Spionaggio aziendale e divieto di controllo a distanza dei lavoratori nel provvedimento del Garante Privacy

Date : 10 luglio 2017

La questione relativa ai cd. “controlli difensivi” del datore di lavoro, previsti dalla normativa in materia di tutela dei dati personali, si intreccia intimamente con i rischi derivanti dalle pratiche di spionaggio industriale operate da insider.

Come è noto, se non in casi eccezionali, i datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, e ciò anche dopo la modifica operata dall’art. 23 del d. lgs. 151/2015, uno dei 4 decreti attuativi del Jobs Act, a modifica dell’art. 4 della L. 300/70 (cd. Statuto dei lavoratori).

Il Garante mantiene un atteggiamento critico (più ancora della giurisprudenza di merito e di legittimità) sulla lettura e sulla registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò costituirebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori.

I controlli sull’utilizzo delle email e dei sistemi informatici e telematici aziendali dovranno essere improntate al concetto di *privacy by design* ai sensi del Reg. 2016/679/UE, e ai seguenti principi:

- il principio di necessità- secondo cui i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- il principio di correttezza che deve informare il trattamento in ogni suo profilo;
- la necessaria determinatezza, legittimità ed esplicitazione del fine perseguito dal trattamento, che concorre ad un'interpretazione "adeguatrice" del terzo comma del nuovo articolo 4 come modificato dal Jobs Act;
- i principi di pertinenza e non eccedenza dei dati trattati, che impongono una minimizzazione nel ricorso al trattamento dei dati personali secondo le effettive necessità e con le modalità meno invasive possibile;
- il divieto di profilazione;
- la necessaria legittimazione soggettiva al trattamento, che impone di limitare ai soli soggetti preposti l'autorizzazione allo svolgimento di attività di monitoraggio sul lavoro;

- il rinvio, di cui all'art. 113, al divieto, sancito dallo Statuto, di indagini "sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore";
- la minimizzazione dei controlli difensivi o comunque rivolti agli strumenti elettronici;
- l'assoluta residualità dei controlli, con appositi sistemi informativi, sull'attività e il comportamento dei lavoratori in quanto tale;
- il tendenziale divieto di accesso alle comunicazioni elettroniche del dipendente;
- la residualità del ricorso ai sistemi biometrici e il divieto di utilizzo di dati genetici per la valutazione dell'attitudine professionale del dipendente, salvi ovviamente i casi previsti dalla legge per particolari circostanze.

Qualora si rilevino comportamenti anomali, gli eventuali controlli da parte del datore di lavoro dovranno quindi essere effettuati con gradualità.

In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

Il Garante per la protezione dei dati personali prescrive anzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli.

Occorre quindi, se non si è già provveduto, stilare le istruzioni agli incaricati sull’utilizzo della posta elettronica con gli effettivi passaggi relativi alle modalità di controlli, quali, a titolo esemplificativo, il software utilizzato, le modalità di contestazione dell’addebito, l’oggetto e i tempi della memorizzazione, le modalità di cancellazione, l’indicazione di coloro che materialmente effettueranno il controllo, la possibilità di controllo individuale in caso di anomalie ripetute, il divieto di utilizzo degli strumenti aziendali per fini privati, illeciti, o comunque non attinenti alle mansioni affidate.

È stato, pertanto, ritenuto illecito, e conseguentemente vietato, il trattamento effettuato da una società mediante la raccolta e la successiva produzione in giudizio di alcune e-mail (con indicazione sia dei dati cd. “esterni” – data, ora, mittente, destinatario- che del loro contenuto) scambiate tra determinati dipendenti e tra questi e terze persone, senza aver previamente adottato un disciplinare o strumento analogo sull’utilizzo della posta elettronica aziendale e senza aver fornito una specifica informativa ai dipendenti.

Il Garante ha, altresì, ritenuto che la società, nel trattare per finalità ulteriori – effettuazione di controlli per dichiarati scopi di tutela del patrimonio aziendale – dati raccolti al diverso fine di consentire la continuità e l’efficienza dei sistemi aziendali, abbia violato il principio di finalità dei trattamenti effettuati (v. art. 11, comma 1, lett. b), del Codice).

Analizzando i 53 provvedimenti del Garante inerenti alla liceità delle indagini difensive si può riscontrare come i controlli sui dipendenti vengano ritenuti statisticamente leciti prevalentemente nei casi in cui sia pendente un giudizio di lavoro sull’impugnazione del licenziamento da parte del dipendente.

In tali casi il Garante ammette che il datore non sia tenuto a fornire al dipendente la documentazione, servendo la stessa come prova in giudizio e ammettendo il differimento dell'ostensione dei documenti al dipendente.

Un altro caso in cui il controllo sulle email è risultato lecito ha riguardato l'invio di messaggi denigratori da parte del dipendente ai danni dell'azienda, di cui la stessa ha avuto conoscenza essendo stati gli stessi pubblicati on line. Il Garante ha ritenuto in tal caso corretta la procedura di immediata contestazione dell'illecito e la conseguente apertura delle e-mail in presenza del dipendente e di un suo fiduciario.

Un altro caso ancora ha riguardato insulti telefonici ai clienti da parte del centralinista dell'azienda. A seguito di un reclamo da parte di un cliente e la conferma di tali condotte da parte di altri dipendenti, il Garante ha da un lato inibito al datore di lavoro l'utilizzo dei dati acquisiti (registrazione delle telefonate), dall'altro ha però legittimato l'azienda nel non voler consegnare i dati personali dei denuncianti al dipendente, poiché egli non avrebbe comunque il diritto di conoscere i dati personali di terzi.

Il punto nodale della legittimità o meno dei controlli appare quindi la modalità di acquisizione della notizia dell'illecito.

Nulla quaestio quindi se vi siano modalità di conoscenza "pubbliche" (on line) o reclami di terzi, qualche problema potrebbe invece sorgere quando il datore di lavori abbia sospetti non confermati e voglia procedere ai controlli per fugare i propri dubbi sulla fedeltà del dipendente.

In tali casi la linea di confine tra un controllo lecito ed uno illecito diventerebbe molto sfumata e la possibilità di scivolare nell'illiceità un rischio concreto.

La situazione, sotto il profilo procedurale, si semplifica allorquando si rinvengano gli estremi di reati, come le fattispecie previste agli articoli 621, 622 e 623 c.p in relazione a violazione di segreto industriale, 615-ter c.p. di accesso abusivo a sistema informatico o telematico, o di appropriazione indebita e ricettazione di documenti.

In questi casi, anche per avallare i controlli interni, potrebbe essere utile predisporre una denuncia-querela, contro ignoti, non indispensabile ma utile per legittimare la possibilità di investigazioni difensive ai sensi dell'art. 391-bis c.p.p. (oltreché di indagini o controlli difensivi privacy).

Così, nel caso in cui l'analisi a campione fornisse riscontri, la stessa potrà essere seguita da una contestazione disciplinare di addebito con relativa sospensione cautelare e disattivazione di tutti i dispositivi aziendali al fine di preservare le prove.

Potrà essere buona prassi inviare all'interessato il materiale che lo riguarda avvertendolo che saranno svolte indagini allo scopo di verificare se le comunicazioni illecite sono davvero partite dal computer aziendale in dotazione allo stesso e di verificare l'eventuale esistenza di altre comunicazioni illecite sullo stesso tema.

Contestualmente il datore di lavoro potrà provvedere al ritiro delle dotazioni aziendali e a disabilitare l'utenza utilizzata per l'accesso ai sistemi informativi aziendali, invitando l’interessato a rientrare in azienda in un giorno concordato per assistere alle operazioni dirette ad accertare, tramite accesso al computer in sua dotazione, l'esistenza di eventuali anomalie circa l'utilizzo da parte sua della posta elettronica o dei servizi informatici o telematici.

Le verifiche dovranno avvenire per il tramite del solo incaricato già indicato nell’informativa, che deve ritenersi l’unico soggetto legittimato a conoscere ed aprire le email aziendali a seguito di richiesta del titolare con strumenti che garantiscano l’inalterabilità e l’originalità della prova, ad esempio con un write blocker, o filmando le operazioni e procedendo alla sigillatura del dispositivo di copia, così da assicurare la conformità della prova digitale acquisita ai sensi della L. 48/2008 e della Convenzione di Budapest del 2001. Ciò al fine di evitare la commissione di ulteriori attività dannose per la società e per scongiurare la cancellazione di eventuali dati aziendali nel tempo necessario ad effettuare le verifiche indispensabili di quanto emerso.

In seguito tale materiale potrà essere allegato alla querela contro ignoti e messo a disposizione degli inquirenti affinché ne traggano le dovute conclusioni sull’individuazione di estremi di reato.

A cura di: **Elena Bassoli**