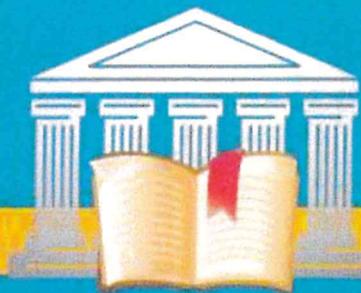


TeLex Anie

NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI



Segnalazioni giuridiche a cura
del Servizio Centrale Legale

N. 10 Anno XXII
Ottobre 2017

I CRITERI DI AGGIUDICAZIONE DOPO IL CORRETTIVO: LE ULTIME INDICAZIONI OPERATIVE DELL'AUTORITÀ

Il tema dei criteri di aggiudicazione è stato uno degli argomenti più discussi sia in occasione dell'entrata in vigore del Codice dei contratti pubblici (D.Lgs. 50/2016), sia a seguito della pubblicazione del Decreto correttivo al Codice dei contratti pubblici (D.Lgs. 56/2017).

Questo perché il nuovo Codice supera l'impostazione della previgente normativa, che stabiliva una piena equivalenza tra il criterio del prezzo più basso e quello dell' O.E.P.V., arrivando ad accordare a quest'ultimo criterio (O.E.P.V.) una netta preferenza.

Il nuovo Codice infatti stabilisce che in via generale il criterio prevalente per l'aggiudicazione è quello del miglior rapporto qualità prezzo (art. 95, co.2).

Oltre ad accordare tale preferenza al criterio di cui sopra, il Legislatore del 2016 si è spinto oltre, prevedendo al comma 3 dell'art. 95 alcune ipotesi tassative al ricorrere delle quali l'utilizzo del criterio dell'offerta economicamente più vantaggiosa è addirittura obbligatorio.

Conseguentemente l'aggiudicazione al minor prezzo diventa criterio residuale e circoscritto a determinate ipotesi previste al comma 4 dell'art. 95, peraltro – a testimonianza del favor del Legislatore nei confronti del criterio dell'O.E.P.V. – il ricorso al criterio del minor prezzo non è nemmeno obbligatorio stante la formulazione della norma che prevede: "Può essere utilizzato il criterio del minor prezzo".

Lo schema individuato dal Codice del 2016 non viene stravolto dall'entrata in vigore del decreto correttivo, tuttavia quest'ultimo introduce alcune significative modifiche sia in tema di offerta economicamente più vantaggiosa che relativamente al criterio del minor prezzo.

In tema di offerta economicamente più vantaggiosa la modifica più significativa operata dal correttivo riguarda l'introduzione del comma 10-bis, a norma del quale è previsto un tetto massimo al punteggio attribuibile per l'elemento prezzo, che viene stabilito in 30 punti.

La previsione del tetto può certamente dirsi un'ulteriore conquista per gli operatori economici dei settori altamente specializzati, che da sempre lottano per l'introduzione dell'obbligo dell'utilizzo dell'OEPV come criterio di aggiudicazione.

Significativa anche la modifica apportata dal correttivo al comma 4, lett. a), che ha innalzato, per i lavori, da 1 mln a 2 mln di euro la soglia al di sotto della quale è possibile aggiudicare le offerte con il criterio del minor prezzo, ponendo tuttavia come condizione che

l'affidamento dei lavori avvenga "con procedura ordinaria" e sulla base del progetto esecutivo.

La previsione normativa emendata recita: "fermo restando quanto previsto dall'articolo 36, comma, 2 lettera d), per i lavori di importo pari o inferiore a 2 mln di euro, quando l'affidamento dei lavori avviene con procedure ordinarie, sulla base del progetto esecutivo".

La formulazione ha, sin da subito, generato forti dubbi interpretativi in quanto sembrava condizionare la possibilità del ricorso al massimo ribasso all'utilizzo di "procedure ordinarie" (tagliando fuori tutte le procedure negoziate a inviti) anche per l'assegnazione di opere di importo inferiore al milione di euro tanto da spingere il MIT a chiedere un chiarimento interpretativo all'ANAC.

L'Autorità ha risolto il dubbio interpretativo, nel senso auspicato sia dagli enti appaltanti che dalle imprese, stabilendo che alla luce della finalità della disposizione, che è quella di semplificare le procedure, si potranno continuare ad aggiudicare gli appalti al di sotto di 1 mln di euro anche attraverso l'utilizzo di procedure semplificate.

L'Autorità infatti chiarisce che il rinvio reciproco operato dall'articolo 95, comma 4 e dall'articolo 36, comma 2, lettera d) serve a ribadire che sopra il milione di euro si applicano le procedure di scelta del contraente di cui agli articoli 59 e seguenti, in quanto l'innalzamento della soglia è stato previsto dal Legislatore soltanto per derogare all'utilizzo del criterio dell'offerta economicamente più vantaggiosa, in favore dell'utilizzo del criterio del minor prezzo, per gli affidamenti ricompresi tra un milione e due milioni di euro.

Servizio Centrale Appalti ANIE

LEGISLAZIONE OSSERVATORIO

INTERNET OF THINGS: ASPETTI LEGALI

L'espressione Internet of Things (letteralmente "internet delle cose") è stata utilizzata per la prima volta nel 1999 da K. Ashton, ricercatore presso il Massachusetts Institute of Technology, per descrivere l'interconnessione tra gli oggetti che, attraverso appositi sensori, si connettono alla rete internet, trasferendo dati (e, quindi, informazioni) attraverso un proprio indirizzo IP che ne consente l'individuazione univoca. Ogni settore della vita quotidiana è coinvolto nel suddetto processo connettivo ed il fenomeno è destinato ad amplificarsi in maniera esponenziale: si stima, infatti, che entro il 2020, nel mondo ci saranno almeno tra i 40 e i 50 miliardi di oggetti in grado di interfacciarsi attraverso la rete. In effetti molti esempi sono sotto gli occhi di tutti: si parte dalla domotica (con termostati, serrature, lampade che si comandano con un tocco sullo smart phone, elettrodomestici di ogni tipologia e dimensione, ecc.) passando per i cosiddetti wearables (orologi, occhiali, ecc.) sino ad arrivare ad ogni possibile declinazione già da tempo messa in atto in ambito aziendale. Entro breve, inoltre, intere città saranno completamente cablate ed intrise di sensori di ogni genere, anche (ma non solo) per permettere la piena implementazione dei self driving vehicles: da qualche anno sono in atto le sperimentazioni sulle automobili, ma esempi già pienamente operativi e funzionanti si possono rinvenire nei servizi di trasporto pubblico (treni, metropolitane, ecc.) delle città più evolute. Come è facile intuire, l'enorme quantità di dati

che vengono scambiati tra gli oggetti e, quindi, necessariamente tra i titolari del trattamento dei dati, preposti alla gestione delle relative informazioni, oltre a costituire un patrimonio enorme in termini di abitudine e profilazione degli utenti, comporta, inevitabilmente, la necessità di valutare gli aspetti legali sottesi e, spesso, non sufficientemente tenuti in debita considerazione dalle aziende che forniscono prodotti e servizi smart.

Nel settembre 2016, infatti, il Global Privacy Enforcement Network (GPEN) ha rilevato la grave carenza nella tutela della privacy degli utenti di due terzi dei dispositivi oggetto del sondaggio. Non è necessario volgere lo sguardo ai colossi oltre oceano per comprendere che le suddette criticità riguardano anche le piccole e medie aziende e ciò per ovvie ragioni: la quantità di dati scambiati è ormai tale, anche nei processi più semplici, da rappresentare una risorsa incredibile in termini di informazioni commerciali, grazie all'acquisizione dei dati personali anche sensibili (o "particolari" in base alla nuova definizione contenuta del Regolamento EU 2016/679 sulla protezione dei dati, applicabile dal prossimo maggio). Molte aziende, anche indipendentemente dal fatto che ciò rappresenti o meno il proprio core business, sono oggi impegnate, più o meno consapevolmente, nel c.d. data mining, l'operazione che consiste nell'estrazione e nell'esame di grandi quantità di dati anche attraverso software sempre meno costosi ed in grado di analizzare ed interpretare le abitudini degli utenti al fine di veicolare un'offerta commerciale sempre più personalizzata (c.d. profilazione). Già nel 2014, il "Gruppo di lavoro articolo 29" (organismo europeo preposto ad assicurare che le autorità varie garanti si uniformino nell'applicazione della normativa sulla privacy) ha evidenziato le varie problematiche relative alla diffusione dell'Internet of Things, quelle riguardanti la gestione del flusso dei dati, la perdita degli stessi, la conservazione oltre i termini necessari per le finalità per cui sono raccolti e, non da ultimo, la corretta informazione agli interessati ed la possibilità di essere anonimi. In particolare, le questioni fondamentali concernono:

- l'assenza di controllo sui dati generati dai dispositivi connessi;
- l'inadeguata informativa sul consenso richiesto all'interessato in relazione ai dispositivi connessi e l'eventualità che il consenso sia stato prestato per scopi diversi da quelli che emergono attraverso l'analisi dei dati sottesi;
- la carenza di controllo sulle informazioni relative alle abitudini e le preferenze degli interessati a seguito dell'aggregazione automatica dei dati;
- l'assenza di possibilità di rimanere anonimi e, infine, i rischi legati alla sicurezza fisica degli interessati.

A fronte delle suddette criticità, il Gruppo di lavoro ha elaborato delle linee guida per i soggetti coinvolti nel processo, valide anche alla luce della nuova normativa. Affinché il trattamento sia legittimo, primaria importanza è stata riconosciuta al consenso al trattamento dei dati: deve risultare evidente la volontà espressa dell'interessato. I titolari inoltre devono rendere semplice ed immediata la revoca del suddetto consenso. In alternativa, il trattamento deve essere necessario per l'esecuzione del contratto e tale requisito è da interpretarsi in senso restrittivo: è richiesto che ci sia un collegamento diretto tra il trattamento dei dati e lo scopo del contratto. Da ultimo, gli interessi meramente economici dei titolari non sono idonei a legittimare in trattamento dei dati in assenza delle predette eventualità (consenso o trattamento necessario per l'esecuzione del contratto). Stabilita la legittimità del trattamento, i dati devono essere trattati in ottemperanza ai principi di correttezza e conformità alla normativa e ciò implica che:

- i dati possono essere raccolti solo per finalità espressamente specificate e preventivamente individuate dai titolari;
- devono essere raccolti solo i dati necessari e per una durata minima in relazione allo scopo (ciò comporta che debbano essere cancellati non appena il contratto si estingue);
- il trattamento dei dati sensibili deve avvenire solo previo consenso dell'interessato;
- i titolari devono fornire un'adeguata informativa agli interessati, mantenere un livello di sicurezza adeguato per la protezione dei dati e garantire agli interessati il diritto all'accesso, alla rettifica ed alla cancellazione dei dati;
- la valutazione di impatto preventiva (DPIA) deve essere svolta prima del lancio di qualunque applicazione;
- i dati grezzi devono essere eliminati non appena i dati necessari al trattamento sono stati estratti;
- l'adeguamento alla normativa sulla privacy deve avvenire sin dalla fase di progettazione (privacy by design) e la tutela della protezione del dato deve diventare l'impostazione predefinita affinché siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default);
- gli utenti devono avere il pieno controllo dei propri dati.

I produttori di dispositivi, i programmatori e, in generale, tutti i soggetti coinvolti nel processo IOT sono inoltre tenuti, tra le altre cose, a:

- fornire agli utenti informazioni sulle tipologie dei dati raccolti, su quali dati vengono trasmessi ai sensori, e su come tali dati saranno da processati e combinati;

- disabilitare le interfacce wireless quando non utilizzate;
- fornire all'utente strumenti per selezionare i dati che verranno trasferiti al titolare;
- garantire all'utente il diritto di accesso ai dati e l'abilità a trasferirli;
- notificare agli utenti le falle di sicurezza non appena scoperte.

Oltre a tutto quanto sopra, rimarranno valide ed applicabili tutte le norme del Regolamento, incluse le elevate sanzioni ivi previste in caso di inottemperanza.

*Avv. Giacomo Gori
Cocuzza & Associati, Studio Legale*

corretto trattamento dei dati in ambito professionale (*Opinion on data processing at work 2/17- 8 June 2017 - Article 29 Data Protection Working Party*).

■ **DIRITTO AL RISPETTO DELLA VITA PRIVATA, DELLA LIBERTÀ E DIGNITÀ DEL LAVORATORE.** Principio fondamentale è quello per cui ogni lavoratore, indipendentemente dal tipo di contratto a lui applicato, ha diritto al rispetto della vita privata, della sua libertà e dignità; ogni lavoratore deve essere adeguatamente informato sulle modalità di trattamento dei dati personali in maniera chiara, semplice ed esauriva, soprattutto qualora siano previste forme di controllo del lavoratore, che comunque dovranno essere rispettose anche delle norme nazionali.

■ **PROPORZIONE TRA CONTROLLO E FINALITÀ.** Ogni trattamento deve essere proporzionato alla finalità perseguita e deve essere limitato quanto più possibile l'uso dei dati personali. In applicazione del predetto principio, con riguardo agli strumenti di geolocalizzazione, ad esempio, i Garanti europei segnalano che possono essere utilizzati per finalità strettamente aziendali e al lavoratore deve essere lasciata la possibilità di disattivare, se necessario, il localizzatore (come i gps).

■ **CONTROLLI DELLA POSTA ELETTRONICA E INTERNET.** E' legittimo introdurre strumenti e tecnologie 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.

■ **SOCIAL NETWORK.** 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.

■ **OFFERTA DI SPAZI PRIVATI SU COMPUTER AZIENDALI E SERVIZI CLOUD.** 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 dedicate 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.

■ **IL CONSENSO DEI LAVORATORI NON È SUFFICIENTE PER LEGITTIMARE IL TRATTAMENTO.** Il consenso al trattamento, per

PRIVACY

PRIVACY E RAPPORTO DI LAVORO. LE LINEE GUIDA DEI GARANTI EUROPEI

Maggio 2018 è sempre più vicino e, da settembre, le aziende e le pubbliche amministrazioni, se non già fatto, dovranno lavorare alacremente per mettersi in regola con il Regolamento sulla Privacy.

Si segnala quindi un documento dei Garanti europei della privacy riuniti nel Gruppo "Articolo 29" (WP29) che, tenendo conto sia della normativa vigente sia delle novità introdotte dal Regolamento UE 2016/679, definisce un quadro dei principi fondamentali per il

essere considerato valido, deve essere libero. Partendo da tale assunto, i Garanti hanno evidenziato che, stante la disparità di potere tra le due parti del contratto di lavoro (datore di lavoro e dipendente) per le aziende ed enti pubblici non sarà sufficiente acquisire il consenso dei dipendenti per il trattamento dei loro dati. I Garanti suggeriscono, quindi, di valutare, quale base legale del trattamento, il ricorso a disposizioni normative o contrattuali oppure di far valere il proprio “legittimo interesse” (esempio: diritto alla sicurezza), in un rapporto comunque di bilanciamento con i diritti e le libertà dei lavoratori alla luce dei principi di necessità e proporzionalità. Oltre che *libero*, il consenso dovrà, naturalmente, essere *informato*. Ancora una volta, quindi, sono e saranno importanti le **policy aziendali**.

*Avv. Damiana Lesce, Avv. Valeria De Lucia e
Avv. Paola Lonigro
Trifirò & Partners Avvocati*

NON ESISTE DIRITTO ALL'OBLIO PER I DATI PERSONALI PRESENTI NEL REGISTRO DELLE IMPRESE

L'utilizzo sempre più diffuso delle banche dati, con relativa elaborazione e comunicazione a terzi di informative reperite da agenzie di servizi, a fronte della consultazione dei Registri delle Imprese, pone in primo piano il tema di garantire, da una parte, l'interesse ed il diritto di terzi a conoscere atti e fatti importanti della vita delle società di capitali iscritte nei predetti Registri e, dall'altro, la tutela dei dati personali, soprattutto con riferimento alle circostanze risalenti nel tempo, è di attualità.

Il caso in esame prende spunto da un'azione civile promossa dall'amministratore di una Società, che aveva vinto un appalto per la costruzione di un complesso turistico in Italia. Realizzate le unità immobiliari, le stesse rimanevano invendute ed in proposito l'amministratore lamentava che ciò sarebbe stato determinato dal fatto che, presso il Registro delle Imprese della Camera di Commercio competente, risultava ancora annotata nel 2007 (anno dei fatti) la circostanza che lo stesso era stato amministratore e liquidatore di una precedente società, dichiarata fallita nel 1992 e poi cancellata dai registri nel 2005.

In altre parole, l'attore lamentava che pur essendo decorsi oltre quindici anni dal fallimento e due anni dalla cancellazione, la Camera di Commercio aveva ommesso di rimuovere i dati riguardanti la sua pregressa posizione di amministratore e liquidatore di una precedente azienda fallita. Questo avrebbe consentito a società specializzate nella raccolta ed elaborazione di informazioni di mercato, di reperire ed utilizzare detta informativa, pregiudicando le trattative in corso per la

vendita degli immobili, con lesione dell'immagine personale e commerciale dell'interessato. Per tali ragioni veniva avviata la causa avanti il Tribunale di Lecce contro la Camera di Commercio coinvolta, con richiesta, tra l'altro, di risarcimento danni determinati dalla mancata “anonimizzazione” dei dati che lo collegavano al citato fallimento. La tesi dell'attore veniva accolta dal Tribunale, motivando che - decorso un tempo congruo e cancellata ormai la società dal Registro delle Imprese - non vi fosse necessità di mantenere nel predetto Registro i dati personali dell'interessato, trattandosi di informazioni di dubbia utilità, stante il periodo trascorso.

Avverso la decisione del Tribunale è stato proposto ricorso avanti la Suprema Corte di Cassazione, investita quindi del quesito inerente l'esistenza o meno di un obbligo di cancellare o rendere anonimi, a richiesta di parte, i dati personali conservati - per obbligo legislativo - dalla Camera di Commercio nel Registro delle Imprese, allorché sia decorso un lasso di tempo ritenuto congruo.

I Giudici di Legittimità dopo una disamina della questione, hanno rimesso la vertenza avanti alla Corte di Giustizia Europea, sotto due questioni principali: a) la verifica della compatibilità con la normativa europea in materia di privacy dell'impianto di pubblicità obbligatoria e di ordine pubblico previsto dalla normativa italiana, attuato con il sistema del Registro delle Imprese; laddove tale sistema prevede che chiunque, senza limiti di tempo, possa conoscere i dati relativi alle persone fisiche ivi risultanti; b) l'applicazione della prima direttiva 68/151/CEE del 9 marzo 1968 (e successive modificazioni) ed in particolare la verifica se detta direttiva lasci la possibilità per una limitazione temporale/soggettiva della disponibilità dei dati, in modo che i medesimi non siano oggetto di pubblicità illimitata, ma semmai disponibili solo per un tempo limitato o nei confronti di portatori di specifici interessi.

La Corte di Giustizia dell'Unione Europea, con sentenza del 9 marzo 2017 Causa 398/15, ha dato innanzitutto rilevanza al principio che la pubblicità dei dati delle società e dei loro amministratori, imposta dalla normativa e realizzata attraverso il Registro delle Imprese, ha la funzione di garantire la certezza dei diritti nelle relazioni tra società di capitali e terzi, nonché di tutelare i diritti di questi ultimi, posto che la società di capitali offrono come unica garanzia il proprio patrimonio sociale. In tale contesto, peraltro, la Corte sottolinea che, anche dopo molti anni dalla cessazione dell'attività di una società, possono sorgere questioni per le quali è necessario disporre dei dati delle persone fisiche, contenute nel Registro delle Imprese.

Quanto sopra considerando sia la molteplicità di diritti e rapporti giuridici di una società, che coinvolgono una moltitudine di soggetti anche residenti in diversi Stati

membri; sia la diversità nei termini di prescrizione previsti dai molteplici ordinamenti nazionali; cosicché decorso il quale non sarebbe più necessaria la permanenza di determinate informative nel Registro e la relativa pubblicità delle stesse.

Sulla base di queste considerazioni gli Stati membri non sono obbligati a garantire alle persone fisiche (i cui dati sono scritti nel Registro delle Imprese) un diritto ad ottenere, trascorso un certo lasso di tempo, la cancellazione dei dati personali che li riguardano. In altre parole, rispetto al diritto dei singoli alla cosiddetta privacy, deve prevalere la tutela dell'interesse dei terzi alla trasparenza e al buon funzionamento del mercato interno, cosicché le persone fisiche che ricoprono incarichi presso società di capitali - in quanto agiscono per il loro tramite - debbono essere consapevoli dell'obbligo di rendere pubbliche determinate informative.

Non riconosciuto, in sostanza, il "diritto all'oblio", la Corte non esclude che in situazioni particolari, trascorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società, l'accesso ai dati personali contenuti nel Registro delle Imprese possa essere circoscritto a chi dimostri avere un interesse specifico alla loro consultazione.

Tuttavia, per ottenere un simile risultato, occorre una specifica disciplina normativa, che introduca nell'ordinamento giuridico una tale limitazione.

Nel caso sottoposto alla Corte, la stessa non ha ritenuto che la doglianza formulata dall'amministratore - relativa ad un pregiudizio nella vendita di immobili imputabile alla circostanza che i potenziali acquirenti avessero avuto accesso ai dati dello stesso amministratore presenti nel Registro delle Imprese - fosse sufficiente a giustificare la cancellazione di tali dati o l'inibizione dell'accesso ai medesimi. In conclusione, l'indicazione che si ricava dalla sentenza è di riconoscimento, in via normale, della prevalenza della tutela degli interessi dei terzi alla trasparenza; tuttavia non si esclude la possibilità (attraverso specifici atti normativi) di regolamentare in modo più restrittivo l'accesso di particolari situazioni che ogni Stato può valutare. Da ciò si desume che la tematica deve considerarsi tutt'altro che chiusa, con spazio per possibili evoluzioni normative.

Avv. Vittorio Provera
Trifirò & Partners Avvocati

DIRETTORE RESPONSABILE

Maria Antonietta Portaluri

REDAZIONE

Alessandra Toncelli – Mirella Cignoni – Mattia Ciribifera

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Dott. Ennio Piovesani, BBM Partners, Buffa, Bortolotti & Mathis (Torino) - Avv. Giacomo Gori, Cocuzza & Associati, Studio Legale (Milano) - Avv. Giorgio Candeloro, Avv. Alessandro Di Giò, Avv. Giuseppe Mastrantonio, Freshfields Bruckhaus Deringer (Milano) - Avv. Valeria M. Affer, Avv. Duilia Delfino, L&TS Network (Milano) - Avv. Damiana Lesce, Avv. Valeria De Lucia, Avv. Paola Lonigro, Avv. Vittorio Provera, Trifirò & Partners Avvocati (Milano).

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

TeLex Anie



FEDERAZIONE NAZIONALE
IMPRESE ELETTROTECNICHE
ED ELETTRONICHE



Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it