Sole 24 Ore .lavoro
27-FEB-2019
da pag. 32
Dir. Resp.: Fabio Tamburini
foglio 1 / 3
www.datastampa.it
Tiratura: 0 - Diffusione: 0 - Lettori: 803000: da enti certificatori o autocertificati
Superficie: 51 %

Social, accesso alla rete e privacy: le aziende in cerca di regole

L'utilizzo degli strumenti tecnologici è in aumento esponenziale, si pensi al ricorso costante a Pc, device mobile, alle app che geolocalizzano il lavoratore. Tutti questi strumenti raccolgono, archiviano ed elaborano informazioni e dati personali, inclusi quelli dei dipendenti che li utilizzano; ciò solleva sempre più frequentemente il tema dei controlli sul lavoratore e la tutela della riservatezza.

Pogliotti e Tucci —*a pag. 32*

Tecnologie. L'articolo 4 dello Statuto e le interpretazioni restrittive del Garante spiazzano le imprese che procedono in ordine sparso. Ma l'accesso corretto resta un tema strategico

Social, uso della rete e privacy: aziende in cerca di regole

Giorgio Pogliotti
Claudio Tucci

L'utilizzo degli strumenti tecnologici è in aumento esponenziale, si pensi al ricorso ormai costante a Pc, device mobile, alle app che geolocalizzano il lavoratore, all'uso della tecnologia biometrica per accedere ad aree aziendali riservate, o per l'autenticazione ai sistemi informativi. Tutti questi strumenti raccolgono, archiviano ed elaborano informazioni e dati personali, inclusi quelli dei dipendenti che li utilizzano; ciò solleva sempre più frequentemente, e non soltanto nel lavoro digitale, il tema dei controlli sul lavoratore e la tutela della riservatezza.

L'argomento è salito alla ribalta nelle scorse settimane quando la Cassazione ha confermato il licenziamento disciplinare di una segretaria che passava il proprio tempo lavorativo su Facebook, ma già ad aprile 2018 gli ermellini avevano dato l'ok all'espulsione dall'azienda di un dipendente che, sempre su Facebook, aveva denigrato il proprio datore con un post dai contenuti diffamatori. Alcune imprese hanno interdetto l'uso del cellulare se si guida un'auto aziendale, altre puntano sulla "moral suasion" o su codici comportamentali. In ballo c'è il bilanciamento tra l'interesse aziendale e la tutela della riservatezza del dipendente.

Nel 2015 una risposta è arrivata dalla riscrittura del articolo 4 dello Statuto dei lavoratori del 1970. La nuova normativa ha ridimensionato il ruolo delle autorizzazioni sindacali o amministrative, esentando le imprese dal richiederle per installare gli strumenti finalizzati a rendere il lavoro (l'autorizzazione rimane necessaria quando tali dati vengono acquisiti tramite controlli attivati a tutela del patrimonio aziendale o della sicurezza). Inoltre, è previsto che le informazioni acquisite tramite strumenti autorizzati o esentati sono utilizzabili anche a fini disciplinari, purché siano state acquisite nel rispetto della normativa privacy.

La distinzione, all'apparenza agevole, tra strumenti di lavoro e sistemi di controllo, evidenzia Arturo Maresca, ordinario di diritto del Lavoro all'università «Sapienza» di Roma, «ha generato dubbi indotti dalla resistenza a cogliere il carattere innovativo del dato normativo, e forse anche dalle suggestioni provocate dalle potenzialità di controllo insite negli strumenti di lavoro e dalla varietà delle funzioni in cui si articolano i sistemi informatici che rendono indistinguibili quelle focalizzate sul processo lavorativo e quelle di controllo». Di fronte a queste complessità c'è stato chi si è spinto ad operare una distinzione all'interno degli strumenti di lavoro in base alla necessità del loro impiego, come se fosse possibile sindacarne l'utilizzo.

Per non rischiare, spiega Sandro Mainardi, ordinario di diritto del Lavoro all'università di Bologna, «alcune aziende hanno rivisto i propri regolamenti, altre hanno intrapreso la strada dell'articolo 8 della legge Sacconi del 2011, optando per le intese "in deroga". Altre ancora, stanno ricorrendo ai "controlli difensivi", se c'è il fondato sospetto di illecito. Le interpretazioni restrittive del Garante privacy e le applicazioni pratiche difficili rispetto alla varietà della strumentazione di lavoro stanno spiazzando le imprese, quando piuttosto serve sensibilizzare i datori verso l'informativa ai propri dipendenti e policy interne sull'utilizzo degli strumenti tecnologici».

Il punto, che fa fatica a imporsi, è che l'articolo 4 ha introdotto «nuovi equilibri - sottolinea Maresca - valorizzando l'onere del datore di lavoro di informare preventivamente il dipendente sull'uso degli strumenti e sull'effettuazione dei controlli, connettendo la tutela lavoristica con quella in materia di riservatezza dei dati personali che però, avendo portata generale, non può sovrapporsi alla norma speciale (articolo 4) fino ad interdirne la funzionalità». «A me pare che la rapidità e la pervasività con cui le nuove tecnologie entrano nel lavoro impongano anche al legislatore un cambio di paradigma - aggiunge Pierangelo Albini, direttore dell'area Lavoro, welfare, capitale umano di Confindustria -. Inutile limitarne l'introduzione, meglio concentrarsi su trasparenza e conoscenza. Essere correttamente informati e avere, quindi, piena consapevolezza delle potenzialità degli strumenti e delle nuove tecnologie, è ciò che davvero garantisce i lavoratori. Su queste basi è facile costruire il confine fra lecito e illecito».

Quindi come muoversi? «Non esiste una ricetta standard ma sicuramente ogni azienda, piccola o grande che sia, deve implementare un vero sistema di gestione dei dati efficace e funzionale - risponde Francesco Ferretti, ad di Si.Qu.Am, società di consulenza del gruppo Pc System -. Di questo sistema devono sicuramente far parte: la predisposizione di informative privacy trasparenti e comprensibili, l'assunzione di un regolamento interno che disciplini l'uso degli strumenti tecnologici utilizzati per lavoro e che approcci alla tematica in modo trasversale, l'adozione di procedure interne in primis quella da seguire in caso di incidenti di sicurezza».

Il corretto utilizzo degli strumenti tecnologici «è strategico perché ha impatti notevoli sull'organizzazione delle imprese - chiosa Stefano Passerini, responsabile dell'area sindacale di Assolombarda -. Basti pensare alle cosiddette black box, ovvero sistemi Gps che vengono installati sulle auto aziendali. Nel caso in cui i Gps costituiscono uno strumento di lavoro vero e proprio (ad esempio, i portavalori) non necessitano di autorizzazione o di accordo sindacale».

DIPENDENTI COMUNE DI ROMA

Online, ma per fini istituzionali

VIRGINIA RAGGI È sindaco di Roma. La sua giunta ha approvato un regolamento per l'accesso a internet

Per i dipendenti capitolini la navigazione in internet è consentita per «fini istituzionali e di servizio, fatte salve situazioni personali di tipo emergenziale». Non per navigare sui social network. Lo prevede il regolamento per l'assegnazione e l'utilizzo delle dotazioni informatiche approvato il 13 febbraio dalla Giunta Raggi. L'accesso a internet non è consentito per «scopi di profitto, per visione di siti non pertinenti con contenuti illeciti o porno», per «download di software inclusi quelli gratuiti», senza la preventiva autorizzazione scritta del dipartimento. Le navigazioni e le comunicazioni sono tracciate e conservate per il monitoraggio «a tutela dell'amministrazione e per eventuale richiesta dell'autorità giudiziaria». Sul dominio istituzionale è assegnata una casella di posta elettronica, uno strumento di lavoro da utilizzare «per lo svolgimento dell'attività istituzionale e di servizio». Non si può usare l'email per inviare o memorizzare messaggi di natura «oltraggiosa, discriminatoria», sì invece all'utilizzo per registrazione a dibattiti, forum e mailing list per motivi istituzionali e di servizio. Viene disciplinato anche l'utilizzo del telefonino assegnato a sindaco, assessori, presidenti dell'Assemblea capitolina, presidenti dei municipi, capigruppo, e altre figure che possono avere anche tablet, Pc, o book reader.

ELETTRONICA

Soluzioni ad hoc per i lavoratori

EMANUELE GALTIERI. Il manager è vicepresident, direttore hr comunicazione e it di Elettronica

Elettronica è da 70 anni leader mondiale nella progettazione, sviluppo e fornitura di sistemi di sorveglianza strategica, difesa e contromisure elettroniche, presente con oltre 3mila sistemi presso le Forze Armate di 30 Paesi. Tutti i quadri e i dirigenti di Elettronica, oltre al computer, hanno un cellulare aziendale, che spetta anche al personale in altri ruoli. «La peculiarità del core business della società, operante nel mercato Aerospace & Defence e le specificità dei clienti (ministeri della Difesa) - spiega Emanuele Galtieri, vicepresident direttore hr - impone ad Elettronica l'obbligo di assicurare una gestione molto accurata delle informazioni "classificate". Ciò ha implicato lo studio di soluzioni ad hoc per evitare che le policy di sicurezza minaccino la qualità del clima interno per i dipendenti testimoniata dalla certificazione Great Place to Work». Tra le soluzioni adottate: web filtering verso alcuni siti "pericolosi", chiavette Usb crittate, sistemi di file sharing cifrati, cifratura delle email per documenti Company Confidential o Restricted. Le necessità operative ovunque sono assicurate da una rete protetta (Vpn). L'azienda dispone di un Isoc, un centro operativo per la sicurezza che monitora costantemente gli eventi di reti e utenti con l'uso di machine learning.