Il riconoscimento facciale negli stadi: un'inafferrabile oscillazione tra agile accesso ed attività di polizia in attesa dell'AI Act

di Lorenzo Sottile

Abstract: *Facial recognition technologies in football stadiums. An elusive oscillation between easy access and law enforcement activities pending the AI Act* - Following tests conducted at the Millennium Stadium in Cardiff in 2017, a novel correlation has emerged between facial recognition technologies and football, a trend observable in other European countries. This paper examines the primary critical issues arising from the contentious deployment of such systems within sports venues by analyzing the decisions of various Data Protection Authorities.

In the run-up to the AI Act, these systems face the challenge of managing the complexity created by the diverse applications of these technologies for different purposes. This diversity has blurred the distinction between authentication and identification purposes, making it difficult to determine the appropriate regulatory framework.

Keywords: Facial recognition technologies; Football stadiums; Data protection authorities; Security; AI act

1. La genesi dell'utilizzo delle tecnologie di riconoscimento facciale negli stadi di calcio

Il 3 giugno del 2017 si è disputata, presso il Millennium Stadium di Cardiff, la finale di UEFA Champions League tra Juventus e Real Madrid.

L'evento calcistico più atteso dell'anno non è stato, tuttavia, caratterizzato soltanto dallo spettacolo offerto dai giocatori in campo e dalle tifoserie sugli spalti: per la prima volta in Europa sono state sperimentate soluzioni innovative per la gestione dell'ordine pubblico e della sicurezza durante le manifestazioni sportive.

In seguito ad un bando di gara promosso dal Governo del Regno Unito, la *South Wales Police* era stata dotata di un sistema di riconoscimento facciale (*Automated Facial Recognition*) operante sia in modalità *real time* che statica, collegato ad un archivio di 500.000 immagini a disposizione delle forze dell'ordine[1]. In funzione presso la stazione ferroviaria centrale della città, all'interno dello stadio e nelle zone limitrofe, il sistema *AFR* avrebbe

[1] Il sommario del contratto e la breve descrizione del programma possono leggersi qui: https://www.contractsfinder.service.gov.uk/Notice/6281c974-6fd5-4632-ab1b-9f9ef3510b2e.

DPCE online
ISSN: 2037-6677

dovuto scansionare i volti dei 170.000 spettatori attesi per la partecipazione all'evento, allo scopo di monitorare in maniera pervasiva i punti nevralgici della capitale, considerati come potenziali target di attacchi terroristici[2].

Tale circostanza ha permesso di valutare l'applicazione delle nuove tecnologie di controllo all'ambito calcistico. Difatti, nonostante l'esito fallimentare dell'esperienza gallese, il progetto pilota ha favorito successivi utilizzi degli strumenti di riconoscimento facciale all'interno degli stadi di altre città per il perseguimento di finalità eterogenee: riduzione dei tempi di attesa all'ingresso, individuazione degli autori di comportamenti violenti o discriminatori e dei destinatari di misure restrittive per l'accesso alle strutture, generali esigenze di prevenzione e sicurezza.

Già da questi cenni si colgono le potenzialità di una tecnologia biometrica che, basandosi su algoritmi di *deep learning*[3], permette l'autenticazione e l'identificazione di un soggetto in maniera univoca a partire dal suo volto[4].

Quanto all'autenticazione, viene effettuata una comparazione 1:1; il sistema si limita a confermare o negare che una persona sia chi dichiari di essere in virtù del confronto operato tra l'immagine del volto ad esso sottoposta ed una già acquisita nel corso della fase di registrazione[5].

L'identificazione risulta, invece, una pratica maggiormente invasiva, presupponendo una comparazione 1: molti. Poiché l'obiettivo per il quale si ricorre allo strumento è quello di conoscere l'identità di un soggetto, l'immagine del viso di quest'ultimo verrà acquisita e confrontata con altre presenti all'interno di un *database* alla ricerca di una corrispondenza, che, ove esistente, sarà espressa da un risultato percentuale[6].

Il sistema funziona attraverso il trattamento di dati biometrici[7], i quali sono stati inseriti dall'art. 9, par. 1 del regolamento 2016/679/UE (GDPR) e dall'art. 10 della direttiva 2016/680/UE (LED) tra le "categorie particolari di dati", che richiedono, quindi, tutele rinforzate, specialmente quando siano

[2] Secondo quanto emerso dall'intervista della BBC Wales al *chief constable* Matt Jukes il 4 maggio del 2018, https://www.bbc.com/news/uk-wales-south-west-wales-44007872.

[3] Il *deep learning* è una sottocategoria del *machine learning* in cui gli algoritmi di reti neurali artificiali tentano di simulare il funzionamento del cervello umano, permettendo al sistema di imparare da grandi quantità di dati.

[4] Come riportato nel *Parere 2/2012* del *Gruppo di lavoro Articolo 29*, tra le principali finalità delle tecnologie di riconoscimento facciale è presente anche la categorizzazione, ossia la classificazione di una persona in base a dei requisiti predeterminati: ad esempio, l'età, il genere, il colore dei capelli, ma anche l'origine etnica, l'orientamento politico e il credo religioso. Tuttavia, si è deciso di non farne menzione nel testo perché, ad oggi, non sono stati rilevati casi di categorizzazione all'interno degli stadi.

[5] Per un apparato teorico-definitorio più ampio, P.J. Phillips et al., *Evaluation Methods in Face Recognition*, in S.Z. Li, A.K. Jain (a cura di), *Handbook of Face Recognition*, Londra, 2016, 552 e ss.; E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Dordrecht, 2013, *passim*.

[6] Giova precisare che l'identificazione tramite riconoscimento facciale può avvenire sia in differita sia in tempo reale e che i *database* possono essere di diversi ordini di grandezza, sino a contenere milioni di volti.

[7] Definiti dall'art. 4 del GDPR come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca».

trattati da autorità competenti nell'ambito di attività di *law enforcement*, quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali.

Infatti, a differenza dell'art. 9 del GDPR, che, al par. 2, contiene un ampio elenco di eccezioni al divieto di trattamento dei dati in parola, l'art. 10 della LED autorizza il trattamento di questi ultimi «solo se strettamente necessario e soggetto a garanzie adeguate per i diritti e le libertà dell'interessato», in presenza di una delle tre condizioni prospettate: l'esistenza di una previsione normativa dell'Unione europea o del singolo Stato membro; la salvaguardia dell'interesse vitale dell'interessato o di altra persona fisica; la circostanza che i dati siano stati resi manifestamente pubblici dallo stesso interessato.

Nella vicenda della partita disputata a Cardiff, le ragioni di sicurezza relative alla gestione dell'evento "critico" avevano giustificato l'adozione delle tecnologie di riconoscimento facciale. Tuttavia, su 2470 *match* segnalati dall'applicativo, erano stati registrati 2297 falsi positivi, con un tasso di errore dello strumento pari al 92%. Nonostante gli agenti della *South Wales Police* avessero deciso di non intervenire nelle ipotesi di riconoscimento inesatto – confermando l'insostituibilità dell'operato umano anche nel caso di ricorso agli "ausili" tecnologici –, sono evidenti le problematiche potenzialmente derivanti dall'inaccuratezza dei sistemi di cui si discute, idonei ad avere ripercussioni in grado di incidere significativamente nella sfera dei diritti e delle libertà fondamentali dei soggetti analizzati dalla "macchina".

Non stupisce, dunque, che l'11 agosto 2020, seppur con riferimento ad un diverso caso di utilizzo del sistema *AFR* rispetto a quello sopra esposto, la *Civil Division della Court of Appeal* abbia dichiarato illegittimo il suo uso da parte della *South Wales Police*[8]. In particolare, la sentenza aveva accertato l'incompatibilità del sistema di riconoscimento facciale con l'art. 8, par. 2 della Convenzione Europea dei Diritti dell'Uomo[9], ritenendo altresì carente la valutazione d'impatto sulla protezione dei dati e riscontrando la mancata osservanza, da parte delle autorità pubbliche, dell'obbligo di garantire pari opportunità ed evitare effetti discriminatori per i soggetti coinvolti[10].

[8] Court of Appeal, Civil Division, R (OTAO) Bridges v. The Chief Constable of South Wales Police and others, [2020] EWCA Civ 1058, 11 agosto 2020. È stata così ribaltata la sentenza di primo grado della *High Court of Justice* del 4 settembre 2019, la quale aveva "salvato" il sistema *AFR Locate* rigettando le censure presentate nel ricorso. Per un approfondimento in merito a quest'ultima pronuncia, si vedano A. Pin, *Non esiste la "pallottola d'argento": l'"artificial face recognition" al vaglio giudiziario per la prima volta*, in *DPCE*, 4/2019, 3075 e ss.; J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Dir. pen. cont.*, 1/2020, 231 e ss.

[9] «Non può esservi ingerenza di una autorità pubblica nell'esercizio del *diritto al rispetto della vita privata e familiare* a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

[10] Un commento alla sentenza si può rintracciare in G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 229 e ss.

DPCE online
ISSN: 2037-6677

Le (infauste) vicende relative alla sperimentazione del Millennium Stadium, così come l'assenza di una normativa nazionale o sovranazionale che disciplinasse compiutamente i sistemi di riconoscimento facciale, non hanno tuttavia scoraggiato la realizzazione di progetti successivi da parte di società calcistiche e Governi in altri stati europei, sulla falsariga del caso gallese.

È possibile, infatti, considerare il 2017 una sorta di "anno zero", a partire dal quale tali tecnologie hanno conosciuto una considerevole espansione negli stadi di calcio di molte città europee. Il loro successo, come evidenziato, è sicuramente legato alle potenzialità offerte dalle molteplici applicazioni cui i sistemi possono essere destinati, ma alla loro diffusione ha contribuito, in modo decisivo, anche la volontà degli Stati di concorrere nel "mercato biometrico" e le istanze di sicurezza che hanno orientato le politiche dell'Unione Europea in materia di prevenzione e repressione di atti di violenza in occasione delle manifestazioni sportive.

Proprio in merito a quest'ultimo aspetto, numerosi sono stati gli interventi attuati dopo la "strage dell'Heysel"[11] e l'adozione, da parte del Consiglio d'Europa, della Convenzione del 1985 sulla violenza e i disordini degli spettatori durante le manifestazioni sportive, segnatamente nelle partite di calcio. All'interno di fonti di varia natura, sono state, quindi, individuate misure idonee a fronteggiare situazioni pericolose che potrebbero insorgere durante i grandi eventi sportivi, riguardanti, ad esempio, le modalità di comunicazione e di cooperazione tra forze di polizia e i divieti d'accesso agli impianti in cui si svolgono gli incontri[12].

Nel contesto descritto, le tecnologie di riconoscimento facciale hanno assunto un'indubbia centralità, propiziata dall'assenza di regole normative che ne disciplinino l'utilizzo e dalle insistenti richieste dei vertici delle federazioni calcistiche che hanno visto negli strumenti biometrici la soluzione per raggiungere l'obiettivo della sicurezza a qualsiasi costo.

A ben guardare, però, pur attribuendo rilevanza alle finalità di sicurezza, è necessario promuovere un bilanciamento che coinvolga la tutela del diritto alla protezione dei dati personali e degli altri diritti e libertà interessati dal trattamento.

Senza sposare posizioni luddiste e rifiutando l'errata equazione "ultras=tifoso violento", occorre sviluppare un'indagine meticolosa della casistica relativa all'impiego delle tecnologie biometriche, per far luce sui principali nodi critici che vengono in rilievo: in particolare, l'eterogeneità degli scopi in vista dei quali vi si ricorre può portare alla confusione tra finalità di autenticazione e identificazione e alla sovrapposizione tra il trattamento effettuato dai *club* e le operazioni di polizia, con la conseguente

[11] Si tratta della tragedia verificatasi il 29 maggio 1985 allo stadio Heysel di Bruxelles, in cui persero la vita 39 persone e ne rimasero ferite 600.

[12] Cfr. Raccomandazione (96/C 131/01) sugli orientamenti per prevenire e limitare i disordini in occasione della partite di calcio; Decisione (2002/348/GAI) concernente la sicurezza in occasione di partite di calcio internazionali; Risoluzione (2003/C 282/01) per l'adozione negli Stati membri del divieto di accesso agli impianti dove si svolgono partite di calcio di rilevanza internazionale; Risoluzione (2006/C 322/01) concernente un manuale aggiornato di raccomandazioni per la cooperazione internazionale tra forze di polizia e misure per prevenire e combattere la violenza e i disordini in occasione delle partite di calcio di dimensione internazionale.

indecisione sulla disciplina applicabile tra GDPR e LED. Inoltre, non devono essere sottovalutati il rischio di trasformazione della concezione degli spazi pubblici nonché la ridotta salvaguardia della sfera dei diritti e libertà dei cittadini in determinati contesti.

La prospettiva scelta per procedere all'analisi delle criticità appena delineate mira ad approfondire le decisioni sul tema delle Autorità garanti per la protezione dei dati personali di alcuni Paesi europei, che ben riflettono la difficoltà di porre un argine agli utilizzi controversi delle tecnologie di riconoscimento facciale e alla loro diffusione.

2. Il caso italiano: la vicenda dello Stadio Olimpico di Roma

L'esperienza italiana relativa al rapporto tra riconoscimento facciale e stadi di calcio appare significativa, sebbene si tratti di un solo caso isolato: già nel 2016 – quindi, ancor prima della sperimentazione nella capitale gallese – il Garante della privacy aveva autorizzato presso lo Stadio Olimpico di Roma l'installazione di un sistema di videosorveglianza provvisto della funzione di riconoscimento facciale[13].

In una fase segnata dall'acuirsi di episodi di violenza fisica tra tifoserie e nei confronti delle Forze dell'Ordine, infatti, il Ministero dell'Interno e la Questura di Roma avevano presentato una richiesta di verifica preliminare in merito alla possibilità di integrare gli strumenti di controllo sino ad allora adottati con il nuovo *software*, il quale avrebbe consentito di identificare i responsabili dei comportamenti vietati attraverso la comparazione delle immagini acquisite all'ingresso con quelle riprese durante la manifestazione sportiva.

Nonostante l'intrusività del trattamento, l'*Authority* aveva reso un parere positivo, ritenendo idonee le modalità operative del sistema, considerate rispettose dei principi di necessità, proporzionalità, finalità e correttezza nel trattamento dei dati ai sensi degli artt. 3 e 11 del d. lgs. 30 giugno 2003, n. 196 (Codice della privacy) e conformi agli obblighi di sicurezza e alle misure minime *ex* art. 31 e ss.

Il Garante aveva concluso osservando come il sistema non avrebbe arrecato un pregiudizio rilevante ai destinatari del trattamento, attraverso una decisione in linea con le tutele meno rigide previste del Codice della privacy rispetto a quelle introdotte successivamente dal GDPR. Sarebbe dunque auspicabile un ulteriore – e più aggiornato – controllo dell'Autorità amministrativa sull'impiego del dispositivo alla luce dei parametri maggiormente stringenti previsti dal GDPR.

In primo luogo, si avverte l'improrogabilità di una valutazione d'impatto del trattamento biometrico (art. 35 GDPR), che tenga conto dei tassi di errore registrati in occasione delle sperimentazioni realizzate e delle conseguenze prodotte sui diritti e le libertà dei soggetti interessati.

In secondo luogo, occorre rendere accessibili alle persone profilate le informazioni relative alla composizione dei *database* consultati e che vi sia una descrizione del sistema di telecamere integrato con il riconoscimento

[13] Secondo quanto si evince dal Provvedimento n. 338 del 28 luglio 2016.

DPCE online
ISSN: 2037-6677

facciale, con l'indicazione puntuale del numero di lenti e della loro precisa angolazione[14].

In terzo luogo, dovrebbe essere rivista l'autorizzazione "in bianco" concessa al Ministero dell'Interno nel parere richiamato, laddove è stato disposto che in caso di collocamento di «impianti analoghi in altri stadi calcistici» non sarebbe stata richiesta alcuna verifica preliminare. Difatti, è rischioso, in un ambito tanto delicato, ragionare "per analogia", soprattutto in virtù del fatto che non sono state diffuse pubblicamente informazioni sul sistema di riconoscimento facciale impiegato e sui risultati da esso raggiunti in seguito al suo utilizzo presso lo Stadio Olimpico.

Invero, grazie ad un'inchiesta giornalistica condotta nel 2023 da IrpiMedia[15], sono trapelati alcuni dettagli degni di nota: nel 2021 la società "Sport e Salute S.p.a.", che gestisce le infrastrutture di sicurezza dello Stadio Olimpico, si è dotata di un *software* in grado di identificare preventivamente i soggetti sottoposti a Daspo. Tale aspetto non genera alcuna criticità, considerato il richiamo a tale finalità contenuto anche nella descrizione del sistema fornita nel 2016; tuttavia, la società non rientra tra i soggetti cui non si applica la moratoria sull'utilizzo del riconoscimento facciale in luoghi pubblici o aperti al pubblico introdotta dalla legge 3 dicembre 2021, n. 205[16]. Inoltre, ad un'attenta lettura del documento relativo all'affidamento diretto da parte di "Sport e Salute S.p.a." all'azienda fornitrice del *sofware* "Reco 3.26 S.r.l.", risalente al 2021, emerge l'installazione del *Real time face identification system* presso i varchi d'ingresso dello Stadio Olimpico[17].

Ebbene, il Garante per la protezione dei dati personali si era già espresso il 25 marzo 2021, censurando proprio l'impiego della modalità "*Real Time*" del sistema S.A.R.I. – fornito, peraltro, dalla stessa azienda – sul presupposto della non sussistenza di una base giuridica idonea al trattamento dei dati biometrici con tale modalità, e sottolineando il rischio di una «sorveglianza universale allo scopo di identificare alcuni individui»[18].

In conclusione, alla luce degli "aggiornamenti tecnologici" che hanno interessato lo stadio, potrebbe ravvisarsi un contrasto tra il provvedimento del 2016 e quello del 2021, meritevole di attenzione da parte dell'*Authority*.

3. Il caso danese: l'atteggiamento permissivo del Datatilsynet alla luce dell'"interesse pubblico sostanziale"

In Danimarca, nel 2019, la società calcistica del Brøndby IF si è rivolta al Garante privacy nazionale (denominato "Datatilsynet") per chiedere l'autorizzazione ad implementare le tecnologie di riconoscimento facciale automatizzato all'ingresso dello stadio di proprietà del *club*, con l'espressa

[14] Nel Provvedimento n. 338 del 2016, difatti, si faceva riferimento solamente a cifre approssimative: «*circa* sessanta telecamere» e «un *ristretto numero* di telecamere […] orientato verso i settori più critici dal punto di vista dell'ordine pubblico».
[15] R. Coluccini, *Quello che la polizia non dice sulle telecamere allo Stadio Olimpico*, in *IrpiMedia*, 22 novembre 2023.
[16] La moratoria è stata successivamente prorogata dal 31 dicembre 2023 al 31 dicembre 2025 dalla legge 3 luglio 2023, n. 87.
[17] Consultabile al seguente link: 2061375.pdf (sportesalute.eu).
[18] Provvedimento n. 127 del 25 marzo 2021.

finalità di identificare le persone – i cui volti sono stati inseriti all'interno di una *watchlist* – destinatarie di un divieto di assistere alle partite, per aver violato, in precedenza, le regole di condotta.

Analogamente a quanto accaduto in Italia, il Datatilsynet, con un provvedimento del 24 maggio del 2019[19], ha dato un parere positivo, fondando la propria decisione sull'esistenza di un interesse pubblico sostanziale («væsentlige samfundsinteresser»), in linea con quanto disposto dall'art. 9, par. 2 del GDPR, richiamato dall'art. 7(4) del *Data Protection Act* danese[20].

La stessa base giustificativa è stata utilizzata anche nel successivo atto autorizzatorio, emesso il 9 giugno 2023[21] a fronte di una duplice richiesta della medesima società: da un lato, quella di estendere il sistema di riconoscimento facciale attivo presso gli ingressi anche alle telecamere di sorveglianza presenti all'interno dello stadio, al fine di facilitare l'arresto degli autori di reati o dei contravventori dei limiti di accesso; dall'altro, quella di usare un dispositivo mobile di *automated facial recognition* per identificare i propri tifosi durante le trasferte (sia fuori che dentro gli stadi), a fini di contrasto dei numerosi atti di violenza e vandalismo da parte di coloro a cui era stato vietato l'ingresso nelle "mura amiche".

Anche in relazione alla vicenda danese, pur riconoscendo che le esigenze di sicurezza durante gli eventi sportivi possano rappresentare un interesse pubblico sostanziale, occorre soffermarsi su alcuni profili di dubbia compatibilità dell'utilizzo dei sistemi biometrici con la normativa europea sulla protezione dei dati personali.

Perplessità sorgono, innanzitutto, in merito all'assenza di una definizione solida della nozione di "interesse pubblico sostanziale" all'interno della legislazione danese e in merito ai requisiti di necessità e proporzionalità del trattamento. Infatti, dopo la pubblicazione del primo parere dell'*Authority*, come sottolineato da Jasper Lund, membro dell'associazione European Digital Rights (EDRi), le cautele che circondano il trattamento di "particolari categorie di dati" sono state pregiudicate in vista dell'utilizzo di tecnologie intrusive, senza valorizzare istanze alternative di pari importanza. L'impiego dello strumento riguardava, infatti, un numero molto ridotto di volti di persone presenti all'interno della *watchlist* (circa cinquanta), senza che vi fossero informazioni disponibili su quante di esse stessero effettivamente cercando di eludere la misura e senza che si fosse verificato un aumento degli arresti in occasione delle partite di calcio[22].

Inoltre, non può tacersi la questione relativa all'inaffidabilità della tecnologia in parola, la stessa rispetto a quella in dotazione alla *South Wales Police*, caratterizzata da un'elevata percentuale di imprecisioni e pregiudizi sistematici suscettibili di dar luogo ad un alto tasso di riconoscimenti erronei.

---

[19] https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion.

[20] Atto n. 502 del 23 maggio 2018.

[21] https://www.datatilsynet.dk/afgoerelser/tilladelser/2023/jun/2022-51-0375.

[22] Così, J. Lund, *Danish DPA approves Automated Facial Recognition*, in *EDRi*, 19 giugno 2019.

DPCE online
ISSN: 2037-6677

4. Il caso francese: l'inflessibile posizione espressa dall'*avertissement* della Commission Nationale de l'Informatique et des Libertés

A differenza dei casi sinora esaminati, l'Autorità garante francese per la protezione dei dati personali ha assunto una posizione molto rigida riguardo all'utilizzo delle tecnologie di riconoscimento facciale negli stadi.

Pur non essendo stata consultata dalla società calcistica che aveva manifestato l'intenzione di introdurre dispositivi intelligenti all'interno del proprio stadio, la Commission Nationale de l'Informatique et des Libertés ha effettuato tempestivamente un controllo già nella fase di sperimentazione del progetto.

Le finalità del sistema erano state inquadrate nell'individuazione di oggetti abbandonati, nella lotta al terrorismo e nell'identificazione delle persone soggette alla *interdiction commerciale de stade*, una misura, quest'ultima, legata alla facoltà riconosciuta agli organizzatori di eventi sportivi di rifiutare o annullare l'emissione di biglietti d'ingresso o di negare l'accesso alle persone che hanno violato o stanno violando le disposizioni delle condizioni generali di vendita o i regolamenti interni relativi alla sicurezza delle manifestazioni sportive[23]. Si tratta, invero, dell'unico strumento a disposizione delle società per impedire l'ingresso allo stadio di determinati individui e che, pertanto, non va confuso con i divieti giudiziari o amministrativi che possono essere imposti soltanto dalle autorità giudiziarie e dai prefetti.

Nell'ottica di un possibile utilizzo delle tecnologie di riconoscimento facciale per finalità eterogenee, il Garante è intervenuto preventivamente, il 18 febbraio 2021, tramite un *avertissement*, nel quale ha dichiarato che, in assenza di una specifica disposizione legislativa o regolamentare, l'utilizzo di tale sistema da parte di una società sportiva sarebbe stato illegittimo. La CNIL aveva altresì informato il *club* che stava sperimentando il sistema biometrico[24] che, in caso di attivazione dello strumento, sarebbero state applicate le misure correttive previste dal GDPR e dalla *Loi Informatique et Libertés*, comprese le sanzioni pecuniarie.

Una direzione ben chiara quella indicata dalla CNIL, che ha dispiegato i suoi effetti anche in vista dell'organizzazione delle Olimpiadi di Parigi 2024. Difatti, la *LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024*, all'art. 10, quarto comma, ha precisato che le immagini raccolte dalle telecamere di videosorveglianza nonché quelle acquisite da aeromobili autorizzati non verranno sottoposte a sistemi di riconoscimento facciale né ad alcun trattamento di dati biometrici.

5. Il caso spagnolo e le soluzioni interlocutorie dell'Agencia Española de Protección de Datos

[23] Ai sensi dell'art. L. 332-1 del *Code du Sport*.
[24] Si trattava, in particolare, del FC Metz, il quale tuttavia non era esplicitamente citato nel provvedimento.

Negli ultimi due anni, la Agencia Española de Protección de Datos si è trovata a dover affrontare più volte la questione dell'impiego delle tecnologie di riconoscimento facciale negli stadi, in quanto sollecitata sia dalla Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia sia da La Liga[25].

Infatti, a seguito dei numerosi episodi di razzismo e xenofobia verificatisi sugli spalti in occasione di manifestazioni sportive, la Comisión si era rivolta all'AEPD affinché chiarisse se fosse compatibile con la normativa sulla protezione dei dati la stipula di un accordo con i *club* che prevedesse l'installazione di sistemi di biometrici per il controllo degli accessi alle *gradas de animación*[26] e l'identificazione univoca dei tifosi presenti in quelle zone "calde".

La facoltà di installare simili apparecchiature avrebbe potuto basarsi sulla competenza attribuita alla stessa *Comisión* dall'art. 13, primo comma, della *Ley 19/2007*[27], che prevedeva la possibilità di disporre misure di sicurezza aggiuntive per gli eventi sportivi "ad alto rischio", tra le quali, alla lett. b), la promozione di sistemi di verifica dell'identità delle persone che intendevano accedere agli impianti. Allo stesso modo, il trattamento dei dati biometrici avrebbe potuto trovare fondamento nella nozione di "interesse pubblico" di cui all'art. 9, par. 2, lett. g) del GDPR, coincidente con la sicurezza e l'integrità degli spettatori, e con la prevenzione della violazione dei diritti fondamentali delle persone nonché dei crimini d'odio.

Tuttavia, se nel caso sottoposto all'Autorità danese, quest'ultima aveva ritenuto sufficiente la sussistenza di un generico interesse pubblico sostanziale per autorizzare l'implementazione di un sistema di riconoscimento facciale, diversamente, l'AEPD ha adottato un approccio molto rigoroso. In particolare, nell'*informe* N/REF: 0098/2022[28] il Garante spagnolo ha precisato che l'accordo prospettato non sarebbe stato conforme alla normativa sulla protezione dei dati personali, in quanto l'art. 13 della *Ley 19/2007* non contiene un riferimento esplicito all'utilizzo di sistemi biometrici. Inoltre, l'Autorità ha sottolineato come il trattamento dei dati biometrici *ex* art. 9, par. 2, lett. g) del GDPR non trovi corrispondenza in una fonte di rango primario che specifichi, tra l'altro, quale sia l'interesse pubblico essenziale capace di giustificare la limitazione del diritto alla protezione dei dati (e in quali circostanze), e che stabilisca regole precise tali da rendere prevedibile, per l'interessato, l'imposizione di una simile restrizione e le sue conseguenze.

Attualmente, in Spagna, soltanto il consenso libero e informato dell'interessato potrebbe consentire il trattamento dei suoi dati biometrici. Infatti, ad oggi, sono solamente due i sistemi di riconoscimento facciale attivi nel Paese, uno installato presso lo stadio El Sadar dell'Osasuna[29] e l'altro

[25] Organizzazione associativa sportiva spagnola composta dai club e dalle società sportive di calcio coinvolte nelle varie categorie professionali dei campionati spagnoli.
[26] L'equivalente della zona degli spalti occupata dalla tifoseria più attiva.
[27] Si tratta della *Ley 19/2007 contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.*
[28] Il testo integrale è reperibile al seguente link: 2022-0098.pdf (aepd.es)
[29] Per maggiori informazioni sulla genesi dell'implementazione del sistema, si veda N. Hernández, *Accesos más rápidos y seguros: el primer sistema de reconocimiento facial de LaLiga ya está operativo*, in *El Español*, 22 maggio 2022.

DPCE online
ISSN: 2037-6677

presso lo stadio Mestalla del Valencia[30]. In entrambi i casi il sistema è impiegato a fini di autenticazione, per facilitare l'accesso all'impianto sportivo degli abbonati, e presuppone una procedura di inserimento dei dati personali, della foto dell'abbonamento e di un documento d'identità e, infine, lo scatto di un *selfie* all'interno di un'*app* ufficiale. Ciò consente di recarsi direttamente presso l'ingresso riservato, ove, esibendo semplicemente il proprio volto, si accede all'impianto eliminando, così, i lunghi tempi di attesa all'entrata.

Per quanto concerne La Liga, quest'ultima aveva avviato una gara d'appalto per lo sviluppo di una tecnologia di riconoscimento facciale per regolare l'accesso dei tifosi allo stadio. Appresa tale circostanza dalla stampa, l'AEPD ha deciso di intervenire, nell'ambito delle sue competenze, per vigilare sul rispetto della normativa del GDPR. Pertanto, attraverso l'*advertencia* AI/00394/2023[31] ha informato *La Liga* del dovere di svolgere "*el triple juicio de proporcionalidad*" (ossia, il *juicio de idoneidad, de necesidad y proporcionalidad en sentido estricto*) prima di trattare i dati biometrici, sottolineando l'importanza di valutare prioritariamente se esistano altri sistemi meno invasivi capaci di raggiungere lo stesso scopo.

In particolare, la soluzione interlocutoria prospettata nell'*advertencia* ha lasciato trapelare una vena critica relativa alla scelta della Liga, laddove l'Autorità garante ha affermato che il sistema biometrico proposto per l'accesso può essere utile per l'organizzazione degli eventi sportivi, ma «non è affatto necessario» nell'ottica del GDPR, poiché non si tratta dell'unico sistema in grado di realizzare la finalità prescelta. La "necessità" dell'impiego di un certo strumento, infatti, non deve essere confusa con la "convenienza" per l'organizzazione: la maggiore velocità di verifica e la riduzione dei costi non sono ragioni idonee a giustificare l'utilizzo dei sistemi in parola.

6. Un primo bilancio conclusivo

Alla luce delle considerazioni sin qui svolte, vengono in evidenza alcuni aspetti che presentano come minimo comun denominatore una sorta di "opacità", intesa nella sua accezione più propria di condizione di "non trasparenza".

La novità del tema, il quale interseca, tuttavia, questioni classiche del diritto pubblico attinenti al rapporto tra autorità e libertà[32], è potenzialmente in grado di ostacolare i tentativi di fare chiarezza sullo stato dell'arte e sulle prospettive future del rapporto tra le tecnologie di riconoscimento facciale e il mondo del calcio (o, più in generale, dello sport).

Eppure, l'analisi di ciò che accade all'interno degli stadi appare un punto di osservazione privilegiato, poiché tali luoghi sono stati interpretati come "laboratori" ove sperimentare misure di controllo da estendere, in un

[30] Á.C. Álvarez, *Facephi permitirá entrar 'por la cara' en Mestalla a los abonados del Valencia CF*, in *elEconomista.es*, 4 giugno 2021.
[31] Consultabile al seguente link: ai-00394-2023-advertencia.pdf (aepd.es).
[32] Basti pensare alla tensione tra il mantenimento dell'ordine pubblico e della sicurezza e la tutela dell'effettività del diritto di riunione.

secondo momento, ad altri spazi pubblici e accessibili al pubblico[33]. La parabola descritta potrebbe essere, quindi, evocativa del percorso intrapreso dagli impieghi dei sistemi di riconoscimento facciale su una scala più ampia.

Volendo trarre delle conclusioni a partire dai punti di contatto emersi dai casi presentati, il primo elemento *opaco* che accomuna le varie esperienze può individuarsi nelle ambiguità del funzionamento e degli scopi dell'adozione degli applicativi in esame. Infatti, raramente è possibile reperire puntuali indicazioni circa le modalità con cui essi operano: nelle vicende analizzate si fa generico riferimento al controllo dei varchi d'ingresso, ma non sempre si comprende se si stia parlando di autenticazione o identificazione oppure di un monitoraggio che avviene in tempo reale o *ex post*. Allo stesso modo, la confusione è dimostrata dalla sovrapposizione delle molteplici finalità, tra cui la prevenzione, la sicurezza, la gestione degli accessi, la lotta al razzismo e alle discriminazioni e l'individuazione degli autori di reati e dei destinatari di misure impeditive di accesso.

Stante la difficoltà di distinguere concetti quali "autenticazione" e "identificazione", occorre che gli eventuali utilizzatori dei sistemi di riconoscimento facciale compiano uno sforzo definitorio delle attività che stanno svolgendo, perché dalla configurazione degli aspetti elencati derivano diverse implicazioni, sia sul piano dei diritti e delle libertà sia sugli strumenti giuridici che possono essere attivati a tutela di questi ultimi.

Il secondo profilo di *opacità* – o meglio, di oscurità – riguarda la totale assenza di informazioni relative al concreto utilizzo e ai risultati prodotti dalla tecnologia biometrica in esame. La mancata conoscenza del numero di casi in cui i sistemi vengono impiegati, dei loro tassi di errore e dei *bias* discriminatori presenti al momento della loro progettazione od operatività determinano evidenti problematiche, impedendo un controllo pubblico di tali tecnologie e rendendo impossibile effettuare una seria e completa valutazione, per ciò che qui interessa, dei vantaggi conseguenti al loro uso all'interno degli stadi di calcio.

Al difetto di trasparenza degli utilizzatori dei dispositivi si aggiunge un terzo elemento *opaco*, legato al momento in cui la macchina genera un *alert* in seguito all'identificazione di un soggetto il cui volto è presente nel *database* interrogato. Nei provvedimenti delle *Authorities* vengono richiamate soltanto le norme del GDPR, dal momento che titolari del trattamento risultano le società calcistiche. Tuttavia, a livello pratico, e salve le ipotesi di autenticazione dietro consenso, la corrispondenza rilevata dal *software* di riconoscimento facciale implica automaticamente il coinvolgimento delle Forze dell'ordine; tuttavia, il trattamento, da quanto si evince, rimane comunque sottoposto alla disciplina del GDPR e non a quella più stringente prevista dalla LED per le attività di *law enforcement*. Si verifica, dunque, una situazione singolare, poiché la quasi totalità degli scopi perseguiti attraverso l'utilizzo di tali tecnologie negli stadi rimanda ad attività di controllo di polizia cui non fa seguito l'adozione dell'opportuna normativa.

Considerati questi aspetti non è dunque casuale, giungendo all'ultimo tratto di *opacità*, che gli interventi delle Autorità garanti di cui si è dato conto

[33] Paradigmatico il caso italiano della misura del Divieto di accesso alle aree urbane (DACUR), la quale rappresenta una delle varie declinazioni dell'"originale" Divieto di accesso alle manifestazioni sportive (DASPO).

DPCE online
ISSN: 2037-6677

siano stati caratterizzati da decisioni disomogenee sul tema, pur avendo alla base gli stessi parametri normativi. Per certo, l'uniformità delle posizioni delle *Authorities* non è attesa o richiesta, anche in virtù della competenza esclusiva in materia di sicurezza riservata agli Stati membri dall'art. 4, par. 2 del Trattato sull'Unione Europea, la quale ammette così l'esistenza di scenari variegati. Ciononostante, potrebbe profilarsi di indubbia utilità la ricerca di un orientamento uniforme che possa guidare l'interpretazione e l'applicazione del GDPR relativamente all'impiego del riconoscimento facciale negli stadi. Del resto, una simile opzione sarebbe in linea con le ragioni di armonizzazione sottese alla scelta del regolamento quale fonte per disciplinare i sistemi di intelligenza artificiale.

Nel quadro appena tratteggiato non rimane allora che attendere l'entrata in vigore del regolamento sull'intelligenza artificiale[34] (il c.d. "AI Act") per verificare l'impatto che avrà sull'utilizzo delle tecnologie in parola nell'ambito delle manifestazioni sportive e constatare se contribuirà a rimuovere i fattori di opacità rilevati.

Il testo definitivo, approvato dal Parlamento europeo e dal Consiglio dopo un tortuoso *iter* legislativo, fornisce già alcune valide indicazioni. In particolare, l'uso dell'identificazione biometrica in tempo reale in spazi accessibili al pubblico per finalità di *law enforcement* è inserito tra le pratiche vietate dall'art. 5. Tuttavia, al par. 1, lett. h) dello stesso articolo sono contemplate tre eccezioni che ne ammettono l'utilizzo qualora sia strettamente necessario e al solo fine di confermare l'identità di un soggetto determinato[35]: a) la ricerca mirata di specifiche vittime di rapimento, tratta o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; b) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica di persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; c) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, dell'esercizio dell'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'Allegato II[36], punibile nello Stato membro interessato con una pena detentiva o una misura di sicurezza della durata massima di almeno quattro anni. Inoltre, ai sensi dei par. 2 e 3 dell'art. 5, l'impiego di tali tecnologie è subordinato al completamento di una valutazione d'impatto sui diritti

[34] Occorre puntualizzare che il regolamento sarà pienamente applicabile dopo 24 mesi dall'entrata in vigore, salve le eccezioni delle pratiche di IA vietate, le quali dovranno essere gradualmente eliminate entro sei mesi, così come i codici di condotta e le norme di *governance* generali, da seguire rispettivamente dopo nove e dodici mesi. D'altro canto, gli obblighi per i sistemi ad alto rischio saranno ritardati di un altro anno, con applicazione dopo 36 mesi.

[35] Come indicato dal par. 2 dell'art. 5.

[36] All'interno della lista figurano: terrorismo; tratta di esseri umani; sfruttamento sessuale di minori e pornografia minorile; traffico illecito di stupefacenti o sostanze psicotrope; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario, lesioni gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive; sequestro, detenzione illegale e presa di ostaggi; reati sotto la giurisdizione della Corte penale internazionale; illecita cattura di aeromobile o nave; violenza sessuale; reati ambientali; rapina organizzata o a mano armata; sabotaggio; partecipazione a una organizzazione criminale coinvolta in uno o più reati tra quelli elencati.

fondamentali e ad un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente[37].

Quanto ai sistemi di identificazione biometrica *ex post*, essi sono stati inseriti, invece, tra le pratiche ad alto rischio: il loro utilizzo non è quindi proibito, ma deve essere comprovato il legame con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa, oltre alla necessaria previsione di misure di trasparenza e l'obbligo per i *deployer* di ottenere l'autorizzazione delle autorità competenti (art. 26, par. 10).

Per la prima volta, l'AI Act introduce una disciplina *ad hoc* per le tecnologie di riconoscimento facciale, delineando un'articolazione di tutele che investe sia il momento della loro produzione e immissione nel mercato, sia quello della concreta operatività. Insieme al GDPR e alla LED, il regolamento andrebbe quindi ad offrire quella base giuridica, invocata da anni, idonea a precludere un uso arbitrario dei dispositivi biometrici, svincolato da precisi parametri normativi.

Emergono, però, alcune criticità che attenuano, in una certa misura, la portata "rivoluzionaria" del regolamento: non convince pienamente l'ampio ventaglio di reati che giustificherebbe l'adozione di sistemi di riconoscimento facciale in tempo reale nonché l'aver circoscritto il divieto di questi ultimi alle attività di *law enforcement* in spazi accessibili al pubblico, facendo così ricadere le ipotesi "scoperte" sotto il GDPR con le problematiche sopra menzionate[38]. Congiuntamente ai "deboli" limiti che corredano la modalità *a posteriori*[39], il rischio presentato è quello di un utilizzo delle tecnologie biometriche per finalità ulteriori rispetto a quanto previsto[40]. La perplessità principale riguarda, tuttavia, l'eventualità che un'autorità amministrativa indipendente possa concedere l'autorizzazione per attivare i sistemi di riconoscimento facciale. Dal momento che il trattamento incide sulla sfera dei diritti fondamentali degli individui, dovrebbe spettare esclusivamente all'autorità giudiziaria la valutazione sul bilanciamento tra interessi costituzionalmente garantiti. Per di più, si pensi anche al fatto che le agenzie formalmente indipendenti potrebbero comunque subire le influenze governative[41].

Le disposizioni dell'AI Act riportate consentono, quindi, di constatare un approccio non particolarmente restrittivo delle istituzioni europee sul tema. Di conseguenza, la questione dovrà essere valutata alla luce dei meccanismi di salvaguardia predisposti dal regolamento, ma soprattutto

[37] Fatte salve le situazioni d'urgenza debitamente giustificate dove l'uso del sistema può essere avviato senza autorizzazione, a condizione che essa sia richiesta, al più tardi, entro 24 ore dall'impiego. L'autorizzazione dovrà comunque essere preceduta da una valutazione preventiva d'impatto sui diritti fondamentali.

[38] Così M. Veale, M. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 4/2021, 101.

[39] In questi termini, P. Hacker, *Comments on the Final Trilogue Version of the AI Act*, 23 gennaio 2024, 8.

[40] R.J. Neuwirth, *Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act*, in *Computer Law & Security Review*, aprile 2023.

[41] P. Hacker, *Comments*, cit., 7.

DPCE online
ISSN: 2037-6677

della prassi applicativa, la quale coinvolgerà, senza dubbio, anche gli eventi sportivi.

A partire dai provvedimenti delle Autorità garanti per la protezione dei dati personali di diversi Paesi europei, non resta dunque che monitorare con sguardo critico le future modalità d'impiego delle tecnologie biometriche, con un *focus* sull'ambito calcistico che potrebbe rappresentare un "banco di prova" per testare l'effettività degli strumenti approntati dall'AI Act.

Lorenzo Sottile
Dipartimento di Scienze Politiche e Internazionali
Università degli Studi di Genova
lorenzo.sottile@edu.unige.it