CONTROLLI A DISTANZA, PRIVACY E RAPPORTO DI LAVORO

CBA

Avv. Gianvito Riccio

15 giugno 2016

I controlli consentiti

(Art. 4, c 1, St. Lav.)

Sono quelli c.d. preterintenzionali: il datore di lavoro utilizza a fini organizzativi, produttivi, per la sicurezza del lavoro e per la tutela del patrimonio aziendale apparecchiature tali da presentare la possibilità di controllare a distanza il lavoratore (Es. telecamere tradizionali o dotate di tecnologia intelligente).

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 [...]

I controlli consentiti

(Art. 4, c 1, St. Lav.)

Condizione di legittimità:

- accordo sindacale con le 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 comparativamente più rappresentative sul piano nazionale;
- in subordine, autorizzazione amministrativa da parte dell' ITL.

L'accordo con le RSA è necessario anche per le strumentazioni che siano intrinsecamente strutturate e provviste delle caratteristiche di "idoneità al controllo" (o potenzialità allo scopo) anche se di fatto inattuato (*es. telecamere per riprese televisive*).

I controlli consentiti

(Art. 4, c 2, St. Lav.)

In generale, quasi tutti gli strumenti informatici e telematici possono essere utilizzati per rendere la prestazione lavorativa.
La procedura dell'accordo sindacale/autorizzazione ITL dovrà trovare applicazione ogni qual volta sia utilizzato un applicativo/software/tecnologia avente finalità ulteriore rispetto al corretto espletamento della prestazione stessa.

L'accordo non è richiesto anche nell'ipotesi di installazione di strumenti di registrazione degli accessi e delle presenze.

Un esempio: il **riconoscimento biometrico**, installato sulle macchine allo scopo di impedire il loro utilizzo a soggetti non autorizzati, può essere considerato uno strumento indispensabile a rendere la prestazione lavorativa (art. 4, c 2) → non è necessario accordo / autorizzazione (Circ. INL n. 5 del 19/2/18)

La geolocalizzazione dei veicoli

L'installazione di sistemi GPS richiede la stipulazione dell'accordo sindacale o l'autorizzazione ITL.

Secondo la nota dell'Ispettorato del Lavoro n. 2/2016, infatti, i sistemi di geolocalizzazione rappresentano un elemento "aggiunto" agli strumenti di lavoro, in quanto non sono utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro → Ne consegue che, in tali casi, la fattispecie rientri nel campo di applicazione di cui al comma 1 dell'art. 4 L. n. 300/1970.

Recentemente, il Garante (prov. n. 232/2018), pur ritenendo lecito un sistema di geolocalizzazione su dispositivi forniti ai dipendenti, ha stabilito delle misure da adottare a tutela della privacy:

- Icona sul dispositivo che segnali che la localizzazione è attiva
- Oscuramento della visibilità della posizione geografica, decorso un periodo determinato di inattività dell'operatore sul monitor presente nella centrale operativa

La geolocalizzazione dei veicoli

Solo in casi del tutto particolari - qualora i sistemi di localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa (e cioè la stessa non possa essere resa senza ricorrere all'uso di tali strumenti), ovvero l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. D.M. 01.12.2010 n. 269 Allegato D - uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00, ecc.) – si può ritenere che gli stessi finiscano per **"trasformarsi" in veri e propri strumenti di lavoro** e pertanto si possa prescindere, ai sensi di cui al comma 2 dell'art. 4 della L. n. 300/1970, sia dall'intervento della contrattazione collettiva che dal procedimento amministrativo di carattere autorizzativo previsti dalla legge.

Call Center

Ispettorato Nazionale del Lavoro, circolare n. 4 del 26 luglio 2017

«Esistono poi ulteriori software che consentono, invece, il monitoraggio dell'attività telefonica e delle produttività di ciascun operatore di Call Center […] che raccolgono ed elaborano in tempo "quasi reale" i dati relativi agli stati di attività telefonica di ciascun operatore […], il tempo dedicato al lavoro per ciascuna commessa e le pause effettuate da ogni singolo lavoratore.
I suddetti software, pur funzionali a più o meno generiche esigenze produttive, consentono di realizzare un monitoraggio individualizzato costante e continuo su tutti gli operatori […]»

« Si ritiene che tali sistemi non solo non rientrano nella definizione di strumento utile a "rendere la prestazione lavorativa" (c2) ma non si ravvisano neanche quelle esigenze organizzative e produttive che giustificano il rilascio del provvedimento autorizzativo da parte dell'Ispettorato del Lavoro (c1)»

Le violazioni del divieto, conseguenze sul piano civilistico

- Inutilizzabilità del dato informativo acquisito (es. fotogramma illegittimamente conseguito con impianto audiovisivo)
- Condotta antisindacale (art. 28 St. Lav.)
- NOVITÁ GDPR: Responsabilità risarcitoria del Titolare / Responsabile del trattamento per il cd. "danno da trattamento" (art. 82 Reg. UE n. 2016/679), nelle ipotesi di danni derivanti all'interessato per violazioni del Regolamento.
  Caso di esonero da responsabilità: il Titolare dimostra che il danno non è a lui imputabile (art. 82, c 3)
- NOVITÁ GDPR: Sanzioni amministrative (rinvio)

Le violazioni del divieto, le sanzioni penali

Art. 171 del D. Lgs. n. 196/2003

Le violazioni della normativa sono punite:

- con l'ammenda da 154 a 1.549,00;
- ovvero con l'arresto da 15 giorni a un anno, salvo che il fatto non costituisca reato più grave.

Nei casi più gravi:

- le pene sono applicate congiuntamente;
- l'ammenda può essere aumentata sino al quintuplo;
- è prevista la pubblicazione della sentenza.

- NOVITA' GDPR: Il Reg. (art. 84) delega ciascuno Stato membro nell'individuazione di sanzioni "altre" rispetto a quelle amministrative, "effettive, proporzionate e dissuasive" → Possibili future modifiche di coordinamento delle norme interne del Codice Privacy (es. art. 171 in esame, art. 167, sul trattamento illecito dei dati)

Le violazioni del divieto, le sanzioni penali

Art. 21 d.lgs. N. 758/1994

In caso di accertata violazione, l'organismo ispettivo competente fissa un termine per eliminare la violazione stessa.
Il ripristino della situazione di legalità può avvenire tramite, a seconda dei casi:

- ❑Rimozione degli impianti illegittimamente installati;
- ❑Sottoscrizione di accordo sindacale;
- ❑Rilascio dell'autorizzazione ITL.

Entro e non oltre sessanta giorni dalla scadenza del termine fissato nella prescrizione, l'organo di vigilanza verifica se la violazione è stata eliminata secondo le modalità e nel termine indicati dalla prescrizione. Quando risulta l'adempimento alla prescrizione, il contravventore potrà essere autorizzato al pagamento in sede amministrativa, nel termine di trenta giorni, di una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione commessa. Il pagamento costituisce una ipotesi di estinzione del reato.

A chi la parola sui controlli a distanza?

Soggetti legittimati alla stipulazione degli accordi sindacali in materia di controlli a distanza sono, da un lato il datore di lavoro, dall'altro le parti sociali ed, in particolare:

- La rappresentanza sindacale unitaria
- Le 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.

L'intervento dell' ITL

Se non sono presenti le RSA o le stesse non raggiungano un accordo, è necessario inoltrare apposita richiesta all' Ispettorato Territoriale del Lavoro. L' ITL effettua un preventivo accertamento di tipo tecnico sullo stato dei luoghi per verificare:

- la reale sussistenza delle esigenze organizzative, produttive e di sicurezza che giustifichino l'installazione;
- che le telecamere non riprendano postazioni fisse di lavoro

Nelle attività economiche in cui mancano RSA ed a forte rischio di rapina (es. farmacie, tabaccherie, distributori di carburante) i requisiti per la richiesta all' ITL si presumono sussistenti (Min. Lav. Nota 7162 del 16.04.2012)

L'Istruttoria

(Circ. INL n. 5 del 19/2/18)

- non coinvolge normalmente aspetti tecnici di particolare complessità («solo casi assolutamente eccezionali»)

- accerta l'effettiva sussistenza della ragioni (organizzative / produttive; sicurezza; tutela patrimonio aziendale), e la correlazione delle strumentazioni alle finalità individuate nell'istanza

- per istanze di installazione impianti di allarme / antifurto con videocamere, l'autorizzazione viene rilasciata «in tempi assolutamente rapidi, **stante l'inesistenza di qualunque valutazione istruttoria**», in quanto le riprese iniziano ad allarme inserito, e nessun controllo sui lavoratori può manifestarsi (INL, Prot. 299 del 28/11/17)

Sulla Videosorveglianza *(Circ. INL n. 5 del 19/2/18)*

- non appare fondamentale specificare l'esatto posizionamento e il numero delle telecamere (ferma restando la correlazione con le ragioni legittimanti il controllo)

- nel caso il lavoratore venga direttamente inquadrato dalla telecamera, sussistendo le ragioni giustificatrici del controllo, non sono necessarie condizioni quali «l'oscuramento del volto» o «l'angolo di ripresa»

- l'accesso alle immagini deve essere necessariamente tracciato, con sistemi di conservazione dei log di accesso per un congruo termine (almeno 6 mesi); se effettuato da remoto e su immagini in tempo reale è autorizzato solo in casi eccezionali debitamente motivati

- devono essere autorizzate anche le riprese su luoghi dove l'attività lavorativa viene svolta in modo saltuario / occasionale (es. carico / scarico merci)

Art. 4 St. Lav. comma 3 e Codice in materia di protezione dei dati personali

I dati raccolti tramite strumenti di controllo a distanza possono essere utilizzati 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.

NOVITA' GDPR: Il Regolamento n. 2016/679 introduce nuovi adempimenti in materia di trattamento dei dati personali (rinvio)

Art. 4 St. Lav. e Codice in materia di protezione dei dati personali

Il monitoraggio tecnologico del lavoratore coinvolge inevitabilmente la sfera della riservatezza dello stesso. Il disposto dell'art. 4 St. Lav. deve essere integrato sia con i principi espressi dal D.Lgs. n. 196/2003 (e dal GDPR Reg. UE n. 2016 / 679) che con le pronunce ed i regolamenti del Garante della *Privacy*.

I regolamenti del Garante della *Privacy* definiscono:

- il tipo di apparecchiatura utilizzata per il controllo (informatica, di geolocalizzazione, di videocontrollo);
- il tipo di esigenze (funzionali, operative, di sicurezza) che vengono concretamente in rilievo;
- ulteriori obblighi e condizioni di liceità per l'installazione di sistemi di controllo preterintenzionali.

Le finalità e le modalità di utilizzo dei dati raccolti

- Qualora il datore di lavoro fornisca ai lavoratori strumenti di lavoro deve, previamente, informare, in modo particolareggiato, i dipendenti su quali siano: le modalità corrette di utilizzo e, qualora vengano previsti controlli sull'uso di detti strumenti, deve indicare in che misura e con quali modalità vengono effettuati (laddove necessario anche in accordo con le organizzazioni sindacali), utilizzando ad esempio un disciplinare interno, chiaro, aggiornato e affiancato da un'idonea informativa

- Proprio l'informativa ai lavoratori richiede una particolare attenzione da parte delle aziende. In quanto le *policy* ed i regolamenti aziendali dovranno essere rivisti ed aggiornati alla luce delle nuove disposizioni → NOVITA' GDPR: Nuovi requisiti informativa (artt. 13 e 14)

- L'informativa dovrà essere fornita ad ogni singolo lavoratore con strumenti idonei a provarne l'effettiva conoscenza. Inoltre, dovrà essere preventiva all'utilizzo dello strumento lavorativo.

I controlli vietati

- Il controllo intenzionale: destinato unicamente al monitoraggio del lavoratore. Violazione della Costituzione (Art. 41 comma 2 e 13 Cost.) in quanto lede la dignità del lavoratore e la sua libertà personale;

- il controllo occulto: è effettuato all'insaputa dei lavoratori (è vietato anche se potenziale) Garante della *Privacy* – Provv. n. 164 del 04.04.2013.

I controlli difensivi

Una categoria controversa

I controlli difensivi si realizzano tramite l'utilizzo occulto da parte del datore di lavoro di apparecchiature per l'accertamento di condotte illecite dei lavoratori (Es. Telecamere a circuito chiuso).

I controlli difensivi: Una categoria controversa

Sussiste un consolidato orientamento secondo cui i controlli difensivi sono:

❑ vietati quando il controllo è diretto all'accertamento dell'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro.

❑ ammessi quando i controlli sono diretti alla tutela di beni estranei al rapporto stesso (Cass. n. 3122 del 17 febbraio 2015, secondo cui «*devono ritenersi legittimi i controlli – anche se "occulti" – diretti ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine*»).

Un esempio recente: (Cass. n. 13266 del 28 maggio 2018) è lecito il controllo informatico sul *pc* del dipendente per accertarne l'uso extra-lavorativo (giocare a Free-Cell), in quanto il controllo:

- era avvenuto *ex post*, cioè dopo l'attuazione del comportamento, a seguito dell'emersione di elementi fattuali che raccomandavano l'avvio di un'indagine
- era indirizzato ad accertare singoli comportamenti illeciti e lesivi del patrimonio e immagine aziendale
- non configura sorveglianza sull'esecuzione della prestazione lavorativa

Badge a radio frequenza (RFID)

Cass. Sez. Lav. 13.05.2016, n. 7121

Il *badge* con tecnologia RFID è idoneo a consentire la trasmissione mediate sistema *on line* alla centrale operativa di tutti i dati acquisiti tramite la lettura magnetica del *badge* del singolo lavoratore riguardanti non solo l'orario di ingresso e di uscita ma anche le sospensioni, permessi, le pause, così realizzando in concreto il controllo costante e a distanza circa l'osservanza da parte degli stessi dipendenti del loro obbligo di diligenza, sotto il profilo del rispetto dell'orario di lavoro.

Necessita di accordo sindacale o procedura autorizzativa

Conforme, da ultimo, Cass. n. 17531 del 14.07.2017

Uso improprio degli strumenti di lavoro

CASE OF BĂRBULESCU v. ROMANIA

(Application no. 61496/08)

In questa importante sentenza i giudici di Strasburgo stabiliscono che non viola l'art. 8 CEDU e la direttiva 95/46/CE sulla tutela della *privacy* il datore di lavoro che effettua un monitoraggio delle mail e degli altri mezzi di comunicazione aziendali, utilizzati dai lavoratori, al fine di garantire il giusto funzionamento della società e di controllare che i dipendenti, durante l'orario di lavoro, svolgano la loro attività lavorativa.

Condizione di legittimità: Assenza di aspettativa di *privacy* del lavoratore

Sul controllo delle email il Garante della Privacy (*Newsletter* del 29/3/18) ha stabilito che:

- È illecito il controllo *massivo* e la *conservazione illimitata* delle email dei dipendenti in vista di futuri contenziosi
- Il controllo deve riguardare contenziosi in atto o situazioni precontenziose specifiche, non ipotesi astratte e indeterminate (vietato il controllo *indiscriminato*)
- L' obbligo di disattivare e rimuovere la casella email dopo il licenziamento del lavoratore

Reg. UE 2016/679 (GDPR)

Il quadro normativo

- **Reg. UE 2016/679 (GDPR)**: in vigore dal 25/5/2018, quindi già pienamente applicabile e vincolante
- **D.Lgs. n. 196/2003 (Codice Privacy)**: non verrà abrogato, ma verrà modificato da un D.Lgs. di coordinamento tra normativa nazionale e GDPR
- **D.Lgs. di coordinamento**: non è ancora stato emanato (scadenza delega: 22 agosto). Armonizzerà la normativa nazionale (Codice Privacy) con il GDPR, solo nelle materie in cui lo stesso Regolamento prevede la competenza dei singoli Stati Membri (ad es.: sanzioni non amministrative, art. 84; rapporto di lavoro, art. 88)

Nelle more dell'emanazione del D.Lgs. di armonizzazione, il GDPR sarà integralmente attuato. Le disposizioni del Codice Privacy saranno applicabili solo se riguardanti materie non disciplinate dal GDPR (es. le sanzioni penali, art. 167 e 171) e comunque qualora non siano in contrasto col medesimo (es. la figura dell'Incaricato al trattamento, art. 30).

I Principi Generali del GDPR

"Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali" (art.1, c. 2)

I dati personali devono essere:

- ❑ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- ❑ raccolti per finalità determinate, esplicite e legittime, e trattati in modo non incompatibile con tali finalità
- ❑ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati») (art. 5)

❑**Accountability**: il Titolare / Responsabile del trattamento dovrà adottare tutte le misure necessarie a dimostrare la concreta attuazione del Regolamento

❑**Privacy by design**: ogni trattamento di dati personali deve essere progettato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati

❑**Privacy by default**: prevedere impostazioni di Privacy predefinite, in modo da trattare solo i dati personali strettamente necessari ad ogni specifica finalità, resi accessibili solo ad un numero predefinito di persone (art. 25)

GDPR e Rapporto di Lavoro (1)

La base giuridica del trattamento dei dati (art. 6):

- Esecuzione del contratto di lavoro (es. finalità retributive) (par. 1, lett. b)
- Adempimento di obblighi legali del datore (es. conguaglio delle imposte) (par.1, lett. c)
- Interesse legittimo del datore di lavoro (par. 1, let. f): in questo caso il Titolare dovrà *(i)* valutare preventivamente che il trattamento sia necessario e proporzionale alla finalità legittima perseguita, e *(ii)* adottare misure atte a bilanciare tali finalità con i diritti e libertà fondamentali del lavoratore.

Il consenso non viene considerato come base giuridica in quanto dovrebbe essere liberamente prestato dall'interessato → non accade nel rapporto di lavoro (*WP29 opinion n. 2/17*)

GDPR e Rapporto di Lavoro (2)

Ambito territoriale di applicazione (art. 3). Applicazione a trattamenti effettuati:

- da tutti i Titolari stabiliti nell'Unione (anche se il trattamento dei dati avviene all'esterno dell'Unione)
- nei confronti di interessati che si trovano nell'Unione, anche se il Titolare non è stabilito nell'Unione

Ampliamento di tutela a lavoratori di gruppi multinazionali che non hanno sedi legali né secondarie nell'Unione, ma con dipendenti che lavorano in territorio europeo

Gli adempimenti del datore di lavoro (1)

Redigere e sottoporre agli interessati un' Informativa aggiornata (artt. 12-14), «*in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro*», con i requisiti indicati nel Regolamento, tra cui:

- ❑ identità del Titolare/Responsabile
- ❑ finalità e base giuridica del trattamento → specificazione del legittimo interesse perseguito dal datore
- ❑ periodo di conservazione dei dati
- ❑ esistenza dei vari diritti dell'interessato (rinvio)
- ❑ esistenza di un processo decisionale automatizzato
- ❑ eventuali destinatari o categorie di destinatari dei dati

Nel caso di dati non ottenuti presso l'interessato, ulteriori requisiti:

- ❑ la fonte da cui hanno origine i dati
- ❑ le categorie di dati personali in questione

Il rispetto delle norme sull'informativa (e del GDPR in generale) è requisito essenziale ai fini dell'utilizzabilità dei dati «a tutti i fini connessi al rapporto di lavoro» (*ex* art. 4, c. 3, St. lav.)

Gli adempimenti del datore di lavoro (2)

- Effettuare analisi e valutazione dei rischi del trattamento e adottare misure di sicurezza tecniche e organizzative adeguate (artt. 5 e 32), nonché comunicare tempestivamente ad interessato e Autorità di controllo eventuali violazioni dei dati personali (artt. 33, 34)

- Nomina del *Data Protection Officer* (DPO): ha il ruolo di sorvegliare l'attuazione del GDPR. La nomina è obbligatoria nei casi di attività prevalentemente rischiosa del Titolare (trattamento dati su larga scala / dati particolari) (art. 37). In tutti gli altri casi è comunque *best practice.*
  Possibile conflitto di interessi (art. 38 c. 6): il DPO non può ricoprire ruoli manageriali di vertice all'interno della società (*WP29 opinion n. 2/17*)

- Registro dei trattamenti (art. 30): contiene tutto ciò che riguarda il trattamento dei dati (finalità, categorie di dati/interessati/destinatari, misure di sicurezza, ecc.) → obbligatorio per imprese (i) con più di 250 dipendenti, o (ii) che effettuino trattamenti rischiosi non occasionali, o (iii) trattamenti su dati particolari.
  In tutti gli altri casi è comunque *best practice*

Le responsabilità del datore di lavoro

- Civile: Responsabilità risarcitoria per il cd. "danno da trattamento" (art. 82), per danni derivanti all'interessato per violazioni del Regolamento.

- Amministrativa: 2 tipi di sanzioni pecuniarie
  - Art. 83, c. 4: Fino a **€ 10 M**, o per le imprese, fino a **2% fatturato mondiale** anno prec. → violazioni degli obblighi del Titolare / Resp., *ex* artt. 8, 11, 25-39, 41-43 (es. PIA, DPO, tenuta Registro, comunicazione *data breach*, ecc.)
  - Art. 83, c. 5: Fino a **€ 20 M**, o per le imprese fino a **4 % fatturato mondiale** anno prec. → violazione (i) dei principi base del trattamento (artt. 5-9), (ii) dei diritti degli interessati (artt. 12-22, es. essere informati, accesso, rettifica, ecc.), (iii) obblighi ai sensi delle legislazioni degli Stati membri adottate per il coordinamento al Regolamento, (iv) inosservanza di un ordine/negato accesso dell'Autorità di controllo (art. 58)

- Penale: Il Reg. (art. 84) delega ciascuno Stato membro nell'individuazione di sanzioni "altre" rispetto a quelle amministrative, "effettive, proporzionate e dissuasive" → Possibili future modifiche di coordinamento delle norme interne del Codice Privacy (es. art. 167, sul trattamento illecito dei dati; art. 171, su controlli a distanza)

I diritti dei lavoratori (1)

- Informazione (artt. 12-14): ricevere l'informativa completa e aggiornata di tutti i requisiti

- Accesso ai dati (art. 15): diritto di (i) ottenere copia di tutti i propri dati personali, (ii) conoscere tutte le informazioni ad essi relative (finalità, categorie di dati, destinatari, periodo di conservazione, ecc.), (iii) accedere al proprio fascicolo personale detenuto dal datore di lavoro (orientamento della Cassazione S.U. sent. n. 2397/14, confermato di recente da Cass. sent. n. 6775/16)

- Rettifica / integrazione di dati inesatti / incompleti (art. 16)

- Portabilità dei dati (art. 20): nei casi di trattamento fondato sull'esecuzione di un contratto di lavoro (art. 6, par. 1, let. b), l'interessato ha diritto a ricevere i propri dati personali (in formato leggibile da dispositivo automatico) e trasferirli presso altro titolare

I diritti dei lavoratori (2)

- Opposizione al trattamento (art. 21): nei casi di trattamento fondato sull'interesse legittimo del Titolare (datore), l'interessato può opporsi al trattamento → spetta al datore provare la prevalenza dei propri interessi su libertà / diritti del lavoratore

- Cancellazione dei dati («diritto all'oblio», art. 17): nei casi di (i) trattamento non più necessario rispetto alle finalità, (ii) trattamento illecito; (iii) opposizione *ex* art 21

- Limitazione di trattamento (art. 18): nei casi di (i) inesattezza dei dati, nelle more della verifica del Titolare, (ii) trattamento illecito, (iii) opposizione *ex* art. 21, nelle more della verifica del Titolare sulla prevalenza del proprio interesse

- Ricorso all'Autorità di controllo (art. 77): qualora l'interessato ritenga che il trattamento violi il Regolamento

- Ricorso giurisdizionale avverso decisione giuridicamente vincolante dell'Autorità di controllo (art. 78)

Delega in materia di rapporti di lavoro (art. 88)

Gli Stati hanno facoltà di adottare norme più specifiche per il trattamento dei dati personali nell'ambito di rapporti di lavoro, ad ulteriore tutela della dignità e dei diritti fondamentali dei lavoratori, ed in particolare riguardo:

- Trasferimento dati all'interno di un gruppo imprenditoriale
- Trasparenza del trattamento
- Sistemi di monitoraggio sul posto di lavoro

Possibili nuove norme / modifiche, tuttavia

il vigente art. 4 St. lav. (modificato dal D.lgs. n. 81/15), gli orientamenti del Garante della Privacy e dell' INL appaiono in linea con le disposizioni del GDPR, avendo recepito i principi di trasparenza, giustificatezza, proporzionalità e non eccedenza del trattamento dei dati, come già enunciati nella *Raccomandazione del Consiglio d'Europa CM / Rec (2015)5*

Avv. Gianvito Riccio

gianvito.riccio@cbalex.com

www.cbalex.com

20122 **MILANO**
Galleria San Carlo, 6
Tel. +39 (0)2 778061
Fax +39 (0)2 76021816
E-Mail: milano@cbalex.com

00198 **ROMA**
Via Guido D'Arezzo, 18
Tel. +39 (0)6 89262900
Fax +39 (0)6 89262921
E-Mail: roma@cbalex.com

35137 **PADOVA**
Galleria dei Borromeo, 3
Tel. +39 (0)49 0979500
Fax +39 (0)49 0979521
E-Mail: padova@cbalex.com

30135 **VENEZIA**
Santa Croce, 251
Tel. +39 (0)41 2440266
Fax +39 (0)41 2448469
E-Mail: venezia@cbalex.com

D-80539 **MÜNCHEN**
Ludwigstrasse, 10
Tel. +49 (0)89 99016090
Fax +49 (0)89 990160999
E-Mail: muenchen@cbalex.com