MB.O LAW REVIEW

RIVISTA GIURIDICA ON-LINE

www.mbolaw.it

# *LA TUTELA DEL DIRITTO ALLA PRIVACY DEL LAVORATORE DOPO LA CESSAZIONE DEL RAPPORTO DI LAVORO*

3/2021

di *Luigi Previtera*

mb·o
STUDIO LEGALE
BONA·OLIVA
& ASSOCIATI

# *LA TUTELA DEL DIRITTO ALLA PRIVACY DEL LAVORATORE DOPO LA CESSAZIONE DEL RAPPORTO DI LAVORO*

**LUIGI PREVITERA,** *AVVOCATO, STUDIO LEGALE MB.O, TORINO*

ABSTRACT

***Il diritto alla tutela della privacy nell'ambito del rapporto di lavoro è materia che conosce regolamentazioni precise.***

***Tuttavia, dopo la cessazione del rapporto di lavoro, venuto meno il vincolo contrattuale, possono sorgere situazioni critiche sulla gestione del patrimonio di dati che, volontariamente o meno, il dipendente può avere lasciato in azienda.***

***Oggetto del presente approfondimento è proprio l'esame degli obblighi insistenti sul datore di lavoro e sul lavoratore in materia di diritto alla privacy, nel momento in cui il rapporto di lavoro cessa.***



* * *

## 1. Principi generali in materia di privacy nel rapporto di lavoro

La tutela della privacy nel rapporto di lavoro interessa principalmente il controllo del trattamento dei dati relativi al soggetto interessato (il lavoratore) ad opera del titolare del trattamento (il datore di lavoro), alla luce delle disposizioni contenute nel Codice della Privacy (Decreto legislativo 30 giugno 2003, n. 196, in vigore dal 1º gennaio 2004) e dal successivo Regolamento UE 2016/679 denominato GDPR (General Data Protection Regulation, recepito in Italia con il D. Leg. 101/2018).

Nel Regolamento UE n. 2016/679 all'art. 88 si prevede che "*gli Stati membri possono prevedere, con legge o tramite accordi collettivi, norme più specifiche per assicurare la tutela dei diritti e delle libertà rispetto al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro*". Tale norma di apertura consente di adattare in maniera equa e funzionale la normativa ai precipui obiettivi perseguiti nell'ambito di un rapporto di lavoro.

Le condizioni di liceità previste dall'art. 11 D.Lgs. 196/2003 e dall'art. 5 Regolamento UE 2016/679 costituiscono presupposto imprescindibile per il trattamento dei dati personali dei dipendenti da parte del datore di lavoro.

Nello specifico, condizioni di liceità relative alle modalità di svolgimento del trattamento sono quelle di necessità e trasparenza.

In altre parole, le modalità di trattamento devono essere predefinite e rese note all'interessato con riferimento alle modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati; in ogni caso il controllo deve essere limitato a quanto strettamente necessario e non, come a volte accade, prolungato nel tempo e generalizzato.

Quanto invece ai dati che possono formare oggetto di trattamento, sarà necessario rispettare i principi della pertinenza, adeguatezza e non eccedenza. I dati personali raccolti e trattati dal datore di lavoro devono essere solo quelli strettamente funzionali al perseguimento delle finalità dichiarate dal titolare del trattamento nell'informativa resa ai lavoratori.

Diretto corollario di quanto detto è che, ad esempio, il periodo di conservazione dei dati personali deve essere limitato al minimo necessario. L'adeguatezza, invece, impone che i dati raccolti siano formalmente idonei al raggiungimento dello scopo perseguito.

Il trattamento dei dati è lecito solo se ricorrono talune condizioni specificamente previste dall'art. 6 del GDPR.

Sulla scorta della suddetta previsione normativa ed a tutela del prestatore di lavoro-interessato, oltre al consenso di quest'ultimo si rinvengono altre condizioni di liceità del trattamento dei dati personali. Il consenso assumerebbe così carattere residuale.

Tali condizioni si riscontrano nell' "*esecuzione di un contratto di cui l'interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dello stesso*", nel "*perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali*". Altre condizioni citate dall'art. 6 sono "*l'obbligo legale al quale è soggetto il titolare del trattamento*" e "*l'esecuzione di un*

*compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*".

Ai sensi dell'art. 9 del GDPR, il trattamento è vietato se rivolto a "*categorie particolari di dati personali*" (dicitura che sostituisce i cd. *Dati sensibili* previsti nel Codice Privacy). Il Legislatore europeo, però, nello stesso art. 9 ha previsto al paragrafo 2, lett. b), una deroga al divieto di trattamento di tali tipologie di dati, autorizzando il trattamento, fra le altre ipotesi, "*quando è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione e degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato*".

La disciplina generale sul legittimo trattamento dei dati personali, in materia di rapporto di lavoro, si rinviene peraltro anche nelle Linee Guida emanate dall'Autorità Garante della privacy del 23 novembre 2006, che offrono una pregnante regolamentazione in materia di rapporto di lavoro privato.

In estrema sintesi, le suddette Linee guida del Garante della Privacy stabiliscono:

- che il datore di lavoro deve obbligatoriamente trattare i dati personali dei dipendenti nel rispetto dei principi di liceità, trasparenza, pertinenza e secondo le finalità preindicate;
- la possibilità di diffondere i dati personali da parte del datore di lavoro è consentita solo per dare esecuzione agli obblighi derivanti dal contratto di lavoro od obblighi di legge.
- La necessità da parte del datore di lavoro di rendere al dipendente adeguata e completa informativa sul trattamento dei dati posto in essere;
- l'identificazione puntuale delle figure soggettive che possono trattare i dati, eventualmente con le relative nomine di tali soggetti a titolari del trattamento;
- la classificazione dei dati idonei a rivelare lo stato di salute e l'accesso alle cartelle sanitarie e di rischio che è vietato al datore di lavoro.

Le Linee Guida indicano anche quali sono le tipologie di dati personali oggetto di tutela e, dunque, sottoposti all'applicazione delle disposizioni contenute nel Codice Privacy e nel GDPR. Tali dati si sostanziano in:

- dati anagrafici dei lavoratori, dati biometrici (utilizzabili e raccoglibili entro certi limiti), fotografie e dati sensibili riferiti anche a terzi;

- dati idonei a rivelare lo stato di salute, il credo religioso o altre categorie particolari di dati;
- informazioni connesse al rapporto di lavoro (tipologia di contratto, qualifica, retribuzione);
- dati contenuti in atti o documenti che il lavoratore ha fornito al momento dell'assunzione, resi disponibili in albi, bacheche o assunti dal datore di lavoro[1].

### 1.1. In particolare: l'obbligo di informativa

Il rispetto dell'obbligo di informativa comporta la predisposizione di un documento aziendale denominato *Privacy Policy*, allo scopo di soddisfare l'esigenza di trasparenza e correttezza del trattamento stesso, sin dalla fase di progettazione del trattamento, anche allo scopo di poter comprovare in qualsiasi momento la legittimità del trattamento e la corretta informazione in merito a modalità e limiti forniti all'interessato.

Ai sensi degli artt. 13 e 14 del GDPR, l*a Privacy Policy* deve tassativamente contenere l'indicazione degli strumenti che consentono il controllo a distanza nonché le modalità e le regole di utilizzo di tali strumenti, la tipologia di controlli effettuati dall'azienda, i dati conservati e i soggetti abilitati ad accedervi, nonché le modalità e i tempi di conservazione dei dati stessi e le eventuali sanzioni che potranno essere comminate al dipendente in caso di violazione delle norme preposte.

La *policy* non può essere predisposta in via generica, ma deve contenere un chiaro riferimento al possibile svolgimento dell'attività di controllo e alle relative modalità di utilizzo.

---

[1] Le medesime disposizioni emanate con riferimento al rapporto di lavoro privato trovano applicazione anche nel rapporto di pubblico impiego, con delle particolarità.
Tra le principali peculiarità si segnalano:

- in materia di assenze per malattia, certificati e visite mediche, all'amministrazione possono essere prodotti certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. In ogni caso l'amministrazione, in caso di dati ultronei autonomamente forniti dal dipendente, deve limitarsi all'uso necessario, astenendosi dunque dall'utilizzare queste informazioni.
- In materia di diffusione dei dati in Internet le amministrazioni devono assicurare l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete e garantire il "diritto all'oblio[1]" del lavoratore. Ad esempio, nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati pertinenti ed è sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati;
- anche nell'ambito del pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride) per controllare le presenze o gli accessi sul luogo di lavoro e tali sistemi possono essere attivati solo in presenza di particolari esigenze).

L’informativa privacy, in sostanza, non può essere genericamente riferita alla pluralità di strumenti e mezzi informatici messi a disposizione del lavoratore, dovendo lo stesso essere dettagliatamente informato della possibilità di essere controllato dal datore di lavoro durante l’effettivo utilizzo dello strumento stesso.

Ad esempio, il lavoratore deve essere reso edotto della possibilità per il datore di lavoro di verificare la tipologia dei siti Internet visitati e di accertare la durata degli accessi ai siti medesimi.

Sul presupposto che l’informativa al dipendente non necessita di una raccolta di autorizzazioni e consensi al trattamento da parte dell’interessato, in quanto basi legali lecite sono lo stesso contratto d’assunzione e gli obblighi legali nascenti dal rapporto di lavoro, è invece importante informare correttamente il lavoratore della possibilità per il titolare del trattamento di trasmettere i dati, anche a soggetti terzi (consulenti, elaboratori di buste paga ecc.).

Sarebbe inoltre opportuno segnalare nell’informativa, se del caso anche in apposito ed autonomo documento allegato alla stessa, eventuali altri strumenti di raccolta dei dati personali, come ad esempio badge di rilevazione presenze, diffusione di immagini del personale mediante social media, impianti di videosorveglianza, installazione di sistemi di rilevazione GPS su veicoli aziendali, sistemi di controllo mediante rilevatori biometrici.

## 2. Tutela della privacy alla cessazione del rapporto di lavoro

Avendo tracciato le coordinate normative ed i principi generali che sostengono il complesso normativo in materia di privacy, ai fini del presente contributo è necessario soffermarsi sulle peculiarità della disciplina posta a tutela del diritto alla riservatezza allorquando il rapporto di lavoro cessa.

Se difatti nella fase preliminare e iniziale del rapporto di lavoro e in costanza di esso le regole e la disciplina in materia di privacy sono sostanzialmente chiare e ben delineate dal Legislatore (italiano ed europeo), ciò che succede successivamente alla cessazione di tale rapporto pone considerevoli problemi interpretativi, causati anche dalla difficoltà di individuare le norme da applicare.

Si tratta, in altre parole, di ricostruire e individuare i corretti adempimenti a carico delle parti del rapporto di lavoro, partendo dai principi generali esistenti in materia di privacy.

Verranno dunque analizzati i profili problematici che sorgono nella fase terminale del rapporto di lavoro, ossia quando, qualsiasi sia la causa, il rapporto tra datore di lavoro da una parte e lavoratore dall'altra si interrompe.

Diviene in tali casi assai utile soffermarsi ad analizzare gli adempimenti pratici posti in capo alle parti del rapporto di lavoro, e gli accorgimenti relativi al trattamento dei dati personali appartenenti all'ex dipendente, o ai dati dell'azienda da quest'ultimo detenuti anche successivamente alla cessazione del rapporto di lavoro.

## 2.1. Gestione dell'account email dell'ex dipendente e dell'archivio messaggi di posta

Il problema relativo alla gestione degli account email utilizzati dai dipendenti ha generato molteplici problemi interpretativi, soprattutto con particolare riferimento ai risvolti sul piano della tutela della privacy.

In particolare, il maggior problema riguarda la destinazione dell'account email attribuito al dipendente, con il relativo archivio di email, successivamente alla cessazione del rapporto di lavoro.

In altri termini, alla cessazione del rapporto di lavoro sorgono sovente problematiche inerenti la destinazione dell'account dell'ex dipendente.

Che fine fa l'indirizzo di posta assegnato al dipendente una volta che questo cessi di prestare servizio presso l'azienda? Quanto tempo il datore di lavoro può lasciare l'account attivo? E, soprattutto, in che modalità può trattare i dati (personali e aziendali) contenuti nell'archivio dei messaggi di posta elettronica?

### ❖ Disattivazione account email ex dipendente

Recentemente, il Garante per la Protezione dei Dati Personali, con provvedimento del 4 dicembre 2019, ha espressamente sancito il principio che *"**commette un illecito la società che mantiene attivo l'***account email ***aziendale di un dipendente dopo l'interruzione del rapporto di lavoro** e accede alle* email *contenute nella sua casella di posta elettronica. La protezione della vita privata si estende anche all'ambito lavorativo"*[2].

[2] Il Provvedimento del 4 dicembre 2019, Garante Per La Protezione Dei Dati Personali stabilisce difatti che "*ai sensi dell'art. 57, par. 1, lett. f) e 58, par. 2, lett. b) del Regolamento, dichiara illecito* il trattamento descritto nei termini di cui in motivazione, consistente nella persistente attività *dell'account aziendale individualizzato per un ampio periodo di tempo dopo l'interruzione del* rapporto di lavoro, con contestuale accesso ai messaggi ivi pervenuti, ed ammonisce Imper Italia S.r.l. sulla necessità di conformare i trattamenti effettuati sugli account di posta elettronica

La pronuncia in parola prende l'avvio dalle rimostranze di un ex dipendente di una società il quale lamentava la mancata disattivazione dell'account di posta elettronica allo stesso assegnato in costanza di rapporto, e la mancata informativa circa la possibilità per il datore di lavoro di accedere ai messaggi in esso contenuti.

Il Garante ha ritenuto illegittima la mancata disattivazione dell'account di posta elettronica assegnato all'ex dipendente (contenente nome e cognome dello stesso) in quanto in violazione dei seguenti principi:

- principio di correttezza, che presuppone l'informazione preventiva dei dipendenti da parte del Titolare del trattamento, circa le caratteristiche essenziali dei trattamenti che intende effettuare, ivi compresi gli strumenti messi a disposizione nell'ambito del rapporto di lavoro;
- provvedimento n. 551 del 27 novembre 2014, richiamato espressamente, in base al quale "*lo scambio di corrispondenza elettronica (estranea o meno all´attività lavorativa) tra il ricorrente e soggetti esterni o interni alla struttura aziendale configura un´operazione idonea a rendere conoscibili talune informazioni personali relative all´interessato, si pensi (anche a prescindere dal contenuto della corrispondenza che certamente può contenere dati personali che lo riguardano) al trattamento dei nominativi dei mittenti e/o dei destinatari delle e-mail, già di per sé stessi in grado di fornire, come i dati di traffico telefonico, indicazioni rilevanti in ordine ai contatti e alle relazioni dello stesso ricorrente e, quindi, essere considerati dati personali ad esso relativi* ";
- "Linee guida del Garante per posta elettronica e Internet" del 1 marzo 2007, citate dal Garante Privacy nel provvedimento in parola, in base al quale "*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*". Tutto ciò, nell'alveo di un rapporto di lavoro si traduce nella legittima aspettativa di riservatezza del dipendente su alcune forme di comunicazione, anche nell'ipotesi in cui venga a cessare il rapporto di lavoro tra le parti.

aziendale dopo la cessazione del rapporto di lavoro alle disposizioni ed ai principi in materia di protezione dei dati personali indicati in motivazione".

- Principi dettati dalla costante giurisprudenza della Corte europea dei diritti dell'uomo[3].

Pertanto, il Garante ha specificato che, alla cessazione del rapporto di lavoro, il datore di lavoro "*in conformità ai principi in materia di protezione dei dati personali, debba rimuovere gli account di posta elettronica aziendali riconducibili a persone identificate o identificabili (in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure), previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento, provvedendo altresì ad adottare misure idonee ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione; l'adozione di tali misure tecnologiche ed organizzative consente di contemperare l'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte di dipendenti/collaboratori nonché dei terzi (v., da ultimo, provv.to 1° febbraio 2018, n. 53, in www.garanteprivacy.it, doc. web n.* ***8159221****. Si veda anche il provv. 5 marzo 2015, n. 136, doc. web n.* ***3985524*** *e il citato provv. 27 novembre 2014, n. 551; nello stesso senso v. Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, spec. par. 14.5);"*

Da quanto detto, sulla scorta dei principi dettati dal Garante per la Privacy, è opportuno per il datore di lavoro, onde non incorrere in possibili violazioni delle norme previste in materia di tutela dei dati personali porre in essere le seguenti misure preventive atte ad evitare di incorrere in responsabilità da illecito trattamento dei dati personali:

- adottare una procedura di assegnazione formale degli account di posta elettronica e di ogni altro strumento di lavoro, prevedendo in maniera chiara la natura prettamente lavorativa dell'account email assegnato, escludendo dunque ogni utilizzo privato e/o personale;
- predisporre una policy aziendale sull'utilizzo degli strumenti elettronici (tra cui l'account di posta elettronica) che fornisca regole rivolte alla tutela e alla

[3] v. Niemietz c. Allemagne, 16.12.1992 (ric. n. 13710/88), spec. par. 29; Copland v. UK, 03.04.2007 (ric. n. 62617/00), spec. par. 41; Bărbulescu v. Romania [GC], 5.9.2017 (ric. n. 61496/08), spec. par. 70-73; Antović and Mirković v. Montenegro, 28.11. 2017 (ric. n. 70838/13), spec. par. 41-42)

protezione della rete aziendale, che vieti l'utilizzo di siti web estranei all'attività lavorativa (come ad esempio Social network o altre piattaforme similari), che informi circa la possibilità da parte del responsabile IT di accedere agli strumenti aziendali assegnati, anche senza il consenso del lavoratore;

- adottare una procedura di disattivazione dell'account di posta elettronica che preveda in un primo momento la predisposizione di un sistema di risposta automatica volto a rendere noto all'esterno il nuovo riferimento interno aziendale.

Tali accorgimenti risultano fondamentali anche relativamente alla fase successiva alla cessazione del rapporto di lavoro, in quanto predispongono a monte delle regole chiare di riferimento, idonee a prevenire eventuali successive problematiche di tipo pratico.

❖ **Adempimenti del datore di lavoro**

Dal punto di vista prettamente operativo, alla fine del rapporto di lavoro, il datore di lavoro dovrà immediatamente impostare un messaggio di risposta automatica all'account email dell'ex dipendente, con il quale si avverta il mittente di eventuali messaggi che l'account in questione non è più attivo e, soprattutto, non più riferito al lavoratore.

Un esempio di messaggio automatico di risposta potrebbe essere il seguente: "*Si comunica che il presente indirizzo di posta elettronica non è più attivo, poiché titolare della casella di posta elettronica aziendale sig._____ ha cessato il proprio rapporto di collaborazione con la nostra Società. A far data da _____ [30 giorni dopo la cessazione] si procederà alla disattivazione definitiva di tale indirizzo di posta elettronica. Si comunica che fino alla data sopraindicata ogni eventuale e-mail inviata al citato indirizzo di posta elettronica sarà automaticamente inoltrata al seguente indirizzo:* _____. ".

Nella fase precedente alla disattivazione definitiva dell'account di posta elettronica è fatto assoluto divieto di rispondere o scrivere e-mail con l'account del lavoratore cessato.

Successivamente, come detto sopra, il datore di lavoro deve procedere alla disattivazione vera e propria dell'account, esportando, se necessario, eventuali dati aziendali presenti nell'archivio di posta elettronica.

❖ **Diritto di accesso dell'ex dipendente**

Resta inteso, ed è bene sottolinearlo, che l'ex dipendente è in ogni caso titolare del diritto di accesso, in base al quale può chiedere formalmente al datore di lavoro di accedere al

proprio vecchio account (se ancora attivo) per recuperare eventuali suoi dati personali ivi contenuti.

Tale diritto è, per forza di cose, esercitabile sino a che l'account non venga definitivamente eliminato e/o disattivato.

L'esercizio del diritto in questione deve essere azionato mediante richiesta formale di accesso all'ex datore di lavoro che, pertanto, dovrà consentire all'interessato di recuperare i propri dati, non potendo opporvisi.

È bene chiarire che, dal suo canto, l'ex dipendente non può assolutamente bypassare tale procedura accedendo autonomamente all'account email utilizzando le credenziali di accesso in suo possesso.

Tale comportamento integra il reato di accesso abusivo a sistema informatico, disciplinato all'art. 615 ter c.p.[4].

### 2.2. Gestione dati dell'ex dipendente detenuti su supporti informatici di proprietà dell'azienda

Ipotesi che merita un approfondimento a parte, e che trova grande riscontro nella prassi, riguarda le modalità di trattamento e i relativi obblighi incombenti sul datore di lavoro, con riferimento a quei dati personali dell'ex dipendente che siano stoccati all'interno di dispositivi aziendali concessi in uso allo stesso per lo svolgimento della sua prestazione lavorativa.

Basti pensare a tutti quei dati personali (file, immagini, audio o conversazioni di programmi di messagistica istantanea), ma anche a quei contatti telefonici o indirizzi, che siano salvati sulle memorie interne di dispositivi concessi in dotazione dall'azienda al dipendente, in taluni casi con espressa previsione di uso promiscuo.

La normativa in vigore in materia di tutela della riservatezza nulla prescrive espressamente con riguardo a siffatte ipotesi.

Pertanto si ritengono applicabili le norme ed i principi generali dettati dal GDPR con riferimento all'adozione di tutte le misure adeguate a garantire la tutela del dato personale secondo il criterio dell'*accountability* cui deve attenersi il datore di lavoro.

---

[4] La Corte di cassazione, Sezione V penale Sentenza 20 settembre 2018, n. 48895 ha sancito che "Secondo la giurisprudenza di questa Corte integra il delitto previsto dall'art. 615-ter, secondo comma, n. 1, c.p. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita (Sez. un., n. 41210 del 18 maggio 2017, Savarese, Rv. 271061)".

Importanza primaria, anche in questa ipotesi, riveste l'informativa privacy che il datore di lavoro deve obbligatoriamente consegnare al dipendente.

In tale policy aziendale è pertanto opportuno prevedere anche le condizioni e le limitazioni all'utilizzo degli strumenti forniti al dipendente e **le operazioni che lo stesso dovrà porre in essere al momento della cessazione del rapporto di lavoro**.

In primo luogo dovrà espressamente essere prevista la possibilità, se consentita, di uso promiscuo dell'apparecchio (personal computer, tablet, smartphone…) ed eventualmente eventuali limitazioni all'utilizzo di particolari app o funzionalità (social network, messagistica istantanea).

Inoltre, il datore di lavoro, nella suddetta informativa, dovrà informare il dipendente della natura aziendale (e pertanto strettamente legata alla prestazione lavorativa) dello strumento fornito, avvisandolo che ogni dato personale estraneo all'attività lavorativa potrà essere suscettibile di controllo dal datore di lavoro o dal responsabile IT preposto in azienda.

Inoltre, sarebbe opportuno per il datore di lavoro dedicare attenzione anche alle operazioni imposte al dipendente al momento della restituzione degli apparecchi alla cessazione del rapporto di lavoro. Quest'ultimo dovrà, difatti consegnare gli strumenti avendo prima cura di eliminare qualsiasi dato personale ivi stoccato e non anche, si badi bene, gli altri eventuali dati aziendali presenti nello stesso. Infatti, la formattazione integrale dello strumento informatico potrebbe causare la perdita di dati aziendali di particolare valore (si pensi a contatti di eventuali clienti e fornitori), la cui cancellazione ad opera dell'ex dipendente potrebbe causare un elevato danno per l'azienda stessa, oltre che la configurazione di un reato.

Sul punto recentissima giurisprudenza della Suprema Corte ha enunciato il principio secondo cui i dati informatici (files) sono qualificabili cose mobili ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la sottrazione da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer "formattato"[5].

[5] Corte Di Cassazione, sezione penale, sentenza n. 11959 depositata il 10 aprile 2020 secondo cui "il file, pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano *l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente* grandezza dei supporti fisici in cui i files possono essere conserva*ti e elaborati. L'assunto da cui muove l'orientamento maggioritario, giurisprudenziale e della dottrina, nel ritenere che il dato informatico non possieda i caratteri della fisicità, propri della "cosa mobile" (nella nozione*

Da ultimo, breve menzione merita la questione inerente la scheda SIM concessa in uso al dipendente.

Ancora una volta è essenziale la policy privacy predisposta dal datore di lavoro in cui devono essere indicate le modalità di uso della SIM (e della relativa utenza telefonica) e gli eventuali controlli che il datore di lavoro può effettuare. Ovviamente i controlli devono in ogni caso essere effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo garantendo altresì la riservatezza dei dati personali raccolti durante la procedura di controllo.

Va tenuto presente che la SIM, analogamente agli altri strumenti informatici forniti dal datore di lavoro, è di proprietà dell'azienda, ragion per cui, alla cessazione del rapporto di lavoro, il lavoratore è tenuto alla riconsegna della stessa. A nulla rileva l'utilizzo, seppur promiscuo (e quindi anche per fini personali), del numero telefonico, in quanto anche in tal caso non sorge alcun diritto in capo al lavoratore.

### 2.3. Utilizzo nome e simboli aziendali sui profili social del dipendente

Tale ipotesi, alquanto frequente nella prassi, riguarda quella spiacevole situazione in cui l'ex dipendente, pur non essendo più in forze presso l'azienda, continui comunque ad utilizzare il nome, il logo, o altri segni distintivi di quest'ultimi sui propri account social

---

penalistica di quel termine) non è, dunque, condivisibile; al contrario, una più accorta analisi della nozione scientifica del dato informatico conduce a conclusioni del tutto diverse*…Infine, dal punto di vista dell'effettiva realizzazione, attraverso le condotte appropriative di dati i*nformatici, *dell'effetto di definitiva sottrazione del bene patrimoniale al titolare del diritto di godimento ed* utilizzo del bene stesso, le ipotesi di appropriazione indebita possono differenziarsi dalla *generalità delle ipotesi di "furto di informazioni", in cui si è frequentemente rilevato che il pericolo* della perdita definitiva da parte del titolare dei dati informatici è escluso in quanto attraverso la *sottrazione l'agente si procura sostanzialmente un mezzo per acquisire la conoscenza delle* informazioni contenute nel dato informatico, che resta comunque nella disponibilità materiale e giuridica del titolare (valutazione che aveva indotto il legislatore, nel corso del procedimento di discussione ed approvazione della l. 23 dicembre 1993, n. 547 – recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica – , ad escludere che alle condotte di sottrazione di dati, programmi e informazioni *fosse applicabile l'art. 624 cod. pen. «pur nell'ampio concetto di «cosa mobile» da esso previsto»,* in quanto «la sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una «presa di conoscenza» di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la violazione dei segreti»: così la relazione al relativo disegno di legge n. 2773). Infatti, *ove l'appropriazione venga realizzata mediante condotte che mirano non solo all'interversione* del possesso legittimamente acquisito dei dati informatici, in virtù di accordi negoziali e convenzioni che legittimano la disponibilità temporanea di quei dati, con obbligo della successiva restituzione, ma altresì a sottrarre definitivamente i dati informatici mediante la loro cancellazione, previamente duplicati e acquisiti autonomamente nella disponibilità del soggetto agente, si realizza il fatto tipico della materiale sottrazione del bene, che entra a far parte in via esclusiva del patrimonio del responsabile della condotta illecita."

personali (basti pensare all'ipotesi del lavoratore che dichiari sulla home page del proprio account LinkedIn di lavorare ancora presso la vecchia azienda).

Come noto, la regolamentazione contenuta nel GDPR non è applicabile alle persone giuridiche ma alle sole persone fisiche.

Pertanto tale fattispecie, più che nell'alveo della normativa in materia di tutela del dato personale, andrebbe ascritta nelle materia della tutela del nome e dell'immagine della persona giuridica.

Esistono però "zone di grigio" che non vanno tralasciate, come ad esempio il caso in cui la ragione sociale della persona giuridica contenga il nome e il cognome del legale rappresentante o di altra persona fisica.

In questo caso, più che la tutela del nome dell'azienda, oggetto di tutela è il nome della persona fisica, che costituisce dato personale.

Il soggetto interessato potrà pertanto pretendere legittimamente dall'ex dipendente la rimozione dell'informazione contenente i propri dati personali, in applicazione della normativa preposta in materia di privacy.

### 3. Cartella sanitaria e di rischio del lavoratore

Ai sensi dell'art. *18 del D.Lgs. 81/08* il datore di lavoro ha l'obbligo di nominare il medico competente per l'effettuazione della sorveglianza sanitaria nel caso di svolgimento da parte dei lavoratori di attività potenzialmente rischiose per la salute.

Uno dei principali compiti del medico competente è quello di istituzione, aggiornamento e custodia, *sotto la propria responsabilità*, di una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria.

Il medico competente, ai sensi dell'art. 32 GDPR deve adottare tutte le misure tecniche e organizzative adeguate a garantire un livello idoneo di sicurezza per fronteggiare eventuali rischi in materia di gestione dei dati sensibili dei dipendenti.

Relativamente alla gestione della cartella sanitaria, i ruoli del datore di lavoro e del medico competente differiscono sostanzialmente. L'Autorità Garante per la Protezione dei Dati Personali, nella Relazione annuale 2019 ha ad esempio stabilito che il medico competente è l'unico legittimato a trattare in piena autonomia i dati personali di natura

sanitaria del dipendente, cosa non consentita al datore di lavoro che, ad esempio, non può accedere ai dati relativi all'anamnesi familiare del dipendente[6].

Inoltre, sempre con riferimento alla ripartizione delle competenze del medico competente e del datore di lavoro, il Garante della Privacy ha chiarito che il medico competente tratta dati personali di natura sanitaria indispensabili ai fini dell'applicazione della normativa in materia di igiene e di sicurezza del lavoro in qualità di titolare del trattamento, con particolare riguardo alla tenuta delle cartelle sanitarie e di rischio da parte del medico competente.

Recentemente, con Interpello n. 4/2019 il Ministero del Lavoro, prendendo spunto da un quesito formulato dalla Federazione Nazionale dei Medici Chirurghi e degli Odontoiatri, riguardante la possibilità di inserire in un database aziendale tutti i dati sanitari del lavoratore e non solo il giudizio di idoneità, ha sottolineato la necessità di prestare la massima attenzione alla custodia dei dati sensibili contenuti nella cartella sanitaria del lavoratore.

I dati personali del lavoratore, contenuti nella cartella sanitaria e definiti "particolari" ai sensi dell'art. 9 del GDPR possono essere trattati in casi particolari ossia quando "*il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali*" (art. 9, co. 2,

---

[6] Precisamente, la relazione annuale 2019 del Garante per la Privacy riporta testualmente "*l'Ufficio, richiamando i precedenti dell'Autorità, ha precisato che la disciplina di* settore (d.lgs. 9 aprile 2008, n. 81) individua la funzione del medico competente come autonoma rispetto a quella che, pure in tale ambito, deve essere svolta dal datore di lavoro, assegnando specifici e distinti *obblighi in capo all'una e all'altra figura, così delineando l'ambito del rispettivo trattamento* consentito. In particolare, nello svolgimento dei compiti che la legge gli attribuisce in via esclusiva (attività di sorveglianza sanitaria e tenuta delle cartelle sanitarie e di rischio dei singoli lavoratori), *il professionista è l'unico legittimato ex lege a trattare in piena autonomia e competenza tecnica i* dati personali di natura sanitaria indispensabili per tale finalità, non potendo essere in alcun modo trattate dal datore di lavoro informazioni *relative, ad esempio, alla diagnosi o all'anamnesi* familiare del lavoratore, se non con riferimento al solo giudizio di idoneità alla mansione specifica ed alle eventuali prescrizioni che il professionista fissa come condizioni di lavoro. Anche sotto il profilo sanzionatorio, il quadro normativo nazionale distingue chiaramente le responsabilità che ricadono sul datore di lavoro da quelle che invece sono direttamente imputabili al medico competente, sia quando opera in qualità di libero professionista o per conto di strutture convenzionate, sia quando opera in qualità di dipendente del datore di lavoro. Sulla base di tali valutazioni, il Garante ha tradizionalmente considerato il medico competente un autonomo titolare e, nonostante gli accertamenti volti a ve*rificare l'idoneità alla mansione specifica del dipendente* siano obbligatori per legge e svolti a spese e a cura del datore di lavoro (artt. 39, comma 5 e 41, comma 4, d.lgs. n. 81/2008), essi devono essere effettuati esclusivamente tramite il professionis*ta. Egli è, infatti, l'unico soggetto legittimato a trattare i dati sanitari dei lavoratori per* le finalità indicate dalla disciplina di settore, come chiarito dal Garante in un provvedimento nel quale è stato precisato, tra gli altri profili, che il medico competente tratta dati personali di natura *sanitaria indispensabili ai fini dell'applicazione della normativa in materia di igiene e di sicurezza* del lavoro in qualità di titolare del trattamento".

lett. h) Reg. UE 2016/679), e in ogni caso purché siano trattati "*... da o sotto la responsabilità di un professionista soggetto al segreto professionale*" (art. 9, co. 3, Reg. UE 2016/679).

A tal proposito, la legge prevede che il Datore di Lavoro, abbia diritto a conoscere il solo giudizio di idoneità, inidoneità o idoneità con prescrizioni o limitazioni alla mansione specifica ricoperta dal Lavoratore (o dati inerenti le generalità del lavoratore; i fattori di rischio lavorativi a cui lo stesso è esposto; prescrizioni o limitazioni).

il giudizio di idoneità, inidoneità o idoneità con prescrizioni o limitazioni, e non anche la diagnosi svolta dal medico. Quanto al Medico Competente, questo "*... istituisce, aggiorna e custodisce, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria. Tale cartella è conservata con salvaguardia del segreto professionale e, salvo il tempo strettamente necessario per l'esecuzione della sorveglianza sanitaria e la trascrizione dei relativi risultati, presso il luogo di custodia concordato al momento della nomina del medico competente*" (art. 25, co. 1, lett. c), D. Lgs. 81/2008).

Su tali premesse, il Ministero del Lavoro ha ritenuto possibile la memorizzazione su supporto informatico aziendale della cartella sanitaria del lavoratore, purché le informazioni in essa contenute siano accessibili unicamente al Medico Competente, soggetto professionalmente a un obbligo di segretezza[7].

---

[7] Articolo 25 decreto legislativo 9 aprile 2008, n. 81 "Il medico competente: a) collabora con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, *all'attività* di formazione e informazione nei confronti dei lavoratori, per la parte di competenza, e alla organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro. Collabora inoltre alla attuazione e valorizzazione di programmi volontari di "promozione della salute", secondo i principi della responsabilità sociale; b) programma ed effettua la sorveglianza sanitaria di cui all'articolo 41 attraverso protocolli sanitari definiti in funzione dei rischi specifici e tenendo in considerazione gli indirizzi scientifici più avanzati; (c) istituisce, aggiorna e custodisce, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria; tale cartella è conservata con salvaguardia del segreto professionale e, salvo il tempo strettamente necessario per l'esecuzione della sorveglianza sanitaria e la trascrizione dei relativi risultati, presso il luogo di custodia concordato al momento della nomina del medico competente;) d) consegna al datore di lavoro, alla cessazione dell'incarico, la documentazione sanitaria in suo possesso, nel rispetto delle disposizioni di cui al decreto legislativo del 30 giugno 2003, n. 196, e con salvaguardia del segreto professionale; (e) consegna al lavoratore, alla cessazione del rapporto di lavoro, copia della cartella sanitaria e di rischio, e gli fornisce le informazioni necessarie relative alla conservazione della medesima; l'originale della cartella sanitaria e di rischio va conservata, nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, da parte del datore di lavoro, per almeno dieci anni, salvo il diverso termine previsto da altre disposizioni del presente decreto;)".

Stanti le prescrizioni previste in costanza di rapporto, è interessante esaminare cosa accade quando il rapporto di lavoro cessa.

Alla cessazione del rapporto di lavoro il Medico Competente ha l'obbligo di consegnare copia della cartella sanitaria e di rischio al lavoratore e di consegnare all'azienda l'originale sigillata. La cartella sanitaria consegnata sigillata all'Azienda deve essere conservata per un periodo di tempo di 10 anni, garantendo l'adozione di tutte le misure di sicurezza idonee a tutelare i dati personali in essa contenuti.

Fa eccezione il caso dell'esposizione a cancerogeni che comporta la spedizione della cartella all'INAIL e la relativa conservazione per almeno 40 anni, oltre all'informazione del lavoratore sulla necessità di sottoporsi ad una sorveglianza sanitaria mirata anche dopo la cessazione dell'esposizione.

**4. In conclusione**

Da quanto sopra detto, seppur per brevi cenni, emerge l'estrema importanza che, soprattutto negli ultimi anni, riveste il complesso normativo in tema di tutela dei dati personali anche nel rapporto di lavoro.

Tirando le fila delle considerazioni sopra riportate, punto fermo imprescindibile resta la necessità di predisporre una accurata e quanto più dettagliata possibile policy privacy contenente accurata informativa per il dipendente relativamente all'uso degli strumenti informatici forniti in uso dall'azienda, alla gestione e conservazione dei suoi dati personali. È per tale motivo che la redazione della policy privacy, considerata come detto la notevole importanza nonché la complessità delle questioni e delle implicazioni giuridiche, viene spesso affidata dalle aziende a professionisti del settore in grado di anticipare il sorgere di problematiche in costanza di rapporto, finanche alla cessazione dello stesso.

Inoltre, emerge la necessità di responsabilizzare, anche per il tramite della suddetta informativa, il dipendente ad operare diligentemente, rispettando scrupolosamente le prescrizioni di legge e quelle impartite dal datore di lavoro, gestendo consapevolmente i propri dati personali privati ed evitando di stoccare tali dati in apparecchi considerati veri e propri "mezzi per rendere la prestazione lavorativa" e come tali esulanti dalla sfera privata del soggetto.

**FONTI NORMATIVE E GIURISPRUDENZIALI**

- Regolamento UE n. 2016/679 all'art. 88
- Linee Guida emanate dall'Autorità Garante della privacy del 23 novembre 2006
- all'art. 4 dello Statuto dei lavoratori (L. 300/1970)
- l'INL circolare n. 2 del 07/11/2016
- Provvedimento del 4 dicembre 2019, Garante per la Protezione Dei Dati Personali
- Provvedimento n. 551 del 27 novembre 2014
- "Linee guida del Garante per posta elettronica e Internet" del 1 marzo 2007
- D. Lgs. 81/2008
- Interpello n. 4/2019 Ministero del Lavoro
- art. 615 ter c.p.


## CONTATTI

Telefono: +39 011 511 1005
Fax: +39 011 515 0103
Email: info@mbolaw.it

## SEDI

Via Giannone, 1
10121 Torino

Corso Lancieri d'Aosta n. 15/C
11100 Aosta



MBO LAW REVIEW