

Giurisprudenza

## **Privacy ed e-mail aziendale, una guida per capire**

**Si scontrano da una lato il principio di segretezza della corrispondenza e dall'altro l'uso di uno strumento aziendale. Il confine è labile, come testimoniato dai pronunciamenti del Garante e dalle sentenze dei Tribunali.**

Mario Leone Piccinni

03 Dicembre 2009

Sull'uso e la privacy dell'e-mail aziendale, si dibatte da molto tempo in giurisprudenza.

Partiamo da alcuni fatti: secondo il Garante della Privacy, è compito del datore di lavoro stilare idonee misure di sicurezza dei sistemi informativi, soprattutto al fine di prevenire utilizzi illeciti che potrebbero essere fonte di responsabilità di rilievo civile o penale.

Spetta quindi allo stesso datore garantire l'efficienza ed il corretto utilizzo del Web e della posta elettronica da parte dei dipendenti, definendone preliminarmente modalità permesse di utilizzo (policy) nel rispetto della disciplina in tema di diritti e relazioni sindacali.

### **Controllo a distanza dei lavoratori**

E' comunque fatto divieto ai datori di lavoro privati e pubblici, in virtù di quanto previsto dall'articolo 154 del Codice, effettuare trattamenti di dati personali mediante sistemi hardware e software che operano il controllo a distanza di lavoratori, attraverso la lettura e la registrazione sistematica dei messaggi di posta elettronica, l'eventuale memorizzazione metodica delle pagine internet visitate dal dipendente, la registrazione dei caratteri inseriti tramite la tastiera (sistema keylogger), l'analisi occulta di PC portatili affidati in uso.

### **Disciplinare interno**

In tale ottica, il Garante suggerisce ai datori di lavoro la stesura di un disciplinare interno (policy interna) dettagliato e di facile comprensione, eventualmente da sottoporre ad aggiornamenti periodici, il quale andrebbe pubblicizzato adeguatamente presso i singoli dipendenti mediante rete intranet o semplici affissioni negli ambienti di lavoro.

In definitiva, in relazione alle e-mail aziendali, il Codice della Privacy prescrive come necessaria una trasparenza assoluta nei rapporti tra dipendente e datore di lavoro, come previsto del resto dall'articolo 4 dello Statuto dei lavoratori in materia di "uso di attrezzature munite di videotermini", il quale classifica come illegittimi eventuali controlli informatici "all'insaputa dei lavoratori".

### **Quando si può controllare l'e-mail del dipendente**

D'altra parte - e qui nasce il secondo aspetto della querelle posta elettronica-privacy - il Garante ha specificato, che "*...in caso di eventuali assenze non programmate (ad esempio, per malattia), qualora il lavoratore non possa attivare la procedura...di invio automatico di e-mail... 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 esempio, l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati...*".

### **Le sentenze dei Tribunali**

Secondo una sentenza del 2002 del Tribunale di Milano, il datore di lavoro ha facoltà di accedere alla casella di posta elettronica in qualunque momento, "*...tuttavia, personalità dell'indirizzo non significa necessariamente privatezza del medesimo, dal momento che 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...*".

Allo stesso modo, una sentenza del Tribunale del capoluogo lombardo ha altresì escluso che la posta elettronica aziendale possa essere assimilata a quella tradizionale e su di essa possa vigere il principio di

segretezza di cui all'art. 616 del Codice Penale, "...nè, si può ritenere che l'assimilazione della posta elettronica alla posta tradizionale, con conseguenziale affermazione generalizzata del principio di segretezza, si verifichi nel momento in cui il lavoratore utilizzi lo strumento per fini privati -ossia extra lavorativi-, atteso che giammai un uso illecito -o, al massimo, semplicemente tollerato, ma non certo favorito- di uno strumento di lavoro può far attribuire, a chi questo illecito commette, diritti di sorta..."

**In sostanza, la strutturazione dell'indirizzo di posta elettronica con il nome del lavoratore non determina il fatto che la casella diventi "proprietà privata" del dipendente assegnatario. E ci sono diverse sentenze al riguardo, sempre che il lavoratore abbia regolare rapporto di lavoro con l'azienda stessa.**

**.....si fa divieto dell'uso del nome e cognome di una persona fisica, senza il suo assenso, per scopi privati....**

### **Responsabilità e risarcibilità del danno.**

(Avv. [Monica Gobbato](#) - Dott.ssa Marilù Barella - Dott. Piergiorgio Mancone)

In caso di lesione della riservatezza e dell'identità personale, il d.lgs 196/2003 prevede una forma di tutela successiva, rimessa al risarcimento del danno. I profili di responsabilità civili per fatto illecito introdotti dalla legge 675/1996 sono stati confermati *in toto* dal Testo Unico sulla privacy. **Si tratta, essenzialmente, di responsabilità connesse al trattamento illecito di dati personali,** alla falsità di dichiarazioni e notificazioni fatte al Garante, all'inosservanza delle misure necessarie alla sicurezza dei dati e al mancato rispetto delle disposizioni del Garante: ipotesi penalmente sanzionate dagli artt. 167, 168, 169, 170 del Testo Unico, ma anche a tutti i casi in cui per ragioni diverse l'interessato dal trattamento si trovi a subire un danno da questo derivante.

L'uso illecito delle informazioni e la diffusione di informazioni inesatte o incomplete, integrano la fattispecie del c.d. *danno da informazione*. Sostanzialmente sono due le ipotesi in cui tale danno è configurabile: la prima implica la violazione del c.d. principio di finalità e presuppone un uso dei dati differente da quello per il quale l'interessato ha prestato il proprio consenso<sup>1</sup>. La seconda ipotesi comporta la divulgazione di informazioni false o parziali. La falsa informazione, infatti, può danneggiare l'interessato sia in quanto diretta a terzi, poiché lesiva di quella che è la percezione sociale dell'identità personale, sia in quanto diretta allo stesso soggetto cui dati si riferiscono; oppure può danneggiare soggetti diversi dall'interessato in quanto destinatari o semplici fruitori di tali informazioni<sup>2</sup>.

È necessario, innanzitutto, osservare che in risposta al danno da informazione il Testo Unico stabilisce, all'art. 15, che "*chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.*". In base a questa norma il titolare sarà tenuto a risarcire i danni a meno che non provi di aver adottato le misure "idonee" (non le "minime") per evitare il danno. La novità è nel secondo comma, secondo il quale il danno non patrimoniale è risarcibile anche in caso di violazione delle norme attinenti alle modalità del trattamento comprendenti anche le regole sulla conservazione.

Come noto, l'art. 2050 c.c. stabilisce che "chiunque cagioni danno ad altri nello svolgimento di un'attività pericolosa [...] è tenuto al risarcimento del danno, se non prova di aver adottato tutte le misure idonee ad evitare il danno"<sup>3</sup>.

Una ulteriore importante conseguenza di tale previsione normativa è, quindi, l'equiparazione dell'esercizio dell'attività di trattamento dei dati personali all'esercizio di attività pericolose per le quali l'art. 2050 c.c. prevede un alleggerimento significativo dell'onere della prova a carico del danneggiato rispetto alla regola generale di cui all'art. 2043 c.c.: onere del danneggiato sarà, infatti, solo quello di provare il rapporto di causalità tra fatto e danno (e non anche il dolo o la colpa dell'autore del fatto illecito), mentre incomberà al danneggiante l'onere, ben più impegnativo, di

provare di aver posto in essere tutte le misure idonee per evitare l'evento dannoso non essendo sufficiente dimostrare di non aver violato norme di legge o di prudenza o di perizia.

La presunzione di colpa può operare anche quando sia l'autorità giudiziaria ad accertare un nesso causale tra il trattamento e l'evento dannoso.

Mentre incombe al danneggiato dimostrare la sussistenza del nesso di causalità al danneggiante incombe l'onere di provare l'adozione di tutte le misure idonee ad evitare il danno.

Per misure idonee ad evitare il danno devono intendersi tutti gli accorgimenti previsti da norme legislative o regolamentari che disciplinano la specifica attività interessata dalla controversia: nel caso specifico non solo le norme del Testo Unico, il disciplinare tecnico in materia di misure minime di sicurezza (allegato B), ma anche le prescrizioni impartite dal Garante o i codici di deontologia e di buona condotta.

Il fatto del danneggiato o del terzo può produrre effetti liberatori del danneggiante solo nel caso in cui il danneggiante provi l'interruzione del nesso causale tra l'attività pericolosa e l'evento e non semplicemente il concorso del fatto del danneggiato o del terzo nella produzione del danno, che si sia inserito in una situazione di pericolo, che ne abbia reso possibile l'insorgenza a causa dell'inidoneità delle misure preventive adottate.

Il richiamo all'art. 2050 c.c. non rende necessario appurare nel caso concreto se il trattamento sia pericoloso per sua natura o per la natura dei mezzi adoperati, avendo il semplice effetto di chiarire la responsabilità del soggetto operante il trattamento in difetto della prova liberatoria anzidetta.

È il legislatore ad aver valutato preventivamente la pericolosità dell'attività del trattamento dei dati personali: la rilevanza sociale di tale attività ha condizionato la scelta normativa.

Il rinvio all'art.2050 denota un'inversione di tendenza rispetto all'evoluzione della responsabilità civile nel contesto economico in generale. Vi è, infatti, un accrescimento della responsabilità dell'imprenditore, in quanto soggetto dotato di maggiori informazioni e, quindi, maggiormente in grado di evitare il danno. Del resto, il principio dell'oggettivazione del rischio di impresa è sostenuto dall'analisi economica del diritto in quanto principio giuridico atto a scartare dal mercato i soggetti inefficienti, perché costretti a pagare alti risarcimenti per i danni arrecati, e quindi rendere il mercato concorrenziale.

Dunque, il soggetto danneggiato, in forza del richiamo espresso dell'art. 15, comma 1°, del Testo Unico all'art. 2050 c.c., dovrà semplicemente dimostrare il fatto storico, l'evento dannoso mentre al danneggiante spetterà la prova liberatoria, oltremodo gravosa (non a caso spesso definita *probatio diabolica*), consistente nel dimostrare di aver adottato ogni possibile cautela per evitare il danno, non essendo sufficiente dimostrare di non aver violato norme di legge o di prudenza o di perizia<sup>4</sup>.

La lesione di un bene fondamentale della persona, quale la riservatezza, tuttavia, di per sé identifica un danno non patrimoniale costituito dal turbamento psichico che il soggetto ha risentito per effetto della violazione. Secondo l'art. 2059 c.c. il danno non patrimoniale è risarcibile solo nei casi espressamente previsti dalla legge; l'unica norma che espressamente menziona la risarcibilità del danno non patrimoniale è l'art. 185, comma 2°, c.p., che la contempla nei casi di danni provocati da reati.

Per quanto attiene la normativa sulla privacy, sotto il profilo dei rimedi risarcitori, viene, in considerazione l'art. 15 del Testo Unico, il quale al comma 2°, sancisce espressamente la risarcibilità del danno non patrimoniale anche per i casi di violazione dell'art. 11, che, come più volte rilevato, si riferisce alle modalità di raccolta e di trattamento e ai requisiti dei dati personali.

Da ciò si può desumere che il richiamo dell'art. 15, comma 2°, nei confronti dell'art. 11, non è destinato a restringere l'area della risarcibilità del danno non patrimoniale, posto che la lettera della norma, usando l'espressione "anche", sembra perseguire un fine diametralmente opposto, e cioè quello di estendere la sfera di risarcibilità del danno non patrimoniale, ampliandola "anche" (e non limitandola "solo") alle ipotesi di violazione delle disposizioni di cui all'art. 11<sup>5</sup>.

Inoltre, la risarcibilità del danno non patrimoniale per ogni ipotesi in cui si possa ravvisare una responsabilità da illecito trattamento di dati rappresenta una scelta del legislatore motivata da una ben specifica considerazione, e cioè quella che, nella prassi, a causa della particolare natura dei diritti che generalmente vengono lesi da un'illecita attività di trattamento dei dati, i danni risultano essere, nella larghissima maggioranza dei casi, danni di natura non patrimoniale o comunque danni molto difficili da provare nella loro consistenza patrimoniale. La soluzione adottata dal legislatore consente, dunque, un'effettiva operatività della sanzione a carico del responsabile dell'illecito ed una conseguente maggiore efficacia del provvedimento legislativo che disciplina il trattamento dei dati.

Infatti, la norma appena richiamata consente di ricollegare un risarcimento a tutti i casi di trattamento illecito, anziché ai soli casi in cui il trattamento dia luogo ad un'ipotesi di reato, necessariamente contraddistinta dall'ipotesi del dolo specifico<sup>6</sup>.

Come la vecchia legge 675/1996, anche il nuovo Testo Unico privilegia l'adozione di uno strumento risarcitorio non inteso nel senso più tradizionale, cioè con funzione essenzialmente riparatoria, ma uno strumento risarcitorio che, proprio per la sua potenziale idoneità a trovare larga applicazione, svolge, principalmente, funzione preventiva, pur non perdendo la propria caratteristica funzione, qualora il singolo danneggiato si avvalga, in concreto, della tutela risarcitoria<sup>7</sup>.

Non può, infatti, non considerarsi, che al risarcimento del danno non patrimoniale va riconosciuta oltre alla funzione propriamente compensativa, anche una funzione sanzionatoria.

In effetti, se per risarcimento si intende l'eliminazione del danno attraverso l'equivalente pecuniario, è certo che tale funzione non può essere assegnata al denaro rispetto al danno non patrimoniale provocato dalla lesione della sfera di riserbo. Nel caso, il danaro ha piuttosto una funzione soddisfattoria della vittima, e ciò sotto un duplice profilo:

1. quello coincidente con la possibilità che con esso è data di conseguire soddisfazioni materiali che valgano a lenire le sofferenze subite;
2. quello della soddisfazione che risente perché vede colpito chi le ha arrecato ingiustamente dolore<sup>8</sup>.

Ponendoci sotto la prospettiva del danno risarcibile, va subito chiarito che questo non è rappresentato dal trattamento dei dati in sé, ma unicamente delle conseguenze dannose che si siano realizzate per effetto di un illecito trattamento dei dati.

Come accennato sopra, spesso la natura del danno conseguente ad una violazione dei diritti della personalità, ed in particolare del diritto alla riservatezza della vita privata è caratterizzata dalla non patrimonialità; similmente, in ipotesi di illecito trattamento dei dati personali, il danno subito dall'interessato assumerà con ogni probabilità i caratteri del danno non patrimoniale.

Ciò tuttavia, non esclude a priori che possano generarsi danni aventi carattere della patrimonialità.

La lesione della riservatezza può, infatti, cagionare alla persona pregiudizi economicamente valutabili. Si tratta di quei danni che la Corte Costituzionale, indica come danni-conseguenza.

Innanzitutto, un primo tipo di pregiudizio economicamente valutabile può essere identificato:

- nella difficoltà di proseguire la propria attività lavorativa in conseguenza del discredito prodotto
- o nel pregiudizio alla propria aspettativa di lavoro<sup>9</sup>.

Altro tipo di danno patrimoniale può essere rappresentato dal danno alla vita di relazione<sup>10</sup>.

Tale tesi è stata sostenuta anche dalla giurisprudenza, orientata a considerare danno patrimoniale, e quindi risarcibile ai sensi dell'art. 2043 c.c., il danno che si estrinseca in una diminuzione o difficoltà nella vita di relazione.

Nel suo significato specifico il danno alla vita di relazione è distinguibile dal danno morale, poichè il primo può essere identificato pur in assenza di un danno morale<sup>11</sup>.

Per quanto attiene, invece, al tema del risarcimento del danno non patrimoniale, è opportuno evidenziare che attorno alla nozione di danno non patrimoniale sono emerse diverse opinioni. In un primo momento si era fatta largo una nozione più restrittiva che faceva coincidere il danno non patrimoniale con il solo danno morale subiettivo<sup>12</sup>. Parte della dottrina non ha, però, accolto positivamente questa impostazione sostenendo che il danno morale non esaurirebbe la categoria del danno non patrimoniale, potendo rientrare in quest'ultima anche altre diverse fattispecie di danno non aventi il carattere della patrimonialità.

D'altro canto, non poche ricostruzioni dottrinali e giurisprudenziali, hanno tentato di allargare le "maglie" entro le quali l'art. 2059 costringe l'interprete, infatti, il risarcimento del danno non patrimoniale limitato ai "soli casi determinati dalla legge", è stato fin dall'inizio avvertito come una "gabbia" ingiustificata, ancor di più se si considera che "i casi determinati" si riducono, come noto, in concreto, all'ipotesi in cui il danno derivi da reato (art. 185 c.p.) ed a quelle, di cui agli artt. 89, comma 2° c.p.c. e 598 c.p. che contemplano una fattispecie riparatoria autonoma rispetto a quella del reato<sup>13</sup>.

Come avviene per il danno morale, anche nel caso dell'evento dannoso conseguente all'illecito trattamento di dati personali si ripropongono le note questioni dell'onere della prova e dell'operazione di valutazione e liquidazione del danno da parte del giudice, questioni che possono essere risolte sulla scorta delle soluzioni offerte dalla dottrina e dalla giurisprudenza in materia di danno morale.

Quanto all'onere della prova, giova ricordare che la dottrina ha da tempo evidenziato che quando la pretesa risarcitoria vede quale legittimato attivo la stessa vittima dell'illecito la prova del danno morale può considerarsi *in re ipsa*, quindi nel caso di specie, nel trattamento di dati personali contrassegnato da illiceità<sup>14</sup>.

In tema di quantificazione del danno non può che richiamarsi un principio ormai pacifico, ossia che data l'impossibilità di ancorare la valutazione del danno non patrimoniale a criteri oggettivi, l'attività di liquidazione compiuta dal giudice non potrà che avvenire secondo un criterio equitativo.

Il danno non patrimoniale, infatti, non è suscettibile di risarcimento per equivalente (come avviene, invece, per il danno patrimoniale, che può essere risarcito, anche, in forma specifica), e, di conseguenza, la sua liquidazione è affidata all'apprezzamento discrezionale ed equitativo del giudice di merito, il quale deve tener conto: delle sofferenze patite dall'offeso, della gravità dell'illecito, e di tutti gli elementi peculiari del caso concreto. Il giudice, quindi, è chiamato a pronunciarsi sul risarcimento, indicando un ristoro pecuniario che risulti socialmente adeguato alla gravità della lesione. L'adeguatezza del ristoro, infine, deve essere valutata oggettivamente, a prescindere dalla soddisfazione morale che il danneggiato possa provare personalmente, potendosi trattare, anche, di persona incapace di intendere e di volere o di persona giuridica.

Sembra infine, opportuno segnalare che una parte della dottrina ha sostenuto che la lesione conseguente all'illecito trattamento di dati personali potrebbe dare luogo ad un danno esistenziale, "categoria di danno che appare oscillare sull'incerto confine del danno morale da un lato e della lesione alla salute psichica della vittima del fatto illecito dell'altro lato"<sup>15</sup>.

Tale figura di danno, secondo la dottrina che l'ha avvalorata, "sarebbe idonea ad esaurire l'intera area dei pregiudizi di carattere non patrimoniale che risultino diversi dal dolore o dal patema d'animo. E proprio in relazione al diritto alla riservatezza la categoria del danno esistenziale parrebbe poter svolgere una specifica funzione, dando ristoro a quei danni identificabili nella necessità, per la vittima del fatto dannoso, di adottare nella vita di ogni giorno comportamenti diversi dal passato. Non poter, ad esempio, più uscire di casa, nel caso di violazione della privacy, senza essere importunato dai curiosi che di quella vicenda siano stati messi al corrente"<sup>16</sup>.

Appurata quindi la configurabilità del danno derivante da illecito trattamento dei dati personali è necessario individuare i soggetti in capo a cui pende tale responsabilità e dunque l'obbligo di risarcimento. Come visto, al riguardo il codice parla, al già più volte citato art. 15, indiscriminatamente di "chiunque".

Tuttavia, il d.lgs 196/2003 individua senza ombra di dubbio i soggetti cui è ascrivibile il nesso di causalità tra evento dannoso ed imputabilità dello stesso: tali sono il Titolare, cioè "colui che cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza" (art. 4, com. 1, lett. f)) ed il Responsabile ossia, colui che è "preposto dal titolare al trattamento dei dati personali" (art. 4, com.1, lett.g)) "individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" (art. 29, com. 2).

È da ritenersi che entrambi siano, potenzialmente, legittimati passivi, dunque, obbligati in solido ai sensi dell'art. 2055 c.c. nonché sulla base della lettera dell'art. 29 comma 5 in virtù del quale "il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare, il quale anche in base a verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni".

---

<sup>1</sup> Non ultima la pronuncia del Giudice di pace di Napoli in tema di spamming che, sul filone di una giurisprudenza oramai consolidata in materia, ha ribadito come l'invio di posta elettronica indesiderata costituisce fatto illecito produttivo di responsabilità civile proprio per la scorrettezza e l'illiceità del trattamento dei dati personali del titolare dell'indirizzo bersaglio e per l'invasione della sfera di riservatezza di quest'ultimo. In *Foro it.*, 2004, I, p. 2098.

<sup>2</sup> A. Lucarino, *Responsabilità e risarcimento dei danni in seguito al trattamento dei dati personali*, in [www.privacy.it/lucarino02.html](http://www.privacy.it/lucarino02.html)

<sup>3</sup> Secondo un primo indirizzo interpretativo il rinvio all'art.2050 c.c. dimostrerebbe l'intenzione del legislatore a qualificare il trattamento dei dati personali quale attività pericolosa (in tal senso S. Sica, *Commento all'art. 29, comma 9*, in AA.VV., *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, p. 284 ss.). Secondo altro orientamento, invece, il rinvio in oggetto, serve a riflettere il particolare regime probatorio previsto in materia di attività pericolose, ritenendo quantomeno dubbia una possibile equiparazione tra l'attività di trattamento di dati personali e l'attività di produttore di polveri da sparo, di produttore di bombole di gas liquido, o di un imprenditore chimico o farmaceutico (in tal senso M. Franzoni, *Dati personali e responsabilità civile*, in *RCP*, 1998, p. 902).

Tuttavia, una qualsivoglia soluzione dell'ipotesi in esame non può prescindere dal chiarire il concetto stesso di attività pericolosa.

La giurisprudenza del Supremo Collegio ha affermato che il giudizio di pericolosità non deve essere espresso sulla base dell'evento dannoso effettivamente verificatosi, ma secondo una prognosi postuma che il giudice deve compiere sia sulla base di nozioni desunte dalla comune esperienza, sia tenuto conto delle circostanze di fatto che si presentavano al momento dell'esercizio dell'attività, ed erano conoscibili dall'uomo medio, o comunque dovevano essere conosciute dall'agente in considerazione del tipo di attività esercitata. Inoltre, la Suprema Corte ha evidenziato la necessità di tenere distinta la nozione di attività pericolosa prevista dall'art. 2050 c.c. da quella di condotta pericolosa, essendo necessario perché si verifichi la prima che l'attività presenti una notevole potenzialità di danno a terzi, mentre non rileva se un'attività normalmente innocua diventi pericolosa per la condotta di chi la esercita: quest'ultimo caso, infatti, comporta solo la responsabilità secondo la regola generale dell'art. 2043 c.c. Cass., 30 agosto 1995, n. 9025, in *Giur. it.*, 1996, I, 1, p. 446.

4 Si tratta di una prova tutt'altro che semplice da fornire poiché, come spesso evidenziato in dottrina, se le misure adottate fossero state idonee e sufficienti, per definizione il danno non si sarebbe verificato.

5 In tal senso E. Lucchini Guastalla, *Trattamento dei dati personali e danno alla riservatezza*, in *Resp. civ. e prev.*, 2003, p. 650.

6 V. Roppo, *La responsabilità civile per il trattamento di dati personali*, in *Danno e resp.*, 1997, p. 664.

7 In tal senso, E. Lucchini Guastalla, *op. cit.*, p. 651, V. Colonna, *Il danno da lesione della privacy*, in *Danno e resp.*, 1998, p. 27, A. Di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in AA. VV. *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 237.

8 A. Cautadella, *Riservatezza (diritto alla)*, in *Enciclopedia Treccani*, 1991, p. 6.

9 L'ipotesi si presta a ricomprendere tutti i casi in cui gli errati e falsi motivi ovvero le modalità di licenziamento siano tali, anche in relazione alla natura del rapporto, da offendere la reputazione professionale del dipendente e da rendergli apprezzabilmente difficoltoso il reinserimento in un nuovo rapporto di lavoro. C. M. Bianca, *Sull'inadempimento delle obbligazioni*, in *Commentario del cod. civ.* A. Scajola e G. Branca (a cura di F. Galgano), II ed., Artt. 1218-1229, Bologna, Roma, 1979, p. 263. Un ulteriore ma analogo tipo di danno può derivare all'individuo dal vedersi pregiudicata, in conseguenza della divulgazione di notizie riservate, la propria aspettativa di lavoro, cioè la possibilità di reinserirsi senza apprezzabili difficoltà in un nuovo rapporto di lavoro. T. A. Auletta, *op. cit.*, p. 159.

10 Ad esempio, il titolare del diritto al riserbo potrebbe perdere o vedere diminuire in notevole misura la possibilità di contrarre un buon matrimonio oppure potrebbe rimanere escluso da determinati ambienti nei quali aveva modo di conoscere un certo numero di persone che spesso entravano poi nel suo giro d'affari. T. A. Auletta, *op. cit.*, p. 159.

11 Sul punto si segnala una pronuncia del Tribunale di Napoli con la quale il giudice di merito ha riconosciuto ad una casalinga un danno alla vita di relazione quale compromissione delle mansioni di educazione dei figli, di assistenza al coniuge, di collaborazione nell'azienda familiare e nel mantenimento dei rapporti sociali influente sull'attività lavorativa del coniuge stesso. Trib. Napoli, 30 giugno 1977, in *RCP*, 1978, p. 456.

[12](#) Tale orientamento dottrinale è stato accolto dal giudice delle leggi; la Corte Costituzionale con una sentenza del 1986, ha avuto modo di chiarire definitivamente il valore e la portata dell'art. 2059 c.c. riconducendone l'applicazione soltanto quando all'illecito civile, costituente anche reato, consegue un danno morale subiettivo.

La Corte identifica, inoltre, tre tipi di danno, autonomi, seppur connessi tra di loro: il danno biologico, quale danno alla persona, il danno morale e il danno patrimoniale. Il primo è un danno evento e i secondi sono danni-conseguenza, eventuali e possibili quale conseguenza del danno alla persona. Significamene la Corte, con la stessa sentenza, identifica le norme da applicare nelle tre diverse ipotesi di danno, specificando che al danno morale va applicato l'art. 2059 c.c. mentre al danno alla persona e al danno patrimoniale va applicata la disposizione di cui all'art. 2043 c.c. Corte cost., 30 giugno 1986, n. 184, in *Foro it.*, 1986, I, p. 2053.

[13](#) S. Sica, *Commento all'art. 29, comma 9*, in AA. VV. *La tutela dei dati personali. Commentario alla l. 675/1996*, cit., p. 287 ss.

[14](#) E. Lucchini Guastalla, *op. cit.*, p. 654.

[15](#) Così G. Iudica-P. Zatti, *Linguaggio e regole del diritto privato*, III ed. Padova, 2002, p. 454.

[16](#) In tal senso P. Ziviz, *Alla scoperta del danno esistenziale*, in *Contratto e impresa*, 1994, p. 845 ss.

## **LA POSTA ELETTRONICA E' UN BENE AZIENDALE?**

### **SOMMARIO**

- La posta elettronica: bene aziendale o personale?
- Le teorie in materia
- Il caso giurisprudenziale

#### *La posta elettronica: bene aziendale o personale?*

L'avvento delle nuove tecnologie ha portato con sé problematiche giuridiche di rilievo, sulle quali i giudici di merito e di legittimità ancora non si sono pronunciati o soltanto di recente hanno avuto modo di intervenire.

Un argomento di grande attualità che ancora non vede all'orizzonte soluzioni giurisprudenziali consolidate consiste nella possibilità per le aziende di regolamentare l'uso delle email aziendali di ogni singolo dipendente.

Più in particolare, alcune aziende vorrebbero regolamentare il fatto che se un dipendente si assenta per più di x giorni, il suo superiore diretto o chi da lui autorizzato possa leggere la posta elettronica del dipendente assente e quindi non creare un disservizio e stabilire norme che impediscano ai propri dipendenti di usare la mail aziendale per comunicazioni private.

Come si sposano queste esigenze con la normativa vigente?

L'art. 15 della nostra Costituzione sancisce l'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione. La loro limitazione può avvenire solo con un atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge.

Tale diritto fondamentale è rafforzato dalla previsione dell'art. 616 c.p., che prevede il reato di violazione, sottrazione e soppressione della corrispondenza. Chiunque prenda cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottragga o distrugga, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, o la distrugga, è punito con la reclusione fino ad un anno o con una multa da 30 a 516 euro, sempre che il fatto non costituisca più grave reato.

L'art. 5 della L. 23 dicembre 1993 n. 547 ha integrato l'ultimo comma di questa norma rispetto alla norma originaria, evidenziando che per *corrispondenza* si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

Quindi, leggendo la posta elettronica altrui, si commette reato. Può essere considerata "posta elettronica altrui" la posta elettronica c.d. aziendale, cioè, ad esempio [nome.cognome@nomeazienda.it](mailto:nome.cognome@nomeazienda.it)? Il siffatto indirizzo email è un bene personale o aziendale? Quali poteri ha il datore di lavoro su questo spazio di lavoro virtuale?

In linea generale, rimangono pochi dubbi sull'impossibilità di violare il contenuto delle email da parte di soggetti privati.

### *Le teorie in materia*

In dottrina si contrappongono due teorie dominanti.

La prima, molto permissiva, prevede la possibilità per il datore di lavoro, che avvisi non equivocamente il dipendente, di effettuare controlli sul contenuto della posta elettronica. Questo orientamento si basa su una lettura molto estesa del comunicato stampa n. 23 del 12 luglio 1999 del Garante per la Protezione dei Dati Personali, nella quale il Garante sancisce l'assimilabilità dell'email alla posta tradizionale e l'inviolabilità dei messaggi, ma prevede una deroga: *"Non può essere considerata contrastante con la normativa sui dati personali l'eventuale successiva presa di conoscenza della e-mail da parte di soggetti estranei al circuito di posta elettronica, quando il messaggio non sia stato indebitamente acquisito da questi ultimi ma ad essi comunicato da parte di uno dei destinatari del messaggio stesso."*

Il principio espresso indica che chi legge un messaggio a lui non destinato non viola il precetto dell'art. 616 c.p. se ciò gli è permesso dal soggetto legittimato a leggere la posta elettronica: pare davvero troppo azzardato ricavarne il principio per cui sia nelle mani del datore di lavoro la possibilità di accedervi perché proprietario della casella di posta...

La seconda teoria sembra più rispettosa del dettato normativo e sostiene il divieto per il datore di lavoro di intercettare la posta elettronica dei dipendenti, in ottemperanza sia all'art. 15 della Costituzione, sia all'art. 616 c.p., sia all'art. 8 dello Statuto dei Lavoratori. Potrebbe infatti la posta aziendale contenere informazioni personali, dati sensibili, opinioni espresse dal dipendente.

Sarà possibile per il datore di lavoro evitare l'utilizzo improprio della posta aziendale predisponendo un'adeguata policy interna che regoli l'uso, fino a vietarlo, dell'email aziendale per uso personale. Nel caso in cui nascesse il sospetto che ne sia fatto un uso difforme o illecito, il datore di lavoro potrà richiedere all'Autorità giudiziaria l'autorizzazione a effettuare controlli, ma non accedervi autonomamente, neppure previa comunicazione al dipendente.

### *Il caso giurisprudenziale*

Finora soltanto un'ordinanza del Tribunale di Milano, in data 10 maggio 2002, si è pronunciata sull'argomento e ha disposto che il datore di lavoro che controlla la posta elettronica di un dipendente in ferie non commette reato.

Il Tribunale di Milano ha disposto infatti l'archiviazione di un procedimento penale promosso, su denuncia-querela della parte offesa, nei confronti del legale rappresentante di una società e di un suo collaboratore, coinvolti in questa vicenda per aver letto quest'ultimo i messaggi contenuti nella casella di posta elettronica di un dipendente, che in quel momento si trovava in ferie.

Il reato ipotizzato era quello più sopra esposto di violazione della corrispondenza. Il giudice ha ritenuto che tale reato non si era concretizzato, in quanto la casella di posta elettronica aziendale (riportante cioè il nome del server della società titolare) costituisce un bene aziendale soggetto al legittimo controllo del datore di lavoro.

Ancora non sono arrivate al giudizio della Corte di Cassazione sentenze di tribunali di merito che dispongano sull'argomento.

Però, la Corte di Cassazione ha stabilito la legittimità del controllo del tabulato delle telefonate effettuate dal dipendente con il telefono aziendale. In questo caso la questione non era penale, ma civile, riguardando la liceità della prova acquisita a seguito di particolari controlli dell'attività del lavoratore.

La Suprema Corte, con sentenza n. 4746 del 3 aprile 2002 ha stabilito che, ai fini dell'operatività del

divieto di utilizzare apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 dello Statuto dei Lavoratori, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa. Devono ritenersi invece certamente fuori dall'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate.

Questo principio potrebbe, prima o poi, essere applicato anche al controllo della posta elettronica. Ma, non essendoci una giurisprudenza consolidata in materia, è difficile prevedere in anticipo se sarà davvero questo l'orientamento dei tribunali di merito e di legittimità.

Daniela Rocca