BYOD Quando l’ufficio è nello zaino

Date : 12 aprile 2018

La tecnologia ci offre vantaggi sconfinati: ci permette di vedere un film mentre siamo in treno o di fotografare un airone che si libra all’improvviso mentre siamo in riva al lago. La maggior parte delle nostre attività possono svolgersi utilizzando un solo dispositivo che, peraltro, possiamo comodamente conservare nelle nostre tasche o nel nostro zaino.

È questo il punto di partenza del *Bring Your Own Device* (BYOD) che, in italiano, si traduce in *Porta Il Tuo Apparato*. È un fenomeno associato al rapporto di lavoro ed alla possibilità, per il lavoratore, di utilizzare i dispositivi elettronici di sua proprietà per l’attività lavorativa.

Quindi, un principio apparentemente semplice per il quale, tuttavia, occorre qualche riflessione sugli aspetti critici che accompagnano questa scelta organizzativa.

Facoltà o obbligo?

L’utilizzo dei dispositivi di proprietà del lavoratore può derivare da una facoltà, esercitata dal lavoratore, o da un obbligo, imposto contrattualmente dal datore di lavoro.

I dispositivi personali fanno parte della nostra vita e, di fatto, ogni lavoratore ha almeno uno smartphone che porta sempre con sé: perché non utilizzarlo anche per il lavoro? Perché non chiedere al datore di lavoro di realizzare un’app da installare sul proprio telefonino? In questi casi, il vantaggio è reciproco:

- il lavoratore non è costretto a tenere ulteriori dispositivi dedicati all’attività lavorativa;
- il datore di lavoro non deve acquistare dispositivi ulteriori né deve pagare relativi costi di connessione alla rete visto che, con le tariffe attuali, quasi tutti i lavoratori sono dotati di una propria linea fonia/dati flat o, comunque, *abbondante*.

Stessi vantaggi ma visione capovolta se l’iniziativa parte dal datore di lavoro. Il BYOD si avvia come un obbligo contrattuale ed il lavoratore, soprattutto se neoassunto, deve dotarsi di un dispositivo adeguato alle caratteristiche previste dal datore di lavoro.

Sul luogo di lavoro o all’esterno?

Il dispositivo personale può essere utilizzato all'interno dei luoghi di lavoro o, più frequentemente, all'esterno.

Un caso di utilizzo interno, può essere la necessità di misurare costantemente l'altezza dal suolo di un lavoratore e, quindi, attivare un alert per l'obbligo di utilizzare appositi dispositivi di protezione individuale contro il rischio di cadute dall'alto.

Nei casi di utilizzo interno, di solito, la connessione del dispositivo avviene tramite rete WIFI aziendale e, quindi, diventa più intenso il flusso di dati (p.e. localizzazione) nella disponibilità del datore di lavoro con la conseguente possibilità (teorica) di effettuare un controllo sull'attività del lavoratore.

Più frequente è il caso di utilizzo all'esterno. Pensiamo ad un addetto alle vendite che può, tramite un'app, comunicare un ordine dal suo smartphone. In questi casi, la disponibilità di dati sul lavoratore si riduce, se il software è sviluppato con la dovuta sensibilità, ai momenti in cui lo stesso lavoratore attiva l'app.

Gli aspetti tecnologici

Gli aspetti tecnologici del BYOD riguardano, principalmente, la compatibilità dei dispositivi personali sia con riguardo alla loro possibilità di integrare funzioni *lavorative* sia rispetto alle policy di sicurezza aziendali.

Se focalizziamo la nostra attenzione a smartphone e tablet, gli standard sono ormai delineati. Le statistiche più recenti, infatti, raccontano che Android e iOS, in Italia, sono utilizzati nel 98% di smarthpone e tablet in circolazione.

Questo vuol dire che la realizzazione di una app adeguata agli standard funzionali e di sicurezza dipende solo dalle capacità tecnologiche degli sviluppatori. Non si vuole, con ciò, sottovalutare l'impegno richiesto per lo sviluppo ma, semplicemente, sottolineare che si tratta di mondi ben noti e consolidati, ancorché in evoluzione soprattutto relativamente alle vulnerabilità che, via via, possono emergere. In ogni caso, specifici meccanismi di sicurezza sono individuati dal WP29, come si vedrà più avanti, per il trasferimento di dati personali.

Un ulteriore aspetto tecnologico può essere legato alle funzioni di connettività dei dispositivi personali. Le capacità di connessione su rete mobile non dipende dalla app ma dalle caratteristiche hardware dell'apparato e dal grado di copertura del luogo dove il dispositivo viene utilizzato. Per evitare sorprese, potrebbe essere utile effettuare preventivamente test specifici che verifichino l'effettiva capacità di comunicazione del singolo dispositivo nei luoghi dove, in prevalenza, verrà utilizzato.

La tutela dei lavoratori tra diritto nazionale e GDPR

L'aspetto più delicato del BYOD è, tuttavia, il bilanciamento tra il diritto del datore di lavoro a proteggere i dati trattati con i dispositivi personali ed i diritti e le libertà dei lavoratori.

Non dimentichiamo che il nostro ordinamento è ispirato ai principi costituzionali oltre che a quelli stabiliti dalla Convenzione Europea dei Diritti Umani[i]. Quindi, occorre una particolare attenzione sia alle norme del diritto nazionale sia a quelle di derivazione UE:

- legge 300/1970[ii] altrimenti conosciuta come Statuto dei Lavoratori;
- legge 81/2017[iii] altrimenti conosciuta come legge sul Lavoro Agile;
- regolamento UE 679/2016[iv] altrimenti conosciuto come Regolamento Europeo per la Protezione dei Dati Personali (o GDPR).

Lo Statuto dei Lavoratori ha visto una revisione, tra gli altri, dell'art. 4 che è così riformulato

1. *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del Lavoro e delle Politiche sociali.*
2. *La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
3. *Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal Dlgs. n. 196/03.*

La nuova formulazione, oltre ad eliminare concettualmente (ma non sostanzialmente) il divieto di installazione di impianti per il controllo dell'attività lavorativa, consente al datore di lavoro di introdurre strumenti tecnologici finalizzati a rendere la prestazione lavorativa (senza specificare se di proprietà aziendale o del lavoratore) purché i dati provenienti da queste apparecchiature siano trattati in conformità al Codice della Privacy.

Il quadro giuridico si arricchisce con gli articoli 19 e 21 della legge sul Lavoro Agile che, in concreto, è la norma che più frequentemente dovrà essere applicata in caso di BYOD. E, mentre l'art. 21 è un rimando all'art. 4 dello Statuto del Lavoratori, l'art. 19 introduce un vero e proprio diritto alla disconnessione per il lavoratore. Questo si traduce, nel dovere, da parte del datore di lavoro, di stabilire meccanismi che possano consentire al lavoratore di determinare quando e come "staccare" il proprio dispositivo dalle funzionalità aziendali.

Il quadro normativo è completato dal GDPR e, in particolare, dagli approfondimenti contenuti nel parere n. 2 dell'8 giugno 2017[v] fornito dal gruppo dei Garanti Europei (WP29). Il documento

affronta alcune fattispecie particolarmente delicate rispetto all'uso dei dispositivi personali per attività lavorative:

- l'uso di strumenti di scanning dell'apparato, per esempio per rilevare malaware, deve essere calibrato in modo che non possa accedere alle zone di memoria che contengono esclusivamente dati personali (foto, messaggi di testo, ecc.);
- l'uso di software di geolocalizzazione o di monitoraggio del traffico, sebbene giustificato dal legittimo interesse del datore di lavoro a proteggere i dati trattati nella sua qualità di titolare del trattamento dei dati, può essere applicato solo in presenza di adeguate misure che distinguano l'utilizzo privato del dispositivo da quello per attività lavorative;
- il trasferimento di dati dal dispositivo del lavoratore al data center aziendale deve avvenire attraverso una connessione sicura cioè, preferibilmente, attraverso una VPN specificatamente realizzata; inoltre, è preferibile che i dati da trasferire siano contenuti in sandbox appositamente realizzate sui dispositivi personali.

In ogni contesto, quindi, appare opportuno applicare il BYOD senza trascurarne gli aspetti di tutela ed i relativi riflessi tecnologici ed organizzativi.

Note:

[i] https://www.echr.coe.int/Documents/Convention_ITA.pdf

[ii] http://www.normattiva.it/

[iii] http://www.normattiva.it/

[iv] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT

[v] https://ec.europa.eu/newsroom/document.cfm?doc_id=45631

A cura di: **Francesco Maldera**