

Corte di Cassazione Sezione Lavoro

Ordinanza 31 marzo 2026 n. 7985

REPUBBLICA ITALIANA
LA CORTE SUPREMA DI CASSAZIONE
SEZIONE LAVORO CIVILE

Composta dagli Ill.mi Sigg.ri Magistrati:

Dott. LEONE Margherita Maria - Presidente

Dott. PAGETTA Antonella - Consigliera

Dott. PONTERIO Carla - Rel. Consigliera

Dott. PANARIELLO Francescopaolo - Consigliere

Dott. MICHELINI Gualtiero - Consigliere

ha pronunciato la seguente

ORDINANZA

sul ricorso 10403-2025 proposto da:

■■■■■ rappresentato e difeso dall'avvocato ■■■■■

- **ricorrente** -

contro

■■■■■ Società con socio unico, soggetta all'attività di direzione e coordinamento di ■■■■■ Spa, in persona del legale rappresentante pro tempore, rappresentata e difesa dall'avvocato ■■■■■

- **controricorrente** -

avverso la sentenza n. 970/2025 della CORTE D'APPELLO di NAPOLI, depositata il 17/03/2025 R.G.N. 1973/2022;

udita la relazione della causa svolta nella camera di consiglio del 14/01/2026 dalla Consigliera CARLA PONTERIO.

Fatti di causa

1. La Corte d'Appello di Napoli ha respinto il reclamo di █████ confermando la sentenza di primo grado che, al pari dell'ordinanza pronunciata all'esito della fase sommaria, aveva rigettato l'impugnativa del licenziamento per giusta causa intimatogli da █████ Spa il 7.1.2020 in relazione a irregolarità commesse nella attestazione delle presenze in servizio, nel periodo da gennaio a ottobre 2019.

La Corte territoriale ha premesso che al █████ con lettera del 27.11.2019, era stato contestato l'allontanamento non autorizzato dalla sede di lavoro e, segnatamente, che lo stesso in numerose occasioni tra gennaio e ottobre 2019 era entrato e uscito dalla sede aziendale senza effettuare le dovute timbrature tramite il badge marcatempo ovvero aveva inserito manualmente sull'applicativo aziendale gli orari di ingresso e uscita in contrasto con i dati rilevati dal sistema di controllo degli accessi delle sedi di lavoro.

La sentenza impugnata ha giudicato inammissibile la domanda, svolta per la prima volta col reclamo, di illegittimità del licenziamento a causa della illegittima registrazione dei dati raccolti nel tempo dal datore di lavoro in violazione del divieto di controllo a distanza, in quanto nuova e basata su elementi fattuali mai prima prospettati.

Ha ricondotto la fattispecie oggetto di causa, concernente la rilevazione delle presenze tramite strumenti di accesso all'azienda (cd. tornelli), sotto la previsione del secondo comma dell'art. 4 St. Lav., nel testo in vigore dall'8.10.2016, che subordina l'utilizzo dei dati raccolti alla condizione che il datore abbia fornito un'adeguata informazione nel rispetto della normativa sulla privacy, di cui al D.Lgs. 196 del 2003; ha ritenuto soddisfatta la citata condizione, comprovata la commissione degli addebiti, di reiterato allontanamento fraudolento del dipendente dal posto di lavoro in orario di servizio, e proporzionata la sanzione espulsiva applicata.

2. Avverso la sentenza █████ ha proposto ricorso per cassazione affidato a due motivi. En.It. Spa ha resistito con controricorso, illustrato da memoria.

3. Il Collegio si è riservato di depositare l'ordinanza nei successivi sessanta giorni, ai sensi dell'art. 380 bis.1 c.p.c., come modificato dal D.Lgs. n. 149 del 2022.

Ragioni della decisione

1. Con il primo motivo di ricorso si denuncia, ai sensi dell'art. 360, comma 1, n. 3 c.p.c., la violazione o falsa applicazione dell'art. 345, comma 1, c.p.c. per avere la Corte d'Appello dichiarato inammissibile la prima censura del primo motivo di reclamo sul presupposto che, con la stessa, il lavoratore avesse introdotto una domanda nuova in appello. Il ricorrente sostiene che, al contrario, l'eccezione di inutilizzabilità a fini disciplinari dei dati raccolti nel tempo dal datore di lavoro (attraverso l'acquisizione a ritroso dei dati sui passaggi ai tornelli aziendali) si basasse sui medesimi fatti già dedotti nei precedenti gradi di giudizio.

2. Con il secondo motivo si denuncia, ai sensi dell'art. 360, comma 1, n. 3 c.p.c., la violazione o falsa applicazione dell'art. 4 St. lav., dell'art. 2119 c.c. e dell'art. 18, comma 4, St. lav. per avere la Corte di merito escluso che il controllo attuato attraverso gli strumenti contemplati dal comma 2 dell'art. 4 cit. sia subordinato alle finalità indicate dal primo comma e, specificamente, all'esigenza di tutela del patrimonio aziendale; inoltre, per non essersi avveduta che il controllo a distanza del lavoratore tramite strumenti di rilevazione delle presenze è legittimo ove avvenga in modo indiretto, preterintenzionale e accidentale mentre è vietato ove si atteggi come controllo diretto sul quantum della prestazione lavorativa, eseguito in modo intenzionale ed ex ante.

Il ricorrente argomenta, sotto altro profilo, la violazione dell'art. 4, comma 3, St. lav., per avere la Corte di merito considerato assolto l'obbligo di adeguata informazione attraverso la trasmissione della Policy n. 164 dell'11.12.2018, pubblicata sulla rete informatica aziendale tramite invio massivo di una e-mail alle ore 17.00 del 20.12.2018 avente ad oggetto il "Controllo accessi alle sedi aziendali".

3. Il secondo motivo di ricorso, che si esamina in via prioritaria per il suo rilievo assorbente, non è fondato.

3.1. Occorre riportare il testo dell'art. 4, St. lav., nella versione applicabile ratione temporis a seguito delle modifiche apportate dal D.Lgs. n. 151 del 2015, che prevede: "1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.... In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

3.2. Come emerge dal chiaro tenore letterale della disposizione, gli strumenti di lavoro e quelli di registrazione degli accessi e delle presenze non rientrano nel raggio di previsione del primo comma dell'art. 4 e la possibilità di utilizzo "a tutti i fini", quindi anche ai fini disciplinari, dei dati e delle informazioni raccolte attraverso tali strumenti è sottoposta, in base al terzo comma, a due condizioni: la prima è che sia data al lavoratore "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli", la seconda condizione attiene al rispetto "di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

3.3. In riferimento al primo comma dell'art. 4, questa Corte ha operato una distinzione tra i controlli a difesa del patrimonio aziendale, che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell'art. 4 novellato in tutti i suoi aspetti, e i "controlli difensivi" in senso stretto, diretti ad accertare specificamente condotte illecite ascrivibili - in base a concreti indizi - a singoli dipendenti, anche se verificatesi durante la prestazione di lavoro; questi ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situano all'esterno del perimetro applicativo dell'art. 4 (Cass. n. 25732 del 2021 cit., punti 31 e 32; Cass. n. 18168 del 2023, p. 7). Poiché non ha ad oggetto una attività - in senso tecnico - del lavoratore, il controllo difensivo in senso stretto deve essere mirato ed attuato ex post, ossia a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto, perché solo a partire da quel momento il datore può provvedere alla raccolta di informazioni utilizzabili (così Cass. n. 25732 del 2021 cit., punti 40 e 44).

I controlli difensivi in senso stretto sono quindi considerati legittimi solo ove ricorra il "fondato sospetto" del datore di lavoro circa comportamenti illeciti di uno o più lavoratori e purché il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto, dovendosi assicurare un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore (v. Cass. n. 25731 del 2021; Cass. n. 25732 del 2021; Cass. n. 34092 del 2021; Cass. n. 18168 del 2023).

3.4. Nella fattispecie oggetto di causa, la Corte di merito ha correttamente ricondotto la rilevazione delle presenze, tramite gli strumenti di accesso all'azienda, alla disciplina dettata dal secondo comma del citato art. 4, che prescinde sia dai presupposti richiesti dal primo comma e sia dagli ulteriori elementi individuati dalla giurisprudenza come necessari a legittimare i cd. controlli difensivi in senso stretto. Da ciò discende l'infondatezza del primo profilo di censura che pretende, in contrasto con la previsione di legge e con l'elaborazione giurisprudenziale, di subordinare la legittimità della registrazione delle presenze alla finalità di tutela del patrimonio aziendale, contemplata dal primo comma, oppure ai requisiti dei controlli difensivi in senso stretto, ed esattamente all'esistenza di un fondato sospetto di condotte illecite, con il limite di utilizzabilità dei soli dati acquisiti successivamente all'insorgere del sospetto medesimo.

Non è pertinente il precedente di legittimità richiamato dal ricorrente (Cass. n. 10822 del 2025) che concerne l'utilizzo di immagini registrate dagli impianti audiovisivi.

È vero che attraverso i dati raccolti tramite gli strumenti di registrazione degli accessi e delle presenze si attua un controllo sul quantum della prestazione lavorativa, ma tale forma di controllo non coincide e non è equiparabile a quella disciplinata dal primo comma ed attuata attraverso "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori", vale a dire controlli occulti sull'esecuzione della prestazione di lavoro.

Inoltre, ove pure l'analisi dei dati risultanti dagli strumenti di registrazione degli accessi e delle presenze sia sollecitata da un sospetto di illecito addebitabile al dipendente, si tratta di dati legittimamente raccolti ai sensi dell'art. 4, secondo comma, ed utilizzabili "a tutti i fini" in presenza delle condizioni dettate dal terzo comma, collocandosi tale analisi su un piano diverso da quello dei controlli difensivi che, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situano all'esterno del perimetro applicativo dell'art. 4 cit.

4. Una volta sussunta la fattispecie per cui è causa sotto la previsione dell'art. 4, comma 2, la sentenza d'appello ha proceduto a verificare il rispetto delle condizioni poste dal terzo comma ai fini dell'utilizzo, anche a scopi disciplinari, dei dati e delle informazioni raccolte ed ha ritenuto soddisfatte entrambe le condizioni. Su quest'ultimo aspetto si incentra il secondo profilo di censura che risulta parimenti infondato.

4.1. La Corte d'Appello ha esaminato il contenuto della Policy n. 164 dell'11.12.2018 che, al punto 7 dedicato ai "principi generali" prevede: "Al fine di garantire la sicurezza del personale, dei beni materiali ed immateriali dell'Enel e di salvaguardare l'immagine aziendale, l'accesso alle sedi aziendali, sia civile che industriali, deve essere regolato secondo i seguenti principi:

- Tutte le persone, siano essi dipendenti, personale delle imprese fornitrici o visitatori esterni, nonché tutti i mezzi e materiali che hanno accesso alle infrastrutture civili ed industriali aziendali, devono essere preventivamente identificati ed autorizzati. Ogni ingresso e uscita dalle sedi deve essere registrato su appositi registri o sistemi informatici;

- i lettori di badge posizionati sui tornelli di accesso sono finalizzati a rilevare e trasmettere le informazioni sui transiti ai sistemi di controllo accessi ed anche ai sistemi per la rilevazione dell'orario di lavoro. Al fine di assicurare la sicurezza delle sedi e del patrimonio aziendale, possono essere effettuati controlli da parte dell'Azienda al fine di verificare l'applicazione dei principi espressi nella presente policy in conformità a quanto previsto dalla vigente normativa relativa alla protezione dei dati personali (Regolamento Ue 2016/679 - G.D.P.R.)";

- al successivo punto 9.1. dedicato all' "Accesso alle sedi civili" per i Dipendenti Enel, è stabilito che "Ai fini dell'informativa ai dipendenti ai sensi dell'art. 4, comma 3, legge n. 300/1970 e sue successive modifiche ed integrazioni, si evidenzia che i lettori di badge delle sedi ove sono attivi sistemi integrati di controllo accessi, anche ove sia utilizzato lo smartphone, trasmettono le informazioni sui transiti ai sistemi di registrazione degli accessi e ai sistemi di rilevazione della presenza. Anche nelle sedi in cui siano presenti sistemi distinti di identificazione per l'accesso e per la registrazione della presenza

le informazioni acquisite sui transiti in entrata e in uscita e quelle di rilevazione della presenza sono utilizzate per tutti gli adempimenti connessi alla gestione del rapporto di lavoro".

4.2. La Corte territoriale ha poi accertato che la Policy è stata portata a conoscenza di tutti i lavoratori tramite pubblicazione sulla rete informatica aziendale, tramite invio massivo alle 17:00 del giorno 20 dicembre 2018 di una e-mail avente ad oggetto il "Controllo accesso alle sedi aziendali" che informava della avvenuta pubblicazione sulla rete intranet aziendale della Policy in questione e che conteneva il link tramite il quale ogni destinatario poteva visualizzare in formato pdf il documento stesso. Ha inoltre appurato che nel prospetto paga del mese di febbraio 2019 di ogni dipendente era stata inserita una nota informativa della pubblicazione sulla rete intranet aziendale della citata Policy contenente le linee guida per il controllo accessi alle sedi aziendali.

4.3. La valutazione eseguita dai giudici di appello sulla adeguatezza, in ordine al profilo contenutistico, della informazione attuata con la Policy aziendale e sulla idoneità dei modi di comunicazione della stessa ai dipendenti, appare assolutamente coerente al dato normativo e alle esigenze di tutela della riservatezza di cui all'art. 8 della Convenzione europea dei diritti dell'uomo, come interpretato dalla giurisprudenza della Corte europea (v. in particolare sentenza di Grande Camera del 17 ottobre 2019, nel caso López Ribalda e altri c. Spagna; v. anche Cass. n. 15892 del 2007, cit.; Cass. n. 4375 del 2010, cit.; Cass. n. 16622 del 2012, cit.; Cass. n. 9904 del 2016; Cass. n. 18302 del 2016; n. 26682 del 2017), e in alcun modo inficiata dalle critiche sollevate dall'attuale ricorrente; queste si incentrano sul rilievo, peraltro genericamente formulato, secondo cui il legislatore impone al datore di "tenere un comportamento attivo nei confronti del lavoratore" e di spiegare in modo dettagliato da quali strumenti presenti in azienda derivi la possibilità di controllo della prestazione lavorativa, ma detti requisiti sono stati esaminati dai giudici di merito e ritenuti, in base ai dati probatori raccolti, entrambi soddisfatti.

5. Il rigetto del secondo motivo di ricorso porta a ritenere assorbito il primo motivo avente rilievo processuale, atteso che la Corte d'Appello, dopo aver dichiarato inammissibile, perché nuova, la deduzione sulla inutilizzabilità a fini disciplinari delle registrazioni degli accessi, ha comunque affrontato la questione e è giudicato infondata nel merito la prospettazione dell'appellante.

6. Le ragioni esposte conducono al rigetto del ricorso.

7. La regolazione delle spese del giudizio di legittimità segue il criterio di soccombenza, con liquidazione come in dispositivo.

8. Il rigetto del ricorso costituisce presupposto processuale per il raddoppio del contributo unificato, ai sensi dell'art. 13, comma 1 quater, del D.P.R. n. 115 del 2002 (cfr. Cass. S.U. n. 4315 del 2020).

P.Q.M.

La Corte rigetta il ricorso. Condanna il ricorrente alla rifusione delle spese del giudizio di legittimità che liquida in Euro 4.500,00 per compensi professionali, Euro 200,00 per esborsi, oltre spese forfettarie nella misura del 15% e accessori come per legge.

Ai sensi dell'art. 13, co. 1 quater, dà atto della sussistenza dei presupposti processuali per il versamento da parte del ricorrente dell'ulteriore importo a titolo di contributo unificato pari a quello previsto per il ricorso a norma del comma 1 bis dello stesso art.13, se dovuto.

Così deciso nell'adunanza camerale del 14 gennaio 2026.

Depositato in Cancelleria il 31 marzo 2026.