più controversa. I LLM aprono prospettive significative: analisi semantica di contratti, delibere, relazioni di audit, dichiarazioni patrimoniali per rilevare incongruenze linguistiche indicative di manipolazione; sintesi di corpus documentali vastissimi in tempi incompatibili con l'analisi umana; supporto alla redazione di quesiti investigativi complessi. Al tempo stesso, i limiti specifici dei LLM nell'ambito giuridico-investigativo sono di natura diversa rispetto ai sistemi ML tradizionali: le allucinazioni (generazione di informazioni plausibili ma false) introducono rischi di evidenza fabbricata; l'assenza di un audit trail verificabile rende difficile la tracciabilità del ragionamento; la latenza e i costi computazionali dei modelli più capaci ne limitano ancora l'utilizzo su larga scala[35].

Il profilo più critico, sul piano della governance, è quello della protezione dei dati personali: i LLM richiedono che i dati vengano elaborati dal modello, il che pone questioni rilevanti in ordine alla base di liceità del trattamento, alla compatibilità con la finalità originaria di raccolta dei dati e, soprattutto, alle garanzie da assicurare qualora il modello venga utilizzato in modalità cloud (API verso provider esterni) anziché in-house. Questo profilo – di particolare rilevanza per il caso ACOI analizzato nella Parte terza – sarà esaminato nel quadro delle norme applicabili.

3.4. Il riconoscimento facciale, la biometria e i droni

Il riconoscimento facciale, le tecnologie biometriche e i droni rappresentano la categoria più controversa delle applicazioni sperimentali, per ragioni che attengono alla loro natura strutturalmente *dual-use*: sono strumenti potenti di rilevamento dell'identità e di monitoraggio fisico, ma presentano rischi specifici di discriminazione algoritmica, normalizzazione della sorveglianza e potenziale utilizzo come strumenti di controllo politico. Il Regolamento (UE) 2024/1689 (AI Act) ne vieta, in generale, l'uso per la sorveglianza biometrica di massa negli spazi pubblici, con eccezioni tassativamente elencate per le forze dell'ordine in presenza di specifiche condizioni[36].

Le applicazioni anticorruzione più promettenti sono quelle che utilizzano i droni per il monitoraggio di infrastrutture (verifica della reale esecuzione di opere finanziate con fondi pubblici) e quelle che impiegano tecnologie biometriche per rafforzare i sistemi di identificazione dei funzionari pubblici e ridurre i fenomeni di "funzionario fantasma". Il carattere sperimentale di queste applicazioni non è tecnico ma normativo: i vincoli imposti dall'AI Act e, nel contesto italiano, dalla legge 132/2025 ne limitano significativamente il perimetro di utilizzo legittimo nell'ambito dell'azione pubblica.

È opportuno richiamare, a chiusura di questa parte ricognitiva, tre limiti strutturali che attraversano trasversalmente tutte le categorie applicative e che condizionano la praticabilità di qualsiasi sistema AI anticorruzione, indipendentemente dal settore di intervento e dal grado di maturità tecnologica: il *selective labelling problem* – il fatto che i sistemi addestrati su casi di corruzione già accertati replicano e amplificano i bias dell'enforcement precedente, imparando a riconoscere le forme di corruzione già identificate e non quelle ancora invisibili; l'opacità algoritmica – il *deficit di interpretabilità* che accompagna, in misura inversamente proporzionale alla loro accuratezza, tutti i sistemi ML; e il *rischio di cattura algoritmica* – la possibilità che attori corrotti imparino a manipolare i parametri dei sistemi di alert, o che i sistemi stessi vengano strumentalizzati per finalità di controllo politico anziché di prevenzione della corruzione.

35. Per le potenzialità degli LLM nell'analisi documentale anticorruzione e i loro limiti specifici (allucinazioni, mancanza di audit trail, latenza), cfr. OECD 2024-b; Resimić 2025; Gerli 2026. La letteratura sottolinea la necessità di distinguere tra LLM "in-house" e LLM tramite API a provider esterni sotto il profilo della protezione dei dati.

36. APEC 2025, sul riconoscimento facciale come "dual-use technology" con rischi specifici di discriminazione e normalizzazione della sorveglianza. Cfr. anche *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, che ha per la prima volta sottoposto a vaglio giudiziario l'uso del riconoscimento facciale da parte di autorità di polizia nel contesto europeo.

Parte seconda - La governance dei dati in Italia: forze e debolezze

4. I vincoli della tutela dei dati personali

La tutela dei dati personali costituisce, nell'ordinamento italiano ed europeo, il quadro normativo che più direttamente condiziona la praticabilità dei sistemi AI anticorruzione. Questa constatazione, tuttavia, non deve essere letta nel senso che la tutela dei dati personali sia un ostacolo alla prevenzione della corruzione: il quadro giuridico europeo – correttamente inteso – offre, accanto ai vincoli, anche le condizioni positive per un impiego legittimo e proporzionato dei dati personali a fini anticorruzione. La questione non è se il trattamento è possibile, ma a quali condizioni, con quali architetture e con quali garanzie. Chiarire questo punto è premessa indispensabile per una valutazione realistica del *gap* italiano.

4.1. Il GDPR come doppio binario: tutela e circolazione

Il Regolamento (UE) 2016/679 (GDPR) è comunemente percepito come strumento di tutela dei diritti fondamentali e, in quanto tale, come un vincolo alla circolazione dei dati. Questa percezione è corretta ma incompleta. Il GDPR opera, in realtà, su un doppio binario: da un lato, esso costituisce e garantisce il diritto fondamentale alla protezione dei dati personali, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea; dall'altro, esso abilita – attraverso la clausola di necessità e il sistema delle basi di liceità – la circolazione dei dati personali ogniqualvolta essa sia giustificata da un interesse pubblico sufficientemente determinato, proporzionato e garantito. La tensione tra i due binari non è patologica ma strutturale: è la modalità con cui il Regolamento persegue il suo duplice obiettivo, esplicitato nell'art. 1: la protezione delle persone fisiche con riguardo al trattamento dei dati personali "e" la libera circolazione di tali dati[37].

La Corte di giustizia ha precisato, con giurisprudenza costante, che il diritto alla protezione dei dati personali non è assoluto: deve essere "considerato alla luce della sua funzione nella società e bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità". Il bilanciamento non è discrezionale: deve rispettare il test di proporzionalità sancito dall'art. 52(1) della Carta, che richiede che qualsiasi limitazione del diritto sia prevista dalla legge, rispetti il contenuto essenziale del diritto e sia necessaria e rispondente a finalità di interesse generale riconosciute dall'Unione. La prevenzione della corruzione – che attiene al corretto funzionamento delle istituzioni democratiche, all'efficienza dell'uso delle risorse pubbliche e all'uguaglianza dei cittadini di fronte alla legge – rappresenta un obiettivo di interesse generale pienamente riconosciuto dall'ordinamento europeo[38].

4.2. Lo *strict legality standard* e l'evoluzione verso la legalità funzionale

Uno dei nodi più rilevanti per la praticabilità dei sistemi AI anticorruzione nel contesto italiano è rappresentato dall'evoluzione dello standard di legalità applicabile ai trattamenti di dati personali da parte delle pubbliche amministrazioni. La letteratura ha distinto, a questo riguardo, tra uno "standard di legalità formale" e uno "standard di legalità funzionale". Il primo richiede una norma di legge che autorizzi espressamente e tipicamente il singolo trattamento, con un grado di determinatezza analogo a quello richiesto per le limitazioni dei diritti fondamentali nel modello di Stato di diritto formale. Il secondo – quello adottato dal GDPR e, a partire dalla riforma del 2021, dall'ordinamento italiano – richiede che il trattamento sia necessario, proporzionato e pertinente alla finalità pubblica perseguita, ma non

37. Ponti 2025. L'Autore ricostruisce il GDPR come "strumento a doppio binario" che opera simultaneamente come tutela dei diritti fondamentali e come abilitatore della circolazione dei dati, ove la clausola di necessità (art. 6(1)(e)) "permea trasversalmente tutto il sistema, abilitando il trattamento ogniqualvolta esso sia giustificato dall'interesse pubblico cui il trattamento è funzionale".

38. Sul "diritto alla protezione dei dati personali" come diritto fondamentale a struttura non assoluta e soggetto a bilanciamento (art. 8 Carta dei diritti fondamentali UE; art. 52(1) Carta), cfr. Corte giust. UE (GC), 1° agosto 2022, causa C-184/20, *OT c. Vyriausioji tarnybinės etikos komisija*, §§ 63-70, dove la Corte sottolinea che "la protezione di tale diritto fondamentale non è tuttavia assoluta, ma deve essere considerata alla luce della sua funzione nella società e bilanciata con altri diritti fondamentali, conformemente al principio di proporzionalità".

che sia nominativamente previsto da una norma che ne definisca tutti i dettagli operativi[39].

La riforma del Codice in materia di protezione dei dati personali (d.lgs. 196/2003), operata dal d.lgs. 10 agosto 2018, n. 101 in attuazione del GDPR, ha segnato il passaggio definitivo dalla legalità stretta alla legalità funzionale per i trattamenti di dati pubblici. L'art. 2-*ter* del Codice consente il trattamento per finalità di interesse pubblico in presenza di una norma che specifichi le finalità perseguite, i tipi di dati trattabili, le operazioni eseguibili e il titolare del trattamento – una norma di abilitazione parametrica, non un'autorizzazione puntuale per ciascun trattamento. Questo passaggio ha conseguenze dirette per i sistemi AI anticorruzione: significa che la prevenzione della corruzione, in quanto finalità di rilevante interesse pubblico già definita dalla legge 190/2012 e dai suoi decreti attuativi, può costituire la base normativa per trattamenti di dati personali funzionali a tale finalità, senza che sia necessaria una norma ad hoc per ciascun sistema applicativo, purché il trattamento sia necessario e proporzionato rispetto all'obiettivo perseguito[40].

4.3. La base di liceità "compito di interesse pubblico"

Per i sistemi AI anticorruzione operati da soggetti pubblici, la base di liceità principale è quella prevista dall'art. 6(1)(e) GDPR: il trattamento è lecito se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. La norma richiede che la finalità del trattamento sia specificata – il "compito di interesse pubblico" deve avere un fondamento giuridico esplicito – ma non impone che la specifica operazione di trattamento sia nominativamente prevista, né che il sistema tecnologico utilizzato sia dettagliatamente descritto dalla norma abilitante. Il fondamento normativo del "compito di interesse pubblico" nei sistemi AI anticorruzione è, nell'ordinamento italiano, costituito dall'insieme delle norme della legge 190/2012, dei decreti attuativi (d.lgs. 33/2013, d.lgs. 39/2013), degli atti di ANAC (Piano Nazionale Anticorruzione) e, per i contratti pubblici, del d.lgs. 36/2023[41].

Tuttavia, il ricorso a tool epistemici basati su AI comporta ulteriori profili di tensione con il GDPR, che hanno ricadute dirette proprio in termini di assetto e architettura della governance pubblica dei dati. In particolare, vengono in questione i profili relativi al principio della limitazione della finalità del trattamento (art. 5, par. 1, lett. b) del GDPR) e della minimizzazione dei dati (art. 5, par. 1, lett. c) del GDPR).

4.3.1. Limitazione della finalità del trattamento e uso secondario a fini di prevenzione della corruzione

Il principio di limitazione della finalità (*purpose limitation*) impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e che i trattamenti successivi alla raccolta siano compatibili con tali finalità originarie. L'uso di dati raccolti da pubbliche amministrazioni per finalità operative, gestionali, di trasparenza – appalti

39. Ponti 2025, dove si distingue tra "standard di legalità formale" (richiede una norma di legge che autorizzi espressamente il singolo trattamento, con tassatività e tipicità delle basi di liceità) e "legalità funzionale" (il trattamento è legittimo se è funzionale al perseguimento della finalità pubblica).

40. È questo l'effetto delle modifiche all'art. 2-*ter* del Codice privacy apportate dal d.l. 139/2021 convertito in legge 205/2021. In particolare – mentre il comma 1 apre alla possibilità che la base giuridica che giustifichi il trattamento dei dati personali per l'esercizio di compito di interesse pubblico o di un potere pubblico possa essere costituita, oltre che dalla legge o dal regolamento, anche da atti amministrativi generali – è il nuovo comma 1-*bis* a chiarire che "il trattamento dei dati personali da parte di un'amministrazione pubblica […] è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti", ciò che segna il passaggio alla piena vigenza della *necessary clause*; per la articolazione della clausola di stretta legalità e di quella della clausola di necessarietà, cfr., *amplius*, Ponti 2023-a.

41. Regolamento (UE) 2016/679, art. 6(1)(e): il trattamento è lecito "se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Ponti 2025 analizza il rapporto tra la base di liceità pubblica (art. 6(1)(e)) e il principio di necessità come "meta-principio" che permea l'intero sistema: "la clausola di necessità non è un requisito aggiuntivo rispetto alla base di liceità, ma la condizione costitutiva della sua applicabilità".

pubblici, dichiarazioni patrimoniali, registri delle imprese, dati fiscali – come base di addestramento di un sistema AI per la prevenzione della corruzione costituisce un trattamento ulteriore rispetto alla finalità originaria di raccolta, e come tale deve superare un positivo giudizio di compatibilità secondo i criteri dell'art. 6, par. 4 del GDPR[42].

La sfida è in realtà doppiamente articolata. Il ciclo di vita di un sistema AI per la prevenzione della corruzione implica due distinte traslazioni di finalità: una prima traslazione dalla finalità originaria di raccolta alla finalità di addestramento del modello; una seconda traslazione dall'addestramento (o da quella originaria) alla finalità applicativa, ossia all'effettivo utilizzo del sistema AI a fini di prevenzione. Ciascuno dei due passaggi deve essere autonomamente valutato sotto il profilo della compatibilità con la finalità che precede, il che significa che la catena causale che conduce dalla raccolta originaria al deployment applicativo deve essere giustificata in ogni suo anello. L'eventuale compatibilità della finalità di addestramento con quella originaria non esaurisce il problema: occorre altresì valutare se la finalità applicativa – profilare il rischio corruttivo in procedure di appalto o in soggetti specifici – sia a propria volta compatibile con la finalità di addestramento.

Tra i criteri individuati dall'art. 6, par. 4 del GDPR per la valutazione di compatibilità assume rilievo centrale quello delle "ragionevoli aspettative degli interessati" al momento della raccolta originaria. Ad esempio, la Corte di giustizia ha affermato, nel caso *Meta Platforms* (C-252/21), che la compatibilità tra finalità deve essere valutata anche in funzione di ciò che gli interessati potevano ragionevolmente attendersi al momento in cui i loro dati sono stati raccolti[43]. Nel contesto che ci occupa, il parametro delle ragionevoli aspettative è particolarmente problematico. Un funzionario pubblico che dichiara i propri dati patrimoniali ai fini della trasparenza anticorruzione o un operatore economico che partecipa a una procedura di gara fornendo documentazione imprenditoriale e finanziaria può ragionevolmente attendersi che tali dati vengano impiegati per addestrare un sistema di machine learning finalizzato alla profilazione del rischio corruttivo individuale? La raccolta era funzionale a scopi specifici e definiti; l'uso dell'AI introduce una dimensione diversa per natura, impatto e logica elaborativa. Sotto questo profilo, il contesto normativo di riferimento, anche rispetto alla definizione dell'architettura di governance, potrebbe incidere sulla definizione e la consistenza di queste aspettative[44].

L'EDPB ha affrontato questo punto nel Parere (Opinion) 28/2024, con riferimento ai dati disponibili pubblicamente. Al par. 94, il Board afferma che "the fact that personal data are publicly available cannot be considered per se sufficient for the legitimate interests pursued by AI developers or deployers to override those of the data subjects"[45]. Tuttavia, tale ragionamento non appare

42. La valutazione di compatibilità tra finalità originaria e finalità ulteriore del trattamento è regolata dall'art. 6, par. 4 del GDPR, che individua i criteri rilevanti: (a) il nesso tra le finalità; (b) il contesto in cui i dati sono stati raccolti e le ragionevoli aspettative degli interessati in merito all'ulteriore utilizzo; (c) la natura dei dati, con riguardo particolare alla sensitività delle categorie di cui all'art. 9; (d) le possibili conseguenze dell'ulteriore trattamento per gli interessati; (e) l'esistenza di garanzie adeguate. Cfr. WP29 2013.

43. CGUE, sentenza del 4 luglio 2023, *Meta Platforms e a. c. Bundeskartellamt*, C-252/21, in particolare punti 112-124. La Corte ha chiarito che la compatibilità della finalità ulteriore con quella originaria deve essere valutata tenendo conto delle "ragionevoli aspettative" degli interessati al momento della raccolta dei dati: il mero fatto che l'interessato abbia accettato le condizioni generali di servizio non è sufficiente a fondare il consenso a trattamenti ulteriori radicalmente diversi per natura e impatto. Il ragionamento non è direttamente trasponibile al caso dei dati raccolti da pubbliche amministrazioni per scopi gestionali-amministrativi e successivamente utilizzati per addestrare sistemi AI, ma fornisce certamente elementi di cui tenere conto.

44. Il WP29 2013 aveva già individuato, tra i criteri per il giudizio di compatibilità, la considerazione delle "ragionevoli aspettative degli interessati" come elemento autonomo rispetto ai criteri oggettivi della natura dei dati e delle possibili conseguenze. Cfr. anche CGUE, sentenza del 1° agosto 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, punti 76-85, sulla tensione tra obblighi di trasparenza e protezione dei dati personali.

45. EDPB 2024. Il punto centrale dell'argomentazione è al par. 94: "the fact that personal data are publicly available cannot be considered per se sufficient for the legitimate interests pursued by AI developers or deployers to

direttamente trasponibile al caso dei dati pubblici raccolti in forza di obblighi normativi: la pubblica accessibilità dei dati o la disponibilità di tali informazioni in una banca dati pubblica, sebbene non costituisca l'equipollente di un consenso degli interessati al relativo utilizzo per finalità AI, non si pone allo stesso modo relativamente al giudizio di compatibilità con la finalità originaria. Pertanto, non è da escludersi che esista uno spazio (ancora da esplorare) per la costruzione di un'architettura normativa di governance dei dati pubblici che possa agevolare (a determinate condizioni) l'uso dei dati pubblici a fini di addestramento e poi di deployment di soluzioni di AI da destinare (anche) a fini di prevenzione della corruzione.

La soluzione più solida, per sciogliere questo – e al tempo stesso la più significativa per le implicazioni di governance – è quella di una destinazione legislativa esplicita. Ad esempio, se una norma di legge qualificasse determinate basi di dati come fonti autorizzate per i sistemi AI anticorruzione, e identificasse l'anticorruzione come finalità autonoma del trattamento, il problema della compatibilità con le finalità originarie finirebbe per attenuarsi in modo significativo: il trattamento troverebbe la propria base di liceità direttamente nella legge (art. 6, par. 1, lett. c) del GDPR – obbligo legale – o nella ridefinizione normativa del compito di interesse pubblico ai sensi della lett. e)), senza necessità di un giudizio comparativo con finalità antecedenti[46]. La designazione legislativa opera, in altri termini, come una clausola normativa di autorizzazione che incorpora e risolve a monte il problema della compatibilità delle finalità.

Questa prospettiva non è meramente teorica, ma trova riscontro in soluzioni normative già adottate nell'ordinamento italiano e in quello europeo. Il modello delle Basi di Dati di Interesse Nazionale (BDIN) nell'ambito della Piattaforma Digitale Nazionale dei Dati (PDND)[47] appare coerente con questo modello: la designazione legislativa di determinate basi di dati come BDIN, con conseguente priorità nell'interoperabilità, costituisce un atto normativo che definisce il perimetro dei flussi dati autorizzati tra amministrazioni, al di là delle finalità originarie delle singole raccolte. In tale schema, la Banca Dati Nazionale dei Contratti Pubblici – che raccoglie dati sull'intera filiera degli appalti pubblici italiani – potrebbe essere designata per legge come fonte primaria autorizzata per i sistemi AI anticorruzione gestiti dall'ANAC o da altra autorità competente[48]. La designazione costituirebbe la base giuridica del trattamento secondario, rendendolo non più un uso "compatibile" della

override those of the data subjects". Il ragionamento è speculare a quello della CGUE in C-252/21: la pubblica accessibilità dei dati non equivale ad aspettativa degli interessati che tali dati siano utilizzati per qualsiasi finalità, e in particolare per l'addestramento di sistemi AI destinati a profilare il rischio corruttivo.

46. La proposta di ricondurre l'autorizzazione all'uso di determinati dati pubblici per finalità AI a una designazione legislativa esplicita – che costituisce una base giuridica autonoma ai sensi dell'art. 6, par. 1, lett. c) o e) del GDPR – è sviluppata sistematicamente in Ponti 2025, in part. § 3 e § 5. L'Autore evidenzia come la designazione normativa costituisca lo strumento attraverso il quale l'ordinamento risolve a monte il problema della compatibilità delle finalità, incorporandola nella base di liceità.

47. L'art. 50-*ter* del codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), come modificato dall'art. 47 del d.l. 31 maggio 2021, n. 77, convertito con modificazioni dalla l. 29 luglio 2021, n. 108, istituisce la Piattaforma Digitale Nazionale dei Dati (PDND) e prevede al comma 2 che le Basi di Dati di Interesse Nazionale (BDIN) costituiscano la priorità della prima fase di attuazione dell'interoperabilità. Le BDIN includono, tra le principali, il Registro delle imprese, l'Anagrafe Nazionale della Popolazione Residente, la Banca Dati Nazionale dei Contratti Pubblici (BDNCP), il Casellario delle imprese. Cfr. Ponti 2025.

48. La Banca Dati Nazionale dei Contratti Pubblici (BDNCP), gestita dall'ANAC ai sensi dell'art. 222 del d.lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici), costituisce l'esempio più rilevante ai fini del presente discorso. La sua designazione come BDIN implica che i dati in essa contenuti sono resi disponibili, sulla piattaforma PDND, a tutte le amministrazioni pubbliche che li richiedano per l'esercizio delle loro funzioni istituzionali. Una designazione legislativa esplicita della BDNCP (e di altre basi di dati rilevanti per la prevenzione della corruzione) come fonti autorizzate per i sistemi AI anticorruzione costituirebbe una base giuridica ai sensi dell'art. 6, par. 1, lett. c) del GDPR (obbligo legale), eliminando la necessità del giudizio di compatibilità con la finalità originaria della raccolta.

finalità originaria (con tutto il margine di incertezza che ne consegue), ma un uso direttamente autorizzato da norma primaria.

Un modello ancora più articolato è offerto dal regolamento EHDS (Regolamento (UE) 2025/327), che ho definito un caso di "uso strategico" delle basi di liceità del GDPR[49]. L'EHDS predispone un'architettura normativa a doppio livello: il primo utilizza l'art. 6, par. 1, lett. c) e l'art. 9, par. 2, lett. i) e j) per fondare gli obblighi di condivisione dei dati sanitari imposti ai detentori; il secondo utilizza l'art. 6, par. 1, lett. e) e l'art. 9, par. 2, lett. g)-j) per qualificare come compito di interesse pubblico la funzione degli organismi di accesso ai dati sanitari. In entrambi i casi, la norma regolamentare definisce direttamente le finalità dei trattamenti secondari – ricerca, politiche sanitarie, innovazione – senza lasciare margine a un giudizio discrezionale di compatibilità caso per caso. La finalità dell'uso secondario è incorporata nella base di liceità stessa, che la autorizza e al contempo la delimita[50].

La traduzione di questa logica al settore dell'anticorruzione ha implicazioni immediate per l'architettura di governance. Se la designazione legislativa è la soluzione che consente di superare il vincolo della compatibilità delle finalità, allora la condizione necessaria per la piena legittimità dei sistemi AI anticorruzione è un intervento legislativo specifico che: (a) identifichi nominativamente le basi di dati pubbliche autorizzate ad alimentare i sistemi AI (BDNCP, registri titolari effettivi, dichiarazioni patrimoniali dei pubblici funzionari, dati fiscali rilevanti, ecc.); (b) qualifichi la prevenzione della corruzione mediante AI come finalità autonoma di trattamento, costituente base di liceità ai sensi dell'art. 6, par. 1, lett. c) o e) del GDPR; (c) individui il soggetto istituzionale responsabile del trattamento e dell'accesso ai dati; (d) stabilisca le garanzie appropriate, proporzionate alla sensibilità dell'operazione, in termini di minimizzazione, controlli di accesso, tracciabilità, supervisione umana e revisione periodica[51]. In assenza di tale intervento, i sistemi AI anticorruzione opererebbero in una zona di incertezza normativa che li espone a contestazioni e potenziali declaratorie di illiceità del trattamento.

4.3.2. *Il principio di minimizzazione e le architetture compatibili*

Il principio di minimizzazione dei dati si trova in tensione strutturale con la logica di funzionamento dei sistemi AI. I modelli di machine learning – e a maggior ragione i modelli di tipo foundation o large language model – tendono a migliorare le proprie prestazioni predittive all'aumentare della quantità e varietà dei dati di addestramento. Questa tendenza crea un incentivo intrinseco all'espansione, non alla riduzione, dei dataset utilizzati. Il principio di minimizzazione opera invece in senso contrario: i dati devono essere "adeguati, pertinenti

49. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio del 5 febbraio 2025 che istituisce lo Spazio europeo dei dati sanitari (EHDS), 5 marzo 2025. Il regolamento adotta un'architettura di basi giuridiche stratificata che, come evidenziato da Ponti 2025, costituisce un uso "strategico" delle basi di liceità del GDPR: l'art. 6, par. 1, lett. c) e l'art. 9, par. 2, lett. i) e j) fondano gli obblighi di condivisione imposti ai detentori di dati sanitari; l'art. 6, par. 1, lett. e) e l'art. 9, par. 2, lett. g)-j) fondano il compito di interesse pubblico degli organismi di accesso ai dati sanitari. In entrambi i casi, la designazione regolamentare risolve a monte il problema della compatibilità delle finalità, rendendo direttamente autorizzato l'uso secondario dei dati per ricerca, politiche sanitarie e innovazione.
50. Sull'"uso strategico" delle basi giuridiche del GDPR come strumento di governance della circolazione dei dati pubblici, cfr. Ponti 2025, che osserva come l'EHDS abbia costruito un sistema in cui la finalità del trattamento secondario è direttamente definita dalla norma, senza lasciare spazio a un giudizio discrezionale di compatibilità caso per caso. La stessa logica si riscontra nel modello BDIN/PDND, dove la priorità dell'interoperabilità delle basi di dati di interesse nazionale viene imposta per legge come finalità autonoma di circolazione dei dati, distinta dalle finalità originarie di raccolta.
51. Sulla necessità di un intervento legislativo specifico come presupposto per la legittimità dei sistemi AI applicati all'esercizio di funzioni pubbliche, cfr. Ponti 2025, in cui l'Autore argomenta che, in assenza di una base normativa che identifichi con sufficiente precisione le finalità, le categorie di dati e i soggetti destinatari, il trattamento fondato sul compito di interesse pubblico (art. 6, par. 1, lett. e) rimane esposto all'incertezza circa la proporzionalità e necessarietà dell'intervento. La logica funzionale della base di liceità e) deve essere "completata" da una cornice normativa che espliciti i tratti essenziali del trattamento.

e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". La distanza tra le due logiche – massimizzazione dei dati per ottimizzazione del modello vs. minimizzazione dei dati per tutela degli interessati – è la fonte della tensione.

Questa tensione non è ignorata dalla prassi delle autorità di controllo. L'EDPB, nell'Opinion 28/2024, ha elaborato un framework strutturato per la valutazione della minimizzazione nei sistemi AI, articolando il test di necessità in due componenti distinte[52]. La prima componente è di natura qualitativa: riguarda le categorie di dati utilizzate (quali tipologie di dati sono necessarie per la finalità dichiarata?). La seconda componente è di natura quantitativa: riguarda il volume dei dati (quanti dati sono necessari?). Con riferimento alla componente quantitativa, il Board afferma esplicitamente che il volume dei dati di addestramento deve essere valutato rispetto alla possibilità di ricorrere ad "alternative meno invasive". Questo trasforma la valutazione di minimizzazione da accertamento binario sulla non-superfluità dei dati in un confronto sistematico con le opzioni tecnologiche alternative disponibili – un confronto che deve essere documentato e giustificato dal titolare del trattamento.

Un presupposto essenziale perché questa valutazione possa essere condotta è che la finalità del trattamento sia chiaramente e specificamente identificata fin dalla fase di sviluppo del modello. L'EDPB precisa al par. 64 dell'Opinion 28/2024 che anche nella fase di addestramento – quando ancora il sistema non è stato applicato ad uno specifico compito – la finalità deve essere "clearly and specifically identified"[53]. Questo requisito ha conseguenze concrete per i sistemi AI anticorruzione: la generica indicazione "prevenzione della corruzione" come finalità è insufficiente. Occorre invece identificare con precisione la funzione specifica perseguita – rilevazione di anomalie nei contratti pubblici; profilazione del rischio di conflitto di interessi nei procedimenti autorizzativi; identificazione di pattern di collusione nelle gare d'appalto; detection di operazioni sospette di riciclaggio in transazioni pubbliche – perché ciascuna funzione richiede categorie e volumi di dati diversi, e la valutazione di minimizzazione deve essere condotta separatamente per ciascuna di esse.

Una specificità particolarmente rilevante riguarda la questione dell'anonimizzazione dei modelli addestrati. L'intuizione comune secondo cui un modello AI – in quanto aggregazione di parametri matematici – non "contiene" dati personali è smentita dall'Opinion 28/2024. Il Board chiarisce ai parr. 41-42 che i modelli AI non devono essere considerati automaticamente anonimi per il solo fatto che da essi non è possibile estrarre direttamente record personali[54]. La condizione

52. EDPB 2024. Il test di necessità è articolato in due componenti distinte: (i) la necessità tipologica, relativa alle categorie di dati utilizzate (quali dati sono necessari per la finalità?); (ii) la necessità volumetrica, relativa alla quantità di dati (quanti dati sono necessari?). Con riferimento alla seconda componente, il Board afferma esplicitamente che "the volume of data used for training should be assessed against the possibility of using less intrusive alternatives", configurando così la valutazione di minimizzazione come un confronto sistematico con tecniche alternative meno invasive, e non come mero accertamento della non-superfluità dei dati.

53. EDPB 2024: "the purpose of the processing [during development] must be clearly and specifically identified". Il Board chiarisce che la finalità dello sviluppo di un modello AI non può essere descritta in termini generici (es. "sistema anticorruzione"): deve essere articolata con sufficiente precisione da consentire la valutazione della necessità dei dati. Nella pratica, ciò significa che sistemi destinati alla rilevazione di frodi negli appalti pubblici, alla profilazione del rischio di conflitto di interessi, al riconoscimento di pattern di corruzione nei procedimenti amministrativi, richiedono ciascuno una distinta valutazione della minimizzazione, con dataset potenzialmente diversi per natura e volume.

54. Cfr. EDPB 2024. Il Board esclude che i modelli AI debbano essere considerati automaticamente anonimi per il solo fatto che da essi non è possibile estrarre direttamente dati personali individuali. Le due condizioni cumulative che devono essere entrambe soddisfatte sono: (i) che l'estrazione di dati personali dal modello sia impossibile; (ii) che da nessun output del modello, anche attraverso attacchi di tipo inversione o di membership inference, sia possibile ricavare dati personali. Se anche una sola di tali condizioni non è verificata, il modello addestrato rimane assoggettato al GDPR come trattamento di dati personali. La conseguenza pratica è significativa: l'obbligo di minimizzazione non si esaurisce con la fase di training, ma si estende al modello addestrato come tale.

di anonimità è soddisfatta solo se (i) l'estrazione di dati personali dal modello è impossibile e (ii) nessun output del modello – inclusi quelli ottenibili mediante attacchi di inversione (inversion attacks) o di membership inference – consente di ricavare informazioni personali identificative. Finché entrambe le condizioni non sono verificate, il modello addestrato rimane assoggettato al GDPR come trattamento di dati personali, con tutte le conseguenti obbligazioni. Ciò significa che l'obbligo di minimizzazione non si esaurisce con la fase di raccolta e addestramento, ma si estende al modello stesso come prodotto del trattamento: un modello "denso" di dati personali incorporati in forma trasformata è, a tutti gli effetti, un trattamento in corso finché rimane in uso.

La valutazione del volume dei dati in rapporto alle alternative meno invasive – imposta dall'EDPB come elemento del test di minimizzazione – richiede che il titolare del trattamento consideri concretamente le principali tecniche di privacy by design applicabili allo sviluppo AI[55]. Il federated learning consente di addestrare il modello localmente sui dati di ciascun titolare, scambiando solo parametri aggregati del modello e non i dati grezzi: in un sistema anticorruzione distribuito su più amministrazioni, questa architettura ridurrebbe significativamente il rischio di centralizzazione di grandi volumi di dati personali. La *differential privacy* aggiunge rumore statistico calibrato ai dati o ai parametri, rendendo statisticamente impossibile l'inferenza di informazioni individuali pur preservando le proprietà aggregate. I dati sintetici, generati algoritmicamente in modo da replicare le proprietà distributive dei dati reali senza contenere dati personali effettivi, possono in alcuni casi sostituire i dati reali nelle prime fasi di sviluppo o per il testing del modello. Il titolare del trattamento deve documentare per quale ragione queste alternative non sono state adottate, o non sono adottabili nella misura necessaria, per ogni componente del dataset.

Sulla base dell'analisi appena svolta – i.e., quali condizioni operative la legalità vigente in materia di tutela dei dati personali sembra imporre allo sviluppo e all'impiego di sistemi AI per la prevenzione della corruzione – emerge un quadro di requisiti di praticabilità stringenti ma anche definiti. La finalità dell'AI anticorruzione deve essere articolata in termini specifici, funzione per funzione, prima dell'avvio della raccolta dei dati di addestramento. Deve essere condotta – e documentata nella valutazione d'impatto (DPIA) prevista dall'art. 35 del GDPR – un'analisi delle alternative *tecnologiche* (cioè, *diverse* dell'AI) che, a parità di efficacia, risultino meno invasive[56]. Il volume dei dati di addestramento deve essere limitato al minimo statisticamente dimostrato come necessario per le prestazioni richieste, con monitoraggio continuo al procedere dell'addestramento per verificare se la stessa performance possa essere raggiunta con dataset più ridotti. Le scelte architetturali del sistema – federated learning, differential privacy, dati sintetici – devono essere considerate come opzioni primarie e documentate come insufficienti prima

55. Le principali tecniche di privacy by design rilevanti per lo sviluppo di sistemi AI sono: (a) il federated learning, in cui il modello è addestrato localmente su dati distribuiti presso ciascun titolare senza che i dati stessi vengano centralizzati; vengono condivisi solo i parametri del modello (c.d. gradient updates), che possono comunque presentare rischi di re-identificazione ma in misura drasticamente ridotta rispetto alla centralizzazione dei dati grezzi; (b) la differential privacy, che consiste nell'aggiunta di rumore statistico calibrato ai dati o ai parametri del modello in modo da rendere statisticamente impossibile l'inferenza di informazioni individuali, pur preservando le proprietà aggregate; (c) i dati sintetici, ossia dataset generati artificialmente che preservano le proprietà statistiche e distributive dei dati reali senza contenere dati personali effettivi. Su questi approcci nel contesto AI cfr. EDPB 2024; WP29 2014.

56. L'art. 35 del GDPR impone al titolare del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche", e in particolare nei casi di "trattamento sistematico su larga scala di categorie particolari di dati" e di "trattamento che implica la valutazione sistematica e globale di aspetti personali relativi a persone fisiche". Lo sviluppo e l'impiego di sistemi AI per la profilazione del rischio corruttivo ricade in almeno due delle ipotesi elencate nell'art. 35, par. 3, e nei criteri enunciati nella guida EDPB: cfr. EDPB 2024. La DPIA è pertanto obbligatoria e deve includere la documentazione dell'intera valutazione di minimizzazione, compreso il confronto con le alternative tecnologiche meno invasive.

di procedere alla centralizzazione di dati personali reali. L'anonimizzazione del modello addestrato deve essere verificata empiricamente, non presupposta. Solo un percorso di sviluppo che soddisfi queste condizioni cumulative può ritenersi conforme al principio di minimizzazione e, dunque, al quadro complessivo del GDPR.

Tenendo insieme le acquisizioni dei due sottoparagrafi che precedono, emerge una indicazione di fondo per la governance pubblica dei dati nell'ambito dell'anticorruzione. I profili di tensione con il GDPR non sono risolvibili dalla sola virtù tecnica dei sistemi AI, né dalla sola buona prassi amministrativa dei titolari del trattamento: sembrano richiedere entrambi – quello relativo alla limitazione della finalità e quello relativo alla minimizzazione – una risposta normativa strutturata[57]. Per il primo, la risposta è una designazione legislativa che attribuisca direttamente base giuridica all'uso dei dati per finalità AI anticorruzione, sul modello BDIN/EHDS. Per il secondo, la risposta è un quadro di obblighi procedurali – DPIA, valutazione comparativa delle alternative, verifica empirica dell'anonimizzazione del modello – che devono essere incorporati nella base giuridica di trattamento. In questa prospettiva, la questione della governance dei dati per l'AI anticorruzione non è separabile dalla questione di una architettura giuridica funzionale allo scopo[58].

5. La Piattaforma Digitale Nazionale dei Dati e il PNRR

La Piattaforma Digitale Nazionale dei Dati (PDND), disciplinata dall'art. 50-*ter* del Codice dell'amministrazione digitale (d.lgs. 82/2005), nella formulazione risultante dalle successive modifiche, rappresenta l'infrastruttura tecnico-giuridica più rilevante per i sistemi AI anticorruzione che operano sulla sintesi di conoscenza eterogenea. La sua comprensione richiede di distinguere tra la PDND come infrastruttura tecnologica e la PDND come istituzione normativa: sono due piani distinti, e la praticabilità dei sistemi AI anticorruzione dipende dalla coerenza tra i due.

5.1. L'architettura della PDND

L'architettura della PDND costituisce la risposta al problema della "interoperabilità predicata", ossia l'interoperabilità formalmente proclamata nei testi normativi fin dall'(ormai) lontano 2005[59], ma non effettivamente praticata per l'eterogeneità degli standard tecnici adottati dalle diverse amministrazioni. Il modello della PDND è quello di un hub centralizzato che funge da intermediario tra amministrazioni "erogatrici" di dati e amministrazioni "fruitrici", attraverso un sistema di API standardizzate e di Accordi di Accessibilità che definiscono le condizioni giuridiche dello scambio. Il vantaggio è la standardizzazione tecnica e normativa; il limite è che l'architettura a hub presuppone che le amministrazioni erogatrici abbiano già digitalizzato i propri dataset in formati compatibili con le API della piattaforma, il che non è ancora vero per molte delle banche dati rilevanti per la prevenzione della corruzione.

La PDND integra, come nodi prioritari, le Basi di Dati di Interesse Nazionale (BDIN) previste dall'art. 60 CAD, tra cui: l'Anagrafe Nazionale

57. EDPB-EDPS 2021: il Board e il Supervisor evidenziano che la proposta di certificazione (CE marking) del sistema AI non è strutturata in modo da garantire la conformità al principio di minimizzazione dei dati, dal momento che "the proposed AIA does not address the relationship between the certification/conformity assessment and data protection law and the data minimisation principle in particular". Il rischio segnalato è che la conformità tecnica ai requisiti dell'AI Act possa essere percepita – erroneamente – come sostitutiva della conformità al GDPR.
58. EDPB 2018. Le Linee guida chiariscono che anche le decisioni semi-automatizzate (in cui l'output del sistema AI è sottoposto a revisione umana prima di produrre effetti giuridici) rimangono soggette alle garanzie dell'art. 22 del GDPR laddove il contributo umano sia meramente formale. Nel contesto anticorruzione, i sistemi di risk scoring che assegnano punteggi di rischio corruttivo alle singole procedure o ai singoli soggetti rientrano nella categoria della "profilazione" ai sensi dell'art. 4, n. 4, del GDPR, con tutte le conseguenti garanzie.
59. Il testo del d.lgs. 42/2005, istitutivo del Sistema pubblico di connettività (testo in seguito assorbito nel Codice dell'amministrazione digitale), prevedeva già i servizi per la "interoperabilità evoluta" (i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini); e per la "cooperazione applicativa", finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione delle informazioni e dei procedimenti amministrativi.

della Popolazione Residente (ANPR); il Registro delle Imprese; l'Anagrafe Nazionale degli Studenti; il Casellario delle prestazioni sociali; la Banca Dati dei Contratti Pubblici (BDNCP) gestita da ANAC; il Catasto (Agenzia delle Entrate); il Fascicolo del Lavoratore. Queste banche dati coprono, in modo non ancora completo ma tendenzialmente sistematico, le principali fonti informative necessarie per sistemi di cross-referencing automatico a fini di anticorruzione. Il collegamento tra queste basi di dati attraverso la PDND – che richiede la stipulazione di Accordi di Accessibilità tra le amministrazioni interessate – è la precondizione tecnico-giuridica per qualsiasi sistema AI di sintesi di conoscenza eterogenea applicato alla prevenzione della corruzione.

5.2. Potenziale e limiti per i sistemi AI anticorruzione

Il PNRR ha stanziato risorse significative per il rafforzamento della PDND e per il completamento delle infrastrutture di interoperabilità. Le risorse della Missione 1, Componente 1 sono orientate sia all'estensione della copertura delle BDIN sia al potenziamento delle API della piattaforma, sia al supporto tecnico e organizzativo alle amministrazioni erogatrici per l'adeguamento dei propri sistemi informativi. Ponti ha tuttavia avvertito, sin dall'analisi della fase di avvio del PNRR, che la digitalizzazione accelerata imposta dai ritmi di attuazione del Piano presenta tensioni rispetto alle garanzie procedurali che il diritto fondamentale alla buona amministrazione impone nei confronti dei soggetti coinvolti nei processi amministrativi[60].

Per i sistemi AI anticorruzione, la PDND offre un potenziale significativo ma ancora parzialmente teorico. Sul versante del potenziale: la disponibilità di API standardizzate riduce il costo tecnico dell'integrazione di dataset diversi; il sistema degli Accordi di Accessibilità fornisce il quadro giuridico per disciplinare le condizioni dello scambio; la progressiva inclusione di nuove banche dati amplia la copertura informativa disponibile per l'analisi algoritmica. Sul versante dei limiti: la qualità dei dati nelle banche dati erogatrici è ancora disomogenea, con problemi di completezza, aggiornamento e standardizzazione dei formati che limitano l'affidabilità dell'analisi ML; il sistema dei Requisiti di Accessibilità non definisce in modo generalizzato le condizioni per i trattamenti finalizzati alla prevenzione della corruzione, richiedendo negoziazioni bilaterali caso per caso; la struttura pluralistica dell'amministrazione italiana, con migliaia di enti locali e centinaia di amministrazioni centrali, rende molto eterogeneo il grado di adesione effettiva alla piattaforma[61][62].

Sul piano normativo, il quadro dei Requisiti di Accessibilità potrebbe essere rafforzato da un intervento di rango primario o regolamentare che definisca, in modo generalizzato e vincolante, le condizioni alle quali le banche dati della PDND possono essere utilizzate per sistemi AI anticorruzione: un atto normativo che specifichi le finalità di prevenzione della corruzione come ragione sufficiente per l'accesso, i tipi di dati accessibili, le garanzie tecniche e organizzative richieste, le modalità di supervisione e audit. Questo intervento – che potrebbe collocarsi a livello di decreto ministeriale o di regolamento ANAC – scioglierebbe molte delle incertezze interpretative che oggi rendono i sistemi AI anticorruzione basati sulla sintesi di dati eterogenei giuridicamente instabili, esponendoli al

60. Il Piano Nazionale di Ripresa e Resilienza (PNRR), nella Missione 1 (Digitalizzazione, innovazione, competitività, cultura e turismo), Componente 1, ha stanziato risorse significative per il rafforzamento della PDND e per il completamento delle infrastrutture di interoperabilità. Ponti 2022 evidenzia le tensioni tra l'obiettivo di accelerazione delle riforme digitali e le garanzie procedurali imposte dal diritto fondamentale alla buona amministrazione.

61. Sul meccanismo dei "requisiti di accessibilità" come sistema che regola l'adesione (doverosa) delle amministrazioni ai servizi di fruibilità abilitati dalla PNDP, cfr. Ponti 2023-b. I requisiti di accessibilità regolano le condizioni alle quali un'amministrazione "erogante" mette a disposizione di un'amministrazione "fruitrice" i propri dataset attraverso le API della PDND, definendo finalità, frequenza di accesso, standard tecnici e garanzie di sicurezza.

62. Cfr. Longobucco–Ferwerda 2025, dove gli Autori analizzano la disponibilità dei dataset di procurement nei 27 Stati membri e concludono che "Italy has one of the most comprehensive procurement databases in Europe (BDNCP), but the lack of standardized data formats and the fragmentation of access rights between ANAC and other authorities significantly limit its utility for AI-based analytics".

rischio di contestazioni *ex post* da parte del Garante per la protezione dei dati personali.

6. L'AI Act e la legge 9 luglio 2025, n. 132

Il quadro normativo relativo ai sistemi di intelligenza artificiale ha subito, negli ultimi due anni, una trasformazione radicale sia a livello europeo sia a livello nazionale. L'entrata in vigore del Regolamento (UE) 2024/1689 (AI Act) e l'adozione della legge 9 luglio 2025, n. 132 (legge italiana sull'intelligenza artificiale) hanno introdotto, rispettivamente, un sistema di classificazione dei sistemi AI per livello di rischio e un regime di accountability applicabile ai soggetti pubblici che li utilizzano. La disciplina è rilevante per i sistemi AI anticorruzione sia come fonte di requisiti che tali sistemi devono soddisfare, sia come fonte di rischi istituzionali se implementati senza adeguata consapevolezza del quadro applicabile.

6.1. I sistemi AI ad alto rischio nella pubblica amministrazione

L'AI Act classifica i sistemi AI in quattro livelli di rischio: inaccettabile (vietati); alto rischio (ammessi con requisiti stringenti); specifici rischi di trasparenza (soggetti a obblighi di informazione); rischio minimo (non regolati). I sistemi AI di rilevanza per la prevenzione della corruzione che possono ricadere nella categoria ad alto rischio sono, in particolare, quelli destinati "a essere usati dalle autorità competenti ai fini di valutazione dei rischi relativi a persone fisiche al fine di individuare il rischio di un soggetto di commettere reati o di reiterare un reato" (Allegato III, punto 8). Rientrano in questa categoria i sistemi di predictive risk scoring dei contratti pubblici quando producono profili di rischio associati a soggetti specifici (imprenditori, funzionari), i sistemi di screening del conflitto di interessi, i sistemi di analisi delle dichiarazioni patrimoniali[63].

I requisiti per i sistemi ad alto rischio sono significativi: adozione di un sistema di gestione del rischio AI documentato; requisiti di qualità dei dati di addestramento e test; documentazione tecnica e obblighi di conservazione dei log; trasparenza verso gli utenti e obbligo di informativa; supervisione umana significativa; accuratezza, robustezza e cybersecurity; registrazione nel database EU. L'inadempienza espone il titolare del trattamento a sanzioni fino a 30 milioni di euro o al 6% del fatturato mondiale totale annuo, con un regime di enforcement che per le autorità pubbliche prevede la segnalazione all'autorità di vigilanza nazionale[64].

Il requisito più rilevante per il funzionamento pratico dei sistemi AI anticorruzione è quello della supervisione umana. L'art. 14 dell'AI Act richiede che i sistemi ad alto rischio siano "dotati di misure tecniche adeguate per consentire agli operatori di supervisionare in modo efficace il loro funzionamento durante il periodo in cui vengono utilizzati" e che gli operatori umani abbiano la "capacità di comprendere le caratteristiche e i limiti pertinenti del sistema AI ad alto rischio e di supervisionare il suo funzionamento in modo efficace". Questo requisito esclude il modello di automazione piena (fully automated decision-making) in cui il sistema AI produce direttamente un atto o una decisione vincolante senza revisione umana, ma non esclude il modello del sistema AI come strumento di supporto alla decisione umana (human-in-the-loop), a condizione che la supervisione umana sia genuina e non meramente formale[65].

63. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act). L'art. 6 e l'Allegato III individuano i sistemi AI ad alto rischio; il punto 8 dell'Allegato III include, tra questi, i "sistemi AI destinati ad essere usati dalle autorità competenti ai fini di valutazione dei rischi relativi a persone fisiche al fine di individuare il rischio di un soggetto di commettere reati o di reiterare un reato". Per una prima analisi, cfr. in dottrina la letteratura già vasta sul tema, sintetizzata, per i profili di rilievo per il presente studio, in Resimić 2025.

64. Per l'obbligo di registrazione nel database EU dell'Unione europea (art. 71 AI Act) e l'obbligo di adempimenti tecnici pre-mercato (artt. 8-15 AI Act, inclusi: gestione del rischio, qualità dei dati, tracciabilità, trasparenza, supervisione umana, accuratezza e robustezza), cfr. Regolamento (UE) 2024/1689, Capo III, Sezione 2.

65. Sul principio di supervisione umana significativa ("meaningful human oversight") come condizione di legittimità dei sistemi AI ad alto rischio nell'azione pubblica, cfr. AI Act, art. 14; Gerli 2026, dove si analizza il rischio che la supervisione umana si riduca a una "firma di approvazione formale" sul risultato algoritmico, senza reale capacità di comprensione e contestazione – fenomeno che la letteratura anglosassone denomina "automation bias".

6.2. La disciplina italiana della legge 132/2025

La legge 9 luglio 2025, n. 132 ha introdotto nell'ordinamento italiano una disciplina organica dell'intelligenza artificiale che integra il quadro europeo dell'AI Act con disposizioni specifiche per il contesto nazionale. Per i profili rilevanti in questa sede, tre aspetti meritano particolare attenzione. In primo luogo, l'istituzione della Commissione nazionale per l'intelligenza artificiale (art. 3), organo di coordinamento e indirizzo in materia di AI per le pubbliche amministrazioni, con funzioni anche di promozione di standard e linee guida per i sistemi AI nella pubblica amministrazione. In secondo luogo, le disposizioni sull'accountability dei sistemi AI nella pubblica amministrazione (artt. 7-9), che richiedono la designazione di un responsabile AI per ciascuna amministrazione e la predisposizione di un registro dei sistemi AI utilizzati, con indicazione della categoria di rischio e delle misure di governance adottate. In terzo luogo, la disciplina applicativa per i contratti pubblici (art. 13), che in attuazione dell'AI Act e del d.lgs. 36/2023 richiede agli operatori economici di dichiarare l'utilizzo di sistemi AI nella predisposizione delle offerte[66].

La legge 132/2025 non affronta tuttavia il tema più rilevante della governance per i sistemi AI anticorruzione: quello della definizione delle condizioni alle quali tali sistemi possono operare in modo sistematico, con accesso strutturato ai patrimoni informativi pubblici, in un quadro di regole chiare sulla base di liceità, sulle garanzie per i soggetti interessati e sulle modalità di supervisione. Su questi profili, la legge delega alle amministrazioni competenti la definizione delle regole operative, senza fornire criteri vincolanti uniformi. Questa lacuna – che si somma all'assenza di un atto normativo che regolamenti in modo organico il sistema di governance dei dati per la prevenzione della corruzione – costituisce un limite oggettivo che le analisi di gap della Parte terza del presente saggio intendono identificare e analizzare.

Parte terza - Il gap da colmare: il tool ACOI come studio di caso

7. Il divario su piano generale: confronto internazionale e focus sui contratti pubblici

La ricognizione comparata svolta nella Parte prima consente di misurare, con un qualche grado di precisione, il divario tra il sistema italiano di prevenzione della corruzione e i più avanzati sistemi internazionali nel campo dell'applicazione dell'AI. Questo divario, su un piano generale, si articola in tre dimensioni distinte che meritano di essere analizzate separatamente, perché rispondono a cause diverse e richiedono rimedi diversi[67].

La prima dimensione è quella della maturità dei sistemi operativi. L'Italia dispone di sistemi ML operativi in campo fiscale (VeRa, Agenzia delle Entrate) e in campo antiriciclaggio (RADAR, UIF), che rappresentano applicazioni mature e di buon livello. Il confronto diventa sfavorevole nel campo dei contratti pubblici, dove la Spagna (IGAE), il Portogallo (Tribunal de Contas), l'Ucraina (DOZORRO/Prozorro) e il Cile (VigIA) dispongono di sistemi ML integrati nelle procedure di affidamento in tempo reale, mentre l'Italia non ha ancora un sistema equivalente operativo su scala nazionale. Il dato è significativo: la BDNCP gestita da ANAC è, per ampiezza di copertura e per ricchezza informativa, una delle banche dati sugli appalti più complete d'Europa; il mancato sfruttamento di questo patrimonio a fini di analisi ML non si spiega con carenze tecnologiche ma con carenze di governance normativa e organizzativa.

La seconda dimensione è quella della qualità e dell'accessibilità dei dati. La letteratura internazionale ha identificato nell'Italia un caso emblematico

66. Legge 9 luglio 2025, n. 132, Disposizioni in materia di intelligenza artificiale. L'art. 3 istituisce la Commissione nazionale per l'intelligenza artificiale; l'art. 13 contiene la disciplina applicativa per i contratti pubblici. Per i profili di accountability e supervisione umana nella pubblica amministrazione, cfr. artt. 7-9.

67. Gerli 2026, dove si propone una graduatoria della maturità dei sistemi AI anticorruzione negli appalti europei: Spagna (massimo livello di integrazione istituzionale), Portogallo, Ucraina, Estonia, seguiti da un gruppo di paesi con implementazioni parziali o sperimentali. L'Italia è classificata in quest'ultimo gruppo, con il riconoscimento che la BDNCP "ha un potenziale di eccellenza per l'analisi ML" ma che "mancano sia le garanzie di qualità del dato sia i modelli di governance per l'utilizzo sistematico a fini anticorruzione".

di "procurement data gap" strutturale: la ricchezza teorica della BDNCP non si traduce in idoneità pratica per l'analisi ML a causa di problemi di completezza (non tutte le stazioni appaltanti alimentano sistematicamente la banca dati), di standardizzazione (i formati dei documenti di gara non sono uniformi) e di accessibilità (l'accesso alla BDNCP per finalità di ricerca e analisi esterna è soggetto a procedure burocraticamente complesse). Analogamente, il collegamento tra BDNCP e registri societari – precondizione per il rilevamento automatico dei conflitti di interesse nel ciclo degli appalti – non avviene in modo sistematico attraverso la PDND ma richiede integrazioni ad hoc *case by case*[68].

La terza dimensione è quella dell'integrazione dei dati di beneficial ownership. Lo studio di Tello Arista, Fazekas e Volkotrub ha dimostrato che il collegamento tra dati di appalto e dati di beneficial ownership aumenta del 23-31% la capacità di rilevamento delle situazioni a rischio rispetto all'utilizzo dei soli dati di aggiudicazione. L'Italia non figura tra i sei paesi europei analizzati nel campione principale dello studio, per problemi di qualità e completezza dei dati di beneficial ownership disponibili: il Registro dei Titolari Effettivi, istituito dal d.lgs. 90/2017 in attuazione della IV Direttiva antiriciclaggio e successivamente riformato, ha avuto una storia applicativa travagliata, con significativi ritardi di implementazione e problemi di completezza delle dichiarazioni. La risoluzione di questi problemi è condizione necessaria per l'integrazione dei dati di beneficial ownership nei sistemi ML di analisi del rischio negli appalti[69].

Una valutazione realistica del gap deve altresì considerare il sistema ARACHNE della Commissione europea, che costituisce l'unico strumento di risk scoring per gli appalti parzialmente operativo nel contesto italiano, limitatamente però ai contratti finanziati con fondi strutturali e PNRR. ARACHNE incrocia dati di appalto con informazioni su beneficiari, subappaltatori e persone fisiche associate, producendo alert su situazioni di potenziale conflitto di interesse e frode. La sua limitazione ai fondi europei, la sua architettura centralizzata a livello di Commissione e il suo accesso limitato alle stazioni appaltanti nazionali ne fanno uno strumento utile ma insufficiente rispetto alle esigenze di un sistema di monitoring nazionale sistematico[70].

8. Lo studio di caso: il progetto ACOI

Il progetto ACOI (Assessing Conflicts of Interest), condotto da un team di ricerca che includeva ricercatori dell'Università degli studi di Perugia e il centro di ricerca Transcrime – Università Cattolica del Sacro Cuore, è un caso di studio che permette di apprezzare, in termini concreti e sistematici, le condizioni giuridiche per l'implementazione di un sistema AI anticorruzione nell'ordinamento italiano. Il progetto ha verificato empiricamente la praticabilità tecnica di uno strumento di screening automatizzato del rischio di conflitto di interessi su un campione reale di dirigenti pubblici, documentando la metodologia,

68. Longobucco–Ferwerda 2025, dove gli Autori definiscono il "procurement data gap" come la distanza tra la ricchezza teorica delle banche dati disponibili e l'effettiva idoneità dei dati per l'analisi ML, tenuto conto di: completezza della copertura; struttura e standardizzazione dei formati; qualità e coerenza delle informazioni; accessibilità effettiva per soggetti esterni alle amministrazioni titolari. Per l'Italia, il gap più significativo è identificato nella mancanza di collegamento sistematico tra BDNCP e registri societari (Registro delle Imprese), che rende difficile la verifica automatica del conflitto di interessi nel ciclo degli appalti.

69. Tello Arista–Fazekas–Volkotrub 2026, dove si documenta che, nella maggior parte dei sei paesi europei analizzati (tra cui non figura l'Italia per problemi di qualità del dato sui beneficial owner), il collegamento tra contratti pubblici e dati di beneficial ownership aumenta in modo significativo la capacità di rilevamento di situazioni a rischio di conflitto di interessi rispetto all'utilizzo dei soli dati di aggiudicazione: "matching procurement with BO data reveals an additional 23-31% of high-risk awards that would have gone undetected using procurement data alone".

70. Sul sistema ARACHNE della Commissione europea come strumento di gestione del rischio per i fondi strutturali, cfr. Commissione europea 2023. Il sistema è stato oggetto di pareri del EDPS, che ne hanno validato la compatibilità con il GDPR a condizione del rispetto di specifici standard di qualità dei dati e di trasparenza verso i beneficiari.

i risultati e i nodi giuridici aperti per il passaggio dalla sperimentazione all'operatività sistematica.

8.1. La metodologia ACOI

La metodologia ACOI si articola in due fasi sequenziali: una fase di screening automatizzato, in cui algoritmi di cross-referencing incrociano i dati dei dirigenti dell'amministrazione partner con le fonti informative disponibili; e una fase di validazione qualitativa, in cui un LLM dovrebbe elaborare i profili dei casi flaggati dallo screening automatizzato producendo una valutazione in linguaggio naturale che integra il risk score quantitativo con elementi di contesto che arricchiscono, precisano e confermano (o smentiscono) l'analisi automatizzata del conflitto d'interessi. Il modello ha sviluppato un tool sperimentale per l'esecuzione della fase di screening automatizzato, mentre il sistema basato su LLM per l'assistenza alla fase di analisi qualitativa è ancora in fase di sviluppo. Le fonti informative utilizzate nella fase automatizzata sono: l'Anagrafe Nazionale della Popolazione Residente (ANPR), per la verifica dell'identità e dei dati anagrafici del dirigente e dei familiari conviventi; il Registro delle Imprese (Camera di Commercio), per la verifica delle partecipazioni societarie e degli incarichi in organi societari; il Catasto (Agenzia delle Entrate), per la verifica della titolarità di diritti reali su immobili; Orbis (Bureau van Dijk/Moody's Analytics), per i dati sulle partecipazioni societarie internazionali (e la validazione di quelle nazionali).

La fase di screening automatizzato si articola nella ricostruzione della rete di interessi che fa capo al soggetto interessato (dalla verifica del conflitto d'interessi), compiuta mediante l'articolazione della rete familiare più prossima (dati ANPR) e dall'individuazione degli interessi imprenditoriali, societari ed economici di ciascuno dei componenti di tale rete (Registro delle imprese, Catasto, Orbis). Gli interessi così identificati sono posti a confronto con l'interesse pubblico rilevante al caso (la competenza esercitata dall'organo, le funzioni assegnate all'amministrazione di appartenenza). La classe di interessi è codificata e normalizzata in accordo al nomenclatore "NACE". Il calcolo del conflitto è effettuato sulla base di un criterio di somiglianza: se l'interesse pubblico è identico (o affine) ad uno degli interessi che ricadono nella rete dell'interessato, il tool segnala un potenziale rischio di conflitto. Tale fase è utile a "scremare" le posizioni da sottoporre a verifica, così da concentrare la fase di analisi qualitativa solo sul sotto-insieme così selezionato[71].

Il campione analizzato ha riguardato 485 dirigenti di amministrazioni locali, provinciali, regionali e statali. Di questi, 111 sono risultati collegati a imprese attraverso uno o più legami (titolarità di partecipazioni, cariche societarie, rapporti familiari con i soggetti titolari). Dallo screening automatizzato sono emersi 51 casi flaggati come potenzialmente a rischio (il 46% dei 111 collegati ad interessi economico-finanziari). Su questi 51 casi è stata avviata la validazione qualitativa; di questi, 21 hanno confermato un rischio concreto (il 41% dei flaggati). L'architettura tecnica ha garantito la pseudonimizzazione dei record individuali durante tutto il processo di analisi, secondo le indicazioni formulate in accordo con il Garante privacy.

Tale sperimentazione dimostra che la fase di screening automatizzato è idonea a indirizzare le risorse per la valutazione qualitativa ad un sottoinsieme che corrisponde a circa il 10% del campione (51 su 485), un contributo significativo in termini di efficienza ed efficacia operativa. Il futuro sviluppo dell'analisi qualitativa assistita mediante LLM potrà contribuire ad incrementare ulteriormente la capacità epistemica del sistema.

8.2. La base giuridica nella ricerca

La fase sperimentale del progetto ACOI ha adottato, come base di liceità per il trattamento dei dati personali, la combinazione tra l'art. 6(1)(e) GDPR (esecuzione di un compito di interesse pubblico, nella forma della ricerca scientifica di rilevante interesse pubblico[72]) e il combinato disposto tra l'art. 5 e l'art. 89 del GDPR, che consente deroghe ad alcune garanzie previste dal Regolamento quando il trattamento è effettuato a fini di ricerca scientifica, accompagnate da garanzie adeguate. Il regime applicato ha previsto: la pseudonimizzazione dei record individuali fin dalla fase di raccolta

71. Per una descrizione completa dell'approccio metodologico, cfr. Calderoni–Pollicino–Ponti–Valle 2026, *passim*.

72. Infatti, la sperimentazione del tool ACOI è stato realizzato nel quadro di un progetto di ricerca di rilevante interessa nazionale-PRIN 2022, finanziato su fondi PNRR.

dei dati; la limitazione dell'accesso al team di ricerca; il coinvolgimento del DPO dell'Università e la stipulazione di un Data Processing Agreement con l'amministrazione partner; la distruzione dei dati identificativi alla conclusione della fase di ricerca[73]. Inoltre, occorre considerare che, poiché il trattamento dei dati era funzionale all'esecuzione di un'attività di ricerca, la valutazione di compatibilità della finalità del trattamento rispetto a quella originaria è data per presupposta, sulla base di quanto disposto dall'art. 5 del GDPR[74].

La scelta della base di ricerca scientifica è utile per la fase sperimentale, ma il Rapporto ACOI tematizza esplicitamente il fatto che essa non è trasferibile all'operatività sistematica: un sistema istituzionale di screening del conflitto di interessi richiede, come detto, una base giuridica del tutto diversa (e ben più impegnativa).

8.3. Le condizioni abilitanti: piano normativo, giuridico e tecnico

Che la prevenzione del conflitto di interessi costituisca una finalità di interesse pubblico rilevante ai sensi dell'art. 6(1)(e) GDPR e dell'art. 2-*ter* del Codice privacy è già desumibile dall'assetto normativo vigente: la legge 190/2012, il d.lgs. 39/2013 (artt. 6 e 7 sulla vigilanza ANAC in materia di inconferibilità e incompatibilità degli incarichi), e l'art. 222, co. 8-*bis* del Codice dei contratti pubblici fondano già compiti istituzionali di verifica che sono idonei ad attivare tale base di liceità[75]. L'adozione di sistemi AI a supporto dell'esercizio di queste funzioni, tuttavia, richiede, come visto, condizioni abilitanti ulteriori che l'ordinamento non ha ancora pienamente previsto, sul piano normativo, giuridico e tecnico.

Sul piano dell'architettura normativa, occorre statuire in termini espliciti che l'esercizio di compiti funzionali alla prevenzione della corruzione integra un compito di interesse pubblico rilevante. Ciò può contribuire a modificare il contesto giuridico e istituzionale, incrementando le aspettative di un uso dei dati nella disponibilità del settore pubblico a tali fini. Inoltre, tale qualificazione agevolerebbe l'inclusione di alcune tipologie di dati personali particolari (a cominciare da quelli relativi alle cariche pubbliche e alle appartenenze politiche).

La seconda condizione è la designazione legislativa delle banche dati come fonti autorizzate per la finalità AI anticorruzione. Come evidenziato

73. Calderoni–Pollicino–Ponti–Valle 2026, dove si illustra la base giuridica adottata per la ricerca: art. 6(1)(e) GDPR ("esecuzione di un compito di interesse pubblico") per il trattamento dei dati anagrafici e patrimoniali; art. 89 GDPR e art. 110 del Codice privacy per il trattamento a fini di ricerca scientifica. La distinzione tra base ricerca e base a regime è espressamente tematizzata: "la presente ricerca utilizza la base di liceità della ricerca scientifica per la fase sperimentale; l'implementazione a regime richiederebbe una base giuridica diversa e più robusta, individuata nella prevenzione della corruzione come compito istituzionale delle autorità competenti".

74. Sul regime speciale per il trattamento a fini di ricerca scientifica, cfr. art. 89 GDPR e, nel diritto italiano, art. 110 d.lgs. 196/2003 (come modificato dall'art. 37 d.lgs. 101/2018) e il Codice di deontologia per il trattamento a fini di ricerca scientifica, Allegato 4 al d.lgs. 196/2003 (provvedimento Garante 5 giugno 2019, doc. web n. 9124510). Il regime speciale consente deroghe al principio di minimizzazione e al test di compatibilità della finalità, ma è vincolato ai principi di anonimizzazione o pseudonimizzazione dei dati, di limitazione dell'accesso al team di ricerca e di distruzione dei dati identificativi al termine della ricerca. Inoltre, poiché il trattamento dei dati era funzionale all'esecuzione di un'attività di ricerca, la valutazione di compatibilità della finalità del trattamento rispetto a quella originaria è data per presupposta; cfr. art. 5, par. 2, lett. b) del GDPR, ai sensi del quale "un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali".

75. La legge 6 novembre 2012, n. 190 impone a tutte le pubbliche amministrazioni di adottare misure organizzative per la prevenzione della corruzione. Il d.lgs. 8 aprile 2013, n. 39, agli artt. 6 e 7, attribuisce ad ANAC la vigilanza sul rispetto delle disposizioni in materia di inconferibilità e incompatibilità degli incarichi. L'art. 222, co. 8-*bis* del d.lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici) attribuisce ad ANAC funzioni di monitoraggio con strumenti informatici avanzati sulla Banca Dati Nazionale dei Contratti Pubblici. La prevenzione del conflitto di interessi è pertanto già qualificata come finalità di interesse pubblico rilevante ai sensi dell'art. 6(1)(e) GDPR, e come tale idonea – in linea di principio – ad attivare tale base di liceità per il trattamento dei dati personali necessari alla verifica. Cfr. Ponti 2026.

nell'analisi del principio di limitazione della finalità (§4.3.1), le banche dati che ACOI utilizza – ANPR, Registro delle Imprese, Catasto, e la BDNCP per i contratti pubblici – sono state raccolte per finalità diverse da quelle dello screening AI. Il loro uso secondario richiede un positivo giudizio di compatibilità ai sensi dell'art. 6(4) GDPR, che è raggiungibile ma contestabile caso per caso. La soluzione strutturale è una designazione legislativa esplicita che qualifichi tali banche dati come fonti autorizzate per sistemi AI anticorruzione, sul modello di quanto sperimentato a livello Ue con il Regolamento EHDS. Una tale designazione costituirebbe una base giuridica autonoma che incorpora e risolve a monte il problema della compatibilità delle finalità[76].

Sul piano giuridico-infrastrutturale, l'accesso strutturato alle banche dati pubbliche attraverso la PDND – mediante Accordi di Accessibilità ai sensi dell'art. 50-*ter* CAD – deve essere formalizzato per il caso specifico della verifica istituzionale del conflitto di interessi. Questa formalizzazione è tecnicamente possibile nell'ambito del quadro vigente, ma richiede che la finalità anticorruzione AI sia esplicitamente inclusa tra quelle legittimate dagli Accordi di Accessibilità, il che presuppone la designazione normativa di cui sopra[77]. Un problema strutturale aggiuntivo riguarda i dati sulle partecipazioni societarie internazionali: il progetto ACOI ha risolto il punto ricorrendo ad Orbis, banca dati commerciale. Per un sistema istituzionale a regime, questa soluzione è tecnicamente e giuridicamente insostenibile – per ragioni di trasparenza metodologica, sostenibilità economica e qualità del dato –, e nessuna alternativa pienamente pubblica è attualmente disponibile a livello italiano o europeo[78].

Sul piano tecnico, la prima condizione è la conformità ai requisiti dell'AI Act per i sistemi ad alto rischio. Un sistema istituzionale di risk scoring del conflitto di interessi rientra nell'Allegato III, punto 8 del Regolamento (UE) 2024/1689, che qualifica

76. L'utilizzo delle banche dati ANPR, Registro delle Imprese e Catasto per la verifica del conflitto di interessi dei dirigenti pubblici costituisce un uso secondario rispetto alle rispettive finalità originarie di raccolta (gestione anagrafica, pubblicità legale degli atti societari, gestione tributaria della proprietà immobiliare). Tale uso secondario deve superare il test di compatibilità dell'art. 6(4) GDPR. La valutazione di compatibilità può essere positivamente condotta nell'ordinamento vigente – stante il forte legame strutturale tra la finalità anticorruzione e l'interesse pubblico sottostante alle finalità originarie – ma rimane esposta a contestazioni caso per caso. La soluzione più solida è la designazione legislativa esplicita di tali banche dati come fonti autorizzate per i sistemi AI anticorruzione, seguendo il modello delle Basi di Dati di Interesse Nazionale (BDIN) nell'ambito della PDND (art. 50-*ter* CAD, come modificato dall'art. 47 del d.l. 31 maggio 2021, n. 77) e il modello dello Spazio europeo dei dati sanitari (Reg. (UE) 2025/327, EHDS). Cfr. Ponti 2025.

77. L'accesso strutturato alle banche dati pubbliche attraverso la Piattaforma Digitale Nazionale dei Dati (PDND), ai sensi dell'art. 50-*ter* del d.lgs. 82/2005 (CAD) e del d.p.c.m. 14 ottobre 2021 recante le Linee guida sul punto, avviene mediante Accordi di Accessibilità stipulati tra il soggetto erogatore e il soggetto fruitore dei dati. La formalizzazione di tali accordi per ANAC – con accesso a ANPR, Registro delle Imprese, Catasto e BDNCP – costituisce una condizione tecnico-giuridica necessaria per l'operatività istituzionale del sistema di screening. Essa è possibile nell'ambito del quadro normativo vigente, ma richiede il completamento del percorso di onboarding sulla PDND da parte delle banche dati rilevanti e, in particolare, la designazione normativa della finalità anticorruzione come finalità legittima di accesso, che oggi non è esplicitamente contemplata per il caso dei sistemi AI.

78. L'utilizzo di Orbis (Bureau van Dijk/Moody's Analytics) come fonte per le partecipazioni societarie internazionali è stato il principale compromesso tecnico del progetto ACOI in fase sperimentale. La dipendenza da una banca dati commerciale pone tre ordini di problemi per un sistema istituzionale a regime: (i) sostenibilità economica (i costi di accesso ad Orbis sono significativi per utilizzi sistematici su larga scala); (ii) trasparenza metodologica (la qualità e la completezza dei dati non è verificabile dall'autorità pubblica); (iii) interoperabilità sovranazionale (l'assenza di un identificativo comune standardizzato per le persone giuridiche a livello europeo rende difficile il cross-referencing automatico cross-border senza affidarsi a provider commerciali). Il Business Registers Interconnection System (BRIS), istituito dalla direttiva (UE) 2017/1132 e pienamente operativo dal 2021, costituisce una parziale soluzione a livello europeo per i dati dei registri nazionali delle imprese, ma non copre le partecipazioni non registrate nei registri EU. Cfr. Calderoni–Pollicino–Ponti–Valle 2026.

come ad alto rischio i sistemi AI utilizzati da autorità pubbliche per la valutazione del rischio associato a persone fisiche in ambiti di ordine pubblico e prevenzione di illeciti. Ciò comporta obblighi di gestione del rischio, governance dei dati di addestramento e validazione, documentazione tecnica, registrazione degli eventi, trasparenza e – elemento cruciale – supervisione umana significativa[79]. Questo ultimo requisito impone che l'alert prodotto dal sistema non possa mai essere l'atto finale che determina conseguenze per il soggetto interessato: deve essere input a una decisione umana motivata e revisionabile, con piena garanzia del contraddittorio[80].

La seconda condizione tecnica è l'architettura di pseudonimizzazione embedded nel flusso di trattamento. Il codice fiscale è la chiave di join tra le banche dati, ed è disponibile per questa funzione nell'ordinamento italiano; deve tuttavia essere pseudonimizzato immediatamente dopo il linking, con chiavi di de-pseudonimizzazione conservate separatamente e accessibili solo per i casi di rischio confermato. Il progetto ACOI ha adottato questa architettura nella fase sperimentale: deve essere codificata come obbligatoria nella progettazione del sistema istituzionale. Analogamente, la validazione qualitativa mediante LLM deve avvenire in modalità in-house – senza trasmissione dei dati pseudonimizzati a provider terzi tramite API – per evitare le problematiche di data transfer verso responsabili del trattamento esterni (art. 28 GDPR) e per soddisfare il principio di minimizzazione quale inteso dall'EDPB nell'Opinion 28/2024[81].

8.4. Un imperativo europeo non più differibile

Le condizioni normative, giuridiche e tecniche identificate, oltre che opzioni di policy discrezionalmente perseguibili, costituiscono nell'attuale scenario un tassello cruciale della strategia nazionale di prevenzione che la direttiva dell'Unione europea sulla prevenzione e il contrasto della corruzione impone a tutti gli Stati membri di adottare[82]. La

79. Il Regolamento (UE) 2024/1689 (AI Act), Allegato III, punto 8, classifica come sistemi AI ad alto rischio quelli utilizzati da autorità pubbliche "per valutare i rischi, tra cui il rischio di sicurezza o di recidiva, posti da una persona fisica, o per la valutazione della personalità e delle caratteristiche o delle condotte passate di persone fisiche o gruppi nel contesto di attività di contrasto". Un sistema istituzionale di screening del conflitto di interessi che produce risk score su singoli dirigenti pubblici rientra nella medesima categoria. I requisiti dei sistemi ad alto rischio includono: sistema di gestione dei rischi (art. 9); governance dei dati di addestramento e validazione (art. 10); documentazione tecnica (art. 11); registrazione automatica degli eventi (art. 12); trasparenza verso i deployer (art. 13); supervisione umana significativa (art. 14); accuratezza, robustezza e cybersicurezza (art. 15). La supervisione umana significativa (art. 14) esclude che l'alert prodotto dal sistema possa essere l'atto finale che determina misure nei confronti del soggetto interessato: l'alert è input a una decisione umana motivata, con possibilità di contraddittorio.

80. Ai sensi dell'art. 22 del GDPR, le decisioni basate unicamente sul trattamento automatizzato che producono effetti giuridici o che incidono in modo analogo significativamente sulla persona fisica sono in linea di principio vietate, salvo eccezioni tassative. EDPB 2018 chiarisce che il requisito della supervisione umana deve essere "significativa" e non meramente formale: non è sufficiente che un essere umano "approvi" la decisione del sistema AI senza riesaminarla effettivamente. Il modello human-in-the-loop adottato nel progetto ACOI – in cui l'output del LLM è input alla revisione del team di ricerca, non atto finale – è conforme a questo requisito e deve essere mantenuto nel passaggio all'operatività istituzionale.

81. Sul modello di validazione qualitativa mediante LLM in-house nel progetto ACOI, cfr. Calderoni–Pollicino–Ponti–Valle 2026, pp. 14-16. L'utilizzo di un LLM open-source in modalità in-house – senza trasmissione dei dati pseudonimizzati a provider terzi attraverso API – costituisce la scelta tecnica che minimizza il rischio di violazione del principio di minimizzazione (art. 5(1)(c) GDPR) e dell'obbligo di nomina del responsabile del trattamento esterno (art. 28 GDPR). Per un sistema istituzionale a regime, questa scelta deve essere resa obbligatoria dall'architettura tecnica: i dati pseudonimizzati dei dirigenti non devono mai uscire dal perimetro informatico dell'autorità titolare del trattamento. Cfr. EDPB 2024.

82. La direttiva UE sulla prevenzione e il contrasto della corruzione, accordo politico interistituzionale del 9 gennaio 2026 (in corso di adozione formale), all'art. 20 impone agli Stati membri di adottare misure nazionali di prevenzione della corruzione che includano meccanismi di verifica istituzionale affidati a organismi competenti

direttiva sembra optare per il modello della verifica istituzionale – la "trasparenza verticale"[83] affidata a organismi competenti dotati delle risorse necessarie – in coerenza con la giurisprudenza della Corte di giustizia (C-184/20) e anche quella della Corte costituzionale italiana (n. 20/2019) che sembrano precludere alla possibilità che la trasparenza diffusa possa rappresentare uno strumento proporzionato di (efficace) verifica del conflitto di interessi[84]. Il progetto ACOI ha dimostrato empiricamente che questo modello è tecnicamente praticabile nell'ordinamento italiano. Le condizioni abilitanti identificate in questo paragrafo costituiscono l'insieme di interventi – normativi, giuridici e tecnici – senza i quali il risultato sperimentale rischia di rimanere un proof of concept non trasferibile all'operatività sistematica, con un gap che è al tempo stesso verso l'obbligo europeo e verso l'opportunità che la disponibilità tecnica della soluzione ha aperto.

9. Conclusioni: un'agenda non più rinviabile

L'analisi svolta nelle pagine precedenti permette di enunciare, in forma sintetica, le proposizioni principali che emergono dalla ricognizione comparata e dall'analisi dell'ordinamento italiano. Non sono proposte come proposizioni meramente descrittive: sono le premesse di un'agenda normativa e organizzativa la cui urgenza è imposta sia dalle opportunità documentate dalla letteratura comparata sia dagli impegni derivanti dalla direttiva anticorruzione, impegni che occuperanno il legislatore nazionale nell'immediato futuro.

La prima proposizione è di ordine epistemologico: l'intelligenza artificiale non è uno strumento di indagine penale sulla corruzione, ma uno strumento di governance preventiva del rischio. Le sette tipologie di contributo epistemico analizzate nel presente saggio producono conoscenza preziosa e impossibile da generare altrimenti, ma nessuna di esse produce prove nel senso processuale del termine. Il valore dell'AI nell'anticorruzione è nella capacità di rilevare segnali deboli, di costruire mappe di rischio strutturali, di concentrare le risorse di controllo sui punti di maggiore vulnerabilità prima che il danno si produca. Confondere questa funzione con quella investigativa porta a errori sia giuridici sia organizzativi: all'eccesso di aspettative tecnologiche e alla delusione consequenziale; a requisiti di qualità del dato e di robustezza del sistema che si rivelano impossibili da soddisfare quando si tratti di produrre prove; e alla perdita

dotati di risorse adeguate. L'art. 20 sceglie il modello della "trasparenza verticale" – la verifica centralizzata da parte di autorità istituzionalmente competenti – in coerenza con la giurisprudenza della CGUE (sentenza C-184/20, *Vyriausioji tarnybinės etikos komisija*, del 1° agosto 2022) e con la sentenza della Corte costituzionale italiana n. 20/2019, che hanno entrambe escluso la trasparenza diffusa (pubblicazione in chiaro su Internet dei dati personali dei funzionari e dei loro familiari) come strumento proporzionato di prevenzione del conflitto di interessi. Cfr. Ponti 2026.

83. In effetti, mentre le disposizioni in materia di trasparenza "orizzontale" appaiono alquanto generiche (la direttiva inserisce tra le misure di prevenzione "un accesso adeguato ad informazioni di interesse pubblico", art. 29, par. 3), quelle in materia di trasparenza "verticale" appaiono ben più strutturate. Tra le misure suggerite, infatti ci sono "norme sulle dichiarazioni della situazione patrimoniale e *la verifica di tali dichiarazioni*" (art. 29, par. 3, corsivo aggiunto); inoltre, tra i compiti degli "Organismi o unità organizzative anticorruzione", organismi che l'art. 22 impone di istituire, figurano: "la valutazione delle dichiarazioni della situazione patrimoniale dei funzionari nazionali designati a norma del diritto nazionale" nonché "il monitoraggio della conformità alle disposizioni di legge e alle norme sui conflitti di interessi nel settore pubblico" (par. 1, lett. a) e c)).

84. Infatti, se da una parte la sentenza n. 19/2020 della Corte costituzionale italiana ha ridimensionato la praticabilità della prevenzione della corruzione amministrativa per mezzo della diffusione al pubblico di informazioni e dati personali dei funzionari pubblici, limitandola si soli funzionai politici e ai funzionari di carriera con ruoli apicali (cfr. Ponti 2019-b) dall'altra la CGUE è giunta alla conclusione per cui una normativa che prevede la pubblicazione in rete della dichiarazione di interessi privati "in quanto, in particolare, tale pubblicazione riguardi dati nominativi, relativi al coniuge, convivente o partner nonché ai parenti o conoscenti del dichiarante che possono dar luogo a un conflitto di interessi", non è compatibile con il quadro normativo posto a tutela dei dati personali (cfr. C-184/20, *Vyriausioji tarnybinės etikos komisija*, del 1° agosto 2022, in part. par. 116). Sul punto, cfr. Ponti 2026, nonché Gerhold–Lauenstein 2022, e Jacques 2023.

del valore genuino degli strumenti AI, che è nella capacità preventiva, non in quella probatoria.

La seconda proposizione è di ordine comparato: il divario tra l'Italia e i sistemi più avanzati non è tecnologico ma normativo e organizzativo. La BDNCP è una delle banche dati sugli appalti più ricche d'Europa; il codice fiscale consente cross-referencing sistematici che altri ordinamenti devono costruire ad hoc; la PDND offre l'infrastruttura per l'interoperabilità dei dataset pubblici; ANAC ha le competenze istituzionali per la funzione di verifica. Ciò che manca è l'architettura normativa di governance che renda questi strumenti utilizzabili sistematicamente a fini anticorruzione: regole chiare sulla base di liceità per il trattamento; Accordi di Accessibilità standardizzati sulla PDND per le finalità anticorruzione; garanzie procedurali per i soggetti interessati dagli alert; modelli di supervisione umana conformi all'AI Act. Il gap da colmare non richiede investimenti tecnologici di grande entità: richiede intelligenza normativa e coordinamento istituzionale.

La terza proposizione riguarda i canali della verifica del conflitto di interessi: la trasparenza diffusa come meccanismo generale di verifica è sostanzialmente preclusa dal quadro europeo-fondamentale; tale circostanza costituisce, ai fini del nostro discorso, una opportunità. La pubblicazione in chiaro su Internet dei dati patrimoniali e delle partecipazioni societarie dei funzionari pubblici e dei loro familiari, infatti, non è giudicata come proporzionata all'obiettivo di prevenzione del conflitto di interessi, secondo un approccio che è caratteristico della giurisprudenza dalla Corte di giustizia (C-184/2020), e che la Corte costituzionale italiana (n. 20/2019) sembra condividere negli esiti (anche se non nei percorsi argomentativi). La direttiva europea anticorruzione sembra muoversi sulla medesima falsariga: il modello alternativo – la verifica istituzionale, affidata ad autorità competenti con accesso strutturato ai dati attraverso canali di trasparenza verticale, con adeguate garanzie procedurali per i soggetti interessati – non è una soluzione di ripiego ma il modello sistematicamente preferito dall'ordinamento europeo, e l'unico compatibile con il quadro dei diritti fondamentali. Il progetto ACOI ha dimostrato, in sede sperimentale, che questo modello è tecnicamente praticabile nell'ordinamento italiano. La questione ora aperta è se si vuole compiere il passaggio dalla sperimentazione all'operatività sistematica: e la risposta a questa domanda non è tecnica ma politica e normativa.

La quarta e ultima proposizione riguarda l'urgenza dell'agenda. L'art. 22 della direttiva UE anticorruzione impone agli Stati membri di istituire organismi competenti per la prevenzione dotati delle risorse umane, finanziarie e tecnologiche necessarie per adempiere effettivamente ai propri compiti[85]. L'Italia ha già gli organismi (ANAC) e già le risorse informative (BDNCP, ANPR, Infocamere, catasto, banche dati tributarie, etc.). Quello che deve costruire, con urgenza, è l'architettura normativa che renda l'utilizzo di queste risorse sistematico, proporzionato e garantito: un intervento legislativo che specifichi le condizioni del trattamento dei dati per finalità anticorruzione; un sistema di Accordi di Accessibilità standardizzati sulla PDND; un quadro di garanzie procedurali per i soggetti interessati dagli alert; un modello di supervisione e audit dei sistemi AI conforme all'AI Act. Non si tratta di creare qualcosa di nuovo dal nulla: si tratta di connettere ciò che esiste in modo che funzioni nel modo in cui dovrebbe funzionare da tempo. È un'agenda non più rinviabile.

Riferimenti bibliografici

ANAC (2013), *Piano Nazionale Anticorruzione*, 2013

85. Uno dei tratti qualificanti della direttiva è rappresentato dall'esplicito vincolo agli Stati membri a che gli organismi o le unità organizzative "incaricati della prevenzione e della repressione della corruzione siano forniti personale qualificato in numero sufficiente e le risorse finanziarie, tecniche e tecnologiche necessarie per l'efficace esercizio delle funzioni connesse all'attuazione della presente direttiva" (cfr. art. 22): pertanto, nella misura in cui le applicazioni di AI si presentano come idonee ad incrementare non solo l'efficienza, ma pure l'efficacia dell'azione di prevenzione, esse (alla luce della direttiva) smettono di rappresentare una semplice opzione, ma si configurano come elemento necessario, ai fini del dispiegamento della strategia nazionale di contrasto della corruzione, e quindi non eludibile.

APEC Policy Support Unit (2025), *Technologies for Preventing, Detecting, and Combating Corruption*, Issues Paper No. 15, 2025

N. Appelman, R. Ó Fathaigh, J. van Hoboken (2021), *Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands*, in "Journal of Intellectual Property, Information Technology and E-Commerce Law", vol. 12, 2021, n. 4

E. Ash, S. Galletta, T. Giommoni (2025), *A Machine Learning Approach to Analyze and Support Anti-corruption Policy*, in "American Economic Journal: Economic Policy", vol. 17, 2025, n. 2

Banca d'Italia, Unità di Informazione Finanziaria per l'Italia (2026), *Quaderno Statistiche – Segnalazioni di operazioni sospette (SOS)*, secondo semestre 2025, 2026

Banca d'Italia, Unità di Informazione Finanziaria per l'Italia (2025), *Rapporto annuale per il 2024*, n. 17, 2025

BBC News (2018), *A digital game or a powerful weapon against boardroom crime?*, 3 settembre 2018

F. Calderoni, M.C. Pollicino, B. Ponti, S. Valle (2026), *Applicazione di un modello di screening automatico e validazione qualitativa del rischio potenziale di conflitto di interessi,* Studio condotto da Transcrime – Università Cattolica del Sacro Cuore nell'ambito del Progetto ACOI (Assessing conflicts of interest), Università Cattolica del Sacro Cuore, 2026

Commissione europea (2023), *Nota metodologica Arachne*, versione 3.2, 2023

Controladoria-Geral da União (2022), *Alice: Desafios, resultados e perspectivas da ferramenta de auditoria contínua de compras públicas governamentais com uso de inteligência artificial*, in "Revista da CGU", vol. 14, 2022, n. 26

EDPB (2024), *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, 17 dicembre 2024

EDPB (2018), *Guidelines 01/2018 on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (ex WP251rev.01)*, Version 2.0, 6 febbraio 2018

EDPB-EDPS (2021), *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 giugno 2021

FAO (2024), *Global Forest Observations Initiative (GFOI), GFOI Forest Foresight – Predicting deforestation*, 2024

J. Gallego, G. Rivero, J. Martínez (2021), *Preventing rather than punishing: An early warning model of malfeasance in public procurement*, in "International Journal of Forecasting", vol. 37, 2021, n. 1

M. Gerhold, J. Lauenstein (2022), *Litauens Ethikkommission als Datenschutzverletzerin: Nordische Transparenz und europarechtlicher Datenschutz*, in "Europarecht", vol. 67, 2022, n. 6

C. Gerli (2026), *Artificial Intelligence in Anti-Corruption. Comparative Insights from Public Procurement across the EU*, Tesi di dottorato, Università di Bologna, 2026

GIZ (2024), *Inspector AI tackles money laundering*, 25 marzo 2024

Global Fishing Watch (2022), *Global analysis shows where fishing vessels' identification switched off*, 1 novembre 2022

GOV.UK (2025), *Initial findings of our e-discovery review*, 2 febbraio 2025

F. Jacques (2023), *Protection des données à caractère personnel: la Cour de justice a-t-elle transformé le RGPD en un instrument d'une sensibilité extrême? Note d'observations sous CJUE (GC), 1er août 2022, C-184/20 (OT)*, in "Revue du Droit des Technologies de l'information", vol. 91, 2023, n. 2

E. Katona, M. Fazekas (2024), *Hidden barriers to open competition: Using text mining to uncover corrupt restrictions to competition in Hungarian public procurement*, GTI Working Paper 2024:01, Government Transparency Institute, 2024

N. Köbis, C. Starke, I. Rahwan (2022), *The promise and perils of using artificial intelligence to fight corruption*, in "Nature Machine Intelligence", vol. 4, 2022, n. 5

A. Longobucco, J. Ferwerda (2025), *Fighting Corruption with Artificial Intelligence: Searching for Suitable Public Procurement Data in the EU*, BridgeGap Working Paper 25-01, 2025

G. Mancini Palamoni (2024), *Il paradigma digitale dell'evidenza pubblica*, in "Ceridap", 2024, n. 2

F. Odilla (2025), *The Digitalisation of Anti-Corruption in Brazil: Scandals, Reforms, and Innovation*, Routledge, 2025

F. Odilla (2023), *Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology*, in "Crime, Law and Social Change", 2023

F. Odilla, A. Mattoni (2023), *Unveiling the layers of data activism: The organising of civic innovation to fight corruption in Brazil*, in "Big Data & Society", vol. 10, 2023

OECD (2026), *Anti-Corruption and Integrity Outlook 2026*, OECD Publishing, 2026

OECD (2025-a), *AI in fighting corruption and promoting public integrity, in Governing with Artificial Intelligence*, OECD Publishing, 2025

OECD (2025-b), *Using digital technology to strengthen oversight of public procurement in Portugal: The use of data analytics and machine learning by the Tribunal de Contas,* OECD Publishing, 2025

OECD (2024-a), *Strengthening Oversight of the Court of Auditors for Effective Public Procurement in Portugal: Digital Transformation and Data-Driven Risk Assessments*, OECD Publishing, 2024

OECD (2024-b), *Generative AI for anti-corruption and integrity in government: Taking stock of promise, perils and practice*, OECD Publishing, 2024

OECD (2019), *Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments*, OECD Publishing, 2019

Open Contracting Partnership (2024), *Red Flags in Public Procurement: A Guide to Using Data to Detect and Mitigate Risks*, 2024

OpenText (2018), *UK Serious Fraud Office Selects OpenText to Expedite Data Discovery and Investigations,* 10 aprile 2018

F.S. Paolo, D. Kroodsma, J. Raynor, T. Hochberg, P. Davis, J. Cleary, L. Marsaglia, S. Orofino, C. Thomas, P. Halpin (2024), *Satellite mapping reveals extensive industrial activity at sea*, in "Nature", vol. 625, 2024, n. 7993

I. Parvanova (2025), *The use of big data by anti-corruption authorities*, U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute, 2025

B. Ponti (2026), *Verifica del conflitto di interessi e prevenzione della corruzione. Il nodo del trattamento dei dati personali,* in E. Carloni (a cura di), "Abuso di potere e pubblica amministrazione. Integrazione ed effettività dell'anticorruzione tra prevenzione e repressione", Il Mulino, 2026, in corso di pubblicazione

B. Ponti (2025), *Trattamento dei dati personali e standard di legalità: elementi di preminenza delle esigenze di circolazione?*, in "Rivista italiana di informatica e diritto", 2025, n. 2

B. Ponti (2023-a), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

B. Ponti (2023-b), *Tre scenari di digitalizzazione amministrativa «complessa»: dalla interoperabilità predicata alla standardizzazione praticata*, in "Istituzioni del federalismo", 2023, n. 3

B. Ponti (2022), *Le diverse declinazioni della "Buona amministrazione" nel PNRR*, in "Istituzioni del federalismo", 2022, n. 2

B. Ponti (2019-a), *La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi,* in "Il diritto dell'informazione e dell'informatica", 2019, n. 2

B. Ponti (2019-b), *Il luogo adatto dove bilanciare. Il «posizionamento» del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019*, in "Istituzioni del federalismo", 2019, n. 2

A. Rachovitsa, N. Johann (2022), *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case*, in "Human Rights Law Review", vol. 22, 2022, n. 2

M. Resimić (2025), *Harnessing artificial intelligence (AI) for anti-corruption. Benefits and challenges in prevention, detection and investigation*, U4 Helpdesk Answer 2025:24, U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute, 2025

M. Rusinov (2025), *The Use of Network Analysis for the Detection of Corruption in Public Procurement: The Bulgarian Case as a Testing Ground*, in "Public Policies.bg", vol. 16, 2025, n. 2

South China Morning Post (2019), *China's corruption-busting AI system 'Zero Trust',* 4 febbraio 2019

I. Tello Arista, M. Fazekas, A. Volkotrub (2026), *Using Beneficial Ownership Data for Systematic Risk Assessment in Public Procurement. The Example of 6 European Countries,* in "European Journal on Criminal Policy and Research", 2026

U4 Anti-Corruption Resource Centre (2023), *Unlocking AI's potential in anti-corruption: Hype vs. reality*, 2023

WP29 – Article 29 Data Protection Working Party (2014), *Opinion 05/2014 on Anonymisation Techniques*, WP216, 0829/14/EN, 10 aprile 2014

WP29 – Article 29 Data Protection Working Party (2013), *Opinion 03/2013 on purpose limitation*, WP 203, 2 aprile 2013

WWF Netherlands (2022), *Forest Foresight Prospectus*, 2022

D. Zinnbauer (2025), *Artificial intelligence in anti-corruption – a timely update on AI technology*, U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute, U4 Brief 2025:1, 2025