Data protection e Reg. UE 2016/679: la privacy nell'Europa 4.0

Industria 4.0 e data protection

Rapporto di lavoro e privacy

Torino, 6 novembre 2017

(Regolamento 2016/679 – 25.05.2018) (D.Lgs. 196/2003) -Documento dei Garanti europei della privacy riuniti nel Gruppo "Articolo 29" (WP29) - Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri - direttiva n. 95/46/CE

1. L'attenzione per la protezione dei dati personali nel rapporto di lavoro

La protezione dei dati personali nell'ambito della relazione lavorativa è riconosciuta formalmente nel *Regolamento generale sulla protezione dei dati personali,* che affida a ciascuno Stato il compito di prevedere, tramite leggi o contratti collettivi, discipline più specifiche per assicurare la protezione dei diritti e delle libertà con riferimento al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (art. 88 Reg.).

L'interesse per la protezione della riservatezza nel contesto delle relazioni di lavoro è maturato in questi ultimi anni. Nella direttiva madre n. 95/46/CE non si prevedeva alcuna disciplina peculiare per il trattamento dei dati personali dei dipendenti.

Durante l'*iter* dei negoziati tra Consiglio e Parlamento Europeo per l'approvazione del Regolamento, nell'aprile 2015 nel Consiglio d'Europa la tutela della riservatezza nel contesto lavorativo è oggetto della Raccomandazione del Comitato dei Ministri, nella quale è

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

ricordata agli Stati l'esigenza di tutelare i dati personali del dipendente nei diversi ambiti in cui vengono raccolti e trattati.

Nello stesso periodo l'Italia modifica l'art. 4. Stat. Lav., disponendo che i dati registrati dagli strumenti di controllo, telematici e informatici possano essere raccolti, utilizzati "a tutti i fini del rapporto" e conservati dal datore di lavoro qualora questi abbia fornito al lavoratore «adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli» e, su di un altro versante, che i controlli medesimi avvengano nel rispetto di quanto disposto dal Codice della Privacy.

Due condizioni concorrenti che valorizzano la portata giuslavoristica dell'impianto normativo a tutela della riservatezza.

Approfondiremo in seguito il tema del controllo a distanza del lavoratore.

2. Attività del Garante in relazione al rapporto di lavoro.

Significativamente potenziati nel Regolamento risultano il ruolo e i poteri riconosciuti alle Autorità Garanti.

In Italia il Garante, in merito al rapporto di lavoro, ha svolto un'importante attività di precisazione delle disposizioni contenute nel Codice della *Privacy* elaborando Linee Guida e Provvedimenti Generali.

Nel 2006 ha adottato le Linee Guida per il trattamento dei dati personali nell'ambito del rapporto di lavoro privato.

Le tematiche del provvedimento riguardano: il comportamento del datore di lavoro, che deve trattare i dati dei dipendenti nel rispetto dei principi di liceità, trasparenza, pertinenza e finalità; la diffusione dei dati, consentita solo per dare esecuzione agli obblighi derivanti dal

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

contratto di lavoro o dalla legge; l'informativa che il datore di lavoro deve rendere; l'identificazione dei soggetti che possono trattare i dati; la disciplina dei dati idonei a rivelare lo stato di salute.

Il Garante ha poi adottato le Linee Guida per i lavoratori pubblici, precisando in particolare i punti relativi alle assenze per malattia; alla diffusione dei dati in Internet; ai dati biometrici e alle comunicazioni tra amministrazione e lavoratore.

3. Raccomandazione del Comitato dei Ministri

Ho già accennato al fatto che il Regolamento riserva a ciascuno Stato la facoltà di prevedere, tramite leggi o contratti collettivi, discipline più specifiche per assicurare la protezione dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (art. 88 Reg.); ciascuno Stato sarà tenuto ad adottare una politica conforme a quanto previsto nella Raccomandazione del Comitato dei Ministri.

Secondo la CEDU, (CEDU, sez. III, 25 ottobre 2007, V.V. C. Olanda) la Raccomandazione non potrà essere disattesa in quanto la legislazione nazionale che fosse contrastante con i principi in essa contenuti sarebbe in violazione di quel diritto alla vita privata tutelato dalla Convenzione all'art. 8 e la cui interpretazione estensiva di "diritto a stabilire relazioni con altri esseri umani", include le relazioni di lavoro o di affari.

Nella prima parte della Raccomandazione (artt. 1 – 13) si richiamano i principi generali in materia di protezione dei dati personali dei lavoratori contenuti nel Regolamento e si prescrivono norme volte a diminuire al massimo la circolazione dei dati e a garantire la maggior trasparenza possibile nel loro utilizzo. Nella seconda parte della Raccomandazione (artt. 14–21) si individuano con maggior precisione

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

le possibili forme di controllo derivanti dall'utilizzo delle nuove tecnologie, ponendo diverse garanzie a favore dei lavoratori, soprattutto in materia di trasparenza e giustificatezza del trattamento dei dati personali connessi all'uso di *Internet* e posta elettronica.

L'estrazione dei dati relativi al traffico *internet*; l'accesso allo scambio di comunicazioni elettroniche, l'analisi delle informazioni di geolocalizzazione sono assimilabili a un trattamento dei dati personali del dipendente. Tali attività se realizzate tramite "strumenti di lavoro" dovranno essere assoggettate ai limiti vigenti per la protezione dei dati (informativa preventiva dell'interessato; principio di trasparenza; rispetto dei principi di necessità, pertinenza, proporzionalità e non eccedenza del trattamento) mentre se realizzate tramite "strumenti di controllo" dovranno essere assoggettate a ulteriori vincoli in coordinamento con le logiche collettive di protezione sindacale (consultazione autorizzativa delle rappresentanze sindacali).

Non si preclude a ciascuno Stato di consentire al datore di lavoro di accedere ai dati relativi alle navigazioni *internet* dei propri dipendenti, previa informativa e in presenza di un ragionevole motivo, né di accedere alle comunicazioni elettroniche in quanto necessario per motivi di sicurezza o altre legittime ragioni, previa informativa e adozione di misure finalizzate a evitare accessi abusivi (art. 14). E si legittima, previa consultazione sindacale, l'uso di apparecchiature di videosorveglianza se volto a tutela della salute, della produzione, della sicurezza e dell'efficiente organizzazione della produzione e solo indirettamente consenta un controllo sull'attività dei lavoratori (art.15).

4. Sentenza Barbulescu 2 – controllo datoriale sulle comunicazioni elettroniche del lavoratore

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

In attuazione di tali principi, la Grande Camera della CEDU riscrive le linee fondamentali di protezione del lavoratore dal controllo datoriale sulle *e-mail* aziendali, nella sentenza *Barbulescu c. Romania* del 5 settembre 2017.

Fino ad oggi il sistema giuridico italiano ha riconosciuto il potere di controllo del datore di lavoro sulle comunicazioni del lavoratore trasmesse tramite strumenti informatici aziendali, in presenza di regolamento recante espresso divieto di uso delle risorse aziendali per scopi personali.

In sede penale, è esclusa, in capo al datore che controlli le comunicazioni elettroniche del lavoratore, la configurabilità del reato di violazione della corrispondenza e di accesso abusivo a sistema informatico (Cass., n. 47096/07 e Trib. Milano, 10 maggio 2002), pur riconoscendosi la pertinenza della casella di posta al lavoratore (Cass. n. 38331/16).

La giurisprudenza ha escluso l'applicazione dei limiti previsti dall'art. 4 dello Statuto dei Lavoratori ai cd. controlli difensivi, che il datore attua per dimostrare un illecito posto in essere dal lavoratore (Cass. n. 4746/2002; n. 4375/2010), giungendo peraltro, attraverso un'estensione della nozione, a legittimare fatti penalmente indifferenti e rilevanti solo sul piano disciplinare o in relazione alla mera difesa dell'immagine aziendale (Cass. n. 2722/2012) o addirittura al corretto adempimento della prestazione lavorativa, pur però poi escludendo che i dati dei controlli a distanza possano essere utilizzati per provare l'inadempimento contrattuale dei lavoratori (Trib. Milano, 16 giugno 2001 e Trib. Genova, 2 maggio 2005; Cass., n. 16622/2012).

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

La Cassazione ha ammesso la legittimità del licenziamento del lavoratore che aveva violato il divieto di accesso alla rete *Internet* e di utilizzo della posta elettronica per scopi personali, divieto contenuto nel codice disciplinare affisso nella bacheca aziendale. (Cass. n. 17859/2014)

Altra sentenza ancora ha sottolineato la necessità di far riferimento alle sanzioni previste dalla contrattazione collettiva per l'uso indebito delle risorse informatiche e della posta elettronica. (Cass. n. 22353/2015)

Perfino la giurisprudenza contabile è intervenuta in materia, ravvisando la responsabilità del dipendente pubblico per il danno cagionato all'amministrazione in relazione al tempo di lavoro sottratto durante le attività su Internet per scopi personali (Corte dei conti del Piemonte, 13 novembre 2003).

Anche la dottrina, con specifico riferimento all'uso di Internet sul lavoro per scopi personali, ha affermato in diverse occasioni la liceità del controllo datoriale, fondandolo sulla proprietà degli strumenti aziendali, sulla correlata responsabilità del datore, o ancora sull'obbligo di lavoro.

Come già detto, il legislatore ha modificato l'art. 4 dello Statuto dei lavoratori, in modo che da un lato si escludono gli strumenti utilizzati dal lavoratore per rendere la prestazione dagli strumenti di controllo per i quali è prescritta apposita procedura autorizzatoria e, dall'altro lato, si consente l'utilizzazione delle informazioni raccolte attraverso i detti strumenti «a tutti i fini connessi al rapporto di lavoro», sia pur alla duplice condizione che al lavoratore sia data adeguata informazione

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

delle modalità di uso degli strumenti e dell'effettuazione dei controlli e che sia rispettato il codice della *privacy*.

Si è poi aggiunta la sentenza della Cedu del 12 gennaio 2016 (*Barbulescu c. Romania*): nel caso di un divieto espresso di uso dei computer aziendali per scopi personali contenuto in un regolamento aziendale reso noto ai dipendenti, la Corte aveva ritenuto legittimo il monitoraggio fatto dal datore sulle comunicazioni elettroniche del lavoratore e legittimo il successivo licenziamento del lavoratore per il solo fatto della violazione del regolamento.

In data 5 settembre 2017, la Grande Camera della Corte europea è tornata sulla decisione, pervenendo, a maggioranza, ad una soluzione del tutto diversa, e stabilendo alcuni principi fondamentali:

- l'applicabilità della protezione della *privacy* anche nel caso in cui il datore di lavoro abbia approvato un regolamento recante espresso divieto di uso delle *e-mail* aziendali per scopi personali;
- obbligo dello Stato di assicurare che siano predisposte misure protettive contro eventuali abusi da parte del datore di lavoro;
- lo Stato, per garantire il diritto previsto dall'art. 8 della Convenzione, deve prestare attenzione a vari fattori, tra i quali la previa informativa datoriale circa il monitoraggio delle *e-mail*, la portata ed estensione del controllo, la giustificazione dello stesso, la configurabilità di misure alternative meno invasive, la gravità delle conseguenze del controllo, la previsione di garanzie in favore del dipendente.

Si ritiene essenziale la predisposizione di un regolamento aziendale in difetto del quale nessun controllo datoriale appare legittimo (principio già affermato dalla stessa Corte nel 2007), e si indica analiticamente

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

quale debba essere il contenuto del regolamento e quali tutele spettino in ogni caso al lavoratore.

Si deve così verificare:

(i) se il dipendente sia stato preventivamente informato della possibilità che il datore controlli la corrispondenza e altre comunicazioni e dell'attuazione di tali misure;

(ii) quale sia l'estensione del controllo da parte del datore e il grado di intrusione nella *privacy* del dipendente;

(iii) se il datore abbia fornito motivazioni legittime per giustificare il monitoraggio delle comunicazioni e l'accesso ai loro contenuti effettivi;

(iv) se fosse stato possibile istituire un sistema di monitoraggio basato su metodi e misure meno intrusivi, rispetto all'accesso al contenuto delle comunicazioni del dipendente;

(v) quali siano le conseguenze del monitoraggio per il lavoratore e quale l'uso da parte del datore dei risultati dell'operazione;

(vi) se siano state predisposte adeguate misure di salvaguardia in favore del lavoratore.

Infine, lo Stato deve assicurare che un dipendente la cui comunicazione sia stata monitorata abbia accesso a un rimedio davanti a un organo giudiziario, competente a determinare se siano stati osservati i criteri predetti e se le misure contestate siano state legittime.

Non si tratta dunque solo di prevedere un regolamento dal contenuto ampio, ma di assicurare concretamente strumenti operativi con i quali rendere effettive quelle garanzie.

La decisione *Barbulescu 2* non è stata unanime, e diverse opinioni dissenzienti (tra cui quella del giudice italiano) hanno richiamato

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

l'ampio margine di apprezzamento di cui gli Stati dispongono in materia, che consente agli ordinamenti nazionali di prevedere forme di tutela non necessariamente laburistiche, ma penalistiche, di tutela della *privacy* o di risarcimento del danno.

La sentenza *Barbulescu 2* rende operanti direttamente all'interno del rapporto di lavoro tutte le garanzie che la disciplina della *privacy* in genere prevede ed ha dunque un contenuto fortemente progressivo per le tutele del lavoratore.

Nell'ordinamento italiano, il Garante della *privacy* ha in più occasioni (dapprima nelle *Linee Guida per posta elettronica ed Internet* del 2007 e poi in vari provvedimenti) previsto vari ed intensi limiti al controllo della posta elettronica dei dipendenti ed anche la Cassazione (n. 18443/2013), ha applicato al trattamento dei dati del lavoratore, operato dal datore per dimostrare l'illiceità della sua condotta (consistita in reiterati e non autorizzati accessi alla rete effettuati sul luogo di lavoro) i canoni della correttezza, pertinenza, necessità e non eccedenza rispetto alle finalità del loro utilizzo previsti dalla legge sulla *privacy*, nonché i principi rafforzati relativi alla tutela dei dati sensibili.

Dopo la *Barbulescu 2*, è certo che i detti limiti oggi valgano anche ai fini della legittimità del controllo datoriale, sicché le previsioni di regolamenti aziendali, codici disciplinari, norme contrattuali possono assumere rilievo solo nei limiti evidenziati, dovendo invece in ogni caso essere assicurati in favore del lavoratore strumenti di tutela verso i controlli a distanza posti in essere dal datore.

5. Il nuovo campo di applicazione materiale

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

Tornando all'esame del Regolamento, si segnala l'aggiornamento della nozione di "dato personale"; vi rientra qualunque dato o informazione attinente a un lavoratore identificabile direttamente o indirettamente nonché qualunque valutazione riferibile al suo comportamento in costanza di rapporto, non solo raccolti in occasione dell'assunzione e della gestione del rapporto lavorativo ma anche lasciati durante le navigazioni sul *web* tramite strumenti elettronici forniti dall'azienda, connessi all'uso delle *mail* nonché salvati in profili personali dei *social network*.

Nella nozione di "trattamento" rientrano tutte le operazioni del datore di gestione del rapporto, comprese quelle che comportino la comunicazione dei dati personali rilevanti nei casi di distacco o di somministrazione del personale.

Anche la cancellazione o distruzione del dato personale rientra nella nozione di trattamento, con inevitabili riflessi sui comportamenti dell'azienda in occasione della conclusione del rapporto in relazione alla distruzione dei dati personali contenuti negli strumenti aziendali in dotazione al lavoratore.

6. Campo di applicazione territoriale

Dal punto di vista territoriale, il Regolamento troverà applicazione se il soggetto a cui si riferiscono i dati "si trovi", realmente o virtualmente, nel territorio europeo ovvero se il Titolare o il Responsabile del trattamento è stabilito nell'Unione, indipendentemente dal luogo in cui sia effettuato il trattamento dei dati personali.

Tale estensione risulterà di notevole importanza per i dipendenti di società appartenenti a gruppi multinazionali. Consentirà una protezione della riservatezza dei dipendenti che lavorano o vivono

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

nell'Unione, anche nelle ipotesi in cui Titolari e Responsabili del trattamento non avranno sedi legali, né sedi secondarie nell'Unione Europea o il trattamento dei dati sia effettuato da altra società consociata avente sede fuori dall'Unione Europea.

7.L'informativa e il diritto di accesso del lavoratore al proprio fascicolo.

Nel Regolamento l'obbligo di informativa acquista una autonoma rilevanza, anche nelle fattispecie in cui non è necessario ottenere il consenso per procedere al trattamento.

L'interessato avrà diritto ad essere informato dell'esistenza di qualsiasi trattamento da parte del datore di lavoro, delle sue finalità, dell'esistenza di un'eventuale profilazione e delle conseguenze di essa anche ai fini della valutazione della persona in termini di rendimento; dovrà essere garantita un'agevole intelligibilità del quadro d'insieme del trattamento e l'adeguatezza della informativa.

Tali previsioni obbligheranno le aziende a riformulare le informative da consegnare ai lavoratori sul trattamento dei dati, sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli.

Significativo per il dipendente risulta altresì il potenziamento del diritto di accesso ai dati personali, incluse le relazioni predisposte dal datore di lavoro e inserite nel fascicolo personale.

Nel nostro ordinamento il diritto di accesso al fascicolo personale detenuto dal datore di lavoro, pure previsto dal Codice della *Privacy,* sinora è stato oggetto di interesse prevalentemente nel rapporto di lavoro di pubblico impiego, in quanto riconosciuto dalla giurisprudenza come diritto di accesso ai procedimenti amministrativi.

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

Nel rapporto di impiego privato l'attenzione a questi profili è stata meno intensa; tuttavia il Garante ha più volte ribadito l'obbligo per le aziende di consentire e facilitare l'accesso del dipendente al complesso di tutti i dati personali presenti negli archivi aziendali (i giudizi, le note di qualifica o i risultati degli esami di accertamento).
Qualora il dipendente non riuscisse a consultare queste informazioni, si applicherebbero le sanzioni penali previste dalla legge sulla *privacy*, nonché l'obbligo di risarcimento delle spese eventualmente sostenute a causa dell'illecito contegno dell'azienda.
Da ultimo è stato riconosciuto dalla Suprema Corte il diritto soggettivo del dipendente ad accedere al proprio fascicolo personale radicato nel contratto di lavoro (Cass. S.U. n. 2397/14), e la Cassazione ha confermato la fonte contrattuale di tale diritto (Cass. n. 6775/16), derivante dai generali obblighi di buona fede e correttezza che incombono sulle parti del rapporto di lavoro ai sensi degli artt. 1175 e 1375 c.c.; inoltre trova conferma in molti contratti collettivi i quali obbligano il datore di lavoro a conservare, in apposito fascicolo, tutti gli atti e i documenti, da chiunque prodotti, che attengono al percorso professionale, all'attività svolta e ai fatti più significativi che riguardano il dipendente e il diritto di quest'ultimo di prendere visione liberamente degli atti e documenti inseriti nel proprio fascicolo personale.
Nel regolamento sono riconosciuti il "diritto di rettifica", ossia di modifica dei dati personali "senza ingiustificato ritardo"; il "diritto all'oblio"; il "diritto di limitazione di trattamento", il "diritto alla portabilità del dato".
Queste disposizioni imporranno una maggiore attenzione alle aziende nelle attività di conservazione ed eventuale cancellazione dei dati

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

riferibili alla storia lavorativa dei dipendenti, anche in occasione nella distruzione dei dati contenuti nei *pc* e *personal devices* concessi in dotazione dalle aziende ai propri dipendenti.

8. Gli obblighi per i Titolari e i Responsabili del trattamento dei dati personali e le sanzioni

Nel Regolamento vi è un aggravio degli obblighi di Titolari e Responsabili; si pensi alla previsione di un'Analisi e Valutazione dei Rischi e alla conseguente adozione di Misure di Sicurezza Tecniche e Organizzative "adeguate" (e non più "minime") e, per i processi considerati "pericolosi" per i dati personali, alla valutazione d'impatto sulla protezione della riservatezza e ai controlli periodici sull'adeguatezza ed effettività delle misure predisposte; e alla nomina di un Responsabile della Protezione dei Dati.

Sono previsti adempimenti documentali, in sostituzione dei meccanismi autorizzativi con preventivi obblighi di notifica attuali, come l'obbligo di tenuta di registri.

Analogamente a quanto è avvenuto nella materia della salute e tutela della sicurezza sul lavoro (dir. n. 389/89) e nella disciplina della responsabilità amministrativa dell'impresa (d.lgs. n. 231/2001 e l. n. 123/2007), nella gestione della tutela della riservatezza si promuove la diffusione di modelli organizzativi assistiti da precisi sistemi documentali, di codici di condotta e di sistemi di certificazione volontaria.

I poteri relativi alle certificazioni saranno affidati all'Autorità di Controllo che potrà altresì graduare le sanzioni amministrative pecuniarie in caso di adesione a modelli organizzativi certificati.

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

Purtroppo all'adozione di modelli di certificazione volontaria non viene riconosciuta alcuna efficacia esimente da responsabilità. Si tratterà di verificare se l'Autorità di Controllo potrà e vorrà riconoscere alle certificazioni volontarie su questa materia valenza analoga a quella riconosciuta ai modelli organizzativi dal d.lgs. n. 231/2001.

9. Inutilizzabilità dei dati acquisiti in violazione del Regolamento

Solo il rispetto delle disposizioni in tema di informativa del lavoratore e della disciplina sulla protezione dei dati personali consente l'utilizzabilità del dato personale acquisito "*a tutti i fini del rapporto di lavoro*" (ossia a fini retributivi o disciplinari) (art. 4, St. lav.).

Resta da capire se il legislatore italiano, nell'introdurre "*misure appropriate e specifiche a salvaguardia dei diritti"* dei lavoratori (art. 88, co. 2, Reg.) e nel prevedere dissuasive sanzioni (art. 84 Reg.), riconoscerà effettività processuale al principio dell'inutilizzabilità dei dati personali del dipendente illecitamente raccolti.

Il rimedio generale dell'inutilizzabilità, introdotto nel vigente Codice della *Privacy* (art. 11, c. 2), è stato depotenziato dalla giurisprudenza, che, in assenza di specifiche disposizioni processuali hanno dato una lettura riduttiva della norma.

Le Corti penali riconoscono l'ammissibilità di mezzi istruttori precostituiti fondati su dati acquisiti in violazione delle norme a tutela della privacy in considerazione del principio di prevalenza dell'esigenza di ordine pubblico relativa alla prevenzione dei reati rispetto alle disposizioni a tutela della riservatezza. Le Corti civili riconoscono l'inutilizzabilità anche processuale dei dati illegittimamente raccolti e dei mezzi istruttori basati sugli stessi nei casi in cui tali dati comprovino meri illeciti di natura civilistica.

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it

Per aumentare l'efficacia delle norme a tutela della privacy in ambito giuslavoristico, potrà essere opportuno valutare l'emissione di una norma processuale che sancisca chiaramente l'inammissibilità dei mezzi istruttori, fondati su dati ottenuti in violazione della normativa a tutela della Privacy.

In conclusione, sarà opportuno per le aziende italiane prevedere specifiche Norme vincolanti d'impresa e ridefinire la modulistica elaborata per l'assolvimento degli obblighi di informazione e trasparenza, anche attinenti ai controlli a distanza, con i contenuti che abbiamo esaminato in questo intervento e il testo in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Avv. Alberto Maffei

Via Cibrario 28,10144, Torino – Tel. 0114731420 – Fax. 0114731529
albertomaffei@cnfpec.it – almaffei@libero.it