

## Uso della posta elettronica aziendale e controllo datoriale

### 1. Premessa

Nell'esaminare il tema non si può assolutamente prescindere dalle "Linee guida" emanate dal Garante per la privacy con la Delibera n. 13 del 1 marzo 2007, relativamente a "posta elettronica e internet" nonché da eventuali regolamenti, schema di regolamenti o disciplinari emanati da associazioni di categoria con invito ad essere applicati dalle proprie aziende associate, dopo averli debitamente pubblicizzati e notificati ai dipendenti e alle R.S.A.

Il contenuto di tali disciplinari è incisivamente illustrato dalla precitata delibera n. 13/2007 del Garante per la protezione dei dati personali e di esso diremo in prosieguo al punto **3.1**.

Va, peraltro, detto sin dalla premessa, che qualora l'azienda abbia avuto l'avvertenza o l'accortezza di porre in essere tali regolamenti o disciplinari – in ciascuno dei quali ricorre l'usuale affermazione che gli strumenti informatici (internet e posta elettronica) di cui sono stati dotati i lavoratori, sono e restano di pertinenza aziendale, e la loro assegnazione è solo funzionale al corretto disimpegno delle mansioni – l'uso privato di essi o non conforme alle precisazioni contenute nel disciplinare, da parte dei dipendenti, esonerano l'azienda dall'incorrere nel reato penale ex art. 616 c.p. (violazione di corrispondenza privata), nel caso specifico *sub specie* di cognizione della posta elettronica indirizzata al dipendente.

Ciò in quanto il reato penale in questione si attualizza con espresso riferimento alla cognizione della corrispondenza cd. "chiusa" e non già a quella cd. "aperta", tra cui la Cassazione fa rientrare le comunicazioni via e-mail dei dipendenti utilizzando l'account aziendale, in quanto, se anche protetto da password, quest'ultima deve essere (ovvero è normalmente) comunicata e detenuta in busta chiusa dal Responsabile o preposto del dipendente, legittimato all'utilizzo in casi di emergenza o di assenze prolungate del lavoratore nel cui account confluiscono indistintamente comunicazioni aziendali e personali.

### 2. La giurisprudenza sul tema

Al riguardo il Tribunale di Torino del 15 settembre 2006, n. 143 ha affermato quanto segue: «*Il dipendente che utilizza la casella di posta elettronica aziendale si espone al rischio che anche altri della medesima azienda - unica titolare del predetto indirizzo - possano lecitamente accedere alla casella in suo uso non esclusivo e leggerne i relativi messaggi in entrata e in uscita ivi contenuti, previa acquisizione della relativa password, la cui finalità non risulta essere allora quella di proteggere la segretezza dei dati personali custoditi negli strumenti posti a disposizione del singolo lavoratore, bensì solo quella di impedire che ai suddetti strumenti possano accedere anche persone estranee alla società (come anche si evince dal tenore della stessa guida sulla sicurezza informatica e nell'ultimo parere del Garante della privacy). Ne deriva quindi che, in caso di accesso alla posta elettronica aziendale del dipendente, non sembra dunque potersi ravvisare un elemento essenziale della fattispecie delittuosa di cui all'articolo 616 del Cp rappresentato, sotto il profilo oggettivo, dalla alienità della corrispondenza medesima, apparendo infatti corretto ritenere che i messaggi inviati tramite l'e-mail aziendale del lavoratore (anche se*

*nell'estensione dell'indirizzo compare il nome dello stesso dipendente) rientrano nel normale scambio di corrispondenza che l'impresa intrattiene nello svolgimento della propria attività organizzativa e produttiva e, pertanto, devono ritenersi relativi a quest'ultima, materialmente immedesimata nelle persone che sono preposte alle singole funzioni: le attrezzature, comprese quelle informatiche, devono allora reputarsi direttamente correlate alla funzione del soggetto che nel frangente rappresenta l'impresa e, solo in via mediata, assegnate alla singola persona comunque fungibile nel rapporto col mezzo medesimo».*

Nello stesso senso il Tribunale di Chivasso del 15.9.2006, secondo cui: «Le attrezzature lavorative e, tra queste, quelle informatiche, devono considerarsi direttamente correlate alla funzione del soggetto che rappresenta l'impresa e, solo in via mediata, devono reputarsi assegnate al singolo dipendente, comunque fungibile nel rapporto con lo strumento aziendale. L'indirizzo di posta elettronica aziendale, al di là dell'uso solo apparentemente personale da parte del dipendente quale principale utilizzatore aziendale, può sempre essere a disposizione di soggetti diversi, appartenenti alla sua stessa impresa. Anche se nell'estensione dell'indirizzo di posta elettronica compare il nome del dipendente che procede all'invio, i messaggi inviati attraverso l'e-mail aziendale rientrano nel normale scambio di corrispondenza che l'impresa intrattiene. Pertanto, in caso di accesso alla casella di posta elettronica aziendale del dipendente da parte dell'impresa, non può ravvisarsi una violazione dell'art. 616 c.p., che contempla il reato di violazione, sottrazione e soppressione di corrispondenza. Non sussiste, infatti, un diritto esclusivo del lavoratore ad accedere in via esclusiva al proprio computer aziendale e ad utilizzare in via esclusiva e riservata la propria casella di posta elettronica aziendale».

In senso conforme Cass. 19 dicembre 2007, n. 47096, che ha stabilito che: «Non integra il reato di cui all'art. 616 cod. pen. la condotta del superiore gerarchico che prenda cognizione della posta elettronica contenuta nel computer del dipendente, assente dal lavoro, dopo avere a tal fine utilizzato la password in precedenza comunicatagli in conformità al protocollo aziendale».

In ambito penalistico – avendo invocato in giudizio il lavoratore la violazione della propria corrispondenza privata, violazione ritenuta invece insussistente – merita riferire l'articolata motivazione dell'ordinanza penale di Trib. Milano 15 maggio 2002 (Giud. Pellegrino), che ha così ragionato: «Va detto innanzitutto come non possa mettersi in dubbio il fatto che l'indirizzo di posta elettronica affidato in uso al lavoratore, di solito accompagnato da un qualche identificativo più o meno esplicito, abbia carattere personale, nel senso cioè che lo stesso viene attribuito al singolo lavoratore per lo svolgimento delle proprie mansioni.

Tuttavia, "personalità" dell'indirizzo non significa necessariamente "privatezza" del medesimo dal momento che, salve le ipotesi in cui la qualifica del lavoratore lo consenta o addirittura lo imponga in considerazione dell'impossibilità o del divieto di compiere qualsiasi tipo di controllo/intromissioni da parte di altri lavoratori che rivestano funzioni o qualifiche sovraordinate (fattispecie che potrebbe effettivamente indurre a qualche dubbio), **l'indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore consuetudinario** (ma sempre appartenenti all'azienda) a prescindere dalla identità o diversità di qualifica o funzione:

*-ipotesi, frequentissima, è quella del lavoratore che "sostituisce" il collega per qualunque causa (ferie, malattia, gravidanza) e che va ad operare, per consentire la continuità aziendale, sul personal-computer di quest'ultimo anche per periodi di tempo non limitati.*

*Così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti è inconfigurabile in astratto, salve eccezioni di cui sopra, un diritto all'utilizzo esclusivo di una casella di posta elettronica aziendale.*

***Pertanto il lavoratore che utilizza - per qualunque fine - la casella di posta elettronica, aziendale, si espone al "rischio" che anche altri lavoratori della medesima azienda che, unica, deve considerarsi titolare dell'indirizzo - possano lecitamente entrare nella sua casella (ossia in suo uso sebbene non esclusivo) e leggere i messaggi (in entrata e in uscita) ivi contenuti, previa consentita acquisizione della relativa password la cui finalità non è certo quella di "proteggere" la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società.(...).***

*Tanto meno può ritenersi che leggendo la posta elettronica contenuta sul personal del lavoratore si possa verificare un non consentito controllo sulle attività di quest'ultimo atteso che **l'uso dell'e-mail costituisce un semplice strumento aziendale a disposizione dell'utente-lavoratore al solo fine di consentire al medesimo di svolgere la propria funzione aziendale** (non si possono dividere i messaggi di posta elettronica: quelli "privati" da un lato e quelli "pubblici" dall'altro) e che, come tutti gli altri strumenti di lavoro forniti dal datore di lavoro, rimane nella completa e totale disponibilità del medesimo senza alcuna limitazione».*

## **2.1. Il controllo datoriale ricondotto dalla Cassazione tra i legittimi controlli difensivi**

Va altresì evidenziato che il datore di lavoro è pienamente legittimato – analogamente alla similare fattispecie del controllo diretto o tramite terzi presso i registratori di cassa dei supermarkets – a porre in essere dei controlli a posteriori (cd. difensivi) sulla correttezza dell'operato del dipendente che utilizzi la posta elettronica nel caso in cui ne sospetti l'uso abusivo, senza incorrere nel divieto, ex art. 4, l. n. 300/70, di controllo all'insaputa sulle modalità di esecuzione della prestazione. Al riguardo va fatto presente che la nuova formulazione dell'art. 4 dello Statuto dei lavoratori del 1970 (risultante da uno dei decreti attuativi del cd. Jobs act) ha eliminato il preesistente divieto assoluto di controllo dell'attività lavorativa eventualmente derivante, in forma indiretta, da apparecchiature e strumentazioni sia assegnate al lavoratore per motivi di lavoro sia strumentali all'adempimento della prestazione (lettori di badge e posta elettronica). Ne è sortita la conseguente legittimazione alla cognizione delle comunicazioni via e-mail e delle registrazioni delle presenze al lavoro ed al loro controllo da parte del datore di lavoro, peraltro condizionandolo alla rispondenza ad esigenze organizzative e produttive aziendali nonché ad intese sindacali o autorizzazioni della Direzione regionale del lavoro (ai sensi del residuo comma 2 del citato art.4 S.d.L.), volte ad

evitare controlli in forma massiva e generalizzata, irrispettosi dei criteri di correttezza e pertinenza.

Quindi, poiché la posta elettronica costituisce uno dei tanti strumenti il cui utilizzo è richiesto da esigenze produttive e organizzative aziendali, il controllo dell'attività del lavoratore tramite l'accesso e la lettura dell'account aziendale utilizzato dal dipendente è riconducibile tra le ipotesi di cui al secondo comma dell'art. 4 dello Statuto dei Lavoratori e, pertanto, il datore di lavoro non incorre nel divieto ex art. 4 dello Statuto dei Lavoratori.

Difatti, pur rappresentando una forma di controllo a distanza lesivo dei diritti dei dipendenti, l'accesso da parte del datore di lavoro all'account aziendale utilizzato dal dipendente può ritenersi ammissibile se inquadrabile come modalità di "controllo difensivo", ovvero laddove fosse finalizzato a prevenire o reprimere gli illeciti commessi dal lavoratore in danno dell'impresa.

La conferma viene dalla recente Cass., sez. lav., **23 febbraio 2012, n. 2722, che – relativamente ad un cd. controllo difensivo a posteriori su un bancario** che aveva divulgato con messaggi elettronici diretti ad estranei notizie riservate concernenti un cliente dell'istituto e aveva effettuato operazioni finanziarie da cui aveva tratto vantaggio personale, ha stabilito: **«tale fattispecie è estranea al campo di applicazione dell'articolo 4 dello statuto dei lavoratori. Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetuazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il cd. controllo difensivo, in altre parole, non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'istituto bancario presso terzi».**

Tesi altresì confermata dalla 4 sezione della Corte europea dei diritti umani che, con sentenza (peraltro non vincolante i tribunali italiani ma costituente significativo precedente) del 1 dicembre 2015 – le cui motivazioni sono state rassegnate soltanto in data 12 gennaio 2016 - ha statuito che, di fatto, **il datore di lavoro è legittimato a controllare le e-mail inviate e ricevute dai dipendenti tramite l'account di posta aziendale e finanche legittimato a licenziare il dipendente in caso di utilizzo dell'account aziendale per fini privati in spregio alla policy aziendale che, invece, ne impone l'uso per soli fini professionali.**

La pronuncia in esame muove dal caso 61496/08 presentato da un ingegnere romeno per ottenere l'annullamento del suo licenziamento per violazione della *privacy* dato che, a suo dire, il datore di lavoro lo avrebbe licenziato soltanto dopo essere venuto a conoscenza dell'utilizzo della messaggeria Yahoo! (servizio di messaggeria intestato all'azienda e creato appositamente per motivi di lavoro) per fini privati e non esclusivamente per motivi di lavoro in violazione delle regole aziendali interne.

Ebbene, i giudici di Strasburgo hanno decretato che il controllo da parte del datore di lavoro dell'account di posta aziendale del dipendente non rappresentava invero una violazione della sua *privacy* e che il frequente utilizzo per fini privati e personali dell'account aziendale ne giustificava dunque il licenziamento. La legittimazione al



controllo aziendale è stata fatta discendere dalla fondata considerazione che l'account aziendale, pur essendo utilizzato dal lavoratore, risulta comunque uno strumento aziendale di proprietà del datore di lavoro il quale, pertanto, ne ha piena disponibilità di accesso e lettura laddove fosse necessario per appurare il corretto adempimento del dipendente ai compiti professionali durante l'orario lavorativo (cd. controllo difensivo).

## **2.2. La sanzione deve essere proporzionata al reale danno arrecato dall'infrazione**

Peraltro va evidenziato come a mitigare il ricorso alla sanzione espulsiva del lavoratore che abbia utilizzato in modo improprio e a fini personali la posta elettronica aziendale e le dotazioni informatiche assegnategli, sono intervenute due sentenze di legittimità, ravvisando nel licenziamento in tronco una sanzione sproporzionata all'infrazione riscontrata nel caso di specie, al tempo stesso legittimando il licenziamento al solo riscontro di un grave danno arrecato all'azienda dal comportamento trasgressivo del dipendente, in forma di notevole sottrazione al tempo di lavoro o di concreto e rilevante pregiudizio all'attività produttiva.

La Corte di cassazione, con sentenza n. 6222 del 18 marzo 2014, ha affermato che *«il datore di lavoro non può irrogare un licenziamento per giusta causa quando questo costituisca una sanzione più grave di quella prevista dal contratto collettivo applicabile in relazione ad una determinata infrazione»*.

Nel caso di specie un lavoratore impugnava il licenziamento disciplinare intimatogli, dopo una sospensione cautelare, a seguito di contestazione disciplinare con l'addebito di uso improprio di strumenti di lavoro e in particolare del P.C. affidatogli, delle reti informatiche aziendali e della casella di posta elettronica. Deduceva la nullità della sanzione, chiedendo la reintegrazione nel posto di lavoro e il risarcimento del danno; il Tribunale adito accoglieva la domanda e la Corte di Appello confermava tale decisione, rilevando che il fatto contestato corrispondeva alla fattispecie disciplinare prevista dal contratto collettivo applicabile, ove è stabilita solo una sanzione conservativa per l'infrazione consistente nell'utilizzazione "in modo improprio di strumenti di lavoro aziendali".

Con la successiva del 2 novembre 2015, n. 22353, la Cassazione ha statuito che è eccessivo il licenziamento come sanzione disciplinare nei confronti del dipendente che abbia approfittato degli strumenti messi a disposizione dall'azienda per svolgere attività che nulla c'entrano con la prestazione lavorativa; nonostante l'abuso di chi utilizzi il personal computer in dotazione, la linea internet e la casella di posta elettronica aziendale per scopi personali, il datore di lavoro deve pur sempre rispettare la proporzione tra sanzione e illecito disciplinare.

Condizione per conservare il posto di lavoro – specifica la Corte – è tuttavia che l'utilizzo personale della posta elettronica e della navigazione in internet non abbiano determinato una significativa sottrazione di tempo all'attività di lavoro, né il blocco del lavoro, con grave danno per l'attività produttiva. Insomma, il punto nodale per stabilire se vi sia o meno possibilità di licenziamento resta sempre la dimostrazione di un effettivo e rilevante "danno" per l'azienda.

Nel caso di specie, sono risultati del tutto irrilevanti, ai fini dell'accoglimento della tesi del datore di lavoro, i numerosi preavvisi inviati ai dipendenti con cui l'azienda aveva chiesto un uso più attento della strumentazione aziendale.

Pertanto, per i giudici della Cassazione, è da escludere la particolare gravità del comportamento del lavoratore che abbia fatto un uso indebito degli strumenti aziendali, con la conseguenza della liceità dell'irrogazione di sole sanzioni disciplinari più miti di natura conservativa (sospensione, multa, ecc.).

### ***3. Gli oneri posti a carico dal Garante sul datore di lavoro in tema di sussidi informatici***

La delicatezza dei nuovi mezzi tecnologici di comunicazione, suscettibili in carenza di sensibilizzazione e di informativa specifica nei confronti del lavoratore utente – delicatezza che si può riverberare nel controllo all'insaputa delle modalità di disimpegno dell'attività lavorativa (vietato dall'art. 4 Statuto dei lavoratori) e dei diritti di privacy (tramite indebita acquisizione datoriale di dati personali e sensibili, e così via) – ha indotto il Garante dei dati personali, a disporre a carico dei datori di lavoro che assegnino la strumentazione informatica ai dipendenti ad essere più incisivo della giurisprudenza e di maggior *favor* verso i lavoratori, imponendo ai datori di assolvere a specifici oneri (che qualora non assolti colorano il comportamento datoriale di illiceità).

Ciò in quanto è stato riconosciuto che il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.). Talché il Garante ha disposto che *«grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.*

*Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative».*

#### ***3.1. Linee guida della delibera n. 13/2007 del Garante***

«In questo quadro, può risultare opportuno – dice il Garante - adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

-se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;

in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle

oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);

quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;

-se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);

**-se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime – specifiche e non generiche – per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);**

**-quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;**

le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti (...)).».

### **3.2. Onere di informativa (ex art. 13 del Codice privacy: d.lgs. n. 196/03)**

«All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli – insiste il Garante - si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice privacy, anche unitamente agli elementi indicati ai punti 3. e 3.1.

**Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.**

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (*art. 4, secondo comma, l. n. 300/1970*); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti».

### **3.3. Posta elettronica**

«Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i *file* allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (*artt. 2 e 15 Cost.; Corte cost. 17 luglio*

1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale).

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

**La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.**

**Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").**

È quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

-il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficio reclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);

-il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;

-il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati; in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura



del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

**-i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi,** precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale».

Roma, novembre 2016

**Mario Meucci** - Giuslavorista