

LegnanoNews

Le news di Legnano e dell'Alto Milanese

Controllo lavoratori a distanza: reato senza accordo o autorizzazione

Manuel Sgarella · Thursday, October 1st, 2026

Telecamere, geolocalizzatori, algoritmi, software e che registrano l'attività al computer: ogni strumento che permette al datore di lavoro di osservare a distanza ciò che fanno i dipendenti rientra nelle regole dello **Statuto dei lavoratori sul controllo a distanza**, che lo ammettono per le finalità definite dalla legge e solo dopo un accordo con i sindacati o un'autorizzazione dell'Ispettorato del Lavoro. L'impresa che salta anche una sola di queste procedure commette **reato** e non può usare i dati raccolti nemmeno per contestare un illecito disciplinare. *(L'approfondimento sul tema è realizzato dallo [Studio Arancio Cislighi di Varese](#))*

In sintesi:

- l'art. 4, comma 1, della L. n. 300/1970 consente di installare strumenti di controllo a distanza previo accordo con RSU o RSA, oppure, per le imprese con unità in più province o regioni, con le associazioni sindacali comparativamente più rappresentative sul piano nazionale;
- in mancanza di accordo serve l'autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro, o della sede centrale per le imprese con unità nell'ambito di più sedi, con provvedimenti definitivi;
- l'art. 4, comma 2, esclude dalla procedura gli strumenti usati dal lavoratore per rendere la prestazione e quelli di registrazione di accessi e presenze;
- la violazione del comma 1 è punita, per effetto dell'art. 171 del D.Lgs. n. 196/2003 e dell'art. 38 della L. n. 300/1970, con l'ammenda da 154 a 1.549 euro o con l'arresto da 15 giorni a un anno;
- per la Cassazione penale (Sez. III, sent. n. 22148/2017) il consenso scritto dei dipendenti non sostituisce l'accordo sindacale o l'autorizzazione.

Controllo a distanza dei lavoratori: finalità e accordo

Il **controllo a distanza dei lavoratori** è consentito dall'art. 4, comma 1, della L. n. 300/1970 solo per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, e gli strumenti che lo rendono possibile si installano dopo un accordo collettivo con la RSU o le RSA; quando l'impresa ha unità produttive in più province della stessa regione o in più regioni, l'accordo può essere firmato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. La norma, riscritta dall'art. 23 del D.Lgs. n. 151/2015, ha sostituito il divieto generale della versione del 1970 con un sistema di finalità tipiche e di procedure.

Ai fini della norma conta la **possibilità di controllo**, anche quando l'impresa installa l'impianto per altri scopi: l'art. 4 si applica agli strumenti "dai quali derivi anche la possibilità" di controllare a distanza l'attività, e una telecamera antifurto che inquadra la cassa o il reparto richiede la stessa procedura di un impianto installato per organizzare la produzione. Dal 2015 anche la tutela del patrimonio aziendale figura tra le finalità del comma 1, e gli impianti installati a questo scopo seguono l'accordo o l'autorizzazione; alla Cassazione si deve la sopravvivenza di uno spazio distinto per i **controlli difensivi** mirati su singoli illeciti, che hanno regole proprie.

Autorizzazione INL: sede competente e criteri

Senza accordo sindacale l'impresa deve ottenere l'**autorizzazione dell'Ispettorato Nazionale del Lavoro**: la competenza è della sede territoriale o, per le imprese con unità produttive dislocate nell'ambito di più sedi territoriali, della sede centrale, e i provvedimenti rilasciati sono definitivi. Con la nota n. 4757/2025 l'Ispettorato ha chiarito che le unità produttive situate in province diverse ma afferenti allo stesso ufficio territoriale si coprono con un'unica istanza.

I criteri dell'istruttoria sono fissati dalla **circolare INL n. 5/2018** del 19 febbraio 2018: l'Ispettorato verifica che le ragioni dichiarate nell'istanza esistano, collega le condizioni d'uso alla **finalità specifica** indicata dall'impresa e non pretende più di predeterminare numero e posizione esatti delle telecamere, purché le riprese siano coerenti con quelle ragioni. L'accesso da remoto alle immagini in tempo reale è autorizzabile solo in casi limitati e con motivazione puntuale, mentre gli accessi alle registrazioni vanno tracciati con log conservati per almeno sei mesi, in luogo della vecchia doppia chiave fisica o logica.

Strumenti di lavoro e rilevazione presenze senza accordo

Accordo e autorizzazione non sono richiesti per gli **strumenti utilizzati dal lavoratore per rendere la prestazione**, come pc, tablet e smartphone aziendali, e per gli strumenti di registrazione degli accessi e delle presenze, ai sensi dell'art. 4, comma 2, dello Statuto. La Fondazione Studi dei Consulenti del lavoro, nella circolare n. 20/2015, ha letto l'esclusione in senso restrittivo, limitandola agli strumenti che servono direttamente al dipendente per svolgere le mansioni assegnate, e la stessa impostazione governa i **controlli informatici sui dipendenti**.

Lo strumento di lavoro perde l'esenzione quando l'impresa lo modifica per sorvegliare chi lo usa. Nella **nota del 18 giugno 2015** il Ministero del Lavoro ha chiarito che pc, tablet o cellulare dotati di **software di localizzazione o filtraggio** diventano mezzi che servono al datore per controllare la prestazione, e la loro modifica richiede le finalità tipiche e l'accordo o l'autorizzazione. Lo stesso criterio vale per le funzioni di intelligenza artificiale aggiunte a strumenti già in uso per misurare la produttività individuale.

Informativa ai dipendenti e uso dei dati a fini disciplinari

Le informazioni raccolte con impianti autorizzati e con strumenti di lavoro sono utilizzabili a tutti i fini connessi al rapporto, compresi quelli disciplinari, a condizione che il lavoratore abbia ricevuto un'**adeguata informazione** sulle modalità d'uso degli strumenti e di effettuazione dei controlli e che sia rispettato il D.Lgs. n. 196/2003, come prevede l'art. 4, comma 3, dello Statuto. Senza questa informativa, secondo la nota ministeriale del 2015, i dati non sono utilizzabili a nessun fine, nemmeno disciplinare.

L'informativa dell'art. 4 si somma a quella dell'art. 13 del Regolamento (UE) 2016/679 e, quando

l'impresa usa sistemi decisionali o di monitoraggio integralmente automatizzati, agli **obblighi informativi del Decreto Trasparenza** previsti dall'art. 1-bis del D.Lgs. n. 152/1997. In pratica la **policy sull'uso degli strumenti** deve indicare che cosa si controlla, con quali modalità e frequenza, chi accede ai dati e per quanto tempo li conserva: il Tribunale di Pisa, con la sentenza n. 800/2026, ha escluso dalle prove le email anteriori alla consegna di una policy con questi contenuti.

Consenso dipendenti e controlli difensivi in giurisprudenza

Il **consenso dei dipendenti**, anche scritto e prestato da tutti, non sostituisce l'accordo sindacale o l'autorizzazione: la Cassazione penale (Sez. III, sent. n. 22148 dell'8 maggio 2017) ha confermato la condanna dell'amministratrice di una società che aveva installato telecamere con il solo assenso dei lavoratori, perché la norma tutela un interesse collettivo di cui sono portatrici le rappresentanze sindacali. La Corte ha ribadito l'orientamento con le sentenze n. 38882/2018 e n. 1733/2020.

Fuori dalla procedura dell'art. 4 si collocano i **controlli difensivi in senso stretto**: la Cassazione (Sez. lav., sent. n. 25732 del 22 settembre 2021) li ammette quando sono mirati ad accertare un illecito attribuibile a uno o più lavoratori sulla base di un fondato sospetto e vengono svolti dopo che il sospetto è sorto. I dati raccolti prima di quel momento, o in violazione dell'art. 4, non possono essere recuperati con l'indagine successiva, e i controlli generalizzati a tutela del patrimonio seguono la procedura ordinaria. I giudici di merito applicano questi criteri anche al **controllo difensivo sulle email aziendali**.

Regole per ogni strumento: pc, email, telecamere, GPS e badge

Il **regime di ogni strumento** dipende dal comma dell'**art. 4 della L. n. 300/1970** in cui ricade, a cui si aggiungono gli obblighi del **Regolamento (UE) 2016/679** sul trattamento dei dati. La struttura della norma è questa:

- il **comma 1** riguarda gli strumenti dai quali deriva anche la possibilità di controllo a distanza dell'attività e ne subordina l'installazione alle finalità tipiche e all'accordo con RSU o RSA o all'autorizzazione dell'Ispettorato;
- il **comma 2** esclude da accordo e autorizzazione gli strumenti utilizzati dal lavoratore per rendere la prestazione e quelli di registrazione degli accessi e delle presenze;
- il **comma 3** condiziona l'uso dei dati raccolti con entrambe le categorie all'informativa sulle modalità d'uso e sui controlli e al rispetto del D.Lgs. n. 196/2003.

Sul piano **privacy** ogni trattamento richiede l'informativa dell'**art. 13 del Regolamento (UE) 2016/679** e, se sistematico o ad alto rischio per i lavoratori, la valutazione d'impatto dell'**art. 35**.

La tabella applica questi riferimenti agli strumenti più diffusi, con la **norma di riferimento** e gli **adempimenti** che ne derivano.

Strumento e riferimento normativo

Telecamere di videosorveglianza nei locali di lavoro
(Art. 4, comma 1, L. n. 300/1970; circolare INL n. 5 del 19 febbraio 2018)

Adempimenti

Accordo con RSU o RSA oppure autorizzazione dell'Ispettorato prima dell'installazione; informativa ai dipendenti; tracciamento degli accessi alle registrazioni.

Strumento e riferimento normativo	Adempimenti
GPS installato sui veicoli aziendali (Art. 4, commi 1 e 2, L. n. 300/1970; circolare INL n. 2 del 7 novembre 2016)	Accordo o autorizzazione, perché il localizzatore è di regola accessorio alla prestazione; solo informativa quando la localizzazione è indispensabile per svolgere l'attività.
Timbratura da remoto geolocalizzata nel lavoro agile (Art. 4, comma 2, L. n. 300/1970 e art. 21 L. n. 81/2017; Tribunale di Cosenza, sent. n. 972 del 1° luglio 2026, che ha annullato il provv. del Garante privacy n. 135 del 13 marzo 2025)	Nessun accordo se la posizione è rilevata solo all'atto della timbratura; informativa (art. 13 GDPR) e valutazione d'impatto (art. 35 GDPR); nessuna verifica a campione della posizione fuori dalla marcatura, come chiarisce la sentenza sulla timbratura da remoto in smart working .
Pc, tablet e smartphone aziendali nella configurazione standard (Art. 4, commi 2 e 3, L. n. 300/1970)	Nessun accordo né autorizzazione; informativa e policy sull'uso degli strumenti per poter utilizzare i dati.
Software di monitoraggio, localizzazione o filtraggio aggiunti agli strumenti di lavoro (Art. 4, comma 1, L. n. 300/1970; nota del Ministero del Lavoro del 18 giugno 2015)	Accordo o autorizzazione prima dell'installazione del software; informativa ai dipendenti.
Posta elettronica aziendale e relativi metadati (Art. 4, commi 1 e 3, L. n. 300/1970; Garante privacy, provv. n. 364 del 6 giugno 2024)	Conservazione dei metadati di norma entro 21 giorni; per periodi più lunghi esigenze documentate e, se la raccolta consente il controllo dell'attività, accordo o autorizzazione.
Badge e rilevatori di accessi e presenze (Art. 4, comma 2, L. n. 300/1970)	Nessun accordo né autorizzazione; informativa ai sensi dell'art. 4, comma 3, e dell'art. 13 GDPR.
Sistemi basati su intelligenza artificiale che osservano o valutano l'attività (Art. 4, comma 1, L. n. 300/1970)	Accordo o autorizzazione quando consentono di controllare a distanza l'attività dei dipendenti.

Procedura per installare strumenti di controllo a distanza

L'impresa che intende installare telecamere, geolocalizzatori o software in grado di controllare i dipendenti deve documentare la finalità, chiudere l'accordo o ottenere l'**autorizzazione** prima dell'attivazione e informare i lavoratori, secondo questa sequenza:

1. individuare e mettere per iscritto la finalità ammessa, tra esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale;
2. verificare se lo strumento serve al dipendente per lavorare o consente di controllarne l'attività e, nel secondo caso, avviare il confronto con RSU o RSA;
3. in assenza di rappresentanze o di accordo, presentare l'istanza alla sede territoriale dell'Ispettorato competente, o alla sede centrale se le unità produttive dipendono da più sedi, descrivendo finalità e caratteristiche dell'impianto;
4. attivare l'impianto solo dopo la firma dell'accordo o il rilascio del provvedimento;
5. consegnare ai dipendenti l'informativa sulle modalità d'uso e sui controlli insieme a quella prevista dal GDPR, aggiornando il registro dei trattamenti e, per i trattamenti sistematici, la valutazione d'impatto;
6. aggiungere l'informativa dell'art. 1-bis del D.Lgs. n. 152/1997 se il sistema decide o monitora in modo integralmente automatizzato, trasmettendola anche alle rappresentanze sindacali;
7. riservare l'accesso a immagini e dati alle persone autorizzate, tracciare gli accessi e fissare tempi di conservazione proporzionati alla finalità.

Sanzioni per controllo illegittimo: reato e violazioni privacy

Installare strumenti di controllo senza accordo o autorizzazione è un **reato contravvenzionale**: l'art. 171 del D.Lgs. n. 196/2003 punisce la violazione dell'art. 4, comma 1, dello Statuto con le pene dell'art. 38 della L. n. 300/1970, l'ammenda da 154 a 1.549 euro o l'arresto da 15 giorni a un anno. Nei casi più gravi arresto e ammenda si applicano congiuntamente, e il giudice può aumentare l'ammenda fino al quintuplo quando, per le condizioni economiche del responsabile, il massimo risulterebbe inefficace.

Al profilo penale si sommano le conseguenze sul rapporto e sulla privacy: i dati raccolti senza rispettare le condizioni dell'art. 4 non sono utilizzabili per un **provvedimento disciplinare**, e il trattamento illecito espone alle sanzioni amministrative dell'art. 83 del Regolamento (UE) 2016/679, che per le violazioni più gravi arrivano a 20 milioni di euro o al 4% del fatturato mondiale annuo, se superiore.

This entry was posted on Thursday, October 1st, 2026 at 9:39 am and is filed under [Altre news](#). You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can skip to the end and leave a response. Pinging is currently not allowed.