AZETA
UFFICIO STUDI
RASSEGNA GIURIDICA
CISL dei LAGHI Como e Varese

Garante Privacy e social network

*Il **Garante per la protezione dei dati personali** ha pubblicato la **Newsletter n. 430 del 24 luglio 2017**, con la quale, tra le altre cose, ha fornito le indicazioni dei Garanti privacy sulle modalità di protezione dell'uso privato dei social network e delle comunicazioni dei lavoratori, oltre che degli spazi riservati sul cloud.*

……..

Con la Newsletter in oggetto, il Garante Privacy ha reso nota la conclusione del primo ciclo di incontri tenutosi con le Pubbliche Amministrazioni e le imprese in vista dell'applicazione del Regolamento europeo sulla protezione dei dati, dando indicazioni alle imprese *sull'utilizzo dei social network senza violare la privacy dei lavoratori*.

I Garanti europei della privacy, riuniti del Gruppo "Articolo 29" (WP29), hanno fornito alle imprese delle indicazioni che tengono conto sia della normativa vigente, che delle novità introdotte del Regolamento UE 2016/679 che troverà applicazione a partire dal 25 maggio 2018 e che sono volte a sfruttare le potenzialità delle reti sociali e delle nuove tecnologie senza, però, violare la privacy dei lavoratori.
Il documento definisce un quadro dei principi fondamentali ed esempi concreti per il corretto trattamento dei dati in ambito professionale.

Sintesi del documento

Il controllo

In sintesi, nel documento si evidenzia che sono possibili i controlli contro la fuga di dati o la compromissione dei sistemi ma senza spiare le comunicazioni dei dipendenti, l'eventuale consultazione dei social network limitata ai soli profili professionali, l'offerta di spazi privati su computer aziendali e servizi cloud, la necessità di ulteriori basi legali rispetto al consenso per trattare i dati personali dei lavoratori.

L'informativa

I Garanti hanno quindi ricordato che ogni lavoratore, indipendentemente dal tipo di contratto a lui applicato, ha diritto al rispetto della vita privata, della sua libertà e dignità. Deve innanzi tutto essere adeguatamente informato sulle modalità di trattamento dei dati personali in maniera chiara, semplice ed esaustiva, soprattutto quando siano previste forme di controllo del lavoratore, che comunque dovranno essere rispettose anche delle norme nazionali.

Il consenso

Le Autorità per la privacy hanno poi rimarcato che aziende ed enti pubblici difficilmente potranno avvalersi del consenso dei dipendenti come base legale per poter procedere all'utilizzo dei loro dati. Il consenso, infatti, per essere considerato valido, deve essere libero, diversamente da quanto accade nella realtà lavorativa dove c'è una forte disparità di potere tra datore di lavoro e dipendente.

Il datore di lavoro potrà quindi valutare, in alternativa, il ricorso a disposizioni normative o contrattuali, oppure far valere il proprio "legittimo interesse": ad esempio, alla sicurezza e alla corretta allocazione delle risorse. A questo proposito, i Garanti hanno ribadito che occorre bilanciare il legittimo interesse del datore di lavoro con i diritti e le libertà dei lavoratori alla luce dei principi di necessità e proporzionalità.

In particolare, ogni trattamento deve essere proporzionato alla finalità perseguita, e deve essere limitato quanto più possibile l'uso dei dati personali. Gli strumenti di geolocalizzazione , ad esempio, possono essere utilizzati per finalità strettamente aziendali e al lavoratore deve essere lasciata la possibilità di disattivare, se necessario, il localizzatore (come i gps).

Gli strumenti

Si possono inoltre introdurre strumenti e tecnologie, come quelle per l'analisi del traffico, per ridurre i rischi di attacchi informatici e la diffusione di informazioni riservate, ma non si può spiare la posta dei dipendenti o la loro navigazione internet. Anche in questo caso devono essere privilegiate misure preventive, assolutamente trasparenti, che segnalino ad esempio ai dipendenti la violazione che potrebbero stare per commettere.

I limiti

Anche l'eventuale consultazione o il monitoraggio dei social network devono essere limitati ai soli profili professionali, escludendo la vita privata di dipendenti o candidati all'assunzione. Vale sempre, infatti, il diritto fondamentale a non essere oggetto di discriminazione come quelle basate sulle idee politiche, l'impegno sociale o altri aspetti della sfera personale o familiare.

Proprio per favorire il corretto utilizzo degli strumenti e delle policy aziendali nel rispetto della privacy dei lavoratori, i Garanti invitano i datori di lavoro a offrire, ad esempio, connessioni WiFi ad hoc e a definire spazi riservati – su computer e smartphone, su cloud e posta elettronica – dove possono essere conservati documenti o inviate comunicazioni personali, non accessibili al datore di lavoro se non in casi assolutamente eccezionali.

In definitiva

E' innegabile che i social network oggi hanno registrato un'impennata nel loro utilizzo per esempio per la fase di ricerca e selezione del personale, con la lettura dei profili, le immagini e altre informazioni che possono essere utili per una valutazione del candidato e questo è tollerabile e tollerato.
I Garanti però hanno correttamente specificato che tale controllo è legittimo se effettuato nel limite dei profili professionali del lavoratore e per ciò che concerne le informazioni pubbliche dei candidato e solo se questo "esame" è necessario ai fini dell'assunzione per esempio per una valutazione di eventuali rischi collegati ad una specifica mansione. Il controllo sistematico ed indistinto dei profili social dei lavoratori, non perseguendo questi fini, non può essere ammesso. Tanto più se esso viene effettuato dopo l'assunzione, quando tale "controllo" datoriale è limitato dalla dimostrazione che esso si rende necessario per la protezione di un legittimo interesse aziendale e , comunque, solo se questa non può essere raggiunta in altro modo e in ogni caso dopo che il lavoratore è stato informato sulla possibilità del "controllo" stesso.

I Garanti hanno anche ricordato che necessaria è l'informativa delle modalità di trattamento dei dati personali del lavoratore in uso all'azienda, in maniera chiara ed esaustiva e che comunque ogni forma di controllo deve rispettare le leggi nazionali.
Sì quindi per esempio al controllo della rete aziendale per il pericolo di una fuga di dati o per l'analisi del traffico, ma con il veto di "spiare" a posta elettronica privata del lavoratore o la sua navigazione internet.