Diritto dello Sport (ISSN 2785-1141) Bologna University Press
Vol. 02 n. 02 (2021) https://doi.org/10.30682/disp0202b

ASSOCIAZIONI SPORTIVE DILETTANTISTICHE (ASD) E PROTEZIONE DEI DATI PERSONALI NEGLI ORIENTAMENTI DEL GARANTE

Fabio Bravo

Professore ordinario di Diritto Privato e Direttore del Corso di Alta Formazione in "*Data Protection e Privacy Officer*" all'Università di Bologna

Abstract

Il contributo, utilizzando un approccio orientato all'analisi della casistica, quale risulta dalla disamina dei provvedimenti del Garante per la protezione dei dati personali, indaga le principali questioni giuridiche concernenti l'applicazione della disciplina sulla privacy nell'ambito delle attività delle associazioni sportive dilettantistiche (ASD), evidenziando altresì l'importanza sia della conoscenza della prassi applicativa, attraverso lo studio del *case law* in tale materia, sia della individuazione di figure interne all'associazione, adeguatamente formate per garantire la *compliance* in tale specifico ambito dell'ordinamento giuridico.

Parole chiave: Associazioni sportive dilettantistiche (ASD), Privacy, Protezione dei dati personali, Responsabile della Protezione dei Dati (RPD), Conformità al GDPR

Abstract

This essay, through the lens of case law concerning the rulings of the Italian Supervisor Authority, analyses the main legal issues relating to the compliance with data protection law by Amateur Sports Associations (ASA). Then it highlights the importance of both expert knowledge of practices, also through the study of case law in this area, and the identification of figures within the association, adequately trained in this specific area of the legal system.

Keywords: Amateur Sports Associations (ASA), Privacy, Data protection, Data Protection Officer (DPO), GDPR compliance

1. Premessa

Il rapporto tra le fonti in materia di protezione dei dati personali delinea un quadro sicuramente complesso,[1] che necessita di essere interpretato mettendo a sistema le numerose norme collocate su piani diversi.[2] La loro

[1] La disciplina del diritto alla *privacy*, benché relativamente recente (la prima teorizzazione si fa risalire a S. Warren, L. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890), ha subito profondi mutamenti nel corso del tempo ed è tuttora in evoluzione, come ben si comprende se si tiene a mente che il legislatore europeo, dopo l'emanazione del Reg. UE 2016/679, noto come GDPR (*General Data Protection Regulation*), ha varato, negli ultimi mesi del 2020, una proposta di regolamento sulla *Governance* europea dei dati (*European Governance Act*), destinato ad incidere ulteriormente ed in modo significativo sulla materia, cfr. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, COM/2020/767 final, Bruxelles, 25.11.2020. Per un primo commento si rinvia a F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256.

applicazione in contesti specifici non sempre risulta agevole. Rimandando ad altra sede l'analisi sistematica della disciplina in materia di protezione dei dati personali e degli adempimenti ivi prescritti,[3] che esula dalle finalità del presente contributo, in queste pagine ci si propone di individuare e discutere, con un approccio casistico aderente ad un'impostazione di tipo giusrealista,[4] quali siano le principali criticità che la disciplina ha presentato e tuttora presenta nello specifico settore di operatività delle associazioni sportive dilettantistiche (ASD). Si procederà, sul piano metodologico, analizzando gli orientamenti del Garante per la protezione dei dati personali che appaiono maggiormente significativi, per poi delineare alcune osservazioni conclusive su quale approccio sia opportuno avere per una più corretta gestione della disciplina in esame nel corso della vita associativa.

2. La casistica rilevante

Nella prospettiva poc'anzi delineata, meritano attenzione sia i provvedimenti specificamente resi dal Garante per la protezione dei dati personali in tema di associazioni sportive dilettantistiche (ASD), sia altre decisioni di particolare interesse anche per quest'ultime, benché emanate con riguardato a società sportive dilettantistiche o in altri contesti, in cui si sono presentati problemi la cui analisi è comunque di rilievo anche per le ASD medesime.

Tra gli orientamenti di maggior interesse, da cui trarre indicazioni utili nel settore in esame ed individuare criticità e problemi applicativi emersi nella prassi, appaiono significativi quelli resi in tema di videosorveglianza, schede di ammissione alle attività didattico-sportive, controlli biometrici degli accessi, raccolta dati tramite *form* su siti Internet dell'associazione, risposte a recensioni su Internet (canali *social*, siti *web* e *blog*), *marketing* e altre comunicazioni commerciali, accesso a valutazioni medico-legali in caso di infortuni e sinistri a fini assicurativi, gestione di certificati medici sull'idoneità o inidoneità all'attività sportiva, utilizzo di immagini su canali *social* e altri contesti (album figurine); consenso dei genitori per i dati relativi a minori.

3. Sistemi di videosorveglianza e schede di ammissione alle attività didattico-sportive

Il Garante, con provv. n. 443 del 27 ottobre 2016, ha sanzionato un'associazione sportiva dilettantistica (ASD) per omessa informativa relativa al trattamento dei dati personali effettuato tramite il proprio impianto di videosorveglianza composto da tre telecamere installate all'esterno dei locali dell'associazione (due verso il parcheggio e una verso l'entrata dei locali) e di una telecamere all'interno dei locali medesimi, in zona adibita a ingresso/bar, con monitor presente nell'ufficio ammnistrativo per la visione e il controllo delle immagini.[5] Il

[2] Attualmente le fonti principali che disciplinano la materia sono collocate a diversi livelli. Sul piano internazionale si pensi all'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, che tutela la vita privata e familiare. Si pensi ancora alla Convenzione n. 108 del 1981, recentemente aggiornata con Protocollo addizionale del 2018 per tener conto dell'evoluzione della disciplina in materia di protezione dei dati personali avutasi nell'UE con il GDPR, dando luogo al nuovo testo noto ora come Convenzione 108+. Nell'ordinamento europeo si pensi all'art. 8 della Carta dei diritti fondamentali dell'UE, che tutela il diritto alla protezione dei dati personali, collocata all'apice del sistema delle fonti dell'UE, nonché al citato Reg. UE n. 2016/679, che ha sostituito la dir. 95/46/CE. Ancora, nel diritto nazionale si colloca il Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003, in cui sono confluiti diversi atti normativi di diritto interno su tale materia, ad iniziare dalla l. 675/96), modificato significativamente dal d.lgs. n. 101/2018 per le necessità di coordinamento con le disposizioni del Regolamento europeo (GDPR). Ancora, sempre nel nostro diritto interno, la disciplina è arricchita da atti normativi subprimari, di valenza generale, emanati dal Garante in materia di protezione dei dati personali, che contribuiscono a delineare una disciplina di dettaglio in questo specifico settore dell'ordinamento.

[3] Per una disamina della disciplina del Reg. UE 2016/679 (GDPR) si rinvia, in particolare, a R. D'Orazio-G. Finocchiario-O. Pollicino-G. Resta (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè, 2021; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, Cedam-Wolters Kluwer, 2019; F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, Cedam-Wolters Kluwer, 2018.

[4] Sulla lettura giusrealista in materia di protezione dei dati personali si veda G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Il diritto dell'informazione e dell'informatica*, 1997, 4-5, pp. 703-734 e, ivi, spec. par. 3. Per un'impostazione di carattere generale sul realismo giuridico si rimanda, tra tutti, alle magistrali pagine di Giovanni Tarello e, in particolare, a G. Tarello, voce "*Realismo giuridico*", in *Novissimo Digesto italiano*, Torino, Utet, 1959; Id., *Il realismo giuridico americano*, Milano, Giuffrè, 1962.

[5] Garante per la protezione dei dati personali, Provvedimento n. 443 del 27 ottobre 2016, doc. web n. 6085311.

procedimento ha preso avvio a seguito di contestazione elevata con verbale del Corpo della Polizia Municipale. Nelle difese articolate nell'ambito del procedimento svolto innanzi al Garante, ove veniva contestata la regolarità del sistema di videosorveglianza anche con riferimento all'assenza di un'adeguata informativa, l'ASD ha sostenuto che gli iscritti all'associazione "sono da considerarsi atleti associati"[6] e che "legittimati ad accedere all'interno dell'area cortile attraverso il cancello […] sono solamente i soci in possesso di regolare tessera […]",[7] precisando che "Al momento della sottoscrizione della richiesta di ammissione a socio, l'aspirante atleta sottoscrive la dichiarazione di consenso ai sensi […]"[8] della normativa in materia di protezione dei dati personali. Secondo l'associazione, da ciò ne deriverebbe che "chiunque acceda all'interno della proprietà della […] ASD sia pienamente informato in merito alla presenza delle telecamere, non essendo possibile, contrariamente a quanto sostenuto dai verbalizzanti, l'accesso del pubblico".[9] Inoltre, l'ASD ha ritenuto di argomentare sostenendo che "Quanto contestato dai verbalizzanti risulta privo di fondamento logico, in quanto teso a sanzionare un soggetto […] per le riprese video ai danni di sé stesso".[10] L'ASD ha poi argomentato che, quanto alle telecamere poste all'esterno dei locali, "risulta evidente dalla documentazione fotografica prodotta che le riprese, sia per l'angolo visuale che per la potenza dell'obiettivo, non siano idonee a far distinguere i tratti somatici di eventuali passanti".[11]

Il Garante, all'esito del procedimento, non ha accolto le argomentazioni difensive dell'ASD, rimarcando che quest'ultima, in qualità di titolare del trattamento, non è esonerata dal rendere l'informativa ai propri associati, che, ancorché facciano parte dell'associazione, sono pur sempre da considerare interessati al trattamento, quali persone fisiche a cui i dati si riferiscono.[12] Inoltre, l'informativa deve avere i contenuti previsti dalla legge (art. 13 del Codice in materia di protezione dei dati personali, ora sostituito dall'art. 13 del GDPR) e non può essere considerata equivalente ad essa la *liberatoria* fatta firmare per l'uso delle immagini fatta firmare agli associati, né è idonea a tale scopo la dichiarazione di consenso ai sensi della disciplina in materia di protezione dei dati personali priva degli elementi informativi richiesti dall'art. 13 cit.[13]

Le questioni relative alla videosorveglianza risultano tra quelle numericamente più significative in relazione ai trattamenti svolti dalle ASD. In altro procedimento, culminato con provv. n. 79 del 25 febbraio 2016, il Garante ha sanzionato un'ASD per informativa incompleta relativa al trattamento dei dati personali effettuato, anche in orari notturni, con impianto di videosorveglianza composto da due telecamere collegate a un apparecchio di videoregistrazione e un monitor.[14] L'omissione ha riguardato alcuni degli elementi informativi previsti dal provvedimento generale del Garante in materia di videosorveglianza, adottato l'8 aprile 2010, con il quale è stata prevista l'informativa in forma semplificata, mediante un'immagine tipizzata che renda facilmente edotto l'interessato di tale tipologia di trattamento, accompagnata dall'indicazione del titolare e delle finalità del trattamento.

Le difese articolate dall'ASD rimarcavano che "il funzionamento di due telecamere è stato effettuato artigianalmente, al solo ed esclusivo fine di sventare/disincentivare furti […]"[15] e che "la videosorveglianza è stata dichiarata in modo chiaro ed esplicito e che i cartelli apposti la rendevano conosciuta da chiunque frequentasse il club"[16] sportivo.

Il Garante ha disatteso le argomentazioni difensive, precisando che la condotta contestata concerne il mancato corretto assolvimento dell'obbligo informativo di cui all'art. 13 del Codice della privacy, ora art. 13 GDPR, secondo le modalità disciplinate dal punto 3.1 del provvedimento generale del Garante in materia di

[6] *Ibidem*.
[7] *Ibidem*.
[8] *Ibidem*.
[9] *Ibidem*.
[10] *Ibidem*.
[11] *Ibidem*.
[12] *Ibidem*.
[13] *Ibidem*.
[14] Garante per la protezione dei dati personali, Provvedimento n. 79 del 25 febbraio 2016, doc. web n. 5422764.
[15] *Ibidem*.
[16] *Ibidem*.

 doi.org/10.30682/disport0202b

videosorveglianza dell'8 aprile 2010. Specificamente, il Garante ha contestato la circostanza che l'informativa apposta dall'ASD risultava "priva dell'indicazione del titolare del trattamento dei dati effettuato mediante l'utilizzo di un impianto di videosorveglianza […]".[17] Altro profilo ha riguardato i tempi di conservazione delle immagini riprese dall'impianto di videosorveglianza effettuato dall'ASD, che, in sede di accertamento, sono risultati superiori a quelli di una settimana previsti nel punto 3.4 del citato provvedimento generale in materia di videosorveglianza, né l'associazione aveva chiesto una verifica preliminare al Garante al fine di poter legittimamente procedere a un allungamento dei tempi di conservazione delle immagini per un periodo maggiore (nel caso di specie era stata riscontrata, dal Comando Compagna della Guardia di Finanza che ha proceduto all'accertamento, che l'associazione sportiva dilettantistica aveva conservato le immagini per un periodo di ventinove giorni).[18]

Altro caso rilevante, in tema di videosorveglianza e impianti sportivi, è stato deciso dal Garante con provv. dell'8 marzo 2008.[19] Non ha riguardato un'ASD ma una società di gestione di un parco termale, che aveva allestito un sistema di videosorveglianza consistente in due coppie di telecamere installate negli spogliatoi maschili e femminili della piscina termale situata all'interno del parco, con registrazione delle immagini. L'impianto di videosorveglianza è stato oggetto di attenzione da parte dell'Arma dei Carabinieri a seguito della denuncia di un furto avvenuto negli spogliatoi della piscina: i militari dell'Arma, nell'ambito dell'attività investigativa, avevano provveduto all'acquisizione della videocassetta riportante le immagini del predetto sistema di videosorveglianza. Dalla loro disamina, come risultante documentalmente anche dall'annotazione di polizia giudiziaria allegata alla comunicazione trasmessa dai Carabinieri al Garante per la protezione dei dati personali, si è avuto modo di riscontrare che le telecamere installate negli spogliatori "puntavano oltre che nella zona adibita a guardaroba direttamente sugli utenti riprendendoli mentre si cambiavano ed immortalando spesse volte parti intime nude".[20] Il caso è significativo, perché nei pressi delle telecamere era stata accertata la presenza dei cartelli contenenti l'informativa in materia di protezione dei dati personali, ancorché scarna, e le telecamere non risultavano nascoste. Il Garante, tuttavia, ha "rilevato che, nonostante l'eventuale visibilità delle telecamere e la presenza, nei pressi, di alcuni cartelli riportanti una scarna informativa, il trattamento di dati personali in esame risulta comunque effettuato in violazione della riservatezza e della dignità delle persone interessate che frequentano il Parco".[21] Ancora, il Garante ha rimarcato anche che il trattamento risultava effettuato "in violazione del principio di pertinenza e non eccedenza […] atteso che i sistemi di videosorveglianza possono essere utilizzati lecitamente a tutela del patrimonio riprendendo eventualmente aree destinate a guardaroba, ma adottando in ogni caso idonei accorgimenti tecnici volti ad inibire riprese indebite di persone mentre utilizzano gli spogliatoi".[22]

Altro caso è stato affrontato dal Garante con provv. n. 434 del 3 ottobre 2013, su accertamento del Nucleo privacy della Guardia di Finanza, che ha riscontrato, con riguardo ad una società sportiva dilettantistica, sia l'assenza di cartelli riportanti l'informativa da rendere con riferimento alle telecamere di videosorveglianza poste nei punti di accesso alla struttura, sia l'effettuazione di "una raccolta di dati personali tramite *scheda di ammissione alle attività didattiche-sportive*, a fronte della quale è stata riscontrata l'inidoneità dell'informativa di cui all'art. 13 del Codice",[23] ora art. 13 del GDPR.

Avverso la duplice contestazione, negli scritti difensivi la società sportiva dilettantistica, titolare del trattamento, ha dichiarato che: (i) per quanto concerne la videosorveglianza, l'informativa era assente "per cause ignote alla società"[24] solamente in corrispondenza delle telecamere poste in prossimità di due dei quattro accessi alla struttura, riservati a fornitori e dipendenti, che tuttavia, a seguito dell'accertamento, venivano immediatamente integrati; (ii) per quanto concerne invece l'informativa privacy relativa al trattamento dei dati

[17] *Ibidem*.
[18] *Ibidem*.
[19] Garante per la protezione dei dati personali, Provvedimento dell'8 marzo 2008, doc. web n. 1391803.
[20] *Ibidem*.
[21] *Ibidem*.
[22] *Ibidem*.
[23] Garante per la protezione dei dati personali, Provvedimento n. 434 del 3 ottobre 2013, doc. web n. 2792767.
[24] *Ibidem*.

raccolti in fase di iscrizione, la stessa "sia sempre stata resa alla clientela attraverso la libera consegna dell'apposita scheda".[25]

Il Garante, valutate le argomentazioni difensive, ha considerato pacifica l'assenza dell'informativa in prossimità di alcune delle telecamere usate nell'impianto di videosorveglianza, ritenendo quindi confermati dalle dichiarazioni della società sportiva dilettantistica l'omissione oggetto di contestazione. Quanto all'inidoneità dell'informativa sulla scheda di ammissione/iscrizione alla struttura, il Garante ha rilevato che l'omissione risulta confermata dalle dichiarazioni rese direttamente alla Guardia di finanza in sede di accertamento, ove era stato precisato che l'informativa, un tempo fornita, a partire da una certa data non sarebbe stata più rilasciata, neanche oralmente, in occasione della compilazione o del rilascio della scheda di ammissione alle attività.

4. Controlli biometrici degli accessi

Un'ulteriore rilevante questione ha riguardato l'uso dei controlli biometrici degli accessi ai locali adibiti all'attività sportiva. Con provv. n. 127 del 29 marzo 2012 il Garante si è pronunciato, su segnalazione di un associato, sull'utilizzo di un sistema di rilevazione dei dati biometrici degli utenti da parte di un'ASD per finalità di accesso alle proprie strutture.[26] A seguito della segnalazione sono stati svolti accertamenti ispettivi nella sede dell'associazione, con acquisizione di documentazione.

Nella segnalazione veniva denunciata l'avvenuta installazione, presso una palestra gestita dall'ASD, di un sistema di rilevazione dei dati biometrici degli utenti per la gestione dell'accesso alla struttura: al momento dell'iscrizione all'associazione veniva acquisita l'impronta digitale dell'associato, mediante lettore ottico/scanner collegato a personal computer situato presso la reception della palestra; l'impronta digitale, così acquisita, veniva poi utilizzata per l'identificazione dell'interessato ai fini dell'accesso alla palestra, mediante apposizione del dito su un lettore ottico situato accanto ad un tornello, con conseguente sblocco del cancello rotativo installato nel tornello medesimo. Nella segnalazione veniva precisato che l'ASD non rilasciava tessere o schede, sicché l'acquisizione dell'impronta digitale per l'impiego biometrico costituiva l'unica modalità di accesso alla palestra. Il relativo trattamento dei dati veniva ritenuto eccedente rispetto alle finalità perseguite dal titolare del trattamento, dato che il controllo dell'identità degli associati si sarebbe potuto fare con strumenti alternativi (quali badge a banda magnetica o con microchip, eventualmente muniti di fotografia) e non sussistevano esigenze di sicurezza tali da giustificare il ricorso alla tecnologia biometrica.

Nella segnalazione veniva anche lamentata l'assenza di un'adeguata informativa in materia di protezione dei dati personali, che tra l'altro veniva fornita – secondo il segnalante – solamente a seguito di specifica richiesta e non spontaneamente e sistematicamente ad opera del titolare del trattamento. Nell'informativa, s'è affermato nella segnalazione al Garante, veniva richiamato un generico riferimento ai trattamenti di dati personali effettuati dall'ASD, senza tuttavia alcuna esplicita menzione del trattamento dei dati biometrici degli utenti, oltre al problema della mancata acquisizione di un consenso specifico a tale tipologia di trattamento ed all'omessa notificazione al Garante del trattamento di dati biometrici prevista dalla previgente normativa ai sensi dell'art. 37 del Codice della privacy, poi abrogato per le esigenze di coordinamento con il GDPR.

Nel corso del procedimento, l'ASD ha rimarcato che le finalità del trattamento dei dati biometrici (attivo fin dal periodo di inizio dell'attività dell'associazione) erano quelle di consentire una maggiore "rapidità e comodità delle operazioni di accesso"[27] degli associati alla palestra e di garantire "una più facile gestione delle scadenze dei periodi di iscrizione all'associazione",[28] assicurando al contempo una "maggiore sicurezza"[29] relativa "all'effettivo diritto di accesso agli impianti della struttura".[30]

[25] *Ibidem*.
[26] Garante per la protezione dei dati personali, Provvedimento n. 127 del 29 marzo 2012, doc. web n. 1891999.
[27] *Ibidem*.
[28] *Ibidem*.
[29] *Ibidem*.
[30] *Ibidem*.

Quanto alla notificazione al Garante, prima richiesta dall'art. 37 (abrog.) del Codice, l'associazione sosteneva di aver provveduto, ancorché in ritardo rispetto all'inizio del trattamento, a causa, tra l'altro, di un "sovraccarico dei server dell'Autorità Garante".[31] Sul punto però, in sede istruttoria, il Garante ha avuto modo di verificare che l'iniziale tentativo di notifica non si era inizialmente concluso per ragioni diverse: mancava infatti la sottoscrizione dell'istanza con firma digitale o altra firma elettronica qualificata.[32]

Inoltre, quanto al sistema biometrico di controllo degli accessi, l'ASD precisava che i dati venivano raccolti dapprima in forma cartacea, al momento della compilazione della scheda di iscrizione, per poi essere successivamente archiviati in forma elettronica, previa informativa resa verbalmente, anche con riguardo al trattamento eventuale dei dati biometrici, qualora vi fosse stato il consenso dell'interessato. Dagli scritti difensivi dell'ASD risulterebbe poi che solamente nel caso in cui l'associato "acconsenta al rilascio del dato biometrico in occasione del primo accesso ai locali della palestra"[33] l'ASD avrebbe proceduto "alla rilevazione ed alla registrazione dell'impronta parziale digitale",[34] lasciando sempre la facoltà, per l'interessato, qualora esprimesse contrarietà a tale trattamento, di "accedere agli impianti mediante il rilascio del tesserino cartaceo sul quale sono riportati i dati […] relativi a: nome e cognome, telefono e periodo di validità dell'iscrizione".[35]

Il processo di iniziale acquisizione del dato biometrico (c.d. procedura di *enrollment*), archiviato e successivamente usato per l'identificazione dell'interessato, prevedeva "il contatto ripetuto per tre volte del dito della mano"[36] dell'interessato. L'impronta digitale, una volta scannerizzata, veniva registrata a seguito di un'elaborazione basata su un algoritmo informatico. L'esito del processo di elaborazione del dato biometrico, usato per fini identificativi, veniva associato ai dati personali anagrafici dell'interessato, unitamente alla data di scadenza dell'abbonamento, al fine di consentirne l'identificazione univoca ad ogni accesso e, di volta in volta, la memorizzazione sul server della data e dell'orario di ingresso alla struttura sportiva. Il server, contenente i dati biometrici e gli ulteriori dati di accesso memorizzati sia in fase di *enrollment* (con generazione dei *template*) che in fase di riconoscimento in occasione di ogni ingresso alla palestra, era ubicato in un apposito locale dietro la segreteria, con accesso riservato al solo personale autorizzato. L'archivio informatizzato dei dati biometrici e degli ulteriori dati, inclusi quelli identificativi, degli interessati era dunque centralizzato. L'ASD rimarcava altresì che il sistema di trattamento era configurato in modo da cancellare automaticamente gli "algoritmi associati ai vari iscritti che risultano non attivi da più di quaranta giorni"[37]. A seguito della cancellazione rimanevano comunque sui server i soli dati anagrafici dell'associato, mantenuti fino alla cancellazione coincidente con la scadenza del periodo associativo o con il mancato rinnovo dell'iscrizione.

Ancora, quanto all'informativa in materia di protezione dei dati personali l'ASD sosteneva che al momento dell'iscrizione all'associazione veniva rilasciata, tramite lo stesso modulo di iscrizione, l'informativa in materia di trattamento dei dati personali. Vero che si tratta di informativa sui trattamenti complessivi dell'ASD, senza indicazione specifica su trattamento dei dati biometrici, ma tale informativa, secondo la ricostruzione dell'associazione medesima, veniva integrata oralmente dal personale addetto alla reception, specificando le caratteristiche del trattamento biometrico e le modalità alternative di accesso alla struttura.

Nel modulo di iscrizione, osservava ancora l'ASD, era prevista anche la raccolta del consenso dell'interessato, essendo previsto uno spazio per l'apposizione della sottoscrizione, preceduto dalla dicitura "firma", senza ulteriori specificazioni.

Nei propri scritti difensivi, l'associazione ha poi dichiarato di aver designato come responsabile del trattamento dei dati, per finalità manutentive, una società esterna e di aver poi provveduto a nominare come incaricati del trattamento il personale della reception e la segretaria dell'associazione, fornendo loro adeguate istruzioni.

[31] *Ibidem*.
[32] *Ibidem*.
[33] *Ibidem*.
[34] *Ibidem*.
[35] *Ibidem*.
[36] *Ibidem*.
[37] *Ibidem*.

Rimarcava poi di aver applicato adeguate e specifiche misure di sicurezza per il trattamento dei dati personali, anche biometrici, degli associati.

L'ASD, infine, faceva presente che il centro sportivo dalla medesima gestito contava circa 900 aderenti l'anno, che la centralizzazione dei *template* generati nel processo biometrico sarebbe stata adottata in quanto ritenuta "il metodo più efficace per garantire la totale protezione dei dati personali dei soggetti sottoposti a trattamento"[38] e che il sistema di trattamento così congegnato sarebbe "stato scelto per evitare rischi di eventuali smarrimenti o furti di tessere contenenti indicazioni dei dati personali dei soggetti sottoposti a trattamento".[39]

Il Garante, nel provvedimento citato, ha chiarito che la raccolta e l'utilizzo di impronte digitali, così come delle informazioni ricavate a partire da dette impronte, nelle procedure di autenticazione o di identificazione costituiscono operazioni di trattamento di dati personali e ciò anche qualora il dato biometrico sia raccolto per soli fini di completamento della fase di *enrollment* e venga successivamente utilizzato quale *template* generato dall'algoritmo informatico per le operazioni di verifica e raffronto. I dati biometrici, precisa ancora il Garante, possono essere usati solo in casi particolari (quali ad esempio circostanze obiettive e situazioni concrete e documentate connotate da elevato rischio), tenendo conto delle finalità e del contesto in cui sono stati trattati e pertanto "non può […] ritenersi lecito un impiego generalizzato e indiscriminato di dati biometrici, specie ove funzionale a soddisfare generiche esigenze di sicurezza, ovvero a perseguire finalità di natura essenzialmente amministrativa".[40] Peraltro, osserva ancora il Garante, anche in presenza di "situazioni di elevato rischio, il titolare del trattamento è comunque tenuto a valutare con estrema cautela il ricorso a tale peculiare trattamento, dovendo a tal fine conservare (e privilegiare) tutte le possibili misure alternative ugualmente efficaci in rapporto alle finalità perseguite, tenendo anche conto dell'obbligo (legislativamente previsto) di configurare i sistemi informativi in modo da escludere il trattamento dei dati personali non necessari in rapporto alle medesime finalità".[41] Nel caso di specie, invece, "le operazioni di accesso alla palestra non risultano connotate da un elevato grado di rischiosità per i beni o per le persone, tale da giustificare l'obiettiva necessità di effettuare un accertamento particolarmente rigoroso dei soggetti legittimati all'ingresso"[42].

Ancora, oltre al rispetto dei principi di necessità e proporzionalità, violati nel caso di specie, l'autorità di controllo ha argomentato anche in riferimento ai principi di liceità e correttezza del trattamento: in particolare, per quanto riguarda l'acquisizione del consenso al trattamento dei dati personali, nel caso di specie non può ritenersi validamente espresso in forma libera e specifica in riferimento a trattamenti chiaramente individuati, il che rende il trattamento illecito (per difetto della condizione di liceità del trattamento). Infatti il consenso acquisito secondo la prassi evidenziata dall'ASD nel caso di specie non è da ritenersi valido perché risulta "genericamente acquisito dall'associazione in relazione a una pluralità di trattamenti indifferenziati svoti 'nell'ambito di pratiche amministrative e sportive interne alla stessa', oltre che per il 'corretto svolgimento delle attività sportive a garanzia di controllo, sicurezza, gestione degli accessi al centro'".[43] Sotto altro profilo, rimarca ancora il Garante nel citato provvedimento, la firma apposta sul modulo di iscrizione non può dirsi effettivamente e unicamente riconducibile ad un consenso al trattamento in materia di dati personali, "ben potendo tale firma essere apposta per 'presa visione' dell'informativa, ovvero rilasciata in relazione a un distinto trattamento (ad es., in riferimento ai dati sensibili, pure trattati dall'associazione […] con specifico riferimento alla raccolta dei certificati medici degli utenti). Non può quindi ritenersi conforme a legge il consenso che si afferma acquisito in relazione al trattamento dei dati biometrici dei clienti, con conseguente violazione, pertanto, anche del richiamato principio di liceità e correttezza […]".[44]

L'ultimo rilievo riguarda la violazione del principio di proporzionalità: "il trattamento risulta sproporzionato rispetto al generico bisogno di regolare e controllare gli ingressi al centro sportivo e di agevolare la gestione degli

[38] *Ibidem*.
[39] *Ibidem*.
[40] *Ibidem*.
[41] *Ibidem*.
[42] *Ibidem*.
[43] *Ibidem*.
[44] *Ibidem*.

 doi.org/10.30682/disport0202b

abbonamenti, tenuto anche conto che non risulta nemmeno provata – e, ancor prima, addotta – l'insufficienza o l'inattuabilità di eventuali misure alternative, sicché si deve ritenere che l'adozione del sistema, anziché essere frutto di scelte attentamente ponderate, abbia risposto soltanto all'esigenza di privilegiare soluzioni poco costose e di rapida attuazione […]; a ciò si aggiunga che il trattamento non risulta proporzionato neanche sotto il profilo delle specifiche modalità tecniche adottate dall'associazione (centralizzazione dei modelli matematici ricavati dall'acquisizione del dato biometrico), ben potendo trovare agevole attuazione anche nel caso in esame accorgimenti meno invasivi – ma parimenti efficaci – quale, ad esempio, la memorizzazione del c.d. *template* su supporti posti nell'esclusiva disponibilità degli interessati".[45]

A seguito dell'accertata illiceità, il Garante ha vietato espressamente il trattamento in questione.

Sulla medesima fattispecie è poi intervenuto nuovamente con provv. 520 del 12 novembre 2014, in relazione alle sanzioni amministrative pecuniarie elevate con separato verbale.[46] In tale ultimo provvedimento l'autorità garante – ragionando sulla base delle norme precedenti al GDPR – ha ritenuto non sufficientemente accertata, nel caso di specie, la contestata inidoneità dell'informativa in materia di protezione dei dati personali e, pertanto, ha finito per applicare la sola sanzione pecuniaria per difetto del consenso, ovvero per difetto di una valida condizione di liceità del trattamento. Con le nuove norme, che fissano all'art. 12 GDPR l'obbligo di rendere l'informativa per iscritto e che impongono al titolare del trattamento l'obbligo di garantire e di dimostrare l'applicazione della disciplina in materia di protezione dei dati personali, ai sensi degli artt. 5 e 24 GDPR (*accountability*), l'esito sarebbe stato diverso.

V'è da dire che in altri precedenti casi il Garante ha usato criteri diversi: nel provv. n. 54 del 10 novembre 2010[47] e nel provv. n. 17 del 29 aprile 2009,[48] resi nei confronti di due società sportive dilettantistiche che facevano uso di sistemi biometrici per l'accesso agli impianti sportivi, l'autorità di controllo s'è limitata a contestare e sanzionare solamente la mancata notifica dei trattamenti al Garante, prevista nella disciplina previgente dall'art. 37 del Codice (poi abrogato per l'esigenza di coordinamento con il GDPR). Ancora, con una nota del Garante datata 9 novembre 1999, intitolata "Impronte digitali in palestra. Attenti alle violazioni della privacy", ma anche con successiva nota del 19 novembre 1999 a firma dell'allora Segretario Generale Giovanni Buttarelli, l'autorità di controllo ammetteva la liceità del trattamento dei dati personali biometrici effettuato per fini di controllo degli accessi agli impianti sportivi, purché ci fosse un'adeguata informativa e il rispetto di una condizione di liceità, come il consenso specifico al trattamento.[49] Sulla base della normativa precedente (che consentiva il rilascio dell'informativa anche oralmente), il Garante precisava, nelle note poc'anzi richiamate, che, quanto al rispetto degli obblighi previsti *ex lege* in tali fattispecie, "occorre informare, anche oralmente, gli iscritti o le persone che comunque accedono al centro sportivo degli scopi per i quali vengono raccolti i loro dati e acquisire, qualora necessario, il consenso alla loro utilizzazione. Va ricordato, infatti, che il consenso non è richiesto se l'utilizzazione dei dati è necessaria per adempiere ad obblighi contrattuali, ma è in concreto indispensabile se, ad esempio, il gestore del centro sportivo comunica i dati a terzi. I dati raccolti dovranno, inoltre, essere utilizzati solo per le finalità di accesso alla palestra e dovranno essere conservati solo per la durata del contratto e con sistemi di sicurezza che evitino il rischio di accessi non autorizzati".[50] Si tratta di esternazioni che l'autorità garante ha reso per rispondere a segnalazioni e richieste provenienti dalla magistratura in ordine all'attivazione di procedimenti penali attivati su esposti degli interessati nei confronti dei gestori di centri sportivi facenti uso di dati biometrici per il controllo degli accessi.

A parte la questione del contratto quale condizione di liceità, oggi non applicabile in quanto i dati biometrici sono classificati nel GDPR, insieme ai dati sensibili, quali dati appartenenti a categorie particolari disciplinati all'art. 9 del GDPR (mentre la necessità di concludere o eseguire il contratto – o misure precontrattuali a richiesta dell'interessato – è condizione di liceità ora prevista solamente per i dati comuni ai sensi dell'art. 6 del GDPR), si

[45] *Ibidem*.
[46] Garante per la protezione dei dati personali, Provvedimento n. 520 del 12 novembre 2014, doc. web n. 3801009.
[47] Garante per la protezione dei dati personali, Provvedimento n. 54 del 10 novembre 2010, doc. web n. 1823212.
[48] Garante per la protezione dei dati personali, Provvedimento n. n. 17 del 29 aprile 2009, doc. web n. 1714163.
[49] Garante per la protezione dei dati personali, nota del 9 novembre 1999 e nota del 19 novembre 1999, doc. web n. 42058.
[50] *Ibidem*.

 doi.org/10.30682/disport0202b

vede il mutato orientamento dell'autorità di controllo, che solo successivamente ha mostrato di dare valore al principio di necessità e di proporzionalità per vietare il trattamento biometrico per finalità di accesso agli impianti sportivi in assenza di specifiche e circostanziate esigenze di sicurezza o di tutela di diritti fondamentali.

5. Raccolta dati tramite *form* su siti Internet dell'associazione

In un caso affrontato dal Garante con provv. n. 519 del 12 novembre 2015 veniva sanzionata un'ASD per un'informativa al trattamento dei dati personali incompleta, presente sul proprio sito web.[51] Segnatamente, la contestazione riguardava l'attività di raccolta dei dati di persone interessate ad iscriversi all'associazione. Il trattamento aveva ad oggetto, in particolare, i seguenti dati: nome, cognome, data e luogo di nascita, tipo e numero di documento di riconoscimento, sesso e indirizzo e-mail.

L'accertamento è avvenuto tramite il Nucleo privacy della Guardia di Finanza.

Nell'ambito del procedimento svolto innanzi all'Autorità di controllo, l'ASD ha sostenuto, nei propri scritti difensivi, che "coloro che richiedono la tessera, e quindi l'iscrizione all'ASD […], devono necessariamente compilare il *form* sul sito internet dell'associazione ma poi, per ritirare la tessera cartacea, devono presentarsi fisicamente presso la sede dell'Associazione stessa […]. In questa sede vengono fornire oralmente le ulteriori informazioni necessarie".[52] Ancora, quanto ad alcuni elementi informativi richiesti dalla legge – e, segnatamente, il conferimento obbligatorio o no dei dati e le conseguenze in caso di eventuale rifiuto –, l'associazione ha argomentato sostenendo che sarebbero comunque "chiaramente enunciati all'utente, in quanto senza apporre il *flag* sulla casella di accettazione al trattamento dei dati personali non è possibile proseguire nella richiesta di iscrizione".[53] Nel corso del procedimento l'ASD dichiarava di aver provveduto comunque ad inserire gli ulteriori elementi informativi.

Le argomentazioni dell'associazione, titolare del trattamento dei dati, non sono state ritenute tali da escludere le responsabilità a proprio carico e l'illiceità della condotta. Il Garante ha avuto modo di evidenziare, nelle motivazioni del proprio provvedimento, che "oltre all'elemento relativo al carattere obbligatorio o facoltativo del conferimento dei dati e a quello relativo alle conseguenze connesse al rifiuto di conferire informazioni personali, che, contrariamente a quanto ritenuto, non sono chiaramente esplicitati nell'informativa presente sul sito internet, si rileva che l'art. 13 del Codice [ora art. 13 GDPR, *n.d.a.*] indica anche altri requisiti di cui l'informativa deve essere necessariamente fornita e che, effettivamente, sono carenti nel testo che era stato predisposto in calce al *form* di raccolta dati in esame. Mancavano, infatti, le indicazioni relative al titolare e alle modalità del trattamento, ai terzi a cui i dati possono essere comunicati e, in particolare, alle modalità con cui esercitare i diritti di cui all'art 7 del Codice"[54] [ora artt. 12 ss. GDPR, *n.d.a.*].

Va poi annotato che il problema non è solo contenutistico: tali informazioni, per assolvere alle funzioni di tutela a cui sono preordinate, devono essere rilasciate in favore dell'interessato preventivamente rispetto al trattamento, "ovvero prima che [il titolare, *n.d.a.*] abbia iniziato il trattamento dei dati personali, a nulla rilevando, dunque, la circostanza (non dimostrata) che queste siano rese esaustivamente agli interessati al momento, successivo, della consegna della tessera".[55]

Il Garante ha conseguentemente sanzionato l'ASD per violazione delle disposizioni in materia di obblighi informativi in favore dell'interessato a cui i dati oggetto di trattamento si riferiscono.

6. Risposte a recensioni sui canali *social*, siti web e blog

Altra rilevante questione attiene al trattamento di dati personali svolto mediante interazione su piattaforme *online* di soggetti terzi e, in particolare, degli *Internet service provider* (ISP), negli spazi virtuali dedicati alle

[51] Garante per la protezione dei dati personali, Provvedimento n. 519 del 12 novembre 2015, doc. web n. 4845615.
[52] *Ibidem*.
[53] *Ibidem*.
[54] *Ibidem*.
[55] *Ibidem*.

 doi.org/10.30682/disport0202b

recensioni, incorporati nel proprio sito istituzionale. In un caso significativo, deciso dal Garante con provv. n. 57 dell'11 febbraio 2021, una società sportiva dilettantistica, ricevendo una recensione negativa da una propria iscritta (che aveva a tal fine utilizzato uno pseudonimo di fantasia per conservare l'anonimato relativo alla propria identità nei confronti dei terzi), aveva replicato a tale recensione indicando le generalità dell'interessata nella risposta visibile *online*, senza restrizione alcuna.[56]

L'interessata, vistasi pubblicare le proprie generalità, chiedeva la cancellazione dei propri dati personali contenuti nel *post* di risposta pubblicato dalla società sportiva dilettantistica, ma, non ricevendo positivo riscontro, si rivolgeva al Garante lamentando di aver subito un "pregiudizio […] per effetto della indebita divulgazione di dati idonei a svelarne l'identità tenuto conto del fatto che il commento era stato da lei pubblicato avvalendosi di uno pseudonimo e che, fermo restando il diritto di replica spettante al titolare, quest'ultimo avrebbe potuto esercitarlo senza diffondere informazioni idonee ad identificarla".[57]

Nel corso del procedimento le argomentazioni difensive del titolare del trattamento rimarcavano che "la recensione rilasciata dalla reclamante nel sito ufficiale del centro sportivo gestito dal medesimo – utilizzando un account Facebook pubblico ed un *nickname* – risultava diretta a 'screditare sia il buon nome della storica società […] che degli addetti alla vendita promozionale abbonamenti in palestra'"[58] e che "è prassi dell'azienda, al momento dell'ingresso di un nuovo socio in palestra, raccogliere i dati identificativi dell'utente, previo consenso scritto al trattamento dei dati personali, con relativa apertura di scheda anagrafica nel programma aziendale […] ai fini del monitoraggio di frequenza e relativa copertura assicurativa"[59] ed, infine, che "il riscontro alla recensione negativa è stato reso al solo fine di salvaguardare l'immagine dell'azienda, non ravvisandosi nella propria condotta alcuna violazione, ma 'la semplice richiesta di firma della recensione con il reale nome identificativo di cui l'azienda era a conoscenza' per quanto sopra descritto".[60]

Il Garante, nell'esaminare il caso, ha ritenuto che la società sportiva dilettantistica abbia posto in essere una condotta illecita sotto il profilo della disciplina in materia di trattamento dei dati personali, in quanto trattasi di "condotta non […] giustificata dal fine di manifestare liberamente il proprio pensiero tenuto conto del fatto che, a fronte della volontà dell'interessata di tenere celata la propria identità resa evidente dall'utilizzo di uno pseudonimo, il titolare avrebbe potuto esprimere la propria opinione senza doverne diffondere i dati identificativi con ciò travalicando i limiti di essenzialità dell'informazione e violando altresì le indicazioni di cui all'art. 5, par. 1, lett. *b)*, del Regolamento [GDPR, *n.d.a.*] – che stabilisce che 'i dati siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità' – avendo utilizzato, per identificarla, i dati della medesima detenuti ad altro scopo".[61] Inoltre, il Garante ha rilevato che, stante la particolarità del trattamento, concernente la diffusione di dati personali contenuti in commenti pubblicati in rete, il trattamento medesimo "deve essere ricondotto nell'ambito delle finalità giornalistiche ed altre manifestazioni del pensiero di cui all'art. 136 del Codice e che pertanto, nel caso in esame, trovano applicazione le corrispondenti disposizioni del predetto Codice, nonché le Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica (G.U. del 4 gennaio 2019, n. 3)".[62]

Nel corso del procedimento, ad ogni modo, il titolare del trattamento provvedeva ad effettuare la cancellazione richiesta dall'interessata.

A fronte dell'illiceità della condotta e tenuto conto dell'ottemperanza, ancorché tardiva, alla richiesta dell'interessata, il Garante ha ritenuto di applicare la sola misura dell'*ammonimento*, ai sensi dell'art. 58, par. 2, lett. *b)*, del GDPR, procedendo contestualmente all'annotazione nel registro interno dell'Autorità di cui all'art. 57, par. 1, lett. *u)*, del GDPR, in ordine alle violazioni e alle misure adottate, anche al fine di tener conto dei casi di recidiva. Sicché il Garante ha "ammonito il titolare in ordine all'esigenza, allorché agisca attraverso l'utilizzo di

[56] Garante per la protezione dei dati personali, Provvedimento n. 57 dell'11 febbraio 2021, doc. web n. 9576735.
[57] *Ibidem*.
[58] *Ibidem*.
[59] *Ibidem*.
[60] *Ibidem*.
[61] *Ibidem*.
[62] *Ibidem*.

siti web, blog o altri sistemi di diffusione del pensiero, di adeguarsi integralmente alle disposizioni previste in materia di trattamento dei dati in ambito giornalistico e di libera manifestazione del pensiero, con particolare riguardo alle misure da adottare per salvaguardare la riservatezza e la dignità degli interessati, oltreché a quelle che disciplinano il principio di finalità nel trattamento di dati personali".[63]

7. *Marketing e* altre comunicazioni promozionali

Un altro aspetto di grande impatto concerne le comunicazioni promozionali e quelle commerciali, riconducibili all'ampio settore del *marketing*, a cui anche le associazioni sportive dilettantistiche non sono estranee.

In un procedimento svoltosi innanzi al Garante e culminato con provv. n. 250 del 15 maggio 2014, a seguito di apposito ricorso, l'*Authority* ha analizzato una fattispecie nell'ambito della quale il destinatario di una comunicazione promozionale indesiderata proveniente da un'ASD si lamentava dell'illecito trattamento dei propri dati personali ed, esercitando i diritti che la legge riconosce all'interessato, chiedeva di avere la conferma dell'esistenza dei dati personali al medesimo relativi e la comunicazione di dati in forma intelligibile, nonché di conoscere l'origine, le finalità, le modalità e la logica applicata al trattamento, oltre agli estremi identificativi del titolare del trattamento, del soggetto eventualmente designato come responsabile del trattamento, del rappresentante del titolare nel territorio dello Stato e indicazione dei soggetti o delle categorie di soggetti ai quali i dati sono stati comunicati.[64] Ancora, l'interessato, in esercizio dei diritti di intervento che la normativa gli accorda in materia di protezione dei dati personali, chiedeva altresì di ottenere la cancellazione e la trasformazione in forma anonima dei dati trattati in violazione di legge, con attestazione che la predetta operazione fosse stata portata a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi, opponendosi al loro trattamento per finalità di carattere commerciale.[65]

L'ASD, nel procedimento innanzi al Garante, ha affermato di aver ottemperato a tutte le richieste dell'interessato prima dell'instaurazione del procedimento, dimostrando documentalmente tale assunto (mediante deposito della nota di riscontro all'interessato) e precisando di aver "confermato, tra l'altro, che l'indirizzo di posta elettronica indicato dall'interessato è stato cancellato e che lo stesso non è stato oggetto di alcuna diffusione o comunicazione a soggetti terzi".[66]

All'esito del procedimento, l'Autorità garante ha dichiarato pertanto il non luogo a provvedere sul ricorso presentato dall'interessato, avendo il titolare fornito un adeguato riscontro alle istanze del ricorrente, precisando nel corso del procedimento le informazioni già comunicate all'interessato anteriormente alla presentazione del ricorso. Le spese del procedimento venivano compensate fra le parti.

Altro caso è stato affrontato dal Garante per la protezione dei dati personali con provv. n. 159 del 23 marzo 2017, relativo ad un trattamento per finalità di *marketing* posto in essere da una società sportiva dilettantistica.[67] L'Autorità di controllo s'è attivata a seguito di ricorso dell'interessato, che si è visto raggiungere da numerose comunicazioni pubblicitarie sia attraverso messaggi sulla propria casella di posta elettronica, sia sul proprio cellulare, tutte provenienti dalla società sportiva dilettantistica con la quale aveva sottoscritto un contratto di abbonamento per la fruizione della palestra, autorizzando contestualmente il trattamento dei dati personali con un consenso genericamente prestato e a fronte di un'informativa carente di alcune indicazioni obbligatorie richieste per legge. Al termine del rapporto contrattuale, l'interessato chiedeva la cancellazione dei dati e formulava espressa opposizione al loro utilizzo per finalità commerciali, ma senza positivo riscontro, vedendosi pertanto costretto ad adire l'autorità di controllo.

Nel corso del procedimento innanzi a quest'ultima, il titolare del trattamento aveva dichiarato di aver provveduto alla cancellazione dei dati personali dell'interessato e di essersi astenuto dall'inviare ulteriori comunicazioni promozionali.

[63] *Ibidem*.
[64] Garante per la protezione dei dati personali, Provvedimento n. 250 del 15 maggio 2014, doc. web n. 3278862.
[65] *Ibidem*.
[66] *Ibidem*.
[67] Garante per la protezione dei dati personali, Provvedimento n. 159 del 23 marzo 2017, doc. web n. 6516447.

Anche in tal caso il Garante, vista l'ottemperanza, ancorché tardiva, del titolare, ha dichiarato il non luogo a provvedere sul ricorso, compensando tuttavia solo parzialmente le spese del procedimento, che sono state poste a carico del titolare del trattamento nella misura di 200 euro.

Nuove modalità di trattamento per finalità di *marketing* sono state attuate in ambito sportivo in occasione della realizzazione della tessera del tifoso, poi proseguita in specifiche card per i tifosi, utilizzate per finalità diverse. La tessera del tifoso, com'è noto, si inseriva nell'ambito delle iniziative ministeriali di carattere strumentale per incrementare la sicurezza degli appassionati di calcio (v. Circolare del Ministero dell'Interno del 14 agosto 2009, n. 555) ed era riconducibile alle agevolazioni previste dall'art. 8 del d.l. 8 febbraio 2007, n. 8, dettato in tema di prevenzione e repressione dei fenomeni di violenza connessi a competizione calcistiche e di sostegno alla diffusione dello sport. L'idea era quella di creare un valore aggiunto all'appartenenza ad una comunità virtuosa di tifosi fidelizzati.

Il programma prevedeva una serie di facilitazioni, privilegi e servizi resi disponibili per il tifoso (inclusi vantaggi nell'acquisto di biglietti per assistere ad eventi sportivi o nella collocazione presso gli stadi nel caso di partite in trasferta) unita ad una "schedatura" del tifoso per attività di controllo da parte delle questure ed alla possibilità di utilizzo della tessera anche con tecnologie *rfid* per l'apertura agevolata di tornelli o comunque per il controllo degli accessi agli impianti sportivi. La tessera veniva usata anche per finalità di *marketing*. L'uso di tali tessere di fidelizzazione è poi proseguito da parte di molte società calcistiche, sostituite da apposite *fidelity card*. Le tessere del tifoso sono oggi usate anche per sport diversi dal calcio ed anche da organizzazioni sportive dilettantistiche, con l'idea di creare fidelizzazione dei *supporter*, con attività e campagne promozionali, secondo le logiche del *marketing*, declinato in forme e modalità di volta in volta diverse. Sulla tessera del tifoso, come prevista dalla predetta circolare ministeriale, il Garante aveva reso alcuni significativi provvedimenti (provv. 16 giugno 2010, doc. web n. 1733656; provv. del 10 novembre 2010, doc. web n. 1779725). In tali provvedimenti (e soprattutto nel cit. provv. del 10 novembre 2010, doc. web n. 1779725) erano state esternate apposite riflessioni sull'eventualità che tale tipologia di tessere venisse utilizzata per la profilazione del tifoso e finalità di *marketing*, insistendo a tal riguardo sulla necessità di un'adeguata informativa in materia di trattamento di dati personali e di una specifica acquisizione del consenso per tale finalità. Al fine di evitare manipolazioni successive da parte del titolare del trattamento, il Garante aveva previsto che il modulo di acquisizione del consenso per finalità di *marketing* prevedesse anche la possibilità di esprimere il diniego del consenso, con modalità tali da non consentire al titolare del trattamento di intervenire *ex post* sul modulo attraverso un'alterazione del diniego medesimo, all'insaputa dell'interessato e contro la sua volontà (sarebbero dunque evitate eventuali manipolazioni successive del modulo, qualora l'interessato non intendesse esprimere il consenso al trattamento per finalità di *marketing*). Ancora, il Garante aveva ritenuta corretta e necessaria l'acquisizione di un distinto consenso in relazione al trattamento eventualmente svolto per finalità di *marketing* da parte di società terze, per permettere agli interessati di autodeterminarsi in relazione alla circolazione dei propri dati ed all'eventuale trattamento da parte di soggetti diversi dalle organizzazioni sportive. Ulteriore distinto consenso va ottenuto poi – come precisato ulteriormente dal Garante, con indicazioni che, sul punto, possono ritenersi ancora attuali – nel caso in cui l'attività di trattamento si svolga effettuando una profilazione del tifoso.

8. Valutazioni peritali medico-legali in caso di infortuni o sinistri

L'attività sportiva, incluso quella dilettantistica, porta sovente al verificarsi di infortuni a danno degli atleti, per i quali vengono attivate coperture assicurative, che richiedono l'espletamento di specifiche perizie medico-legali da parte di fiduciari della compagnia di assicurazione, ai fini della liquidazione dell'ammontare previsto a favore dell'interessato.

La casistica ha fatto registrare fattispecie nell'ambito delle quali, a seguito di infortunio occorso nello svolgimento di un'attività sportiva dilettantistica e di conseguente apertura di un procedimento per la definizione del sinistro da parte della società di assicurazione, l'atleta infortunato ha esercitato il diritto di accesso per ottenere copia anche delle valutazioni medico-legali rese in ambito peritale. In tal senso significativo è il provv. del Garante n. 258 del 22 maggio 2013, reso all'esito di un procedimento nel quale l'atleta infortunato, nella qualità di

interessato al trattamento dei dati personali a lui relativi, aveva chiesto "di ottenere la comunicazione intelligibile dei dati personali che lo riguardano contenuti nella perizia medico-legale redatta dal medico fiduciario incaricato dalla compagnia di assicurazioni, ivi compresa la valutazione peritale espressa dal professionista che l'ha curata".[68]

A parte la dibattuta questione relativa all'applicabilità della disciplina in materia di protezione dei dati personali ai c.d. dati valutativi, che in questa sede non è possibile trattare per esigenze di economia del discorso, qui il Garante ha rilevato che, a fronte dell'esercizio del diritto di accesso dell'interessato e dell'ottemperanza da parte del titolare del trattamento, che forniva copia della perizia senza tuttavia la sottoscrizione del documento da parte del medico legale, sorgeva contestazione in ordine alle modalità di esecuzione del riscontro da rendere all'interessato medesimo. Questi non si sentiva soddisfatto perché, pur accedendo alle valutazioni peritali, non aveva la possibilità di riscontrare o documentare la loro "riconducibilità all'apparente estensore della perizia medico-legale".[69] A tali rilievi, tuttavia, l'autorità di controllo ha replicato che il riscontro fornito dal titolare alle richieste formulate dall'interessato appariva del tutto adeguato, ancorché tardivamente reso nel corso del procedimento. In particolare, quanto alle modalità di riscontro al diritto di accesso esercitato dall'atleta infortunato, il Garante ha preso atto che, dopo la trasmissione della perizia non sottoscritta, la compagnia di assicurazione ha voluto trasmettere, su richiesta dell'interessato, anche la versione munita di sottoscrizione del medico legale. A tal riguardo l'autorità garante ha però chiarito che "l'invio di una copia sottoscritta della relazione peritale [è] profilo […] non strettamente connesso con l'esercizio del diritto di accesso ai dati, che può essere correttamente riscontrato dal titolare del trattamento attraverso l'estrapolazione e la messa a disposizione dei dati, senza dover obbligatoriamente fornire una riproduzione fotostatica completa del documento che li contiene".[70]

9. Certificazioni di idoneità o inidoneità allo svolgimento dell'attività sportiva

Una particolare attenzione va posta ai dati trattati dalle ASD relativamente alle certificazioni di idoneità o inidoneità allo svolgimento dell'attività sportiva, sia essa agonistica o non agonistica. Il problema principale attiene alla qualificazione dei dati e, dunque, all'individuazione della loro natura: si discute, in particolare, se i dati contenuti nel giudizio di idoneità o di inidoneità all'esercizio dell'attività sportiva siano da classificare come dati comuni o se invece vadano collocati nella categoria dei dati "particolari" ovvero "sensibili", con ovvie conseguenze in ordine al diverso regime applicabile, a partire dalle condizioni di liceità del trattamento.

Della questione se ne è interessato il Garante con nota del 31 dicembre 1998, in risposta ad un quesito articolato dalla Federazione medico sportiva italiana, concernente il libretto sanitario sportivo.[71] L'autorità di controllo ha ivi rimarcato che "il referto di inidoneità all'esercizio dell'attività sportiva agonistica, che presuppone nell'interessato o la presenza di patologie o, comunque, la necessità di evitare potenziali rischi indotti appunto dalla pratica agonistica, assume senza dubbio la connotazione di dato sensibile".[72] Al contrario, "il giudizio conclusivo di idoneità all'esercizio dell'attività sportiva agonistica, inteso come dato denotante la normalità psicofisica del soggetto, può ritenersi compreso fra i dati personali 'comuni'".[73]

Ne deriva che, tra l'altro, le organizzazioni sportive siano tenute a rilasciare adeguata informativa e ad acquisire il consenso scritto (o quantomeno espresso, ai sensi del GDPR) e circostanziato, con riguardo sia al trattamento in questione, sia alla successiva comunicazione di dati ad altri soggetti (es. al CONI o a singole federazioni sportive).[74]

[68] Garante per la protezione dei dati personali, Provvedimento n. 258 del 22 maggio 2013, doc. web n. 2575227.
[69] *Ibidem*.
[70] *Ibidem*.
[71] Garante per la protezione dei dati personali, nota del 31 dicembre 1998, doc. web n. 41878.
[72] *Ibidem*.
[73] *Ibidem*.
[74] *Ibidem*.

 doi.org/10.30682/disport0202b

10. Accesso a dati degli associati e loro pubblicazione

Altre rilevanti questioni hanno riguardato il tema dell'accesso ai dati degli associati e la loro pubblicazione su quotidiani o altri mezzi di comunicazione di massa, nonché le modalità di pubblicità delle sanzioni inflitte dall'associazione ai propri iscritti.

Nella Relazione del 2008 all'attività svolta, il Garante ha evidenziato che "L'iscritto ad una federazione ha posto un quesito in tema di accesso ai dati personali degli altri associati (in forma di elenco comprensivo di nominativi e indirizzi) per l'esercizio di prerogative legate all'appartenenza all'associazione".[75] In tale occasione l'autorità di controllo ha avuto modo di evidenziare che "l'associazione […] può determinare 'il se e il come' della conoscibilità, all'interno della realtà associativa, dei dati personali degli aderenti, anche in difetto del consenso dei singoli associati, a condizione che la comunicazione avvenga nel rispetto di 'idonee garanzie' determinate dalla stessa associazione in relazione ai trattamenti effettuati e che l'associazione medesima abbia reso agli interessati, all'atto dell'informativa rilasciata ai sensi dell'art. 13 del Codice [ora art. 13 del GDPR, *n.d.a.*], le determinazioni in merito adottate, prevedendo espressamente le modalità di utilizzo dei dati (che dovranno essere comunque pertinenti e non eccedenti alle finalità sottese alla richiesta […]). Resta comunque salva la possibilità per ciascuna associazione di individuare modalità diverse per veicolare messaggi o comunicazioni di singoli associati all'interno della compagine associativa (facendo così da tramite dei singoli iscritti), nelle forme ritenute più opportune senza che ciò comporti la comunicazione di indirizzari di tutti gli iscritti a taluni di essi […]".[76]

Altro problema rilevante riguarda la gestione delle sanzioni (e dei provvedimenti) disciplinari. A tal riguardo, nella predetta Relazione, il Garante ha ricordato che "Una reclamante ha lamentato che dati personali contenuti in provvedimenti disciplinari emanati nei suoi confronti da una federazione sportiva erano stati affissi in spazi liberamente accessibili ai soci di un circolo sportivo (affiliata alla medesima federazione). La pubblicazione dei provvedimenti disciplinari non sarebbe risultata consentita dallo Statuto del circolo, né doverosa in attuazione di specifiche norme federali".[77] Pertanto il Garante ha ritenuto che l'affissione del provvedimento disciplinare, nel caso specifico, non potesse trovare giustificazione e, tra l'altro, si poneva in violazione degli obblighi informativi previsti dalla disciplina in materia di protezione dei dati personali. In linea generale, è da considerare rimessa "alle determinazioni adottate da organismi senza scopo di lucro le modalità ed i limiti della divulgazione di dati personali relativi agli iscritti; ciò per consentire agli stessi iscritti di valutare in concreto – al di là delle necessarie misure organizzative da predisporre a livello associativo – le possibili 'ricadute' individuali legate ad una più ampia circolazione delle informazioni anche nei confronti di tutti gli altri associati (talvolta di numero assai elevato) oltre la natura (più o meno sensibile) delle informazioni suscettibili di comunicazione)".[78]

Per altro verso, in una nota del 30 novembre 1999, intitolata eloquentemente "Le associazioni non possono nascondere i propri iscritti", il Garante ha preso posizione su un differente aspetto, concernente l'attività divulgativa di soggetti terzi, dichiarando che "Un'associazione non può opporsi alla pubblicazione dei nomi dei propri iscritti, a meno che non vi sia stata una espressa delega da parte degli interessati. Il principio è stato affermato dal Garante nella decisione di un ricorso presentato dal rappresentante legale di un'associazione. Questi aveva chiesto ad un quotidiano di bloccare la annunciata pubblicazione degli elenchi degli iscritti all'associazione".[79] Tuttavia il Garante, nell'affrontare il caso, "ha affermato che non è ipotizzabile, né previsto dalla legge […] un diritto dell'associazione ad esercitare i diritti che rientrano nella personale disponibilità di ciascun interessato, a meno che essa possa dimostrare l'esistenza di una specifica delega del singolo associato".[80]

[75] Garante per la protezione dei dati personali, Relazione 2008 ("Protezione dei dati e nuove tecnologie nel mondo in trasformazione"), del 2 luglio 2009, doc, web b. 1632972.
[76] *Ibidem*, p. 117.
[77] *Ibidem*, p. 116.
[78] *Ibidem*.
[79] Garante per la protezione dei dati personali, nota del 30 novembre 1999, doc. web n. 1164456.
[80] *Ibidem*.

Nella disamina di tale fattispecie, l'autorità di controllo ha chiarito "che il dato dell'adesione a qualsiasi associazione appartiene senz'altro a quest'ultima come riflesso della libera scelta del singolo che conferisce i dati. Tuttavia, la pura e semplice adesione, al di fuori delle ipotesi di delega o procura espressa, non può sottrarre all'interessato la possibilità di far valere diritti tipicamente personali, come quelli previsti"[81] dalla normativa "sulla privacy (diritto di accesso, rettifica, aggiornamento dei dati, opposizione al loro trattamento ecc.)".[82]

Ulteriori ostacoli sorgono poi qualora si consideri che, come nel caso di specie, la pubblicazione dei dati ben potrebbe rientrare nell'esercizio del diritto di cronaca, che implica una valutazione sul bilanciamento degli interessi rilevanti: l'interessato, per poter impedire la pubblicazione di chi esercita il proprio diritto di cronaca, "dovrebbe dimostrare l'esistenza di un motivo legittimo".[83]

11. Pubblicità dei dati relativi alla salute dell'atleta

Il regime di particolare rigore applicabile ai dati sensibili – ovvero, ai sensi dell'art. 9 GDPR, ai dati appartenenti a categorie particolari –, non impedisce che i dati in questione possano essere resi pubblici direttamente dall'interessato, direttamente o tramite altri soggetti. Sicché il Garante, con provv. del 22 giugno 1998, ha affermato che "l'interessato conserva il diritto di rendere pubbliche o meno, anche per interposta persona, le proprie condizioni di salute. Pertanto, considerata la tendenza invalsa a rendere note talune circostanze relative alla forma degli atleti impegnati nelle attività agonistiche, le società sportive, oltre ad acquisire il consenso degli interessati a trattare i dati relativi al loro stato di salute, possono ottenere, a parte, la "delega" a rendere pubbliche talune circostanze rilevanti per l'interesse pubblico sotteso alle attività stesse, da individuarsi *una tantum* ma con precisione, anche con riferimento a determinate categorie di informazioni".[84]

Del resto tale indirizzo è in piena sintonia con quanto oggi previsto dal GDPR, che, all'art. 9, par. 2, lett. *e)*, considera lecito il trattamento di dati particolari, inclusi quelli relativi alla salute, qualora "il trattamento riguarda dati personali resi manifestamenti pubblici dall'interessato", senza necessità del consenso da parte di quest'ultimo.

12. Foto e riprese effettuate dai genitori ad eventi a cui partecipano i figli minori. Diffusione di immagini relative ai minori (foto su *Facebook*; album di figurine)

In occasione di eventi sportivi organizzati dall'ASD nel settore giovanile, accade frequentemente che i genitori immortalino i propri figli in foto e video, con *smartphone*, *tablet*, videocamere o macchine fotografiche, per avere un ricordo. La questione non è dissimile a quella che si presenta in occasione di recite scolastiche o per le foto ricordo di classe, a cui trovano applicazione i medesimi principi.

Il Garante, con nota del 6 giugno 2007 (intitolata "I genitori possono filmare e fotografare i figli nelle recite scolastiche") è tornato a precisare che "le riprese video e le fotografie raccolte dai genitori, durante recite e saggi scolastici, non violano la privacy. È opportuno ricordare a presidi ed operatori scolastici che l'uso di videocamere o macchine fotografiche per documentare eventi scolastici e conservare ricordi dei propri figli non ha ovviamente niente a che fare con le norme sulla privacy. Si tratta, infatti, di immagini non destinate alla diffusione, ma raccolte per fini personali e destinate ad un ambito familiare o amicale: il loro uso è quindi del tutto legittimo".[85] Medesime considerazioni trovano applicazione anche nel caso di eventi, saggi, manifestazioni, partite o dimostrazioni, svolte alla presenza dei genitori, qualora questi ultimi documentino la partecipazione e la prestazione dei propri figli.

A diversa conclusione si dovrebbe invece pervenire, a rigore, qualora l'immagine, foto o video, venga poi caricata su *social network* o altri circuiti che consentono la libera fruizione dei contenuti ad opera del pubblico. In realtà il problema non sembra però porsi per chi organizza l'evento, quanto invece per i genitori, che, nell'utilizzare i dati personali – qualora ad esempio ritraggano non solo i figli propri, ma anche i figli altrui –

[81] *Ibidem*.
[82] *Ibidem*.
[83] *Ibidem*.
[84] Garante per la protezione dei dati personali, Provvedimento del 22 giugno 1998, doc. web n. 31035.
[85] Garante per la protezione dei dati personali, nota del 6 giugno 2007, doc. web n. 1410643.

devono preoccuparsi di rispettare gli adempimenti previsti dalla disciplina in materia, tenendo conto che la c.d. esenzione domestica (l'inapplicabilità della disciplina qualora il trattamento avvenga per scopi esclusivamente personali o familiari), non vige qualora il trattamento venga effettuato al di fuori di tale ristretto ambito, allargandone la fruizione ad una più ampia cerchia di soggetti.

Qualora invece sia l'ASD stessa a voler pubblicare foto o video di eventi in cui siano ripresi i giovani associati, minori d'età, dovrà preoccuparsi di acquisire previamente il consenso informato e specifico al trattamento dei dati personali da parte dei genitori (o del tutore) o sincerarsi che vi sia eventualmente un'altra condizione di liceità prevista dagli artt. 6 o 9 GDPR.

Alcune pronunce del Garante hanno riguardato casi in cui talune ASD del settore calcistico hanno diffuso immagini relative ad atlete o atleti minori, in relazione alle quali i genitori avanzavano richiesta di rimozione.

Un caso è stato affrontato dal Garante, ad esempio, con provv. n. 208 del 2 aprile 2015.[86] Un genitore, esercitando i diritti dell'interessato per conto della figlia minore, chiedeva ad un'ASD di calcio femminile "la 'rimozione delle foto della minore e il ritiro di tutto il materiale pubblicitario cartaceo e on line, pubblicato su Facebook, contenete la foto' della medesima",[87] tesserata presso l'ASD fino a diversi mesi prima. Nel ricorso presentato al Garante il genitore faceva presente che, successivamente alla scadenza del tesseramento della minore, l'ASD, "'per promuovere l'attività della propria scuola calcio, distribuiva volantini e locandine pubblicitarie contenenti fotografie di bambini minori', compresa quella della figlia […], pubblicando altresì la foto anche 'sulla pagina Facebook […]' in assenza di consenso dell'interessata".[88] Il procedimento si era concluso con una dichiarazione di non luogo a provvedere, dopo che il Garante aveva constatato che l'ASD, titolare del trattamento, avesse provveduto alla rimozione del materiale pubblicitario, contenente la foto della minore.

Analogo caso è stato deciso con provv. n. 323 del 27 giugno 2013 del Garante, nell'ambito di un procedimento attivato su ricorso di un genitore che contestava ad una ASD operante nel settore calcistico l'utilizzo di immagini fotografiche che ritraevano il figlio minore con la divisa della squadra di appartenenza, ai fini della pubblicazione di un album di figurine relativo alla scuola calcio da questi frequentata e posto in vendita.[89] Il genitore chiedeva di accedere ai dati personali del figlio, con specifico riguardo sia alle predette immagini fotografiche, sia all'autorizzazione all'utilizzo delle medesime per le finalità pubblicitarie e commerciali, che venivano contestate.

L'ASD, nei propri scritti difensivi, faceva presente "che 'l'Amministrazione del Comune […] ha chiesto di poter disporre delle fotografie dei tesserati per poter realizzare un album fotografico dei 'Piccoli calciatori' delle città […]', analogamente a quanto avvenuto con riguardo alle Associazioni rappresentative di altre discipline sportive praticate nel territorio comunale, precisando altresì che l'ASD […] [resistente] si sarebbe limitata ad indicare alla società cui era stato affidato il relativo incarico 'il fotografo presso il quale erano in giacenza le foto dei propri tesserati'",[90] dichiarando altresì che "all'atto del tesseramento i genitori degli atleti tesserati sottoscrivono la presa visione ed accettazione dell'informativa sulla legge della privacy".[91] Ancora l'ASD, nel medesimo procedimento, precisava ulteriormente che ogni anno i minori che intendono giocare a calcio presso la medesima resistente " 'vengono ufficialmente tesserati per il settore giovanile della F.I.G.C. con sottoscrizione dell'apposito modulo da parte di chi esercita la potestà genitoriale […] che prevede al suo interno la esplicita sottoscrizione dell'informativa ex d.lgs. 196/2003', dichiarando altresì che tale adempimento sarebbe stato posto in essere anche nei riguardi del minore citato nel ricorso 'il cui modulo di tesseramento è […] depositato presso la F.I.G.C.'".[92] Precisava poi il Garante, nel citato provvedimento, che "l'Associazione ha inoltre rilevato che, all'inizio di ogni stagione calcistica vengono effettuate riprese fotografiche dei giovani calciatori, sia individualmente che in gruppo, per varie finalità di cui i genitori dei giovani atleti vengono *informati oralmente*, puntualizzando che 'nel caso in questione, né al momento delle riprese fotografiche, né in un momento

[86] Garante per la protezione dei dati personali, Provvedimento n. 208 del 2 aprile 2015, doc. web n. 4047613.
[87] *Ibidem*.
[88] *Ibidem*.
[89] Garante per la protezione dei dati personali, Provvedimento n. 323 del 27 giugno 2013, doc. web n. 2612723.
[90] *Ibidem*.
[91] *Ibidem*.
[92] *Ibidem*.

 doi.org/10.30682/disport0202b

successivo, alcun familiare ha espresso il proprio dissenso […] nemmeno quando, con le stesse modalità sopra descritte, si è comunicata l'iniziativa oggetto della presente procedura'".[93]

Il Garante, sulla base della precedente normativa in materia di protezione dei dati personali, che consentiva l'informativa orale anche non a richiesta dell'interessato, ha ritenuto adeguato il riscontro fornito dall'ASD nel caso di specie, benché reso solamente a seguito di presentazione del ricorso, ed ha pertanto ritenuto di dichiarare il non luogo a provvedere, ponendo parzialmente a carico della resistente le spese del procedimento. Va ricordato però che l'attuale formulazione dell'art. 12 del GDPR, attualmente vigente, impone di rendere l'informativa per iscritto, ammettendo la possibilità della forma orale solamente in via di eccezione su richiesta dell'interessato; inoltre, stante il principio di *accountability*, il titolare del trattamento è tenuto non solo a garantire la corretta applicazione della disciplina, ma anche a fornirne adeguata dimostrazione, con l'adozione di specifiche misure tecniche e organizzative.

13. Consenso dei genitori per il trattamento di dati relativi ai figli minori

Ultima questione riguarda le modalità con cui viene rilasciato il consenso da parte di chi esercita la responsabilità genitoriale sugli atleti minori.

Il genitore (o, in mancanza, il tutore) ha la rappresentanza *ex lege* del minore ed è pertanto legittimato ad esprimere il consenso al trattamento dei dati personali ai sensi degli artt. 6, par. 1, lett. *a)*, e 9, par. 2, lett. *a)*, del GDPR.[94] Il minore che abbia compiuto quattordici anni può esprimere personalmente il consenso al trattamento solamente qualora riguardi l'offerta di un servizio della società dell'informazione a lui diretto e non sia concernente dati appartenenti a categorie particolari (come ad es. i dati relativi alla salute), occorrendo altrimenti il consenso del genitore (o del tutore).[95]

Va chiarito che ciascun genitore è legittimato ad esercitare, in accordo con l'altro genitore, la responsabilità genitoriale e ad esprimere il relativo consenso, sicché non occorre la sottoscrizione di entrambi i genitori per il consenso al trattamento dei dati personali, fermo restando l'accordo di entrambi. Nella prassi potrebbero sorgere problemi in caso di situazioni conflittuali in seno alla famiglia, ad esempio nelle ipotesi di separazione non consensuale dei coniugi: un genitore potrebbe manifestare la contrarietà alle scelte dell'altro genitore (anche ai fini del riparto delle spese per l'attività sportiva dei figli). Operativamente è buona prassi, nella raccolta del consenso di un genitore al trattamento dei dati personali del figlio o della figlia minore, far precedere la sottoscrizione dalla dichiarazione con cui il medesimo afferma di esprimere il consenso al trattamento in accordo con l'altro genitore, previamente informato a tal fine.

14. Gestione della *privacy* all'interno dell'associazione, formazione e "cultura"

L'analisi che precede consente di concludere rimarcando l'importanza, nella corretta applicazione della disciplina in materia di protezione dei dati personali all'interno dell'associazione, non solo di un'adeguata e specialistica conoscenza della normativa in tale settore, ma anche della "prassi", intesa anche quale conoscenza attenta degli orientamenti applicativi espressi dall'autorità garante nella casistica concreta. Solo in tal modo le norme generali ed astratte, emanate dal legislatore europeo e nazionale, possono essere efficacemente rilette per una più calzante applicazione tarata sulle esigenze della vita operativa con cui quotidianamente si confronta l'ente titolare del trattamento. Lo sforzo proteso alla conoscenza dei "precedenti" applicativi è parte di quanto richiesto dal principio di *accountability* (o responsabilizzazione) di cui all'art. 5, par. 2, e all'art. 24 GDPR e, si noti, è espressamente codificato nelle competenze richieste dall'art. 37, par. 5, GDPR per la designazione del *Data Protection Officer* (DPO) o Responsabile della Protezione dei Dati (RPD), nella parte in cui si prevede che questi

[93] *Ibidem*.

[94] Cfr., su tali temi, F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di*), La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 110 ss. e, ivi, spec. pp. 164 ss.

[95] *Ibidem*, p. 164 ss.

abbia proprio una "conoscenza specialistica della normativa e della *prassi* in materia di protezione dei dati personali […]".[96]

Va infatti tenuto conto che il titolare ed il responsabile del trattamento sono tenuti a designare il responsabile per la protezione dei dati (RPD) o *data protection officer* (DPO) qualora sussistano determinati requisiti di carattere soggettivo o oggettivo, indicati all'art. 37 GDPR. Tale designazione è obbligatoria, infatti, non solo per gli enti pubblici, in ogni caso, ma anche per i soggetti privati i cui trattamenti, rientranti nelle attività principali, siano posti in essere su larga scala ed abbiano ad oggetto dati appartenenti a categorie particolari (incluso i dati relativi alla salute) oppure il monitoraggio regolare e sistematico, sempre su larga scala, del comportamento degli interessati (es.: geolocalizzazione o tracciamento dell'attività *online*).

Anche qualora non sussista l'obbligo di designazione del DPO, quest'ultimo, come più di talvolta avviene, può essere designato facoltativamente (su base volontaria) al fine di incrementare i livelli di efficienza nei trattamenti necessariamente posti in essere dall'ente per raggiungere le proprie finalità istituzionali, assicurando così un maggior livello di *compliance* al GDPR, con garanzie elevate di tutela per gli individui a cui i dati personali trattati si riferiscono.

Più spesso accade che, in luogo della designazione facoltativa del DPO, si proceda con la nomina di un "responsabile *privacy*" o di un "addetto alla *privacy*" (*privacy officer*) interno o esterno all'ente, che abbia parte delle funzioni del DPO medesimo (ad esempio quelle di informazione e consulenza). Anche tale figura può svolgere un ruolo importante nella gestione dell'operatività quotidiana dell'ente, in sintonia con le esigenze di tutela espresse dalla disciplina in materia di protezione (e libera circolazione) dei dati personali.

Altre volte si ricorre a "referenti *privacy*" interni, figure solitamente dedite ad altre funzioni, ruoli o mansioni, dotati però di adeguate conoscenze anche in materia di *data protection*, in grado di dialogare con i consulenti *privacy* esterni dotati di un più elevato livello di specializzazione: i primi interagiscono con i secondi per il mantenimento di un elevato livello di *compliance* al GDPR, avanzando richieste e ricevendo indicazioni anche operative, che poi provvedono ad attuare nello svolgimento degli adempimenti.

A prescindere dagli assetti organizzativi scelti dall'ente per fronteggiare le problematiche applicative in materia di protezione dei dati personali, le figure interne dedicate alla corretta applicazione della disciplina in materia di protezione dei dati personali ormai risultano indispensabili in ogni realtà organizzativa.

Indipendentemente dal ruolo tecnicamente ricoperto (*data protection officer*, *privacy officer* o referente *privacy* interno che interagisce con i consulenti *privacy* esterni) certo è che tali figure necessitano di una formazione

[96] Cfr. art. 37, par. 5, GDPR. Il DPO può essere sia un soggetto interno all'organizzazione del titolare (ad es. un dipendente) sia un soggetto esterno. Il rapporto tra titolare o tra responsabile del trattamento e DPO va contrattualizzato in ogni caso. Tra i compiti del DPO, previsti all'art. 39 GDPR, rientrano i seguenti: (i) informare e fornire consulenza in materia di protezione dei dati personali al titolare o al responsabile che lo abbia nominato, nonché ai loro dipendenti; (ii) sorvegliare l'osservanza della disciplina in materia di protezione dei dati personali e delle *privacy policy* stabilite dal titolare o dal responsabile; (iii) fornire pareri, in particolare sulla valutazione d'impatto di cui all'art. 35 GDPR, se richiesto; (v) cooperare con l'autorità di controllo (Garante); (vi) fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento dei dati personali; (vi) fungere da punto di contatto con gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR (art. 38, par. 4, e art. 39). Ai sensi dell'art. 38 GDPR viene poi previsto che il titolare e il responsabile del trattamento debbano (i) assicurarsi che il DPO sia sempre tempestivamente e adeguatamente informato in ordine a tutte le questioni che riguardano i trattamenti dei dati personali dai medesimi svolti, nei confronti delle quali deve essere sistematicamente coinvolto; (ii) fornire al DPO tutte le risorse necessarie per consentirgli lo svolgimento dei propri compiti, consentendogli di accedere ai dati personali e ai trattamenti (con obbligo di mantenere il segreto professionale), ma anche le ulteriori risorse necessarie per mantenere nel tempo la propria conoscenza specialistica (ad es. in tema di formazione continua); (iii) astenersi dal fornire istruzioni al DPO sullo svolgimento della propria attività e dei propri compiti, tenendo conto che quest'ultimo non ha superiori a cui rispondere e riferisce direttamente al vertice gerarchico del titolare o del responsabile del trattamento che lo abbiano designato; (iv) assicurarsi che il DPO, qualora svolga anche altri compiti ed altre funzioni, diverse da quelle tipicamente previste dal GDPR, non sia mai in conflitto di interessi (ad esempio, non può a rigore svolgere compiti di sicurezza informativa e al contempo, in qualità di DPO, sorvegliare che il proprio operato, quale responsabile della sicurezza informatica, sia stato correttamente svolto. Il conflitto di interessi è evidente). Sulla figura del DPO si veda, in dottrina, C. Solinas, *La nuova figura del responsabile della protezione dei dati*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 879 ss.; A. Avitabile, *Il data protection officer*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 331 ss.

mirata in tale materia, di tipo specialistico, accompagnati da ulteriori percorsi di formazione continua per il mantenimento delle competenze in una disciplina soggetta a continue evoluzioni.[97]

Si tratta di figure che ormai non dovrebbero mancare in nessuna realtà organizzativa, essendo al giorno d'oggi inevitabile il trattamento di dati personali in qualunque ambito ci si trovi ad operare. Non può pensarsi tuttavia che i problemi di *compliance* siano risolti affidando l'attuazione degli adempimenti esclusivamente a figure specificamente individuate all'interno ed all'esterno dell'organizzazione impegnata con il trattamento dei dati personali, dato che diviene fondamentale una progressiva assimilazione della disciplina da parte dell'intera organizzazione, a tutti i livelli. Occorre giungere, in altre parole, a conquistare progressivamente una solida "cultura della *privacy*" per tutti coloro che – dalle posizioni apicali a coloro che ricoprono ruoli più operativi o di semplice collaborazione – partecipano a diverso titolo alla vita dell'ente.[98] Occorre una "cultura" – veicolata dal *data protection officer*, dal *privacy officer* o dal referente *privacy* – che porti a comprendere come la *compliance* in tale materia non sia un mero orpello burocratico, ma (i) questione imprescindibile di tutela di interessi fondamentali di tutte quelle persone fisiche che gravitano, con il trattamento dei dati personali, nella sfera di operatività del titolare del trattamento e che, per tale ragione, si trovano esposte a rischi di pregiudizi (danni) più o meno intensi in ragione di tale trattamento; nonché, al contempo, (ii) un'ottima occasione per mettere a punto sia l'efficienza dei processi interni dell'organizzazione, sia il migliore raggiungimento degli obiettivi istituzionali che l'ente legittimamente persegue, con un approccio – tipico degli strumenti di *compliance* in materia di protezione dei dati personali – improntato ad un progressivo ed incessante miglioramento dell'efficienza interna *goal oriented*.

Non va mai dimenticato infatti che, nella prospettiva del titolare del trattamento, quest'ultimo – nel caso in esame l'associazione sportiva dilettantistica – è il soggetto che stabilisce le *finalità* legittime del trattamento e le modalità per raggiungerle, attraverso lo svolgimento di trattamenti dei dati personali che sono funzionali proprio al raggiungimento di tali finalità, come ben si ricava anche dai principi generali fissati all'art. 5 GDPR, tra cui quello di cui al par. 1, lett. *b)*, secondo il quale i dati personali sono "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità […]". Sicché, gestire correttamente la *compliance* in materia di protezione dei dati vuol dire anche assicurare, mediante adeguati strumenti metodologici, il raggiungimento delle finalità istituzionali in relazione alle quali il trattamento viene svolto e, al contempo, il bilanciamento con le esigenze di tutela degli interessati che entrano in contatto con l'associazione titolare del trattamento.

[97] Si pensi, ad esempio, al Corso di Alta Formazione in "*Data Protection e Privacy Officer*" dell'Università di Bologna (https://site.unibo.it/dpo), che si svolge con il patrocinio del Garante per la protezione dei dati personali, giunto nell'a.a. 2021/2022 all'ottava edizione, da cui si può accedere poi all'Osservatorio *Privacy* e al Gruppo di Ricerca *Data Protection Law*, collegati con il predetto Corso di Alta Formazione, per il mantenimento di competenze nell'ottica della formazione continua.

[98] Si pensi a chi sia designato quale soggetto autorizzato al trattamento dei dati personali, con compiti corrispondenti a quelli del responsabile interno del trattamento dei dati personali o a quelli dell'incaricato del trattamento, secondo la nomenclatura in uso prima dell'applicazione del Reg. UE 679/2016 (GDPR). Si pensi in particolare anche a chi ha compiti decisionali e, individualmente o all'interno di organi collegiali, assume le decisioni rilevanti sull'*an* e sul *quomodo* del trattamento. Per una lettura critica dell'interpretazione diffusasi a livello istituzionale sull'attuale inquadramento della figura soggettiva del responsabile "interno" del trattamento si rimanda a F. Bravo, *Sulla figura del responsabile "interno" del trattamento di dati personali*, in *Il diritto dell'informazione e dell'informatica*, 2019, 4-5, pp. 951-978.