

# Rassegna Stampa

di Lunedì 14 ottobre 2024



**Centro Studi C.N.I.**

# Sommario Rassegna Stampa

<b>Pagina</b>	<b>Testata</b>	<b>Data</b>	<b>Titolo</b>	<b>Pag.</b>
<b>Rubrica Sicurezza</b>				
1	Italia Oggi Sette	14/10/2024	<i>Cybersicurezza: chi deve fare cosa. Il cronoprogramma degli adempimenti (A.Ciccio Messina)</i>	3
<b>Rubrica Innovazione e Ricerca</b>				
12	Il Sole 24 Ore	14/10/2024	<i>La mancanza di competenze digitali sfiora il 55%</i>	6
1	Il Sole 24 Ore	14/10/2024	<i>L'intelligenza artificiale e' gia' realta' nei piani di 10mila imprese italiane (C.Tucci)</i>	7
<b>Rubrica Pubblica Amministrazione</b>				
1	Il Sole 24 Ore	14/10/2024	<i>Una nuova cultura per la manutenzione (R.Brunetta)</i>	9

IMPRESE E P.A. ALL'APPELLO

**Cybersicurezza:  
chi deve fare cosa  
Il cronoprogramma  
degli adempimenti**

Ciccia Messina a pag. 7

**I settori assoldati per la lotta ai cybercriminali**

<b>Settori ad alta criticità</b> <i>(allegato I)</i>	Energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi Tic, servizi spaziali
<b>Settori critici</b> <i>(allegato II)</i>	Servizi postali, gestione dei rifiuti, chimica, alimentare, fornitura di servizi digitali e la ricerca, fabbricazione di dispositivi medici, computer e prodotti di elettronica, apparecchiature elettriche, di autoveicoli, rimorchi e mezzi di trasporto
<b>Pubbliche amministrazioni</b> <i>(allegato III)</i>	Organi costituzionali, presidenza del consiglio dei ministri, ministeri, agenzie fiscali, autorità indipendenti, amministrazioni regionali, locali tra cui Asl e comuni capoluogo e quello con più di 100 mila abitanti e, infine, altri enti
<b>Ulteriori soggetti</b> <i>(allegato IV)</i>	Servizi di trasporto pubblico locale, istituti di istruzione e ricerca, soggetti del settore culturale e società in house o partecipate pubbliche

**SICUREZZA INFORMATICA**

*Cosa devono fare imprese e p.a. secondo il dlgs 138/2024, che recepisce la direttiva Ue Nis2*

# Cybersicurezza a tappe serrate

## All'appello i soggetti coinvolti: via alla registrazione sul web

Pagina a cura di

**ANTONIO CICCIA MESSINA**

**P**arte il conto alla rovescia degli obblighi previsti dalla cybersicurezza a tinte Ue. Tra gli adempimenti più significativi spiccano l'adozione di policy multirischio e l'obbligo di pre-notifica, entro 24 ore, degli incidenti informatici alle autorità preposte alla cybersicurezza. Chiamate a revisionare il proprio apparato documentale e organizzativo, relativo alla sicurezza di dispositivi, reti e sistemi, saranno molte imprese e numerose pubbliche amministrazioni: dovranno percorrere un tragitto a tappe serrate, con le prime scadenze fissate già a gennaio 2025. E quanto prevede il dlgs 138/2024, che ha recepito la direttiva Ue Nis2 n. 2022/2555 e che ha elencato, in quattro allegati, le categorie degli enti coinvolti nella realizzazione della sicurezza delle reti e dei sistemi informativi.

Il dlgs 138/2024 è stato pubblicato nella *Gazzetta Ufficiale* n. 230 del 1° ottobre 2024, entra in vigore il 16 ottobre 2024 e inizia ad avere efficacia dal 18 ottobre 2024: in questo quadro, si può ora fissare il cronoprogramma esecutivo degli adempimenti.

**Un nuovo perimetro di sicurezza.** Il dlgs 138/2024, in attuazione della direttiva 2022/2555, ha esteso la platea degli enti pubblici e privati tenuti a collaborare contro gli attacchi alle reti e alle infrastrutture informatiche.

Il nuovo perimetro di sicurezza comprende tra gli altri, i seguenti settori: energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi Tic e spazio; fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica; pubbliche amministrazioni centrali, regionali e locali.

Delimitato l'ambito di applicazione, il decreto legislativo ha selezionato, utilizzando la

nuova nomenclatura della direttiva Nis2, i soggetti "essenziali" e "importanti", in base ai requisiti dimensionali e alla tipologia di prodotti o servizi forniti. Per esempio, nella categoria dei soggetti essenziali ricadono i soggetti presenti nei settori ad alta criticità che superano i massimali per le medie imprese.

Il provvedimento, peraltro, non solo ha ridisegnato la platea dei soggetti pubblici e privati, ma ha anche imposto agli enti coinvolti di dotarsi di un sistema di gestione efficace contro i criminali informatici e di collaborare con le autorità.

I soggetti essenziali e i soggetti importanti devono, dunque, alzare adeguate barriere per la gestione dei rischi per la sicurezza informatica (articolo 24), tra cui assicurare la continuità dei servizi, secondo un approccio che viene definito nel provvedimento "multi-rischio" e cioè teso a proteggere i sistemi informativi e di rete e anche il loro ambiente fisico da incidenti.

Sempre i soggetti essenziali e importanti sono tenuti a notificare alle autorità di settore gli incidenti informatici significativi. L'articolo 25 del decreto legislativo prevede termini rapidi per la notifica degli incidenti. In prima battuta, si deve mandare una pre-notifica senza ingiustificato ritardo, e comunque entro 24 ore, cui far seguire, al massimo entro 72 ore dalla conoscenza del fatto, una notifica completa, corredata da una valutazione iniziale dell'incidente, della sua gravità e del suo impatto.

Il decreto legislativo, infine, prevede uno specifico apparato sanzionatorio allo scopo di garantire una maggiore uniformità e deterrenza in tutta l'Ue contro condotte lassiste che mettono in pericolo la comunità nazionale: all'articolo 38 sono previste sanzioni amministrative pecuniarie (tra le altre per la violazione degli obblighi di notificazione degli incidenti) fino a 10 milioni di euro o, se superiore, fino al 2% del fatturato, comunque graduate per i diversi illeciti e per i diver-

si soggetti obbligati (essenziali, importanti, pubbliche amministrazioni, ecc.).

**Una piattaforma digitale dei soggetti coinvolti.** Il dlgs prevede una piattaforma digitale dei soggetti tenuti agli adempimenti di cybersicurezza. Si tratta di un registro dei soggetti che sono tenuti agli obblighi previsti dal dlgs 138/2024.

Il termine per la registrazione o l'aggiornamento dell'iscrizione è fissato dal 1° gennaio al 28 febbraio di ogni anno.

Dal 1° gennaio al 28 febbraio 2025, dunque, i soggetti tenuti agli adempimenti di cybersicurezza (chiamati soggetti essenziali e importanti) dovranno registrarsi su una piattaforma digitale messa a disposizione dalle autorità di cybersicurezza (articolo 7).

In fase di prima attuazione, il termine per la registrazione è fissato al 17 gennaio 2025 per fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network (articolo 42).

**Via ogni anno a un elenco dei soggetti essenziali e importanti.** Entro il 31 marzo 2025 e, a seguire entro il 31 marzo di ogni anno successivo, l'Autorità nazionale competente Nis, redigerà l'elenco dei soggetti essenziali e dei soggetti importanti, sulla base delle registrazioni pervenute e verificate. La stessa autorità, tramite la piattaforma, comunicherà ai soggetti registrati l'inserimento nell'elenco e la qualifica.

Dal 15 aprile al 31 maggio 2025 e, poi di ogni anno successivo, i soggetti che hanno ricevuto la comunicazione, integrano le informazioni, sempre tra-

mite la piattaforma digitale, indicando spazio IP, nomi di dominio disponibili, ambito territoriale di fornitura dei servizi, rappresentanti legali (che sono anche responsabili degli inadempimenti in caso di violazioni), punti di contatto.

**Notifica degli incidenti tempestiva.** Il dlgs dedica gli articoli da 23 a 33 alla disciplina degli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente. Sono obblighi di pianificazione, di adeguamento organizzativo e tecnologico, di collaborazione e coordinamento con le autorità di sicurezza. Tra questi obblighi è compreso, all'articolo 25 del dlgs 138/2024, l'obbligo di notifica di tutti gli incidenti che hanno un impatto significativo sull'erogazione dei servizi.

In fase di prima applicazione e cioè fino al 31 dicembre 2025, il dlgs prevede una applicazione graduale. In particolare, l'articolo 42 del dlgs 138/2024 stabilisce che il termine per l'adempimento degli obblighi dettati dal citato articolo 25 è fissato in nove mesi dalla ricezione della comunicazione da parte dell'autorità nazionale dell'inserimento nell'elenco dei soggetti essenziali o importanti. Decorso il termine, gli enti devono notificare gli incidenti seguendo le modalità previste dal dlgs in commento.

**Da approvare misure interne.** Il catalogo degli adempimenti prevede l'approvazione delle misure di gestione dei rischi e della sicurezza informatica e dei piani di formazione (articolo 23), l'adozione di misure tecniche, operative e organizzative, tra cui analisi multi-rischio, precauzioni per la continuità operativa, sistemi di crittografia e controllo degli accessi (articolo 24) e adempimenti specifici per i gestori dei registri di nomi di dominio (articolo 29).

Il termine per l'adempimento degli obblighi è fissato in diciotto mesi dalla medesima comunicazione dell'inserimento negli elenchi dei soggetti nella

piattaforma digitale.

Al palo alcuni provvedimenti attuativi. Peraltro, non ci sono ancora tutti i dettagli della disciplina, alla quale imprese e pubbliche amministrazioni dovranno attenersi.

Innanzitutto, per gli obblighi di notifica e le misure interne l'Autorità nazionale competente Nis potrà stabilire modalità e specifiche di base.

Oltre a ciò, l'articolo 40 affida alla Presidenza del consiglio dei ministri e alla Autorità nazionale di cybersicurezza di adottare, secondo un calendario che arriva fino all'aprile del 2026, numerosi provvedimenti attuativi.

Tra questi si segnala che è stata affidata all'autorità nazionale di cybersicurezza l'individuazione, entro il 16 novembre 2024, dei soggetti ai quali si applicano le norme si applicano a prescindere dalle loro dimensioni (articolo 3, commi 8 e 9).

Entro aprile 2025, inoltre, è atteso il dpcm con le norme di dettaglio su vigilanza e sanzioni.

Sempre in relazione alla transizione al nuovo regime, va segnalato che le regole previste dal dlgs 65/2018 per i soggetti dallo stesso considerati (in particolare disposizioni sulla gestione della sicurezza informatica e sulla notifica degli incidenti a carico di operatori di servizi essenziali) continueranno ad applicarsi fino alla approvazione dei provvedimenti attuativi previsti dall'articolo 40 del dlgs 138/2024.

**Il dlgs 138/2024  
entra in vigore il 16  
ottobre 2024 e  
inizia ad avere  
efficacia dal 18  
ottobre 2024: in  
questo quadro, si  
può fissare il  
cronoprogramma  
esecutivo degli  
adempimenti**



# La mancanza di competenze digitali sfiora il 55%

## A caccia di skill

### Non si trova personale specializzato, specie ai livelli manageriali

Negli ultimi cinque anni, vale a dire dal 2019 a oggi, le richieste di professionisti con competenze in intelligenza artificiale sono aumentate del 157 per cento. Eppure, queste "skill" sono molto difficili da trovare: la mancanza di competenze digitali è infatti il principale ostacolo all'adozione dell'Ia, identificato dal 55% delle aziende intervistate nello studio di 4.Manager, coordinato dal responsabile scientifico, dell'Osservatorio, Giuseppe Torre. Se si pensa che, nel 2023, solo il 46% della popolazione italiana possedeva competenze digitali di base, un dato inferiore alla media Ue del 56%, possiamo forse meglio comprendere l'entità della sfida che ci attende.

E così non sorprende che poco più di un'azienda su due, il 53,6% per l'esattezza, abbia inserito nuove figure professionali legate all'Ia nell'ultimo anno, mentre il 15,2% sta pianificando di farlo nel prossimo futuro. Manca personale specializzato, in particolare ai livelli manageriali. Le imprese italiane stanno cercando profili che combinano competenze tecniche, capacità di analisi critica e leadership. Tra le figure più richieste, spicca l'Ia Integration Specialist, indicata dal 18,6% delle imprese come la figura chiave per guidare l'implementazione dell'intelligenza artificiale. Seguono il Chief Data Officer (9,3%) e l'Ia Strategy Director (8,9%), che sottolineano l'importanza della gestione strategica dei dati. Altri ruoli includono il Data Science Manager (8,4%) e il Chief Ia Officer (7,2%) per una guida specializzata e una gestione

complessa per l'integrazione delle tecnologie emergenti.

La formazione, in particolare quella continua, è quindi fondamentale, visto che il 45,7% dei dirigenti e manager e il 55,2% degli altri lavoratori non hanno mai seguito alcun corso specifico sull'intelligenza artificiale nell'ultimo anno. Le aziende lo fanno e stanno mettendo in campo sempre più iniziative formative interne o in collaborazione con università, Its Academy, centri di formazione. Le competenze tecniche, come la gestione e l'analisi dei dati, sono fondamentali per affrontare le sfide della digitalizzazione, ma altrettanto importanti sono le soft skills come pensiero critico, flessibilità al cambiamento e capacità di gestire il processo di trasformazione. Ai manager poi sono richiesti visione strategica e competenze trasversali.

Un'ulteriore spinta arriverà da 4.Manager che metterà a disposizione delle parti sociali un sistema di Skill Intelligence, basato sull'analisi di quasi mezzo milione di offerte di lavoro e dati provenienti da Inps, Sviluppo Lavoro Italia e dal sistema europeo Esco. Questo strumento consentirà alle aziende di identificare i bisogni formativi e progettare percorsi mirati per affrontare l'evoluzione tecnologica.

© RIPRODUZIONE RISERVATA

**I profili più richiesti sono l'Ia Integration specialist o Strategy director e il Chief data officer**

Intelligenza artificiale nei prodotti o servizi di 10mila imprese

**NEL 1999, ERAVAMO LA TUA NUOVA BANCA. NEL 2024, SIAMO LA TUA BANCA DI SEMPRE.**

15.000€

# L'intelligenza artificiale è già realtà nei piani di 10mila imprese italiane

## Rapporto di 4.Manager

In un anno crescita del 30%  
Boom dei professionisti:  
su da 40mila a 300mila

A settembre quasi 10mila imprese italiane hanno utilizzato, o integrato, l'intelligenza artificiale nelle proprie linee di prodotto o servizio, con una crescita di circa il 30% rispetto al 2023. Parallelamente è cresciuta, in maniera esponenziale, la richiesta di pro-

fessionisti alle prese con l'ia, che sono passati dai 40mila di inizio 2024 agli oltre 300mila di oggi (+650%). A dirlo è il VI rapporto dell'Osservatorio di 4.Manager «Intelligenza Artificiale. Cambiamento culturale e organizzativo per imprese e manager: nuove traiettorie della managerialità», che verrà presentato oggi a Roma.

Tuttavia non mancano gli ostacoli, a partire dalla disomogeneità nell'utilizzo dell'ia tra le grandi realtà e le Pmi e dalla difficoltà a reperire le competenze. Il gap delle skill digitali richieste dalle aziende è arrivato al 55 per cento.

**Claudio Tucci** — a pag. 12

# Intelligenza artificiale nei prodotti o servizi di 10mila imprese

**Il rapporto di 4.Manager.** In un anno la crescita nell'uso dell'ia è stata del 30%  
Boom della domanda di professionisti: da 40mila a 300mila (+650 per cento)

Pagina a cura di  
**Claudio Tucci**

A settembre quasi 10mila imprese italiane hanno utilizzato, o integrato, l'intelligenza artificiale nelle proprie linee di prodotto o servizio, con una crescita di circa il 30% rispetto a 12 mesi prima. Non sorprende quindi la richiesta esponenziale di professionisti alle prese con l'ia, passati da 40mila a inizio 2024 agli attuali oltre 300mila (+650%). Uno sviluppo accompagnato da un forte aumento della partecipazione fem-

minile nel settore, che è salita dal 30 a oltre il 40 per cento. Tuttavia non mancano gli ostacoli: la diffusione dell'intelligenza artificiale nelle aziende rivela una chiara disomogeneità tra le grandi realtà e le Pmi e servono investimenti non solo in tecnologie, ma anche nelle competenze manageriali indispensabili per guidare l'innovazione.

Il VI rapporto dell'Osservatorio di 4.Manager «Intelligenza Artificiale. Cambiamento culturale e organizzativo per imprese e manager: nuove traiettorie della managerialità», che verrà presentato oggi a Roma in occasione

dell'apertura dell'anno accademico della Pontificia Università Antonianum, scatta una fotografia «sul campo» del rapporto lavoro-nuove tecnologie. Molte imprese (48,1%) integrano l'ia per migliorare i processi, mentre il 40% sottolinea l'importanza della collaborazione interdisciplinare per sfruttarne al meglio i benefici. Le realtà più grandi adottano l'intelligenza artificiale al 24% contro il 5% di piccole e medie. Milano, Roma, Torino, Bologna e Napoli sono i principali centri di adozione nei settori It, sviluppo software e servizi di ricerca.

L'adozione dell'ia nelle aziende italiane è però ancora agli inizi: il 35% la utilizza in maniera limitata o sperimentale, mentre solo l'1,9% la considera una priorità strategica. La maggior parte delle aziende è ancora in una fase di esplorazione, cercando di capire come l'intelligenza possa essere applicata in modo efficace ai loro modelli di business. Tutti sono d'accordo su un punto: la leadership aziendale gioca un ruolo centrale in questo processo, ma, anche qui, solo il 23,8% delle imprese dichiara di avere una leadership fortemente proattiva nell'implementazione dell'ia. «Sebbene l'intelligenza artificiale

stia rivoluzionando il mondo dell'impresa il vero valore continua a risiedere nell'intelligenza umana - sottolinea Stefano Cuzzilla, presidente di 4.Manager e Federmanager -. I nostri sistemi produttivi sono miniere di saperi e abilità, in gran parte ancora inesplorate dall'ia, che aspettano di essere valorizzate. Purtroppo ad oggi, l'investimento in formazione è ancora insufficiente rispetto alla portata delle trasformazioni in atto. Serve un concreto cambio di passo».

«L'innovazione tecnologica è un motore dello sviluppo del Paese ed è fondamentale la capacità di guidare il

cambiamento per assicurare alle nostre imprese la disponibilità di competenze e di know-how adeguatamente formato, per aiutarle a massimizzare le opportunità di investimenti in nuove tecnologie ed essere più competitive sui mercati nazionali ed internazionali - aggiunge Alberto Tripi, special advisor di Confindustria per l'Intelligenza artificiale -. Insomma, l'ia apre nuove e ampie opportunità, cambia, trasforma ma non distrugge il lavoro, elevandone il livello qualitativo e aumentando i benefici non soltanto per le imprese ma per gli stessi lavoratori».

© RIPRODUZIONE RISERVATA

**24%**  
Grandi imprese

**Tasso di adozione**

L'adozione dell'AI nelle grandi imprese italiane arriva al 24 per cento

**5%**  
Pmi

**Utilizzo più moderato**

All'interno della piccole e medie imprese l'adozione dell'ia scende al 5 per cento

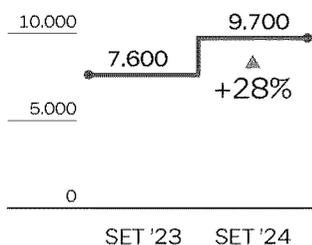
**40%**  
Le donne

**In aumento**

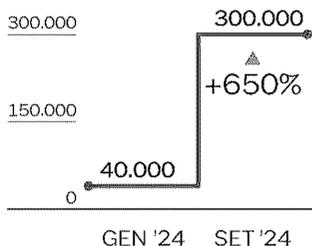
La partecipazione femminile al settore è salita dal 30 a oltre il 40 per cento

**La fotografia**

**LE IMPRESE CHE USANO L'IA**  
Analisi siti corporate



**L'ANALISI DELLA DOMANDA**  
Professionisti con competenze



**GLI OSTACOLI PER LE AZIENDE**  
Variazione percentuale



**STEFANO CUZZILLA**  
Presidente di 4.Manager e Federmanager



**ALBERTO TRIPI**  
Special advisor di Confindustria per l'Intelligenza artificiale

(\*) Software o sistemi esistenti. Fonte: Osservatorio 4.Manager | Sesto Rapporto

SERVIZI E PA

## UNA NUOVA CULTURA PER LA MANUTENZIONE

di Renato Brunetta — a pagina 14



**RENATO  
BRUNETTA**  
Presidente  
del Consiglio  
nazionale  
dell'economia  
e del lavoro

# Al nostro Paese ora serve una nuova cultura della manutenzione

Giorno dopo giorno, senza clamore

Renato Brunetta

**M**igliora l'istruzione, crescono l'emancipazione femminile e la sostenibilità ambientale, soffre la sanità, si rafforzano gli uffici pubblici, resta carente la cultura della manutenzione: è un quadro a luci e ombre quello offerto dalla Relazione annuale sulla qualità dei servizi erogati dalle pubbliche amministrazioni centrali e locali alle imprese e ai cittadini, che si presenta stamane al Cnel. Appuntamento di trasparenza e di valutazione, ulteriore tappa del percorso avviato con la legge 15/2009, durante il mio primo mandato come ministro per la Pubblica amministrazione e dell'innovazione, che ha assegnato proprio al Cnel il compito di redigere questa Relazione. L'edizione di questo anno, pur nella continuità, presenta diversi elementi di novità: in primo luogo un approccio maggiormente orientato alla valutazione dell'impatto sugli utenti finali, nel quadro degli obiettivi di sviluppo sostenibile dell'Agenda Onu 2030. Altro elemento di innovazione è la valorizzazione delle buone pratiche, con il premio del Cnel «Impatto PA», basato su segnalazioni provenienti «dal basso», per privilegiare la prospettiva dei cittadini, delle imprese e delle comunità che ogni giorno interagiscono con la macchina pubblica, frutto di una visione che promuove il dialogo costruttivo e collaborativo tra cittadini/imprese e pubblica amministrazione.

Ma veniamo al punto chiave: lo stato dei servizi pubblici oggi in Italia è duale e frastagliato. Alcuni indicatori di benessere riflettono miglioramenti, come l'aumento della speranza di vita (83,1 anni), un maggior numero di diplomati (65,5% nel 2023 rispetto al 63% del 2022) e una crescita della quota di laureati tra i giovani (25-34 anni). Anche il tasso di abbandono scolastico è in calo (-6 punti percentuali dal 2011 al 2021) e si riduce la platea dei Neet (dal 19% nel 2021 al 16,1% nel 2023). Le donne iscritte all'università superano la media europea (55,9% contro 54,2%) e aumenta il numero di docenti e rettrici donne,

sebbene persistano significativi divari di genere. Dal punto di vista ambientale, la percentuale di raccolta differenziata ha raggiunto una media del 65% a livello nazionale, con punte di eccellenza in molti Comuni, e il riciclaggio è salito al 49,2 per cento.

La gestione delle risorse idriche mostra segnali positivi, con l'aumento degli investimenti per l'approvvigionamento idrico e una buona qualità delle acque balneabili (89% classificate come «eccellenti»). Anche la mobilità sostenibile è in crescita, con l'espansione delle piste ciclabili e un incremento della conversione della mobilità privata verso l'elettrico.

Non mancano, tuttavia, le lacune. Le risorse finanziarie dedicate agli obiettivi di sostenibilità dell'Agenda Onu 2030 sono spesso inferiori alla media europea, soprattutto nel settore della sanità, dove, nonostante la spesa pubblica sia aumentata dal 2020, rimane tra le più basse d'Europa. Di conseguenza, la spesa privata dei cittadini è cresciuta del 5% nell'ultimo anno, a fronte di liste d'attesa per i servizi pubblici spesso insostenibili. Anche la spesa per l'istruzione rimane inferiore rispetto a quella dei principali paesi avanzati. Va detto, e la Relazione lo fa in modo chiaro, che nel corso del 2023 si è ulteriormente consolidato il processo di irrobustimento delle amministrazioni pubbliche, avviato con intensità già nel 2022 grazie alle risorse del Pnrr.

Ma è indispensabile, più che mai, un cambio di paradigma all'insegna di una rinnovata cultura della manutenzione. Una cultura rimossa o marginalizzata perché non si vede, non si annuncia e non genera consenso nell'immediato. Una cultura che, al contrario, dovrebbe acquisire centralità nel disegno delle politiche pubbliche, per il proprio valore sociale. Mi riferisco ai servizi infrastrutturali: scuole, strade, ospedali e anche ferrovie, di cui molto si è parlato proprio in questi giorni. Sei anni fa, il disastro del ponte Morandi ha ricordato a tutti noi, ancora una volta, come l'Italia abbia una storia nobilissima in termini di progettualità, ma non altrettanto dal punto di vista della manutenzione.

Ma c'è dell'altro. Parlare di cultura della manutenzione vuol

dire investire nella rigenerazione urbana e nel recupero delle periferie. Per far questo è necessario superare la logica del breve periodo e del facile consenso. Occorre anche sfuggire alla contrapposizione polarizzante tra pubblico e privato e pensare, invece, a logiche di Public Private Partnership (Ppp). Serve collaborazione, sincronia, corretta ripartizione dei ruoli. È necessario valorizzare i tanti “agenti della manutenzione”, che operano senza grande clamore, giorno dopo giorno, e a cui molto dobbiamo per il benessere collettivo. Penso alle molte reti presenti sul territorio, quelle note e quelle meno note, come la rete – spesso misconosciuta e abbandonata – dei consorzi di bonifica, che hanno

contribuito a cambiare non solo la storia economica, ma anche la fisionomia territoriale del nostro Paese. Penso ancora alla potenziale cura manutentiva dei settori produttivi, che potrebbero svolgere in modo capillare le Camere di commercio. Penso al ruolo che potrebbero avere le piattaforme digitali e l’Ai, laddove la loro potenza di fuoco fosse indirizzata a favorire una strategia di prossimità e di benessere alle persone e ai territori. È indispensabile lavorare uniti, con un ampio coinvolgimento della società civile, impegnata nel confronto su questioni d’interesse comune. E il Cnel, la casa dei corpi intermedi, è una casa aperta. Soprattutto al futuro.

*Presidente del Cnel  
(Consiglio nazionale dell’economia e del lavoro)*

© RIPRODUZIONE RISERVATA

## DAI SERVIZI ALLA RIGENERAZIONE URBANA: NECESSARIO FAVORIRE FORME DI PARTENARIATO FRA PUBBLICO E PRIVATO

