TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 9 Anno XXIV Settembre 2019

INDICE:

APPALTI PUBBLICI

RTI: L'OFFERTA DEVE ESSERE SOTTOSCRITTA DA TUTTI I PARTECIPANTI AL RAGGRUPPAMENTO
Consiglio di Stato, Sez. V, 20/08/2019, n. 5751

Veniva dedotta dall'impresa appellante l'inammissibilità dell'offerta tecnica e di quella economica presentata dal RTI aggiudicatario in quanto le stesse venivano sottoscritte dal legale rappresentate della sola impresa mandataria.

Il Consiglio di Stato, in accoglimento del ricorso, chiarisce il palese contrasto della fattispecie con la disciplina di cui all'art. 48, co. 8, che in tema di RTI impone – in caso di RTI costituendo – l'obbligatoria sottoscrizione dell'offerta da parte di tutti i componenti.
L'art. 48, co. 8, recita: "*È consentita la presentazione di offerte da parte dei soggetti di cui all'articolo 45, comma 2, lettere d) ed e), anche se non ancora costituiti. In tal caso* ***l'offerta deve essere sottoscritta da tutti gli operatori economici che costituiranno i raggruppamenti*** *temporanei o i consorzi ordinari di concorrenti*".
Nello svolgimento della gara veniva commessa un'ulteriore illegittimità da parte della Stazione Appaltante – anch'essa oggetto di pronuncia da parte del Consiglio di Stato – quest'ultima infatti permetteva al RTI aggiudicatario di sanare la carenza di sottoscrizione attraverso lo strumento del soccorso istruttorio.
Come noto tale strumento, ai sensi dell'art. 83, co.9, è utilizzabile per sanare: "*le carenze di qualsiasi elemento formale della domanda (...). In particolare, in caso di mancanza, incompletezza e di ogni altra irregolarità essenziale degli elementi del documento di gara unico europeo di cui all'articolo 85,* ***con esclusione di quelle afferenti l'offerta economica e quella tecnica****, (...).*"

Nell'accogliere il ricorso in appello il Consiglio di Stato chiarisce il principio per cui: "*nelle gare pubbliche la sottoscrizione dell'offerta da parte di tutti i soggetti, che con essa pretendono di impegnarsi nei confronti dell'amministrazione appaltante, risponde a imprescindibili esigenze di ordine generale di certezza della riconducibilità dell'offerta ai medesimi operatori e coercibilità dei relativi impegni nella successiva fase esecutiva, esigenze che non possono ritenersi adeguatamente soddisfatte mediante il mandato con rappresentanza conferito all'impresa capogruppo*".

Nella successiva fase esecutiva, quando il RTI sarà formalmente costituito, al mandatario spetterà la rappresentanza esclusiva, anche processuale, dei mandanti nei confronti della stazione appaltante per tutte le operazioni e gli atti di qualsiasi natura dipendenti dall'appalto.

Quanto affermato chiarisce un'ulteriore questione strettamente connessa con il ruolo ed i compiti della mandataria di un RTI (costituito): **la sottoscrizione dei contratti di subappalto**.
Sul punto infatti costante giurisprudenza (*ex multis* CdS, Sez. V, n. 5906/007) afferma il principio per cui l'**RTI è l'unico centro di imputazione** dei rapporti anche per quanto riguarda i contratti di subappalto e subfornitura stipulati in esecuzione del contratto principale.

Ne consegue che il **potere** contrattuale di sottoscrivere contratti di subappalto deve essere **riconosciuto esclusivamente in capo all'impresa mandataria**, in quanto detto contratto deve intendersi sottoscritto in nome e per conto del RTI e non, eventualmente, della mandate cui lo specifico contratto di subappalto si riferisce.

Servizio Centrale Appalti ANIE

LEGISLAZIONE OSSERVATORIO

SICUREZZA CIBERNETICA E *GOLDEN POWER* – UN NUOVO DECRETO LEGGE ADOTTATO DAL GOVERNO

Il Consiglio dei Ministri, nella riunione del 19 settembre, ha approvato il Decreto legge n. 105/2019 (pubblicato in G.U. il 21 settembre – il ***Decreto***), che introduce disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, oltre ad apportare alcune modifiche alla normativa in materia di c.d. **Golden Power**.

Il Decreto mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, sia pubblici sia privati, mediante **inter alia**:

- l'istituzione di un perimetro di sicurezza nazionale cibernetica, definendo le modalità di individuazione dei soggetti che ne fanno parte, nonché delle rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica;
- la previsione di misure idonee a garantire i necessari **standard** di sicurezza rivolti a minimizzare i rischi;
- la previsione di un meccanismo teso ad assicurare un'attività di procurement più sicura per i soggetti inclusi nel perimetro che procedano all'affidamento di forniture di beni e servizi di **information and communication technology** (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti.

Inoltre, il testo integra il quadro normativo in materia di esercizio dei poteri speciali da parte del Governo, con riguardo a quanto previsto dal Decreto legge n. 21 del 15 marzo 2012 (legislazione in materia di **Golden Power**), in particolare per:

- coordinare l'attuazione del Regolamento (UE) 2019/452, che ha recentemente introdotto un quadro comunitario sul controllo nazionale degli investimenti esteri;

- prevedere che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato valutando gli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa sopra richiamata;
- con riferimento alle autorizzazioni già rilasciate ai sensi del decreto-legge 15 marzo 2012, n. 21, la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi standard; nonché
- stabilire o chiarire che una notifica ai sensi della disciplina **Golden Power** sia dovuta in relazione all'acquisizione di controllo da parte di soggetti extra-UE di infrastrutture o tecnologie critiche, ad oggi menzionate nel Decreto legge n. 21 del 15 marzo 2012 ma per le quali il regolamento di attuazione, atteso per definirne nel dettaglio l'ambito di applicazione, non è stato ancora adottato.

Pare il caso di sottolineare che fra queste infrastrutture critiche siano comprese, ai sensi del citato Decreto legge n. 21/2012, quelle "**finanziarie**". Ed invero, secondo l'interpretazione offerta da vari commentatori, il Decreto è stato adottato, a questo specifico riguardo, per garantire di assoggettare al regime dei **Golden Power** (ovvero per evitare dubbi al riguardo) le infrastrutture dei mercati finanziari italiani, di recente indirettamente coinvolti in vicende connesse ad una offerta di acquisizione del London Stock Exchange da parte della borsa di Hong Kong.

Il Decreto entrerà in vigore il 6 ottobre 2019.

Avv. Filippo Alberti
Freshfields Bruckhaus Deringer

I. Il GDPR non si applica nel caso di videoriprese relative a soggetti non identificabili, né direttamente né indirettamente.

ESEMPI PRATICI:

a. Non si applica se le **telecamere sono finte o se non sono collegate**.
   N.B. È importante notare che anche nel caso di telecamere finte o non collegate si potranno presentare dei profili relativi alla tutela del lavoratore come sancito dallo Statuto dei lavoratori.
b. Non si applica, nel caso di **riprese da un'altitudine elevata**, se i dati non possono essere collegati ad una persona precisa;
c. Non si applica nel caso di **videocamere integrate nelle auto per il parcheggio** se queste sono settate in un modo tale da non riprendere informazioni relative a persone, come ad esempio le targhe o i passanti;

II. "Household exception" – "Eccezione domestica": le garanzie previste dal GDPR non si applicano nel caso in cui le telecamere riprendano esclusivamente attività domestiche e luoghi privati e non riprendano, anche parzialmente, uno spazio pubblico.

ESEMPI PRATICI:

a. Un turista registra un video delle sue vacanz**e** con il cellulare e con una videocamera personale e lo mostra solo ad amici e famiglia, ma non lo mette a disposizione di un numero indeterminato di persone (ad es. caricandolo su YouTube): NON SI APPLICA IL GDPR;
b. Una persona installa una videocamera di sorveglianza che riprende esclusivamente il proprio giardino: NON SI APPLICA IL GDPR;

III. Non è sufficiente affermare che le telecamere sono installate per motivi di "sicurezza": bisogna sempre specificare la base legittimante il trattamento dei dati analizzati tramite la videosorveglianza.

Anche se in teoria si applicano tutte le condizioni di liceità stabilite all'articolo 6 (1) del GDPR, quelle che risultano più applicate nella prassi sono il legittimo interesse (art. 6.1. lett. f) e l'esecuzione di un compito di interesse pubblico (art. 6.1. lett. e). Il consenso può essere utilizzato in casi eccezionali. Quindi sarà opportuno valutare con molta attenzione quale debba considerarsi la base giuridica corretta del trattamento.

PRIVACY

L'EDPB PUBBLICA LE LINEE GUIDA (3/2019) SU GDPR E VIDEOSORVEGLIANZA: UN VADEMECUM CON LE NOVITÀ E GLI ACCORGIMENTI PIÙ IMPORTANTI

L'EDPB ha adottato il 10 Luglio 2019 le "**Guidelines 3/2019 on processing of personal data through video devices"**. Si tratta di un documento che è al momento aperto alla consultazione pubblica (che si concluderà alla fine della prossima settimana).
Le Linee Guida sono della massima rilevanza in quanto rappresentano il primo documento europeo che applica i principi del GDPR al trattamento dei dati effettuati tramite riprese video**.** In Italia, infatti, l'ultimo documento in materia è il "Provvedimento in materia di videosorveglianza**"** dell'8 aprile 2010.
Il trattamento dei dati effettuato tramite videoriprese rappresenta una delle aree più rischiose e oggetto di sanzioni da parte dei garanti europei: si pensi alla sanzione di 200.000 € emanata dal garante francese o quella di 120.000£ del garante britannico.
Analizziamo ora i punti più salienti delle Linee Guida.

IV. Per quanto riguarda le riprese basate sul legittimo interesse: questo deve essere sempre reale e attuale.
Nella pratica, ciò significa che il Titolare deve dimostrare – anche tramite ad esempio un diario degli incidenti o dei danni subiti – di essere in una situazione di pericolo reale prima di incominciare l'attività di videosorveglianza.

ESEMPI PRATICI:
- **a.** Un commerciante vuole aprire una nuova attività ed installare un impianto di videosorveglianza: può giustificare l'impianto dimostrando, anche tramite statistiche, che quel particolare quartiere è oggetto di atti di vandalismo frequenti. **Non è sufficiente,** nel caso di controlli, **riportare statistiche nazionali o generali senza alcun riferimento all'area specifica.**
- b. Nel caso di attività commerciali caratterizzate innatamente pericolose, come la vendita di preziosi o le stazioni di rifornimento, non c'è bisogno di alcuna dimostrazione per l'installazione di telecamere di videosorveglianza;

V. È obbligatorio dimostrare la necessità dell'installazione di un impianto di videosorveglianza.
Prima di installare le telecamere, il Titolare dovrà utilizzare altri strumenti quali: personale di sicurezza, cancelli telecomandati, illuminazione adeguata, vetri antimanomissione, vernice antigraffiti, ecc. Sarà inoltre necessario **limitare geograficamente e temporalmente le videoriprese al minimo indispensabile.**
In generale, **la necessità di utilizzare telecamere di videosorveglianza coincide con i confini della proprietà.** Tuttavia, sono ammesse eccezioni nei casi cui è necessario eccedere questi confini per garantire una tutela effettiva.

ESEMPI PRATICI:
- **a.** Se il titolare di **un'azienda** vuole **difendersi contro i furti,** sarà sufficiente installare delle **telecamere funzionanti solo negli orari notturni e/o al di fuori degli orari normali di lavoro;**
- **b.** Se il titolare **deve necessariamente riprendere anche aree non pertinenti alla sua proprietà**, deve applicare alcuni **accorgimenti tecnici** come ad esempio **pixellare le aree non rilevanti.**

VI. È obbligatorio effettuare un bilanciamento degli interessi coinvolti: legittimo interesse del titolare vs. diritti e libertà fondamentali dell'individuo ripreso.

ESEMPI PRATICI:
- a. Un parcheggio privato ha subito diversi furti documentati alle macchine parcheggiate. Il parcheggio si trova in un'area all'aperto e l'accesso è aperto anche se i confini sono segnalati chiaramente. L'azienda gestrice ha un interesse legittimo ad installare un impianto di videosorveglianza che prevale su quello degli interessati a non essere ripresi all'interno del parcheggio;
- b. Un ristorante vuole installare delle videocamere nei servizi igienici per controllare la pulizia: in questo caso NON è concesso perché **il diritto alla riservatezza degli interessati è prevalente**;

VII. Videoriprese effettuate sulla base del consenso: attenzione!
Come detto sopra, deve essere usato eccezionalmente come condizione di liceità delle videoriprese. È importante **dimostrare che il consenso sia stato prestato liberamente: entrare un'area segnalata con i cartelli non è un'espressione di consenso sufficiente.**

VIII. Diritti degli interessati
Gli impianti di videosorveglianza richiedono alcuni adattamenti relativamente ai diritti concessi agli interessati dal GDPR. I titolari devono informare gli interessati con precisione relativamente alle informazioni di cui necessitano per poter soddisfare le richieste di accesso. Nel caso di richiesta eccessiva o manifestamente infondata, il Titolare può far pagare una somma all'interessato o rifiutarsi di soddisfare la richiesta.

ESEMPI PRATICI:
Se un soggetto richiede l'accesso alle immagini registrate da un impianto di videosorveglianza situato all'ingresso di un centro commerciale con 30.000 visitatori al giorno, dovrà specificare quando ha attraversato l'area indicando al massimo un periodo di 2 ore. Se da queste immagini possono essere individuati altri soggetti, il titolare dovrà anonimizzare la presenza di questi (ad esempio sfocando o pixellando l'immagine) prima di dare la copia all'interessato;

IX. Trasparenza e obblighi informativi: basta il cartello?
Viene consigliato l'utilizzo di un'informativa strutturata (cartello + informativa completa online o cartacea) perché devono essere comunicate tutte le informazioni stabilite all'articolo 13 del GDPR.

X. Periodo di conservazione delle immagini
Il nostro Garante ha sancito un periodo standard di conservazione **di 24 ore**. **Tempi di conservazione superiori devono essere sempre giustificati.**

Avv. Alice Giannini
Studio Legale Stefanelli

DIRETTORE RESPONSABILE
Maria Antonietta Portaluri

REDAZIONE
Alessandra Toncelli – Mirella Cignoni – Mattia Ciribifera

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Avv. Giovanna Buffa, BBM Partners, Buffa, Bortolotti & Mathis (Torino) - Avv. Giacomo Gori, Cocuzza & Associati, Studio Legale (Milano) - Avv. Filippo Alberti, Avv. Luca Feltrin, Freshfields Bruckhaus Deringer (Milano) - Avv. Dario Paschetta, Avv. Mariagrazia Berardo, Frignani Virano e Associati Studio Legale (Torino –Milano – Roma – Bologna) - IMQ International Services Area (Milano) - Avv. Alice Giannini, Studio Legale Stefanelli (Bologna)

Telex Anie

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri

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

Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996