Cristina Vicarelli
Avvocato

Dal BYOD al WYOD: pronti per la prossima sfida?

E' banale ma è vero: l'evoluzione normativa non tiene il passo della tecnologia. E se il discorso è abusato quando si hanno a mente gli ordinamenti nazionali o sovranazionali (si pensi alla lunga gestazione della normativa europea in tema di protezione di dati personali) l'assunto resta valido anche se si guarda alla regolamentazione di stampo privatistico, sempre più costretta tra le opportunità offerte dalla tecnologia e il timore dell'effetto boomerang che potrebbe derivare da un impiego non conforme ad una normativa che appare datata e difficile da adattare al caso specifico. Ne è stato un esempio limpido la diffusione in azienda dei sistemi mobili di proprietà dei dipendenti: smartphone e tablet magari più sofisticati di quelli dati in dotazione dall'azienda stessa, che avrebbero potuto essere impiegati a costo zero per migliorare le performance lavorative. Eppure, a distanza di qualche anno, ancora sono guardati con diffidenza e non sono poche le imprese che, a torto o a ragione, ne hanno vietato del tutto l'impiego, e se ci si attiene al report di Oracle – Byod Index – diffuso nella primavera scorsa, il 44% delle aziende europee è contraria al modello Byod (o lo consente solo in circostanze eccezionali) mentre il 22% vieta completamente la possibilità che i dati o le informazioni aziendali risiedano su dispositivi e il 20% non ha definito alcuna regola in merito (FONTE: Corriere delle Comunicazioni).

Il divario si fa più evidente se si pensa a quanto invece smartphone e tablet siano diffusi nella popolazione europea ed italiana (si veda in proposito il report diffuso da We Are Social)

E' lapalissiano dedurre che poter usufruire di uno strumento avanzato offerto dal dipendente senza costi per l'impresa è sicuramente è più vantaggioso che acquistarne uno proprio, ma è vero che non si può procedere alla cieca, ed è bene regolamentarne l'utilizzo con attenzione, per non rischiare perdite di dati o inopportune divulgazioni,

indebite intrusioni nella sfera privata del lavoratore o, perché no, controversie per lavoro straordinario, notturno o festivo.

L'atteggiamento più rischioso, invece, è certamente quello inerte: non vietare, ma consentire un utilizzo non regolamentato, si risolve in una perdita di controllo da parte dell'impresa sulle informazioni, sui dati personali, e sulle procedure di sicurezza nonché sull'organizzazione del lavoro.

Tuttavia, mentre le aziende sono ancora alle prese con i grattacapi derivanti dall'utilizzo delle tecnologie in mobilità, ecco che già si staglia all'orizzonte una nuova sfida: la wearable technology, la tecnologia indossabile. Che i più attenti osservatori hanno già preconizzato entrerà presto in sul luogo di lavoro, prima portata dai dipendenti più hi-tech, poi, dato che se ne prevede una rapida diffusione, portata un po' da tutti.

Dal Bring Your Own Device al Wear You Own Device: ancora non si è imparato a gestire il **BYOD** che già si passa al **WYOD**.

E nell'unica lettera che muta nell'acronimo, si celano grandi differenze.

Le tecnologie indossabili, infatti, vanno dagli smartwatch agli occhiali, dai braccialetti a capi di abbigliamento veri e propri, come le giacche. Non tutte allo stesso stato di diffusione tra il pubblico, ma alcune prossime a diventare fenomeni di massa, come è accaduto per gli smartphone.

Saranno probabilmente destinate ad integrare sensori che si indossano e piattaforme cloud, e interagiranno con sistemi domotici, si pensi al sensore pensato per il fitness che sa quando l'utilizzatore si sveglia e che, interagendo con un termostato d'ambiente intelligente, può regolare la temperatura della casa accendendo il riscaldamento quando serve...

Ma queste tecnologie non saranno destinate a rimpiazzare smartphone e tablet, semmai interagiranno con esse; certamente aumenteranno il numero di dispositivi che accedono alle reti domestiche. O aziendali...

E questo moltiplicarsi di strumenti interconnessi su un'unica rete potrebbe rappresentare il primo punto dolente per le imprese.

La seconda criticità può essere rintracciata nella peculiarità propria delle tecnologie indossabili. Infatti uno degli aspetti più problematici è che le varie funzioni dei dispositivi indossabili possono essere attivate dal possessore senza che gli altri se ne accorgano.

Gli smartwatch, ad esempio, possono essere dotati di microcamere, e possono rivelarsi idonei quindi a catturare immagini: usati in particolari abbinamenti con uno smartphone, potrebbero caricare documenti su servizi cloud, come ad esempio dropbox; per non parlare dei Google glass, che sono in grado non solo di registrare tutto quello che vede colui che li indossa, senza che i presenti ne abbiano contezza, ma anche di archiviarlo.

Si comprende allora facilmente come sarebbe semplice per chiunque trafugare informazioni riservate dell'azienda. E' bene, pertanto, che le imprese non si facciano cogliere impreparate, ma comincino sin d'ora a mappare le aree di rischio, tenendo conto di queste nuove possibilità, che fino a poco tempo fa erano appannaggio solo degli 007...

Le imprese dovranno correre ai ripari dotandosi di adeguate policy, ben prima che il fenomeno diventi massivo: occorrerà fare attenzione ai punti di accesso alle reti aziendali, e implementarne il monitoraggio, ma occorrerà anche adottare delle buone prassi di gestione delle informazioni e del personale e rafforzare le misure di sicurezza per impedire che attacchi esterni possano sfruttare le tecnologie indossabili dei dipendenti come vie d'accesso al sistema.

Occorrerà sottoporre le tecnologie indossabili dei dipendenti da connettere alla rete a misure di sicurezza equivalenti a quelle cui si sottopongono gli altri device che accedono alla rete aziendale, come tablet e pc.

Occorrerà monitorare e calibrare il flusso dei dati sulla rete con attenzione: le tecnologie indossabili, infatti, sono pensate per interconnettersi ad altri strumenti e sincronizzare i dati con essi. Un alto numero di interconnessioni e sincronizzazioni tra i dispositivi dei

dipendenti rischia, come minimo, di rallentare sensibilmente le connessioni e causare malfunzionamenti della rete.

Sarà consigliabile, in ogni caso, individuare da subito non solo quanti e quali dipendenti saranno autorizzati a connettere i propri dispositivi alle reti, con le dovute cautele, ma anche, a monte, se i dipendenti siano autorizzati a portare con sé questo tipo di dispositivi, individuando, nel caso, le aree in cui imporre divieti più stringenti, per scongiurare attacchi esterni.

Il tutto, sempre, anche avendo riguardo al rispetto della normativa vigente e alle implicazioni privacy. E' opportuno, ad esempio, lasciare questi dispositivi in uso a chi tratta dati sensibili? Vengono alla mente, per fare un parallelo, i provvedimenti del Garante in tema di videosorveglianza, in particolare le misure restrittive applicate alle case di cura.

Oppure: potrà un chirurgo indossare i google glass per migliorare le proprie abilità, oppure si rischia di ledere la riservatezza del paziente?

Se il dispositivo registra parametri vitali del dipendente, fino a che punto potrà essere sottoposto a controllo da parte dei responsabili IT aziendali?

Come sempre, è sul tema della riservatezza e del trattamento dei dati personali che si incaglia il fluire rapido del progresso tecnologico...

A differenza di quanto avvenuto sino ad oggi, pare necessario valutare attentamente la tipologia di tecnologia indossabile e le implicazioni che porta con sé, dato che le funzionalità, tra un tipo di dispositivo e l'altro, possono essere marcatamente diverse.

E pare necessario, tuttavia, iniziare a prendere le misure di queste nuove applicazioni prima che prendano piede, per non farsi cogliere impreparati, dato che esse recano con se inimmaginabili opportunità ed elevatissimi rischi.

E' necessario cominciare subito ad adeguare le policy aziendali e implementare le misure di sicurezza, tenendo a mente che, un divieto assoluto e incondizionato di impiego in ambito lavorativo, che appaia ingiustificato ed esorbitante, rispetto ad uno strumento che

ha una larga diffusione e al quale il lavoratore si è abituato fuori dal luogo di lavoro, rischia di cadere nel vuoto, e rischia di incoraggiare un uso sotterraneo con ampia tolleranza, almeno tra pari, verso i trasgressori, che avrà l'unico effetto di far perdere all'azienda il controllo dei dati personali e delle informazioni riservate. E soprattutto sarà il caso di chiedersi, con creatività e lungimiranza, in quale modo questi dispositivi così sofisticati, messi gratuitamente a disposizione dai dipendenti, possano vantaggiosamente essere inglobati nelle prassi aziendali e quali utilizzi innovativi possano derivarne, in modo da avvantaggiarsi sul piano della competitività non appena faranno la loro comparsa.