ADAPTability/3 – Il social recruiting tra privacy e dati sensibili

La ricerca dei talenti nell'era del web2.0: il social recruiting tra luci ed ombre

Come ci insegna il best seller americano *The Medici Effects* (*The Medici Effect: Breakthrough Insights at the Intersection of Ideas, Concepts, and Cultures di Johansson*), **per creare quelle comunità collaborative di lavoro che saranno – per molti – il motore delle imprese del futuro, è necessario favorire l'incontro di professionalità diametralmente opposte tra loro** nonostante possano sembrare, ad un primo sguardo, addirittura incompatibili. Dove trovare quindi queste figure tanto dissimili da essere compatibili?

Le inserzioni sul giornale appartengono al passato: nell'era del 2.0 l'incontro tra domanda ed offerta di lavoro avviene sul web e soprattutto sui social media, dove per le imprese è possibile analizzare un bacino potenzialmente illimitato di talenti in un tempo molto ristretto. Come si evince dal report *Social recruiting survey 2013*, realizzato da *Jobvite* (su una popolazione di 1600 intervistati appartenenti a 50 diversi settori), la ricerca del personale per mezzo delle nuove tecnologie porta notevoli vantaggi non solo a chi è in cerca di una nuova occupazione, ma anche a coloro che stanno cercando le "nuove leve". Proprio a questi ultimi, il web 2.0 permette di analizzare e confrontare un grande numero di persone in un tempo assai ristretto, ma soprattutto di trovare le competenze di livello elevato che stanno cercando (si veda il Report Deloitte 2013).

I migliori talenti hanno ormai scoperto che il modo più efficace per farsi conoscere e per mostrare la propria immagine, le proprie capacità e competenze sono i social media, i quali diventano, per le aziende, una sorta di piazze da cui scegliere i profili più rispondenti a quelli

cercati.
Chi meglio di una persona con un buon coinvolgimento online, con una buona capacità di confronto intelligente sui social ed in grado di proporre ai contatti, ai follower o agli amici i propri contenuti creativi può risultare appetibile ad una azienda basata sull'intelligenza collaborativa per la quale, così come per il web, valori come **partecipazione**, **comunicazione** e **condivisione** sono le fondamenta?

I vantaggi del social recruiting sembrano dunque inesauribili: maggiore interattività, maggiore comunicatività, maggiore trasparenza.
Detto ciò, è però anche vero che il social recruiting nasconde un suo "lato oscuro". Difatti, se è vero che i social network garantiscono un ampissimo bacino di informazioni sui candidati, in passato inimmaginabili, è anche vero che datori e selezionatori non sanno sempre porre un limite al desiderio di scoprire informazioni e dettagli sui candidati. E purtroppo, talvolta, superano i confini delineati sia dal buon senso che dalla privacy.
Caso ormai famoso è quello del giovane statistico di New York City, Justin Bassett: durante un colloquio di lavoro il selezionatore gli chiese le credenziali di accesso al profilo Facebook in modo da avere una visione a "360 gradi" del candidato. Bassett non esitò a ritirare la propria candidatura per la posizione.
Questo è solo uno dei tanti episodi raccontati su forum o articoli di giornali da candidati che hanno sostenuto recentemente colloqui di lavoro, e che hanno vissuto spiacevoli ed imbarazzanti situazioni, analoghe a quella sopra descritta.
Consapevoli delle violazioni in termini di privacy che molte aziende stavano perpetuando già da tempo ai danni dei propri utenti, il colosso dei social network ha fatto dunque sentire la propria voce nel marzo del 2012: attraverso la pubblicazione di una nota, ad opera del suo Chief Privacy Officer Erin Egan, tale pratica veniva condannata, nonché considerata come una seria violazione della Carta dei Diritti e delle Responsabilità di Facebook.
Per sottolineare la gravità di questo tipo di comportamenti messi in atto dalle aziende, è intervenuto anche il Dipartimento di Giustizia Americano, il quale ha dichiarato che entrare nella pagina social di un dipendente è considerato a tutti gli effetti un **crimine federale**, in quanto vengono ad essere violati i termini di servizio dei social network. Tuttavia, lo stesso Dipartimento ha affermato in seguito che questo tipo di violazioni non possono essere perseguite per legge. Difatti, sebbene richiedere le credenziali di accesso ad un social network violi apertamente i termini di servizio, questi termini non hanno un reale peso legale. Gli esperti dunque concordano sul fatto che la situazione in materia sia attualmente ancora piuttosto nebulosa.

La situazione negli USA

A seguito dei numerosi casi di invasione della privacy da parte di datori e selezionatori che stavano cominciando a rappresentare la quotidianità per lavoratori e candidati, alcuni Stati hanno deciso di promuovere normative ad hoc per arginare il crescente fenomeno.
Il Maryland e l'Illinois sono stati i primi pionieri ad approvare normative che vietassero ai datori di lavoro o ai selezionatori di richiedere a lavoratori e candidati username, password o qualsiasi altra informazione per accedere ai loro profili personali sui social network.
In breve tempo, anche altri stati hanno seguito tale esempio, volendo garantire ai propri cittadini il rispetto di determinati vincoli di privacy. Ad oggi sono 36 gli stati americani che hanno emanato, o hanno in corso di approvazione, normative sul tema del divieto per i datori di lavoro di richiedere i dati personali di accesso ai profili social di dipendenti e candidati.
Come è però tuttavia noto, gli Stati Uniti sono talvolta terra di grandi contraddizioni: difatti alcuni stati, benché prevedano leggi a tutela della privacy del lavoratore, hanno deciso, nel contempo, di approvare normative che garantiscono delle tutele anche ai datori di lavoro. È il caso ad esempio degli stati di **Washington** e della **California** (Lo stato di Washington ha approvato nel maggio 2013 la legge che vieta ai datori di chiedere a dipendenti e candidati username e password per accedere ai loro profili social (S.B. 5211). Nello stato della California invece è in corso di approvazione al Senato), i quali prevedono che, qualora il datore sospetti che un dipendente, e perfino un candidato, stia svolgendo **attività illegali**, come ad esempio la diffusione di informazioni aziendali riservate attraverso i social network, possa svolgere indagini per fugare i propri sospetti. Tra le possibilità che sono date al datore per indagare, vi è anche quella di obbligare il dipendente, o candidato, a **fornire le proprie credenziali di accesso ai profili social**. Sebbene possa essere concesso al dipendente di essere presente mentre il suo profilo social viene scandagliato alla ricerca di attività illecite, garantendo dunque una parvenza di rispetto per la privacy, questo tipo di leggi sembra andare in controsenso rispetto alla tendenza di tutela dei dati personali che molti stati americani stanno perseguendo.
Ovviamente gli stati di Washington e della California non sono gli unici a vivere questo tipo di contraddizioni al loro interno, e altri stati si trovano al momento in difficoltà nel tentativo di cercare una sintesi tra i due orientamenti.

Il caso italiano

Se dunque pare che negli Stati Uniti datori e selezionatori abbiano limiti talvolta molto labili nella ricerca di informazioni su un candidato o un dipendente tramite i social network, la situazione italiana si connota in tutt'altro senso.

Difatti, benchè la nascita dei social media risalga a soli pochi anni or sono, la normativa italiana che vieta ai datori di lavoro di effettuare qualsiasi indagine sulle opinioni circa un lavoratore risale al 1970 con la l. 300.
L'art. 8 dello Statuto dei lavoratori, nella sua straordinaria contemporaneità anche oggigiorno, pone infatti un limite molto preciso rispetto ai casi che si verificano negli Stati Uniti: il datore o il selezionatore non possono carpire, né in maniera diretta né indiretta, informazioni su un lavoratore che non siano attinenti la sua sfera professionale.
Essendo dunque la maggior parte delle informazioni presenti sui social network attinenti la sfera personale di un lavoratore, ne consegue automaticamente che qualsiasi tentativo di intrusione all'interno di un profilo social di un dipendente o candidato sarebbe perseguibile per legge.
Se tuttavia le argomentazioni portate dall'art. 8 della l. n. 300/1970 non fossero sufficienti alla maggior parte di datori e selezionatori, a tutelare la riservatezza dei lavoratori vi è anche il Codice della Privacy che, operando una meticolosa distinzione tra dati generici e sensibili, pone limiti molto severi e restrittivi al loro trattamento.
Considerando che molte delle informazioni che si possono ritrovare nella maggior parte dei profili social possano essere annoverate tra i dati sensibili, pare che per i datori italiani non vi siano al momento grossi appigli legali.
Tuttavia, un'importante considerazione deve essere richiamata all'attenzione dei candidati: nonostante i divieti di legge, la ricerca Adecco *Il lavoro ai tempi del #socialrecruiting e della #digitalreputation* mostra come **il 5% dei selezionatori italiani** abbia dichiarato di aver chiesto ai candidati in sede di colloquio di accedere alle loro pagine Facebook. Un divario dunque tra ciò che la normativa delinea e la realtà quotidiana dei colloqui di lavoro, che sembra mostrare come tale fenomeno non sia esclusiva prerogativa degli Stati Uniti, benché l'Italia avrebbe dovuto fare proprio tale concetto fin dagli anni Settanta.
In conclusione, è al momento evidente l'assenza di una normativa organica che permetta di conciliare le necessità delle imprese e il diritto alla riservatezza dei candidati e dei lavoratori.
È sbagliato infatti concentrarsi solo ed esclusivamente sul mero concetto di utilità a discapito della tutela. In questo senso una soluzione non può che essere un quadro regolatore più attuale che disciplini in modo chiaro e preciso diritti e doveri di entrambe le parti senza per questo limitare eccessivamente i vantaggi reciproci.

Andrea Cefis
ADAPT Junior Fellow
@AndreaCefis

ADAPTability/3 – Il social recruiting tra privacy e dati sensibili

Carlotta Piovesan
ADAPT Junior Fellow
@CarlottaPiovesan

---

[1] Il presente articolo è pubblicato anche in *Il Sole 24 Ore*, *Le Aziende InVisibili* (Il blog di Marco Minghetti), 27 dicembre 2013.

Scarica il pdf