Privacy allo stadio: una partita ancora aperta

di Avv. E. Olimpia Policella

(1 Premessa – La procedura di parere del Garante privacy - 3 Il decreto sulla videosorveglianza negli stadi - 3.1 La registrazione e la conservazione - 3.2 Il diritto di accesso alle immagini - 4 Il decreto sui biglietti nominativi - 4.1 I biglietti nominativi - 4.2 La confusione terminologica - 4.3 Le disposizioni a tutela dei dati personali - 5 Conclusione)

1 Premessa

La normativa della sicurezza negli stadi è stata recentemente arricchita tramite la pubblicazione di tre decreti, emanati da parte del Ministero degli Interni in attuazione del decreto legge n. 28 del 2003, recante "Disposizioni urgenti per contrastare i fenomeni di violenza in occasione di competizioni sportive".
Detti decreti, datati 6 giugno 2005, riguardano:
- la previsione dell'obbligo di utilizzo di sistemi di videosorveglianza negli stadi con capienza superiore a 10.000 spettatori (1);
- l'introduzione dell'obbligo di emettere biglietti numerati e nominativi (2);
- e la previsione dell'obbligo di adottare misure di sicurezza di carattere fisico e logico negli stadi(3).

I decreti inerenti l'obbligo di emettere biglietti nominativi e la videosorveglianza, sono stati adottati dal Ministero, previo parere del Garante privacy considerato il loro impatto sulla sfera di dignità e riservatezza della persona che ritrova una delle maggiori forme di tutela nel riconoscimento del bene giuridico costituito dal dato personale.
L'antitesi tra il diritto, di stampo pubblicistico, ad innalzare il livello di sicurezza dei cittadini ed il diritto, prevalentemente di natura individuale, alla tutela della privacy, non costituisce una problematica nuova ed ha infervorato gli animi di giuristi e politici soprattutto in sede di approntamento di contromisure idonee a fronteggiare nefasti eventi quali l'attacco alle Torri gemelle dell'11 settembre 2001. Le esigenze di carattere individuale, come spesso accade, cedono il passo alle necessità di ordine pubblico e di tutela della sicurezza dei cittadini.
Il compito del Garante, pertanto, in contesti simili, diviene quello di operare un bilanciamento dei contrapposti interessi nonché quello di ricercare e suggerire delle misure che determinino un minore sacrificio per la privacy attraverso la verifica preventiva del rispetto dei principi di liceità e di proporzionalità dei trattamenti eseguiti per ragioni di sicurezza.
La necessità di bilanciare diritti antitetici e soddisfare esigenze di certezza del diritto costituiscono la *ratio* della previsione dell'obbligo, previsto dal Codice privacy, di consultare preventivamente il Garante in caso di adozione di norme o regolamenti che possano incidere sulla materia inerente la tutela dei dati personali.

2 La procedura di parere del Garante privacy

I decreti del Ministero degli interni sono stati, infatti, preceduti dall'emanazione di un parere del Garante privacy richiesto dallo stesso Ministero ai sensi dell'art. 154, comma 4, del Codice privacy.
Il parere del Garante, rilasciato in attuazione dei commi 4 e 5 dell'art. 154 del Codice privacy, seppur costituisce una condizione di legittimità dei provvedimenti emanati dai Ministeri, non sembrerebbe avere carattere vincolante (4).
L'art. 154, comma 4, difatti, stabilisce che il Presidente del Consiglio dei Ministri e ciascun ministro che adotta degli atti amministrativi o di natura regolamentare che incidono sulla tutela dei dati personali è tenuto a consultare il Garante in via preventiva rispetto all'adozione di detti atti.

Il Garante, dal suo canto, è tenuto ad esprimersi entro 45 giorni dalla richiesta; decorso tale termine l'amministrazione potrà procedere indipendentemente dall'acquisizione del parere. Il termine di cui sopra potrebbe essere interrotto una sola volta qualora il Garante richieda ulteriori elementi istruttori. In tal caso il parere dovrà essere adottato entro venti giorni dal ricevimento degli ulteriori elementi istruttori richiesti dal Garante.
L'anomalia riscontrata nel caso di specie va rilevata nella circostanza che il Garante, nell'emanare il parere del 4 maggio 2005, aveva evidenziato la necessità di raccogliere ulteriori elementi istruttori in merito al decreto inerente la numerazione dei biglietti ed aveva indicato l'opportunità di adottare misure che, di fatto, sembrano essere state sostanzialmente recepite nel relativo decreto del 6 giugno 2005. Le modalità di rilascio del parere dell'Authority, quindi, non risultano particolarmente chiare posto che, si ribadisce, il Garante ha avanzato ulteriori richieste istruttorie mentre esse avrebbero dovuto sospendere il termine per l'adozione del parere e costituire oggetto di autonoma valutazione da parte della medesima Authority.
La raccolta di elementi di indagine conoscitiva in merito alla vicenda de qua, direttamente presso le autorità competenti, appare impresa ardua, pertanto, ci si limiterà, con questo breve elaborato, ad esporre gli aspetti salienti relativi all'emanazione di detti decreti ed alle garanzie previste dai decreti per la tutela dei dati personali degli spettatori di competizione sportive.

3 Il decreto sulla videosorveglianza negli stadi

L'art. 1 del decreto sulla videosorveglianza negli stadi importa l'obbligo di adottare sistemi di videosorveglianza che riprendano le aree interne e le immediate vicinanze degli stadi con capienza superiore a 10.000 spettatori (5).
I sistemi di videosorveglianza dovranno essere situati in tutti i locali (anche aperti) in cui il pubblico ha l'accesso, con esclusione dei locali igienici, e dovranno consentire la piena riconoscibilità del pubblico. Le telecamere dovranno essere collocate in special modo sui varchi per l'accesso e per il deflusso degli spettatori.
A garanzia della tutela dei dati personali il decreto ha specificamente regolamentato la durata della registrazione, la conservazione delle stesse registrazioni, i limiti del diritto di accesso alle immagini e l'informativa da rilasciare agli spettatori.

3.1 La registrazione e la conservazione

Per quanto concerne la durata della registrazione il decreto, all'art. 3, ha stabilito l'obbligo di procedere alla registrazione video ed alla registrazione audio (quest'ultima limitatamente all'evento), dall'apertura fino alla chiusura degli impianti nonché durante la preparazione delle coreografie.
Il parere del Garante ha sostanzialmente richiamato alcune disposizioni già presenti nel provvedimento generale sulla videosorveglianza del 29 aprile 2004 ed ha evidenziato come l'introduzione di sistemi di videosorveglianza durante eventi sportivi negli stadi risponda sia ai principi di liceità che al principio di necessità anche in considerazione del fatto che spesso gli stadi italiani si sono trasformati in teatri di episodi violenti. Le modalità di raccolta dei dati sono state considerate proporzionate rispetto alla finalità di repressione dei reati, seppur il Garante ha osservato come se, per un verso, non sia stato fatto esplicito riferimento ai reati inerenti la giustizia sportiva, per altro verso, la tipologia di reati sia desumibile dal tenore letterale dell'intero decreto.
La durata della conservazione dei dati è stata fissata in sette giorni. Qualora si siano verificati dei reati, ovviamente, i dati potranno essere conservati per l'intero periodo necessario all'accertamento delle fattispecie criminose; nel caso, invece, in cui non si sia verificato nessun reato i dati dovranno essere cancellati decorso il periodo massimo di conservazione che, appunto, è di sette giorni.
Detto termine settimanale risponde ai dettami già espressi dal Garante nel provvedimento generale dell'aprile 2004 sulla videosorveglianza nel quale l'Authority ha evidenziato che il Titolare del

trattamento, nel caso in cui abbiano avuto luogo degli illeciti, possa decidere di conservare i dati inerenti le immagini fino ad una settimana.
L'obbligo di conservazione dei dati e l'adozione delle relative misure di sicurezza grava in capo alle società calcistiche che hanno organizzato l'evento sportivo. Detti soggetti sono, peraltro, tenuti al rilascio delle informazioni raccolte all'autorità giudiziaria ed alle altre autorità competenti all'accertamento dei reati.

3.2 Il diritto di accesso alle immagini
Il diritto di accesso alle immagini sussiste non solo in capo ai soggetti interessati, stante il disposto di cui all'art. 7 del Codice privacy, ma anche in capo al delegato delle Leghe nazionali professionisti e dilettanti. Il delegato può accedere alle immagini per scopi di giustizia sportiva e chiederne copia, per estratto, nel rispetto del Codice per la protezione dei dati personali.
A ben vedere il decreto parla in termini impropri di diritti di accesso posto che il diritto di accesso previsto dal Codice privacy (art. 7) concerne la possibilità di ciascun soggetto di avere conoscenza dei dati personali che lo riguardano al fine di poter esercitare pienamente il proprio diritto alla autodeterminazione informativa nel rispetto del principio di trasparenza.
La possibilità riconosciuta al delegato della Lega di accedere alle immagini per esigenze di giustizia sportiva, in verità, a parere di chi scrive, costituisce piuttosto un'ipotesi di comunicazione dei dati da parte delle società calcistiche. In altri termini le società calcistiche, nella loro qualità di titolari del trattamento delle immagini raccolte in occasione degli eventi calcistici, sono tenute a procedere alla comunicazione dei dati ai delegati delle Leghe, a seguito di una loro richiesta, al fine di consentire lo svolgimento di finalità di giustizia sportiva (6).

4 Il decreto sui biglietti nominativi

Il Decreto sui tagliandi di accesso è stato emanato, come anticipato, dal Ministero degli interni al fine di dare attuazione al D. L. 28/2003 ed adeguare il sistema di sicurezza negli stadi.
Il Ministero, probabilmente a seguito dei rilievi formulati dal Garante privacy - tesi ad evidenziare come il Decreto del 2003 prevedesse esclusivamente la misura della numerazione dei biglietti e non anche quella dell'emissione di biglietti nominativi - ha espressamente ritenuto di dover abbinare ai titoli di accesso i nominativi, almeno fino a quando permarranno le attuali condizioni dell'ordine e della sicurezza pubblica. Il Garante, nel parere del maggio 2005, ha lamentato la mancata presentazione di elementi istruttori tali da consentirgli di effettuare una valutazione di proporzionalità dell'emissione di biglietti nominativi rispetto alla finalità perseguita.

4.1 I biglietti nominativi
L'emissione di tagliandi di accesso nominativi, sotto il profilo privacy, implica rischi maggiori per la tutela dei dati rispetto alla previsione della misura di sicurezza costituita dalla videosorveglianza. La previsione dell'obbligo di emettere biglietti nominativi, infatti, determina la costituzione di enormi banche dati che contengono diverse centinaia di migliaia di dati personali non solo degli spettatori ma anche dei rivenditori. Difatti l'art. 3 del decreto stabilisce l'obbligo, per le società organizzatrici di eventi calcistici, di dotarsi di moderni sistemi di emissione dei tagliandi di accesso che consentano, tra l'altro, di associare a ciascun biglietto emesso sia le generalità del rivenditore o cedente che le generalità dell'acquirente o cessionario. Le informazioni debbono essere memorizzate in modo corretto, nel rispetto del principio di qualità dei dati, e con modalità sicure vale a dire adottando quanto meno le misure minime di sicurezza previste dal Disciplinare Tecnico, Allegato B) al Codice privacy (D. Lgs. 196/2003).
I titoli di accesso dovranno riportare una pluralità di informazioni quali la possibilità delle forze dell'ordine di procedere a controlli di prevenzione e sicurezza sulla persona al fine di impedire l'introduzione nello stadio di oggetti o sostanze pericolose, la circostanza che l'uso del titolo di

accesso importa l'accettazione delle norme di regolamento nonché l'indicazione del responsabile del trattamento dei dati ed il fatto che i dati saranno trattati nel rispetto del Codice privacy (7). Le informazioni inserite sui biglietti nominativi confluiranno, automaticamente, in una baca dati accessibile al sistema di controllo degli stadi.

4.2 La confusione terminologica

Si ritiene opportuno, a questo punto, chiarire la confusione terminologica in cui è incorso il Ministero nell'emanazione del decreto posto che ha utilizzato il termine "titolare" al fine di indicare il "proprietario" del tagliando di accesso ed il termine "responsabile" per indicare la società organizzatrice dell'evento calcistico.

Orbene, si ritiene di dover ricordare che i termini "titolare" e "responsabile", sotto il profilo privacy, indicano, rispettivamente, colui che decide in ordine alle finalità e modalità del trattamento dei dati e colui che è dotato di competenze in materia *data protection* e che fornisce il suo supporto al titolare. Nel decreto in commento, invece, il termine titolare è stato riferito allo spettatore che, in ottica privacy, costituisce il soggetto interessato, vale a dire la persona cui si riferiscono i dati personali riportati sul tagliando di accesso, mentre il termine responsabile è stato utilizzato impropriamente per indicare il titolare del trattamento dei dati ossia la società organizzatrice (8).

4.3 Le disposizioni a tutela dei dati personali

Nell'ambito delle attività di emissione e di distribuzione dei titoli di accesso nominativi, le società organizzatrici dovranno indicare il titolare ed il responsabile da inserire sui titoli medesimi.

Il titolare ed il responsabile dovranno:

- assicurare il rispetto della normativa privacy
- e garantire l'immediata disponibilità dei dati raccolti alla autorità giudiziaria e di pubblica sicurezza nonché agli ufficiali di pubblica sicurezza o di polizia giudiziaria debitamente autorizzati.

L'attività di gestione della banca dati, nella quale sono riportati i dati del ricevitore e dello spettatore, è eseguita dalla società organizzatrice o da suo delegato: i riferimenti di entrambi andranno inseriti su appositi cartelli nei varchi per l'accesso ed il deflusso degli spettatori. Detti cartelli dovranno essere visibili anche a distanza al fine di assicurare il rispetto del principio di trasparenza che costituisce uno dei pilastri fondamentali della normativa a tutela dei dati personali.

Anche i titolari ed i responsabili dell'attività di gestione della banca dati dovranno rispettare la normativa privacy e garantire la disponibilità dei dati all'autorità giudiziaria e di pubblica sicurezza.

Una disposizione particolarmente ostica, infine, è costituita dal comma 3 dell'art. 6, che stabilisce il divieto di procedere a delle connessione dei dati. Questa disposizione risulta chiarita solo dal suggerimento rilasciato dal Garante in sede di parere che ha richiesto di precisare la sussistenza di un eventuale intreccio tra banche dati di singole società. Dalla lettura della disposizione si evince, invece, la sussistenza del divieto di intrecciare le banche dati. Una siffatta misura risponde ad esigenze di maggiore garanzia per gli spettatori.

5 Conclusione

Al di là delle nuove norme introdotte dai decreti di cui si è parlato sinteticamente, si ritiene che la formazione e la gestione di banche dati pubbliche utilizzate per finalità di giustizia e di sicurezza pubblica, seppur costituisca una insopprimibile esigenza per la salvaguardia dell'ordine e della sicurezza pubblica, debba essere necessariamente disciplinata con regole maggiormente severe rispetto a quelle attualmente prescritte dall'ordinamento vigente.

Dette regole, a parere di chi scrive, dovrebbero essere, tra l'altro, preordinate:

- alla previsione di norme specifiche che potenzino i poteri di accertamento e di controllo del rispetto del principio finalistico per far sì che i dati raccolti per il perseguimento di una determinata finalità non vengano utilizzati per il perseguimento di scopi ulteriori e non dichiarati, quand'anche detti scopi rispondano ad esigenze di stampo pubblicistico;
- ad una rigorosa regolamentazione del diritto di accesso alle stesse banche dati con una definizione esatta dei soggetti pubblici che possono accedervi;
- alla introduzione di norme di diritto penale specifiche che prevedano dei reati propri nei confronti di pubblici ufficiali ed incaricati di pubblico servizio che, potendo accedere per ragioni di servizio a determinate banche dati, eseguano una comunicazione non consentita dei dati oppure un trattamento contrario o incompatibile con le finalità della raccolta (9).

L'inasprimento delle sanzioni amministrative e penali si palesa, allo stato, come un'insopprimibile esigenza affinché l'ordinamento giuridico possa tamponare la grave mancanza, nel nostro Paese, di una coscienza civile alla tutela del "bene dato personale" che stenta a decollare e conseguentemente di una minore difesa dei diritti da parte degli stessi soggetti interessati.

Note

(1) Il provvedimento è disponibile sul sito ufficiale del Governo all'URL: http://www.governo.it/GovernoInforma/Dossier/sicurezza_stadi/decreto_videosorveglianza.pdf.
(2) Il provvedimento è disponibile sul sito ufficiale del Governo all'URL: http://www.governo.it/GovernoInforma/Dossier/sicurezza_stadi/decreto_biglietti.pdf.
(3) Il provvedimento è disponibile sul sito ufficiale del Governo all'URL: http://www.governo.it/GovernoInforma/Dossier/sicurezza_stadi/revisione_dm_18_marzo_96.pdf.
(4) Il parere del Garante sulla videosorveglianza negli stadi è stato rilasciato il 4 maggio 2005 ed è disponibile sul sito ufficiale dell'Authority alla URL http://www.garanteprivacy.it/garante/doc.jsp?ID=1120732.
(5) La precisazione che le riprese possano aver luogo esclusivamente nelle vicinanze immediate e non semplicemente nelle vicinanze è stata effettuata dietro espresso suggerimento del Garante privacy riportato nel parere del maggio 2005.
(7) V. art. comma 2 del Decreto.
(8) V. anche l'art. comma 5 in cui il termine titolare, invece, sembra essere stato utilizzato per fare riferimento alla società che organizza l'evento calcistico quindi correttamente da un punto di vista privacy.
(9) A detto ultimo riguardo si rileva che il reato di illegittimo trattamento dei dati personali, allo stato previsto per "chiunque" ponga in essere una delle condotte richiamate dall'art. 167 del Codice privacy stabilisce una pena piuttosto blanda di massimo tre anni di reclusione e che l'attuale ordinamento giuridico non prevede alcuna sanzione penale per la violazione del principio finalistico fatta eccezione il caso in cui, per quel che rileva in questa sede, il soggetto pubblico tratti il dato personale in violazione delle funzioni istituzionali di cui all'art. 18 del medesimo Codice ed in presenza di un nocumento per i soggetti interessati e di un dolo specifico.