



# La videosorveglianza sul luogo di lavoro: un nuovo provvedimento del Garante conferma i precedenti approdi interpretativi

📅 18/07/2024

📌 PROTEZIONE DEI DATI E CYBERSECURITY, DIRITTO DEL LAVORO E PREVIDENZA, DIGITAL/TECH

Gaspere Roma  
Jacopo Piemonte  
Federico Aluigi

## I quadro normativo generale

Il tema della videosorveglianza sul luogo di lavoro rappresenta un importante punto di intersezione tra il diritto del lavoro e la protezione dei dati personali. Come noto, in tale area è infatti

richiesto il rispetto dei requisiti posti dall'articolo 4, comma 1, della legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori)<sup>1</sup>, anche per effetto dell'esplicito richiamo all'articolo 114 del Decreto legislativo 30 giugno 2003 n. 196 (Codice della Privacy).

---

<sup>1</sup> Secondo l'articolo 4 dello Statuto dei Lavoratori "... 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 alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. 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. 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. 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 ...".



Questa disposizione statuisce che l'utilizzo di impianti audiovisivi e di altri strumenti da cui derivi la possibilità di controllo a distanza dei lavoratori sia giustificato alternativamente da esigenze organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale. Inoltre, premessa la presenza di almeno una di queste condizioni, occorre ulteriormente l'accordo con le Organizzazioni Sindacali o l'autorizzazione della sede territoriale dell'Ispettorato Nazionale del Lavoro.

Ancora, ai sensi del terzo comma, affinché le informazioni acquisite con tali strumenti siano utilizzabili "a tutti i fini connessi al rapporto di lavoro", tra cui quelli disciplinari e giudiziari, è necessario fornire adeguata informazione nei confronti del lavoratore circa le modalità d'uso degli strumenti e di effettuazione dei controlli, nonché il rispetto del disposto del Codice della Privacy.

### **Il provvedimento del Garante**

Coerentemente con tali premesse, è di particolare rilievo un provvedimento del Garante per la Protezione dei Dati Personali (Garante) dell'11 aprile 2024<sup>2</sup>. Il relativo procedimento veniva instaurato a seguito di una segnalazione da parte di una dipendente di un Comune italiano che lamentava "l'installazione di un sistema di videosorveglianza nella sede del Comune, in prossimità dei sistemi di rilevazione delle presenze e in assenza dell'accordo con le organizzazioni sindacali, nonché l'impiego di tale sistema per l'effettuazione di specifiche contestazioni disciplinari alla dipendente (...) "<sup>3</sup>. Attraverso l'utilizzo delle immagini registrate, l'amministrazione aveva infatti contestato alla dipendente alcune violazioni dei propri doveri d'ufficio, tra cui il mancato rispetto dell'orario di servizio. Si obiettava nei confronti del Comune altresì di non avere fornito un'ideonea informativa sul trattamento dei

dati acquisiti tramite tale apparecchiatura, tanto relativamente ai lavoratori quanto agli utenti e visitatori della sede, e di aver proceduto in assenza dell'indicazione di tutti gli elementi richiesti dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (*General Data Protection Regulation*, GDPR, da ora "Regolamento").

Il Garante ha effettivamente riscontrato profili di illegittimità con riferimento a tali condotte, e ha comminato al Comune una sanzione amministrativa pari a 3.000 euro ai sensi dell'articolo 83 del GDPR<sup>4</sup>.

Illustreremo di seguito in dettaglio il provvedimento.

### **La liceità del trattamento dei dati ottenuti senza previa autorizzazione**

Il Comune in questione aveva asseritamente installato i c.d. "occhi elettronici" per la tutela del patrimonio comunale e dell'incolumità dei propri dipendenti, in seguito a un'aggressione ai danni di un assistente sociale e di un assessore. L'autorizzazione da parte della sede territoriale dell'Ispettorato del Lavoro era stata però concessa solo in una data successiva all'entrata in funzione del dispositivo. Anteriormente a tal data, a seguito di segnalazioni circa alcune condotte della dipendente-reclamante non conformi al contratto di lavoro (nella specie, appunto, gli orari di ingresso e uscita), il Sindaco aveva esaminato le registrazioni del sistema di sicurezza per verificarne la veridicità, e proprio sulla base di detta verifica erano state avviate le contestazioni disciplinari.

Da queste circostanze, osserva il Garante, ne sarebbe derivato, da un lato, l'illiceità del trattamento dei dati così ottenuti per tutto il periodo precedente all'autorizzazione ex art. 4 nei confronti della generalità dei lavoratori; dall'altro,

---

<sup>2</sup> Garante per la Protezione dei Dati Personali, Provvedimento dell'11 aprile 2024, doc. web n. 10013356.

<sup>3</sup> Si veda il par. 1 del provvedimento.

<sup>4</sup> Specificamente, la responsabilità dell'ente è stata fatta derivare dalla violazione dell'articolo 114 del Codice della privacy che a sua volta richiama l'articolo 4 dello Statuto dei lavoratori. La cornice editale in tale caso è stabilita dall'articolo 83 del GDPR.

per ciò che qui interessa, l'impossibilità di utilizzare gli stessi a fini disciplinari.

### **Il profilo della trasparenza**

Il secondo aspetto critico messo in luce dal Garante concerne la trasparenza del trattamento posto in essere. Occorre infatti ricordare che l'utilizzo per fini disciplinari di informazioni raccolte nel rispetto dell'art. 4, commi 1 o 2, dello Statuto dei Lavoratori, non sarebbe di per sé precluso. È però necessaria, oltre alla suddetta autorizzazione, l'ulteriore osservanza del quadro normativo in materia di protezione dei dati, per cui in particolare è necessario "fornire agli interessati ogni necessaria informazione per assicurare ai dipendenti piena consapevolezza degli ulteriori trattamenti che il datore di lavoro si riserva di effettuare"<sup>5</sup>. Da qui, veniva contestata al Comune l'inadeguatezza dell'informativa di secondo livello sul trattamento dei dati personali fornita agli interessati (tanto lavoratori quanto utenti o visitatori), la quale avrebbe dovuto "contenere tutti gli elementi obbligatori a norma dell'art. 13 del Regolamento"<sup>6</sup>. Sul punto, il Comune si difendeva sostenendo di aver assolto a detti obblighi con la pubblicazione del regolamento comunale sulla videosorveglianza, approvato nell'anno 2005. Proprio su queste premesse, veniva però evidenziato come tale documento non contenesse tutti gli elementi richiesti dall'art. 13 del Regolamento, essendo stato oltretutto approvato ben prima dell'implementazione dello stesso. Peraltro, ha precisato il Garante, atti e documenti che, come nel caso di specie, sono redatti dal datore di lavoro per

assolvere ad obblighi diversi rispetto a quelli derivanti dalla disciplina in materia di protezione dei dati, non possono comunque sostituire l'informativa che il titolare deve rendere, prima di iniziare il trattamento, agli interessati in merito alle caratteristiche essenziali dello stesso.

### **L'annosa questione dei "controlli difensivi"**

È significativo, inoltre, l'approfondimento di un tema che emerge da una difesa del Comune che ha richiamato i c.d. "controlli difensivi". Tale categoria è di indubbio interesse giurisprudenziale e dottrinale, e, come evidenziato dal Garante stesso, di difficile inquadramento dogmatico.

La figura dei controlli difensivi è stata elaborata dalla giurisprudenza precedentemente alla modifica dell'art. 4 dello Statuto dei Lavoratori derivata dall'art. 23 del d.lgs. n. 151 del 2015 e dall'art. 5 d.lgs. n. 185 del 2016<sup>7</sup>. La *ratio* era quella di consentire al datore di lavoro di rispondere a eventuali comportamenti illeciti del personale con controlli, senza azioni preliminari, laddove vi fosse necessità di tutelare il patrimonio e l'immagine aziendale, beni considerati estranei al rapporto di lavoro e per questo motivo non rientranti nel campo di applicazione dell'art. 4 dello Statuto dei Lavoratori<sup>8</sup>.

La questione sull'eventuale "sopravvivenza" dei controlli difensivi successivamente alle modifiche dell'art. 4 non si presta ad interpretazione

---

<sup>5</sup> Si veda il par. 3.3 del provvedimento.

<sup>6</sup> Si vedano "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", nonché il "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010; si consultino, da ultimo, le recenti FAQ del Garante in materia di videosorveglianza.

<sup>7</sup> A seguito delle modifiche così introdotte, al comma 2 dell'art. 4 dello Statuto dei Lavoratori si prevede la non applicazione delle causali di installazione agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

<sup>8</sup> Si veda l'Ordinanza della Corte di Cassazione, Sezione Lavoro, del 28 maggio 2018 n. 13266: "... appare allora evidente come esorbiti dal campo di applicazione della norma il caso in cui il datore abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine aziendale: e tanto più se si tratti di controlli posti in essere ex post, ovvero dopo l'attuazione del comportamento addebitato al dipendente, quando siano emersi elementi di fatto tali da raccomandare l'avvio di un'indagine retrospettiva (Cass. 23 febbraio 2012, n. 2722), così da prescindere dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti, invece diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere (Cass. 27 maggio 2015, n. 10955) ...".

univoca<sup>9</sup>. A tal riguardo, la recente giurisprudenza della Corte di Cassazione ha operato una distinzione tra “controlli difensivi” in senso lato e “controlli difensivi” in senso stretto, ritenendo che questi ultimi non rientrino nel perimetro applicativo dell’art. 4 (e quindi “sfuggano” alla relativa autorizzazione ivi richiesta), in quanto “diretti ad accertare specificamente condotte illecite ascrivibili - in base a concreti indizi - a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro”<sup>10</sup>, sebbene “in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore”<sup>11</sup>. Il giudice, nel bilanciamento degli interessi del lavoratore e del datore di lavoro, deve dunque compiere un apprezzamento di tutte le circostanze del caso concreto, tenendo conto del complesso dei principi espressi nel Codice della privacy e nel Regolamento<sup>12</sup>.

Il Comune tentava di fare leva sulla giurisprudenza citata affermando che “la condotta de quo era (...) diretta ad accertare specifiche condotte illecite lesive dell’immagine dell’Ente...” e che “quindi, i dati sono stati trattati in conseguenza di quei “controlli difensivi in senso stretto” (...) estranei dal campo di applicazione dell’art 4 dello Statuto dei lavoratori...”<sup>13</sup>. Tale difesa non ha però trovato “terreno fertile”. A riguardo, è opportuno osservare che il monitoraggio degli ingressi e delle uscite dal luogo di lavoro non è riconducibile a un controllo su una condotta illecita, ma al contrario costituisce un atto di sorveglianza sull’adempimento dell’obbligazione contrattuale<sup>14</sup>, non potendo quindi rappresentare un controllo difensivo. Inoltre, un ulteriore caposaldo che emerge dalla giurisprudenza è costituito dalla necessità che il controllo avvenga *ex post*<sup>15</sup>. In altre parole, la raccolta delle informazioni deve essere effettuata solamente a seguito del fondato sospetto del datore di lavoro circa la commissione

---

<sup>9</sup> Si veda Cassazione Civile, Sez. Lav., 22 settembre 2021, n. 25732, punto 27. Una conferma della sopravvivenza dei “controlli difensivi” può essere rinvenuta nella giurisprudenza della Corte Europea dei Diritti dell’Uomo, caso *López Ribalda e altri c. Spagna*, 17 ottobre 2019, nel quale è stata dichiarata la legittimità di un controllo occulto da parte di un datore di lavoro, compiuto in maniera proporzionata rispetto al fondato sospetto del compimento di gravi illeciti da parte di alcuni dipendenti.

<sup>10</sup> Si veda Cassazione Civile, Sez. Lav., n. 18168 del 26 giugno 2023, punto 2.1, la quale a sua volta cita Cassazione Civile, Sez. Lav., n. 25732 del 22 settembre 2021, punti 31 e 32.

<sup>11</sup> *Ibid.*, punto 2.6, la quale a sua volta cita Cassazione Civile, Sez. Lav., n. 25732 del 22 settembre 2021, punto 37.

<sup>12</sup> *Ibid.*, punto 2.7. In particolare la Corte ha statuito che: “Il rilievo che, per i controlli difensivi in senso stretto, non opera la disciplina speciale dettata dall’art. 4 dello Statuto, come novellato, non significa che, laddove sia comunque riscontrabile un trattamento di dati personali del lavoratore, non occorra rispettare la disciplina generale prevista per la protezione di qualsiasi cittadino dal Codice della privacy, vigente all’epoca dei fatti della presente causa, e, a partire dal 25 maggio 2018, dal Regolamento UE 2016/679 e dallo stesso Codice, come modificato dal D.Lgs. n. 101 del 2018 entrato in vigore il 19 settembre 2018. Se anche nel caso di controlli a distanza attuati nell’osservanza dei commi 1 e 2 dell’art. 4 St. lav., il comma 3 dello stesso articolo pretende il “rispetto di quanto disposto dal D.Lgs. 20 giugno 2003, n. 196”, costituirebbe una ingiustificata aporia del sistema - peraltro priva di base legale - il sottrarre alla disciplina generale della protezione dei dati personali il rapporto del lavoratore con il suo datore. Pertanto, il complesso dei principi espressi nel Codice della privacy e nel Regolamento Europeo 2016/679 (GDPR) deve orientare il giudice nella delicata opera di bilanciamento e di delimitazione del confine tra l’interesse del lavoratore e l’interesse del datore di lavoro, con un temperamento che non può prescindere dall’apprezzamento di tutte le circostanze del caso concreto. Ancor prima lo stesso datore di lavoro, in sede di iniziativa finalizzata ad attuare un controllo per fini difensivi, è tenuto a compiere una valutazione relativa all’impatto concreto nei confronti della sfera personale dei lavoratori, alla stregua dei principi che regolano, per chiunque, le modalità di trattamento dei dati personali.”

<sup>13</sup> Si veda il par. 2 del provvedimento.

<sup>14</sup> Conformemente a tale interpretazione: Cassazione Civile, Sez. Lav., n. 25645 del 1° settembre 2023, che ha riformato le decisioni di merito che ritenevano estraneo all’attività lavorativa il controllo di ingressi e uscite dal luogo di lavoro.

<sup>15</sup> A sostegno della diversa tesi secondo cui il controllo *ex post* sia solo eventuale e che abbia meramente funzione confermativa dell’effettività del controllo difensivo: Cassazione Penale, Sez. 3, n. 3255 del 27 gennaio 2021, punto 4.4, che a sua volta richiama Cassazione Civile, Sez. Lav., n. 13266 del 28 maggio 2018. La natura eventuale di questo presupposto era indiscussa nell’interpretazione del previgente articolo 4 secondo Cassazione Civile, Sez. Lav., n. 25732 del 22 settembre 2021, punti 20-21.

di illeciti da parte del dipendente<sup>16</sup>.  
Appare evidente come questa circostanza non ricorresse nel caso di specie e come il Garante abbia dunque correttamente respinto tale difesa. Per ultimo, nella totale assenza di trasparenza e del rispetto della normativa sulla privacy, un bilanciamento degli interessi del datore di lavoro e della lavoratrice avrebbe comunque portato alla necessità di tutelare prevalentemente la seconda.

### **Considerazioni conclusive**

Il provvedimento analizzato in questo contributo dimostra come il tema della videosorveglianza nei luoghi di lavoro continui a destare un peculiare interesse, tanto per la società civile nel suo complesso quanto per il contesto lavorativo pubblico e privato: regolamentare con precisione l'installazione di videocamere, risulta ad oggi di imprescindibile importanza per poi garantire la possibilità di utilizzare i dati raccolti attraverso tali sistemi. Emerge dunque l'importanza di rispettare rigorosamente le normative vigenti, garantendo trasparenza e adeguata informazione ai lavoratori.

---

<sup>16</sup> Cassazione Civile, Sez. Lav., n. 25732 del 22 settembre 2021, punti da 40 a 44.



**Gaspare Roma**

**PARTNER**

 g.roma@dejalex.com

 +39 02 72554.1

 Via San Paolo 7  
20121 - Milano



**Jacopo Piemonte**

**ASSOCIATE**

 j.piemonte@dejalex.com

 +39 02 72554.1

 Via San Paolo 7  
20121 - Milano

 +32 (0)26455670

 Chaussée de La Hulpe 187  
1170 - Bruxelles



**Federico Aluigi**

**ASSOCIATE**

 f.aluigi@dejalex.com

 +32 (0)26455670

 Chaussée de La Hulpe 187  
1170 - Bruxelles

**MILANO**

Via San Paolo, 7 · 20121 Milano, Italia  
T. +39 02 72554.1 · F. +39 02 72554.400  
milan@dejalex.com

**ROMA**

Via Vincenzo Bellini, 24 · 00198 Roma, Italia  
T. +39 06 809154.1 · F. +39 06 809154.44  
rome@dejalex.com

**BRUXELLES**

Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique  
T. +32 (0)26455670 · F. +32 (0)27420138  
brussels@dejalex.com

**MOSCOW**

Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia  
T. +7 495 792 54 92 · F. +7 495 792 54 93  
moscow@dejalex.com