Informatica

Il Garante dei fannulloni

di Nicola Bortolotti

Ancor più che negli altri mesi dell'anno, in agosto i quotidiani sono perennemente a caccia di notizie curiose, che spesso poco hanno che fare con realtà lavorative o aziendali. Talvolta, però, è proprio approfittando della pausa estiva che fatti interessanti accaduti all'estero – poco "spendibili" quando la foliazione costringe a "tagli" e forte selezione dei contenuti contingenti – assurgono all'onore delle cronache, fornendo spunti di riflessione degni di nota.
Ad alcuni non sarà quindi sfuggito un titolo del Giornale di sabato 8 agosto, che ancora si può leggere in rete all'indirizzo http://www.ilgiornale.it/a.pic1?ID=372706 (è anche scaricabile l'intera pagina in PDF): "Ricarica il cellulare in ufficio e lo licenziano".
Questo è, in breve, il riassunto di una storia che, come si può ben immaginare, non è accaduta in Italia bensì nella rigorosissima (nonché, forse, fin troppo rigida) Germania. Un operaio è stato licenziato per aver ricaricato il proprio cellulare sul posto di lavoro, con ciò provocando alla propria azienda un danno di 0,014 euro, un furto di elettricità di ben quattordici millesimi di euro (non è un errore di stampa), addirittura certificato da un perito all'uopo consultato. L'operaio non era un novellino, avendo svolto il suo lavoro per quattordici anni con l'unico appunto di avere fotografato il luogo dove lavorava (anche questa cosa proibita). La magistratura tedesca, con celerità difficilmente concepibile da chi deve scontrarsi quasi quotidianamente con la censurabile inefficienza del belpaese, aveva confermato la liceità del licenziamento. In Germania (e non solo) il rischio di essere messi alla porta per abitudini che in Italia rappresentano la norma è elevatissimo, ad esempio l'usufruire di un buono sconto del supermercato per cui si lavora o scambiare una email con un famigliare. Il "sequel" di questa paradigmatica vicenda, con tanto di "happy end", è tuttavia sfuggito ai cronisti di casa nostra: senza attendere il ricorso del dipendente, fissato per ottobre, l'azienda – colpita negativamente dalla pubblicità globale ottenuta e, forse, dal timore di essere tacciata di discriminazione razziale, in quanto il licenziato era di origine pachistana – ha reintegrato Mohammed Sheikh (questo il nome dell'autore del "furto"). Capitolo chiuso, come si può leggere, ad esempio – nell'abbordabile lingua inglese – all'indirizzo http://www.canadianhrreporter.com/ArticleView.aspx?l=1&articleid=7107.

Da un eccesso all'altro

Qual è il "fil rouge" che lega questa vicenda, pur interessante, al mondo dell'informatica? Il *trait-d'union* è la risonanza data dalla stampa quasi all'unisono, curiosamente proprio negli stessi giorni di fine settembre, a una decisione del Garante della Privacy di parecchi mesi prima, più precisamente il "divieto" del 2 aprile 2009 pubblicato sul bollettino n. 104 aprile 2009 e reperibile all'indirizzo http://w ww.garanteprivacy.it/garante/doc.jsp?ID=1606053.
Se alcune testate giornalistiche "tradizionali" (ad esempio http://www.repubblica.it/2007/09/sezioni/ tecnologia/diritti-web/garante-web/garante-web.html) hanno condito la notizia con numerose inesattezze di carattere tecnico, altri siti più specializzati (ad esempio Tom's Hardware News http://www.tomshw.it/news.php?newsid=19460) hanno efficacemente ed eloquentemente sintetizzato la questione con titoli del tipo "Spiare online un lavoratore fannullone è illegale".
Mentre in Germania si può licenziare per qualche millesimo di euro, cosa ha partorito l'ineffabile garante, inerte di fronte alla diffusione online delle dichiarazioni dei redditi degli italiani ma sempre più vessatorio nei confronti delle piccole e medie realtà produttive?
Ha – di fatto – posto una serissima ipoteca sulla possibilità per qualunque datore di lavoro di poter individuare un dipendente infedele, creando anche un precedente che – prima o poi – renderà impossibile identificare l'autore di reati anche assai gravi (come la pedopornografia), come si spiegherà meglio più avanti.
Il "casus belli" è così riassumibile: nel 2007 l'anomala attività on-line di un dipendente della "Italian Gasket S.p.A." di Brescia (http://www.italiangasket.com) è stata monitorata per nove mesi e – contravvenendo ad ogni regola aziendale (venivano scaricati voluminosi files per uso personale ed extra-lavorativo) – aveva comportato il suo licenziamento. Ora la Italian Gasket, parte lesa, si trova invece proiettata dal Garante nella parte dell'imputata, con possibili pesanti illeciti penali, perché l'attività di monitoraggio avrebbe violato

l'art. 4, comma 1 della legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) nonché vari articoli del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003).

Nessuna leggerezza

Di primo acchito verrebbe da pensare che la *Italian Gasket* fosse caduta in una grave leggerezza, non avendo informato il dipendente che le sue navigazioni venivano controllate. Il far firmare ad ogni addetto con accesso a Internet un'adeguata informativa rappresenta infatti, ormai da tempo, la prassi abituale seguita in ogni azienda pubblica e privata, pur con sporadiche, colpevoli e talora notevolissime eccezioni (si pensi alla quasi totalità delle scuole italiane). Nel provvedimento del Garante, invece, si legge qualcosa che avrebbe dovuto far sobbalzare sulla sedia qualsiasi addetto ai lavori:

(...)
RILEVATO che al reclamante, al pari di tutti gli altri dipendenti dell'azienda abilitati all'uso della rete Internet, erano "state fornite specifiche istruzioni circa l'utilizzo della postazione informativa individuale" (cfr. all. n. 1 al verbale, recante il "Regolamento aziendale per la sicurezza e l'utilizzo delle postazioni di informatica individuale" del 15 gennaio 2007, ove al punto 6.3. si legge che "è assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa"), peraltro "sottoscritte per presa visione" dai medesimi dipendenti, compreso lo stesso reclamante (cfr. verbale di operazioni compiute del 25 febbraio 2009, p. 2; cfr. altresì all. n. 1 al verbale);
RILEVATO altresì che il reclamante era stato previamente informato circa i controlli che sarebbero stati effettuati sulla propria postazione individuale in ordine agli accessi effettuati alla rete (cfr. allegato n. 2 al verbale del 25 febbraio 2009; cfr. altresì all. n. 1 al verbale del 26 febbraio 2009);
PRESO ATTO di quanto dichiarato dalla società in ordine all'impossibilità di adottare misure di carattere inibitorio per l'accesso a siti non pertinenti l'attività lavorativa, soluzione che, ancorché valutata e sperimentata in passato dalla società, non è stata ritenuta praticabile (cfr. verbale di operazioni compiute del 25 febbraio 2009, cit., p. 2);

Come si può ben constatare, quindi, la Italian Gasket non ha peccato di superficialità, ottemperando alla prassi seguita ovunque.

Qual è stata, dunque, la grave mancanza della parte realmente lesa? Un indizio si può desumere sempre dal provvedimento del Garante, laddove subito dopo si legge:

RILEVATO che, alla luce delle dichiarazioni rese dalla società (secondo cui "nessuna attività di monitoraggio è stata effettuata in passato nei confronti di dipendenti diversi dal [reclamante]": cfr. verbale di operazioni compiute del 26 febbraio 2009, cit., p. 2) e della documentazione prodotta (la quale ha evidenziato che l'attività di tracciamento e di registrazione degli accessi alla rete Internet nei confronti del reclamante è avvenuta "in deroga alla normale prassi aziendale": cfr. all. n. 1 al verbale del 25 febbraio), non risulta allo stato provato che detta attività di monitoraggio abbia in passato interessato anche altri dipendenti;

Figura 1

In sostanza, quindi, la reale colpa della società è stata quella di individuare la mela marcia. Misfatto tanto grave da scatenare l'ira funesta del Garante, che così ha sentenziato:

(...)
RITENUTO che l'installazione di un software con funzionalità appositamente configurate per il tracciamento (sistematico e continuativo) degli accessi ad Internet da parte dell'interessato – con la conseguente memorizzazione di tutte le pagine web visualizzate dal reclamante – risulta essere avvenuta in violazione dell'art. 4, comma 1 della legge 20 maggio 1970, n. 300, che vieta l'impiego di apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori; rilevato, inoltre, che la società non ha neanche provveduto a svolgere gli adempimenti previsti dal secondo comma della medesima disposizione, in relazione alle funzionalità che mediante il software installato legittimamente possono essere perseguite per "esigenze organizzative e produttive" (cfr. verbale di operazioni compiute del 26 febbraio 2009, cit., p. 2);
RITENUTO, pertanto, che il trattamento di dati personali riferiti al reclamante, limitatamente agli accessi effettuati alla rete Internet, non risulta essere stato effettuato lecitamente dalla società (artt. 11, comma

1, lett. a) e 114 del Codice; cfr., altresì, il punto 4 delle menzionate Linee guida);
RITENUTO inoltre che detto trattamento non risulta essere stato lecitamente svolto neanche sotto il profilo della pertinenza e non eccedenza delle informazioni raccolte (art. 11, comma 1, lett. d), del Codice), tenuto conto che il monitoraggio effettuato dalla società (peraltro diretto ed esclusivo nei confronti del reclamante) risulta essere stato prolungato e costante (cfr. le citate Linee guida, punto 6);
(...)
TUTTO CIÒ PREMESSO IL GARANTE
1. ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice, vieta a Italian Gasket S.p.A. l'ulteriore trattamento dei dati personali riferiti al reclamante, limitatamente al monitoraggio degli accessi a Internet (artt. 11, comma 1, lett. a) e d) e 114 del Codice e art. 4, primo comma, l. 20 maggio 1970, n. 300);
2. dispone la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili.

Considerazioni sconcertanti

Il dipendente infedele ma reclamante sapeva di essere monitorato, sapeva di contravvenire pesantemente al regolamento sull'utilizzo aziendale di Internet da lui stesso controfirmato eppure è stato inopinatamente graziato.
Le considerazioni del Garante sono sconcertanti: di fronte a questo precedente (che, c'è da sperare, la giustizia penale vorrà almeno mitigare, se non correggere facendone tabula rasa), alle aziende è stata tolta ogni valida arma nei confronti non solo dei "fannulloni" via Internet ma anche di chi volesse perpetrare illeciti ben più gravi, dallo spionaggio industriale alla pedopornografia.

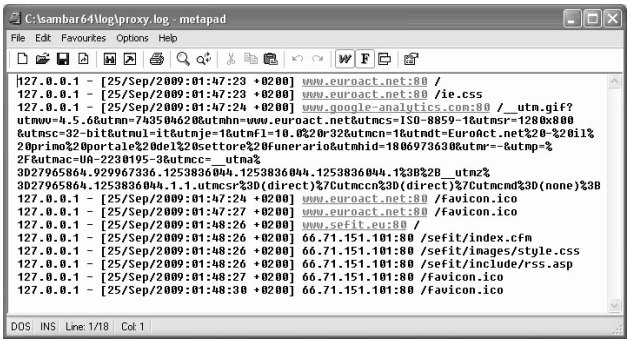

Figura 2

Non solo: strumenti fondamentali per l'aumento della sicurezza ed efficienza aziendale, come i cosiddetti "caching proxy" (tra cui Squid, saggiamente utilizzato da Italian Gasket), diventano de facto strumenti illegali.
Si tratta di un ipergarantismo nei confronti dei dipendenti in malafede difficile da comprendere, che stride a confronto dell'iperlegalismo richiesto invece in Germania.
Per capire quanto pericoloso sia questo divieto del Garante, si pensi che un accesso ad Internet condiviso da realtà piccole o medio-piccole (che, nel caso di Italian Gasket, molto probabilmente era tariffato "a traffico", per cui il dipendente potrebbe aver provocato anche un ulteriore danno quantificabile alla propria azienda) viene di norma identificato "lato provider" da uno stesso indirizzo IP. In altri termini l'attività, sia essa lecita o illecita, puntualmente tracciata nei "log" di attività del provider (che devono essere conservati per alcuni anni e possono essere richiesti e utilizzati dall'Autorità Giudiziaria) è associabile al titolare del contratto Internet e non al singolo terminale della rete aziendale che l'ha generata. Questo qualora non si siano messe in atto adeguate contromisure, ad esempio la navigazione "filtrata" da un proxy gratuito come Squid o Sambar (disponibili per tutte le principali piattaforme, da Linux a Windows), con generazione di un secondo "log" che – unito a quello del provider – possa consentire di giungere al terminale responsabile di una determinata attività. In figura 1 è visibile la semplicissima configurazione richiesta ad ogni browser per l'utilizzo di un proxy, nella fattispecie Mozilla Firefox; in figura 2 vi è un esempio di log prodotto da Sambar.
La scelta di far passare i pacchetti attraverso un proxy, anziché direttamente tramite il firewall-router, consente anche un maggiore controllo preventivo delle attività, con la possibilità di impostare "blacklist" (ossia un elenco di destinazioni proibite, anche se tale strategia è ormai non percorribile, vista gli sforzi che sarebbero necessari per tenere aggiornata la lista) o, scelta ancor meno attuabile, di impostare una "whitelist", ossia permettere la navigazione solo su un elenco predeterminato di siti.
Il fatto che vengano memorizzate in "cache" le pagine e i files più recenti, ne rende l'accesso molto più rapido, pressoché immediato.
Tutto questo, però, al Garante non va bene: non c'è motivazione tecnica universalmente riconosciuta che venga considerata valida. Via libera, dunque, ai "fannulloni", purché ozino via Internet.