Autorità Garante della Concorrenza e del Mercato

Garante per la Protezione dei dati personali

Commissione esaminatrice del concorso pubblico, per titoli ed esami, a un posto nella qualifica di funzionario in prova, nel ruolo della carriera direttiva al livello 6 della tabella stipendiale dei funzionari dell'Autorità Garante della Concorrenza e del Mercato e a un posto nella qualifica di funzionario in prova nel ruolo della carriera direttiva a livello iniziale della tabella stipendiale dei funzionari del Garante per la Protezione dei dati personali, per lo svolgimento di mansioni di traduttore linguistico specializzato nella traduzione dall'italiano all'inglese (F6TR)

Prova scritta del 3 giugno 2024

TRACCIA N. 1

AGCM

Comunicato stampa riguardante il Vademecum per le stazioni appaltanti

Intensificare la lotta ai possibili cartelli tra aziende che partecipano alle gare per gli appalti pubblici con la collaborazione delle stazioni appaltanti. È l'obiettivo dell'Antitrust che ha predisposto un *vademecum* da inviare ai soggetti che bandiscono le gare perché assumano un ruolo di 'sentinella' segnalando all'Autorità anomalie tipiche di comportamenti potenzialmente distorsivi della concorrenza. Dalla sua nascita a oggi l'Antitrust ha avviato in questo settore numerosi procedimenti istruttori, conclusi con l'irrogazione di sanzioni per oltre € 500 milioni. Si tratta di fenomeni che vanno combattuti con determinazione perché comportano una lievitazione dei costi per lavori o forniture e dunque un danno diretto per l'intera collettività.

Il *vademecum* ha l'obiettivo di aiutare le stazioni appaltanti a percepire i segnali di un'alterazione concorrenziale, identificando le anomalie comportamentali sintomo di distorsioni concorrenziali, la cui effettiva sussistenza sarà tuttavia accertata solo all'esito del procedimento istruttorio che l'Autorità dovesse ritenere di avviare in seguito alle segnalazioni pervenute.

L'Antitrust suggerisce innanzitutto di valutare il contesto. I cartelli si realizzano infatti con maggiore frequenza quando i mercati interessati hanno alcune caratteristiche: pochi concorrenti o concorrenti caratterizzati da analoga efficienza e dimensione; riguardano prodotti omogenei; c'è una perdurante partecipazione alle gare delle stesse imprese; l'appalto è ripartito in più lotti dal valore economico simile.

All'interno di questa cornice generale costituiscono segnali di comportamenti anomali:

a) Boicottaggio della gara

I principali sintomi del boicottaggio, finalizzato a prolungare il contratto con il fornitore abituale o a ripartire *pro* quota il lavoro o la fornitura tra tutte le imprese interessate, sono: 1) nessuna offerta presentata; 2) presentazione di un'unica offerta o di un numero di offerte comunque insufficiente

per procedere all'assegnazione dell'appalto; 3) presentazione di offerte dello stesso importo, soprattutto quando le procedure di gara prevedono in queste circostanze l'annullamento della gara o la ripartizione dell'appalto *pro* quota.

b) Offerte di comodo

Le offerte di comodo danno un'apparente regolarità concorrenziale alla gara e nascondono l'innalzamento dei prezzi di aggiudicazione. I principali sintomi sono: 1) offerte presentate dalle imprese che non si aggiudicano l'appalto caratterizzate da importi palesemente troppo elevati o comunque superiori a quanto le stesse imprese hanno offerto in analoghe procedure; 2) offerte contenenti condizioni particolari e notoriamente inaccettabili per la stazione appaltante che ne determinano l'esclusione; 3) la presentazione di offerte più elevate rispetto ai prezzi di listino. In generale una sequenza di gare in cui risulta aggiudicataria sempre la stessa impresa può destare il sospetto che i concorrenti presentino offerte di comodo.

c) Subappalti o ATI (Associazione Temporanea d'Imprese)

I subappalti e le Associazioni Temporanee di Imprese (ATI) permettono di ampliare la platea dei soggetti che possono partecipare a meccanismi di gara, dando spazio anche alle imprese più piccole. In alcuni casi possono però essere utilizzati dai partecipanti alla gara per spartirsi il mercato o addirittura della singola commessa. Possibili indizi sono: 1) imprese, singolarmente in grado di partecipare a una gara, che invece si astengono in vista di un successivo subappalto o optano per la costituzione di un'ATI; 2) la costituzione di ATI o subappalto perfezionati da imprese accomunate dalla stessa attività prevalente; 3) il ritiro dell'offerta da parte di un'impresa che decide inizialmente di partecipare a una gara, che risulta poi beneficiaria di un subappalto relativo alla medesima gara; 4) nei casi di aggiudicazione basata sull'offerta economicamente più vantaggiosa, l'ATI (tra i maggiori operatori) può essere il frutto di una strategia escludente, tesa ad impedire a imprese minori di raggiungere il necessario punteggio qualitativo.

d) Rotazione delle offerte e ripartizione del mercato

Anche l'analisi della sequenza delle aggiudicazioni può segnalare la presenza di un cartello. Quando la pratica spartitoria interessa un singolo committente quest'ultimo avrà indizi per riconoscere 'regolarità' sospette nella successione temporale delle imprese aggiudicatarie o nella ripartizione in lotti delle vincite. Le regolarità sospette potrebbero riguardare non solo il numero di aggiudicazioni ma anche la somma dei relativi importi.

e) Modalità 'sospette' di partecipazione all'asta

Può accadere che gli aderenti ad un cartello presentino le domande di partecipazione all'asta con modalità tali da tradire la comune formulazione. E' questo il caso di: 1) comuni errori di battitura; 2) stessa grafia; 3) riferimento a domande di altri partecipanti alla medesima gara; 4) analoghe stime o errori di calcolo; 5) consegna contemporanea, da parte di un soggetto, di più offerte per conto di differenti partecipanti alla medesima procedura di gara.

GPDP

I *social network*

I *social network* (Facebook, MySpace e altri) sono "piazze virtuali", cioè dei luoghi in cui via Internet ci si ritrova portando con sé e condividendo con altri fotografie, filmati, pensieri, indirizzi di amici e tanto altro. I *social network* sono lo strumento di condivisione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli

individui coinvolti. I primi *social network* sono nati in ambito universitario, tra colleghi che non si volevano "perdere di vista", che desideravano "fare squadra" una volta entrati nel mondo del lavoro. Facebook, per citare uno dei più famosi, agli inizi era esattamente la traduzione virtuale del "libro delle fotografie" della scuola, dell'annuario. Una bacheca telematica dove ritrovare i colleghi di corso e scambiare con loro informazioni. Gli ultimi sviluppi spingono i *social network* a integrarsi sempre più con i telefoni cellulari, trasformando i messaggi che pubblichiamo *on-line* in una sorta di sms multiplo che giunge istantaneamente a tutti i nostri amici.
Gli strumenti predisposti dalle reti sociali ci permettono di seguire i familiari che vivono in un'altra città. Espandono la nostra possibilità di comunicare, anche in ambito politico e sociale trasformandoci in agenti attivi di campagne a favore di quello in cui crediamo. Possono facilitare lo scambio di conoscenze tra colleghi, e tra colleghi e impresa. I *social network* sono strumenti che danno l'impressione di uno spazio personale, o di piccola comunità. Si tratta però di un falso senso di intimità che può spingere gli utenti a esporre troppo la propria vita privata, a rivelare informazioni strettamente personali, provocando "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati.

Il Garante e le tutele su internet

Il Garante per la protezione dei dati personali segue con attenzione gli sviluppi delle forme di comunicazione su Internet ed è impegnato a livello europeo e internazionale per definire regole e comportamenti che tutelino gli utenti e le libertà individuali. La forma di tutela più efficace è comunque sempre l'autotutela, cioè la gestione attenta dei propri dati personali.

Per sempre…o quasi

Quando inserisci i tuoi dati personali su un sito di *social network*, ne perdi il controllo. I dati possono essere registrati da tutti i tuoi contatti e dai componenti dei gruppi cui hai aderito, rielaborati, diffusi, anche a distanza di anni. A volte, accettando di entrare in un *social network*, concedi all'impresa che gestisce il servizio la licenza di usare senza limiti di tempo il materiale che inserisci *on-line*… le tue foto, le tue chat, i tuoi scritti, i tuoi pensieri.

Disattivazione o cancellazione?

Se decidi di uscire da un sito di *social network* spesso ti è permesso solo di "disattivare" il tuo profilo, non di "cancellarlo". I dati, i materiali che hai messo *on-line*, potrebbero essere comunque conservati nei server, negli archivi informatici dell'azienda che offre il servizio. Leggi bene cosa prevedono le condizioni d'uso e le garanzie di *privacy* offerte nel contratto che accetti quando ti iscrivi.

Le leggi applicate

La maggior parte dei siti di social network ha sede all'estero, e così i loro server. In caso di disputa legale o di problemi insorti per violazione della *privacy*, non sempre si è tutelati dalle leggi italiane ed europee.

Chi può fare cosa

Il miglior difensore della tua *privacy* sei tu. Rifletti bene prima di inserire *on-line* dati che non vuoi vengano diffusi o che possano essere usati a tuo danno. Segnala al Garante le eventuali violazioni affinché possa intervenire a tua tutela.

La *privacy* degli altri

Quando metti *on-line* la foto di un tuo amico o di un familiare, quando lo tagghi (inserisci, ad esempio, il suo nome e cognome su quella foto), domandati se stai violando la sua *privacy*. Nel dubbio chiedi il consenso.

La logica degli altri

Le aziende che gestiscono i *social network* generalmente si finanziano vendendo pubblicità mirate. Il valore di queste imprese è strettamente legato anche alla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni a chi ne ha bisogno.

Autogoverno

Pensa bene prima di pubblicare tuoi dati personali (soprattutto nome, indirizzo, numero di telefono) in un profilo-utente, o di accettare con disinvoltura le proposte di amicizia.

Pensarci prima

Ricorda che immagini e informazioni possono riemergere, complici i motori di ricerca, a distanza di anni.

Rispettare gli altri

Astieniti dal pubblicare informazioni personali e foto relative ad altri senza il loro consenso. Potresti rischiare anche sanzioni penali.

Cambiare *login* e *password*

Usa *login* e *password* diversi da quelli utilizzati su altri siti *web*, sulla posta elettronica e per la gestione del conto corrente bancario *on-line*.

Pseudonimi

Se possibile crea pseudonimi differenti in ciascuna rete cui partecipi. Non mettere la data di nascita o altre informazioni personali nel *nickname*.

Essere informati

Informati su chi gestisce il servizio e quali garanzie offre rispetto al trattamento dei dati personali. Ricorda che hai diritto di sapere come vengono utilizzati i tuoi dati: cerca sotto *privacy* o *privacy policy*.

Livelli di *privacy*

Utilizza impostazioni orientate alla *privacy*, limitando al massimo la disponibilità di informazioni, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca. Controlla come sono impostati i livelli di *privacy* del tuo profilo: chi ti può contattare, chi può leggere quello che scrivi, chi può inserire commenti alle tue pagine, che diritti hanno gli utenti dei gruppi ai quali appartieni.