AGI
Avvocati Giuslavoristi Italiani

CONVEGNO NAZIONALE

CON IL PATROCINIO DI

Regione Emilia-Romagna

Comune di Bologna

LAVORO 4.0

Innovazione digitale: categorie giuridiche alla prova

BOLOGNA

25-27 OTTOBRE 2018

AGI
Avvocati Giuslavoristi Italiani

CONVEGNO NAZIONALE

LAVORO 4.0
Innovazione digitale: categorie giuridiche alla prova

BOLOGNA 25-27 OTTOBRE 2018

Prof. Avv. Carlo Zoli

Il controllo a distanza: l'evoluzione normativa alla prova dell'innovazione tecnologica

Esperienze giurisprudenziali a confronto

La formulazione originaria dell'art. 4

"**È vietato** l'uso di impianti audiovisivi e di altre apparecchiature **per finalità di controllo a distanza** dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le **rappresentanze sindacali aziendali**, oppure, in mancanza di queste, con la **commissione interna**. In difetto di accordo, su istanza del datore di lavoro, provvede **l'Ispettorato del lavoro**, dettando, ove occorra, le modalità per l'uso di tali impianti …".

I principali problemi interpretativi:

1. **AMMISSIBILITÀ** dei controlli difensivi;
2. **AMBITO** dei controlli leciti (es. il problema del *badge*);
3. **UTILIZZABILITÀ** dei dati e delle informazioni acquisiti.

- *Era opinione diffusa che la norma fosse:*

➢ ***obsoleta*** *a causa dell'evoluzione tecnologica;*

➢ ***largamente inapplicata*** *nella prassi (es. per l'uso dei PC).*

Obiettivi della riforma del 2015

"**revisione della disciplina dei controlli a distanza** […], tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore" (art. 1 c. 7 lett. f), l. n. 183/2014).

contemperamento più equo e moderno degli interessi contrapposti

ridimensionamento dei limiti procedurali

La nuova formulazione dell'art. 4

"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 rsu o dalle rsa. 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 c.r. sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al 1° periodo possono essere installati previa autorizzazione della sede territoriale dell'INL o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, dalla sede centrale dell'INL. I provvedimenti di cui al 3° periodo sono definitivi.

La disposizione di cui al c. 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 cc. 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 **d.lgs. 30 giugno 2003, n. 196**".

Elementi di continuità

- l'art. 4 fa riferimento a tutti gli strumenti in grado di **captare informazioni**;
- resta implicitamente il **divieto** di utilizzare **strumenti di mera vigilanza**;
- il divieto riguarda **ogni attività (non solo lavorativa) dei lavoratori**;
- sono **tuttora irrilevanti**:

- **l'effettiva utilizzazione** dello strumento (e la realizzazione del controllo);

- **l' intenzionalità** della condotta datoriale;

- **la consapevolezza** dei lavoratori (ai fini della legittimità dell'utilizzazione);

- resta **l'obbligo di rispettare la normativa di tutela della *privacy*** (principi di necessità, trasparenza, proporzionalità e pertinenza).

Elementi di novità

- **Presupposti** che legittimano l'adozione di strumenti di controllo a distanza

  ➡ **tutela del patrimonio aziendale**

- **Procedura** per l'accordo collettivo o per l'autorizzazione amministrativa

- "**Eccezioni**" al c. 1 per:

  ➡ **strumenti utilizzati per rendere la prestazione lavorativa**

  ➡ **strumenti di registrazione degli accessi e delle presenze**

- **Utilizzazione** delle informazioni legittimamente raccolte:

  ➡ ammessa **a tutti i fini connessi al rapporto di lavoro**

Principali problemi interpretativi

1. I controlli **difensivi** possono essere ancora disposti senza autorizzazione amministrativa o sindacale?

2. Cosa deve intendersi per «strumenti **utilizzati** dal lavoratore **per rendere la prestazione**» e per «strumenti di **registrazione degli accessi e delle presenze**»?

3. Quando può dirsi adeguata **l'informazione preventiva**?

1. I controlli difensivi

- T. Milano 28.6.2017 *incidenter* (telecamere puntate verso l'esterno) e App. Genova 17.6.2016 (controllo *ex post* sul pc aziendale in un caso di truffa – fattispecie precedente): non si applica l'art. 4 in caso di controlli diretti ad accertare comportamenti illeciti che riguardino la tutela di **beni estranei** al rapporto di lavoro;

- Cass. 19922/2016 (GPS e "*patrol manager*") (fattispecie precedente): non sono difensivi i sistemi che consentono un **controllo generalizzato**, cosicché i dati raccolti mediante GPS installato per evitare illeciti "non possono essere utilizzati per provare l'inadempimento contrattuale dei lavoratori".

➢ **Per la dottrina prevalente i controlli difensivi sono attratti nel c. 1**

2. La nozione di “strumenti…”

- **<u>Punti fermi</u>**

→ **inesistenza** di una **“nozione ontologica”** di strumenti per rendere la prestazione lavorativa;

→ il controllo sull’attività dei lavoratori **non può essere invasivo e costante**.

- **<u>Profilo controverso</u>**

→ L’area di “immunità” dalla procedura autorizzatoria ricomprende qualunque strumento utilizzato per rendere la prestazione lavorativa, oppure deve trattarsi di strumenti indispensabili?

Segue: le tesi principali

1. Strumenti **indispensabili** per rendere la prestazione (Circ. INL 2/2016 sull'utilizzo dei GPS) o comunque **strettamente funzionali** allo svolgimento del lavoro (parere Garante 13.7.2013 n. 303 in tema di accesso ad internet e alla posta elettronica).

2. strumenti che rendono **più efficiente** il lavoro;

3. strumenti **effettivamente** utilizzati:

- **variante:** solo se il lavoratore abbia un ruolo **"attivo"** nell'uso, con la possibilità di **disconnessione.**

Segue: una soluzione ragionevole

- Andrebbero scomposte le funzionalità dello strumento:

se "serve" al lavoro (pc, tablet, cellulare…) si ricade nel c. 2;

se vi si aggiungono fini o possibilità di controllo sulle attività lavorative (es. modificando il *software* o installando determinati applicativi) serve l'accordo sindacale o l'autorizzazione amministrativa *ex* c. 1 (Comunicato stampa Min. Lav. 18 giugno 2016).

→ ***E' sempre più decisivo il ruolo del Garante nell'effettuare il giudizio di proporzionalità ai sensi della normativa sulla* privacy *e quello di legittimità* ex *art. 4.***

Il caso dei ***call-center***

→*Problema: diffusione di applicativi che, allo scopo di migliorare la gestione di chiamate e fascicoli dei clienti,* ***consentono anche un controllo talvolta costante e pervasivo dell'attività degli addetti***

- T. Pescara 25.10.2017 (*software* per smistare le chiamate e registrarne la durata): rientra nel c. 2 in quanto "indefettibilmente necessario all'espletamento della prestazione lavorativa".

- Parere Garante 8.3.2018 n. 139 (Sky) (*software* per la gestione delle chiamate): non si tratta di meri "strumenti di lavoro" bensì di "strumenti organizzativi, dai quali può indirettamente derivare il controllo a distanza …" → compresi nel c. 1.

- Circolare INL n. 4/2017 (CRM): distingue gli applicativi per il "mero accoppiamento fra chiamata e anagrafica del cliente" (c. 2) da quelli che consentono anche di monitorare attività e produttività, escludendo peraltro nella specie la ricorrenza dei presupposti di cui al c. 1.

Sistemi di **geolocalizzazione** (e affini)

→ *A fronte dell'**esigenza aziendale** di migliorare l'**organizzazione** delle **attività e** la **sicurezza** del lavoro, emergono le **istanze dei lavoratori di** non essere assoggettati ad un **controllo costante.***

- Circolare INL 2/2016 (v. *retro*) (GPS): rientrano nel c. 2 solo se imposti dalla legge o se la prestazione non può essere resa in assenza di tali strumenti.

- Parere Garante 22.5.2018 n. 362 (Trenord - *bodycam* al personale per ragioni organizzative e di sicurezza): sono considerate lecite, ma subordinandone l'applicazione all'adozione di misure di tutela degli interessati.

- Cass. n. 19922/2016 (GPS): non possono essere utilizzati per finalità di controllo dell'attività lavorativa; ammissibilità dei controlli difensivi solo per fondato sospetto.

- I "braccialetti di Amazon": solo una modalità di esercizio del potere direttivo?

Sistemi di gestione
delle attese allo sportello

→ *Al fine di ridurre i tempi di attesa degli utenti, Poste Italiane aveva adottato, senza seguire la procedura sindacale, un sistema di* ***gestione automatizzata delle code per le operazioni di sportello,*** *che consentiva* ***anche il trattamento dei dati*** *dei dipendenti (associando il nome del singolo dipendente).*

Parere Garante 16.11.2017 n. 479: il sistema non è "indispensabile" e comporta un monitoraggio costante dell'attività dei lavoratori, eccedendo così nei mezzi rispetto alle finalità che il datore di lavoro si prefiggeva.

Registrazione degli accessi e delle presenze

→ *Non è agevole stabilire l'**estensione dell'area di "immunità"** dalla procedura sindacale per gli strumenti menzionati dal c. 2.*

- Sono strumenti di registrazione degli accessi e delle presenze quelli che registrano:

- gli accessi informatici?
- l'accesso a specifici locali aziendali?

- È possibile utilizzare dati biometrici?

→ Garante 31.1.2013 n. 38 e 1.08.2013 n. 384: sistema sproporzionato e inammissibile quando sia possibile utilizzare misure di controllo «tradizionali»;

→ Garante 24.5.2017 n. 249 (Min. Difesa): vieta al Ministero di trattare i dati acquisiti tramite un sistema volto a rilasciare una tessera di riconoscimento elettronica per accedere a servizi in rete;

→ T. Prato 19.9.2011: inammissibilità di tale controllo, salvo che per accesso ad aree sensibili (conf. Parere del Gruppo art. 29);

→Regolamento 2016/679/UE: limiti all'utilizzazione dei dati biometrici (regola ed eccezioni)

3. La questione dell'**informativa**

- T. Pescara 25.10.2017:

pur avendo fornito una nozione ampia di "strumenti di lavoro", afferma l'illegittimità della condotta datoriale proprio per non aver rispettato **l'obbligo di puntuale informativa preventiva ai dipendenti.**

- Garante

L'informativa deve essere chiara, trasparente, completa e facilmente accessibile con riguardo tanto ai contenuti, quanto alle finalità e alle modalità di raccolta e conservazione dei dati

(es. Parere 16.11.2017, n. 479; 1.02.2018, n. 53; 29.03.2018, n. 181)

- Artt. 12-15 Regolamento 2016/679/UE