JUS CIVILE

GIULIANA AMORE

Professoressa associata di Diritto privato – Università degli Studi di Catania

DIGITALIZZAZIONE, PROTEZIONE DEI DATI E TERZO SETTORE

SOMMARIO: *1. Premessa. – 2. ETS e trattamento dei dati personali. – 3. Il Registro dei trattamenti e la nomina del d.p.o.: obbligo o facoltà per gli ETS? – 4.* Data breach, policies *e misure adeguate. – 5. Registro Unico Nazionale del Terzo Settore e GDPR.*

1. – Com'è noto, il d.lgs. n. 117/2017, contenente il c.d. Codice del Terzo settore, ha operato una vera e propria opera di «istituzionalizzazione» [1], ancora in corso di attuazione [2] e finalizzata a riorganizzare il settore degli enti senza scopo di lucro [3], favorendone la gestione e migliorandone la trasparenza: un settore normativamente definito mediante un intreccio o combinazione di tre criteri e, precisamente, il perseguimento di finalità civiche, solidaristiche e di utilità sociale, lo svolgimento di attività riconosciute dal legislatore di interesse generale e, infine, una *governance* in grado di impedire la prevalenza di interessi prettamente privati su

[1] Così, M. RISPOLI FARINA, *Il codice del Terzo settore tra novità e contraddizioni*, in D. DI SABATO, O. NOCERINO (a cura di), *Il Terzo settore profili critici della riforma*, Napoli, 2019, 3; già, G. PONZANELLI, *Quali regole giuridiche per il terzo settore?*, in *Riv. dir. civ.*, 3, 1996, 314, osserva come la crescita del *non profit* «conferm(i) il ruolo assolutamente trascurabile delle regole giuridiche sulla nascita e nella diffusione di nuovi fenomeni sociali». Sulla relazione fra le norme giuridiche ed il dinamismo naturale degli enti del Terzo settore, cfr. L. GORI, F. ZANDONAI, *I confini del Terzo settore: una mappa costantemente da riscrivere*, in *Impr. soc.*, 2018, 11 ss.

[2] Recentemente, è stato emanato il d. m. attuativo n. 106/2020.

[3] In tal senso, F. BOSETTI, *Il registro unico nazionale del terzo settore*, in M. GORGONI, *Il codice del terzo settore, Comm. al d.lgs. 3 luglio 2017 n. 117*, Pisa, 2021, 361, secondo il quale «il d.lgs. n. 117/2017, istituendo il Registro unico nazionale del Terzo settore, ha inteso dar corpo ai numerosi auspici che da tempo si formulavano, ispirati ad un'esigenza di riordino e di semplificazione di un sistema pubblicitario frammentario» oltreché disorganico: auspici che rappresentavano, in realtà, solo una parte della più ampia necessità di una riforma dell'intera disciplina del Terzo settore. Com'è noto, ai sensi dell'art. 4 CTS, sono enti del terzo settore le organizzazioni di volontariato, le associazioni di promozione sociale, gli enti filantropici, le imprese sociali, incluse le cooperative sociali, le reti associative, le società di mutuo soccorso, le associazioni, riconosciute o non riconosciute, le fondazioni e gli altri enti di carattere privato diversi dalle società costituiti per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale mediante lo svolgimento, in via esclusiva o principale, di una o più attività di interesse generale in forma di azione volontaria o di erogazione gratuita di denaro, beni o servizi, o di mutualità o di produzione o scambio di beni o servizi, ed iscritti nel registro unico nazionale del Terzo settore. L. GORI, *Terzo settore e costituzione*, Torino, 2022, 1, sottolinea la difficoltà di coniare una definizione di «Terzo settore». Nella letteratura internazionale ha avuto successo la qualificazione del Terzo settore come "*a loose and baggy monster*", ad indicare l'estrema complessità di definire i confini di un complesso di enti, attività e relazioni che si colloca in una zona intermedia fra lo Stato ed il mercato. L'espressione è di J. KENDALL, M. KNAPP, *A Loose and Baggy Monster. Boundaries, Definition and Typologies*, London, 1995, 66 ss. Cfr. anche A. ETZIONI, *The Third Sector and Domestic Missions*, in *Public Administration Review*, 1973, 314 ss., che parla al riguardo di «una terza alternativa, in effetti un terzo settore, è cresciuta tra il settore statale e quello del mercato», tra pubblico e privato.

quelli di più ampio respiro. Trattasi di una riforma intervenuta, peraltro, in un momento caratterizzato e segnato da una trasformazione importante, quella della *digitalizzazione*.

Sotto tale profilo, è la stessa riforma del terzo settore a richiedere agli enti *non profit* di inserirsi nel percorso di trasformazione digitale [4]: trasformazione finalizzata a colmare la carenza di una non immediata ed esponenzialmente incompleta disponibilità dei dati e ispirata a quella cultura dell'*accountability* [5] già da tempo invocata. L'obiettivo di trasparenza e di informazione mediante strumenti digitali nella gestione degli enti del terzo settore, infatti, permea in più punti la nuova normativa: basti pensare all'art. 14 che impone – ai Centri di servizio per il volontariato (Csv) e agli enti che abbiano ricavi, rendite, proventi o entrate superiori a centomila euro l'anno – l'obbligo di pubblicare *online* i bilanci sociali; o all'art. 41 che richiede alle reti associative l'utilizzo di strumenti (anche) informatici idonei a garantire conoscibilità e trasparenza in favore del pubblico e dei propri associati [6].

La "digitalizzazione", poi, investe anche la raccolta fondi e le donazioni: e se il CTS disciplina tale aspetto all'art. 7, indicando ancora una volta il principio di «trasparenza e correttezza nei rapporti con i sostenitori e il pubblico», crescono modalità nuove, spesso veicolate proprio dal *web*, come il *digital fundraising* o *crowdfunding* (raccolta fondi digitale).

Ma l'ambito nel quale il tema della trasparenza "digitale" presenta implicazioni sistematiche maggiormente rilevanti sul piano civilistico appare senz'altro quello della gestione informatica dei dati personali e dei temi connessi alla *privacy*: tutte le organizzazioni *non profit*, infatti, sono tenute ad ottemperare agli obblighi *privacy* scaturenti dal Reg. UE n. 679/2016 (c.d. GDPR, *General Data Protection Regulation*) [7] in quanto "titolari del trattamento", se svolgono anche una sola delle operazioni che concretano un trattamento di dati personali, decidendo la finalità e le modalità del trattamento stesso. Ed invero, ai sensi dell'art. 4 GDPR, l'ente del Terzo settore sarà "titolare di trattamento" ogniqualvolta effettui qualunque operazione applicata a dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, o anche solo la comunicazione, diffusione, messa a disposizione o interconnessione di dati con qualunque mezzo, incluso quello digitale: da qui, l'esigenza di verificare presupposti, limiti e condizioni di operatività delle norme del GDPR per gli enti del terzo settore, tenuti, in generale, ad eseguire una minuziosa mappatura dei dati personali trattati e dei soggetti interessati al fine di effettuare una valutazione dei rischi e verificare la corretta adozione di tutte le misure richieste dalla normativa in materia, per non incorrere nelle pesanti sanzioni di cui al Reg. EU n. 679/2016.

Da ultimo, le riflessioni sulla relazione tra digitalizzazione, protezione dei dati e terzo settore non possono concludersi senza volgere lo sguardo al Registro Unico Nazionale del Terzo Settore (RUNTS), non solo in quanto registro (per l'appunto) telematico [8], ma anche perché esso – finalizzato ad assicurare principalmente

---

[4] Gli strumenti informatici creano, infatti, un'infrastruttura di comunicazione e condivisione dei dati che permette ai volontari e agli operatori del TS di organizzarsi in modo efficiente, collaborare fra di loro e condividere i dati, pur non disponendo di un'infrastruttura informatica propria.

[5] Sul concetto di *accountability*, v. *infra* nt. n. 51.

[6] E più crescono le responsabilità, più aumentano gli obblighi di trasparenza: ai Csv, ad esempio si richiede di rispettare il principio di pubblicità e trasparenza nell'erogazione dei propri servizi, anche mediante modalità informatiche che ne assicurino la maggiore e migliore diffusione. Non ultimo il tema della pubblicazione dei contributi pubblici, il cui obbligo di pubblicazione sui propri siti è stato indicato dalla Legge sulla concorrenza n. 124/2017.

[7] Sulla protezione dei dati personali, cfr. *ex multis*, di recente, R. D'ORAZIO, G. D. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della* privacy *e* data protection, Milano, 2021.

[8] Il RUNTS, istituito presso il Ministero del Lavoro e delle Politiche Sociali in attuazione degli artt. 45 ss. del Codice del Terzo Settore, è il luogo digitale e telematico in cui reperire le seguenti informazioni sull'Ente del Terzo Settore (ETS): la denominazione,

la piena trasparenza degli ETS, da un lato e l'acquisto della qualifica di ETS, dall'altro – solleva un duplice ordine di questioni relative, rispettivamente, all'operatività o meno del GDPR per il trattamento dei dati degli enti raccolti nel RUNTS e alla configurabilità dell'iscrizione nel Registro come pubblicità costitutiva sia della qualifica di ETS sia dell'acquisto della personalità giuridica. Sotto il primo profilo, occorrerà muovere dal concetto di "persona" (fisica o anche giuridica) come presupposto soggettivo di applicazione della disciplina per la tutela dei dati personali; sotto il secondo profilo, se da un lato il CTS non ha abrogato né le disposizioni del libro primo del codice civile in materia di enti *non profit*, né quelle contenute nel d.P.R. n. 361/2000 sul registro delle persone giuridiche, dall'altro, a tali enti è riconosciuta non solo la facoltà di continuare ad operare nella veste di associazione, fondazione o comitato soggetto alle norme del codice civile e del d.P.R. n. 361/2000, ma altresì, *ex* art. 22 CTS, la possibilità di iscriversi al RUNTS attraverso un procedimento "agevolato", per ottenere sia la qualifica di ETS, sia – in deroga alle disposizioni del d.P.R. n. 361/2000 – la personalità giuridica: il che induce fondatamente ad indagare sulla scelta del CTS di mantenere in vita il doppio binario per il riconoscimento della personalità giuridica agli ETS (iscrizione nel Registro delle persone giuridiche, da una parte e iscrizione al RUNTS, dall'altra), ricercandone la *ratio* ed il possibile coordinamento.

2. – Se l'art. 6 del GDPR delinea le basi giuridiche del trattamento, l'art. 9 integra e specifica tali basi nel caso in cui il trattamento abbia ad oggetto categorie "particolari" di dati personali, prevedendo specifiche prescrizioni, come quelle dettate – al terzo comma – per organismi di tipo associativo, fondazioni, o altro ente senza scopo di lucro che tratti dati c.d. "particolari", o "sensibili" [9] secondo la vecchia etichetta: si pensi ai dati che rivelano le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, o in generale quelli relativi alla salute [10].

---

la forma giuridica, la sede legale e le eventuali sedi secondarie, la data di costituzione, l'oggetto dell'attività di interesse generale, il codice fiscale o la partita iva, il possesso della personalità giuridica e il patrimonio minimo, le generalità dei rappresentanti legali, le generalità dei soggetti che ricoprono cariche sociali e tutte le modifiche agli atti fondamentali dell'ente. Inoltre, nel RUNTS saranno riportati i rendiconti o i bilanci d'esercizio e il bilancio sociale. Il RUNTS è composto da sette sezioni, una per ogni tipologia di ETS: organizzazioni di volontariato, associazioni di promozione sociale, enti filantropici, imprese sociali, reti associative, società di mutuo soccorso. Gli aspiranti enti che vogliono iscriversi a una delle sezioni del RUNTS devono essere in possesso di un corredo digitale minimo che comprende l'identità digitale del legale rappresentante (Spid o Cie), la firma digitale e un indirizzo Pec. Sottolinea il particolare impatto dell'adozione del RUNTS, con le implicazioni che tagliano trasversalmente una molteplicità di profili (costituzione, controlli, preservazione dell'autonomia e *accountability* degli ETS; attuazione dell'art. 118 Cost.), M. GORGONI (a cura di), *Codice del terzo settore. Commento al d.lgs. 3 luglio 2017, n. 117* (Seconda edizione aggiornata con il DM 15 settembre 2020), Pisa, 2021; cfr., anche, A. MAZZULLO, *Il nuovo codice del terzo settore. Profili civilistici e tributari*, Torino, 2017; L. GORI, *Terzo settore e Costituzione*, Torino, 2022, 161 ss.; A. FICI, *Profili e principi generali della riforma del Terzo settore*, in AA.VV., *Dalla parte del Terzo settore*, Roma-Bari, 2019, 18 ss.; C. GRANELLI, *Impresa e terzo settore: un rapporto controverso*, in *juscivile*, 2018, 5.

[9] Il GDPR contiene, all'art. 9, una definizione di "categorie particolari di dati personali", che comprendono: i dati che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale"; i dati biometrici e genetici atti ad identificare in modo univoco una persona fisica; dati sanitari (e cioè i dati relativi alla salute) o quelli relativi alla vita sessuale o all'orientamento sessuale della persona.

[10] Pensiamo, ad esempio, alle associazioni che operano per un fine di assistenza sociale o socio-sanitaria, che trattano dati relativi alla salute. Le ODV e gli ETS in generale possono facilmente disporre di dati "particolari" (sensibili): quelli dei beneficiari dell'attività sociale, quando operano proprio nei settori che il legislatore considera più delicati, come ad esempio l'ambito sanitario e della salute (ad es. chi lavora con malati, soggetti portatori di *handicap* o tossicodipendenti, ma anche con anziani portatori di patologie), l'ambito religioso o caratterizzato ideologicamente in senso politico, ma anche filosofico (ad es. un'associazione espressamente e "istituzionalmente" pacifista o antiproibizionista), l'ambito dell'appartenenza etnica (es. associazioni che lavorano con i nomadi o migranti).

Più precisamente, l'art. 9 GDPR presenta una «struttura bifasica» [11], ponendo, da un lato, il divieto generale di trattare categorie "particolari" e individuando al tempo stesso, dall'altro, una serie di eccezioni a tale divieto: una delle deroghe al divieto generale di trattamento dei dati "particolari" è costituita proprio dall'ipotesi in cui il trattamento sia finalizzato al perseguimento di scopi determinati e legittimi, individuati nell'atto costitutivo, nello statuto o nel contratto collettivo della fondazione, dell'associazione o di altro organismo *non profit*. Alla luce dell'astratta meritevolezza delle finalità perseguite e delle funzioni svolte dagli enti del terzo settore, il legislatore ha quindi operato *ex ante* una valutazione di legittimità del trattamento dei dati "particolari" là dove associazioni, fondazioni e in generale enti del terzo settore perseguano, (anche) mediante il trattamento stesso, le loro finalità istituzionali, civiche, solidaristiche e di utilità sociale. In altri termini, trattasi di uno di quei casi in cui al consenso dell'interessato si sostituiscono, quali basi giuridiche per il trattamento delle categorie particolari di dati, esigenze diverse ritenute prevalenti rispetto alla posizione dell'interessato e, nella specie, rappresentate dallo svolgimento di attività da parte di enti senza finalità lucrativa per il perseguimento di scopi politici, filosofici, religiosi, culturali, socioassistenziali, umanistici.

Gli organismi del terzo settore (associazioni non riconosciute, partiti, organizzazioni assistenziali e di volontariato, fondazioni) potranno quindi trattare i dati per così dire "sensibili", anche senza il consenso dell'interessato, a condizione però che, dal punto di vista soggettivo, il trattamento riguardi unicamente i membri, gli *ex* membri o le persone con regolari contatti con gli organismi del terzo settore e i dati personali non vengano comunicati all'esterno: in sostanza, l'ente potrà trattare i dati "particolari" senza il consenso dell'interessato allorché il trattamento abbia carattere meramente interno.

Dal punto di vista oggettivo, poi, perché tale trattamento sia lecito, dovrà perseguire scopi determinati e legittimi indicati nello statuto, nell'atto costitutivo o nei contratti collettivi [12]: ciò, in ossequio al principio c.d. di finalità, sancito dall'art. 5, lett. b) del Regolamento UE come uno dei fondamenti del trattamento e alla cui stregua la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità, che vanno comunicate all'interessato e rispettate. Per gli ETS le finalità del trattamento dei dati tendenzialmente coincidono o sono comprese negli scopi istituzionali indicati nello statuto [13].

V'è di più. In quanto titolari di trattamento, gli ETS dovranno predisporre, per tutte le categorie di interessati – e quindi per i soggetti di cui vengono trattati i dati (associati, dipendenti, relativi familiari, donatori, fornitori, beneficiari, volontari, ecc.) – le relative informative, redatte secondo le indicazioni del Regolamento. Lo scopo è quello di informare, appunto, gli interessati sul tipo di dati oggetto di trattamento, sulle modalità e sui tempi di conservazione o sui destinatari, ecc. [14]. In particolare, l'art. 12 GDPR – rubricato come

---

[11] Così, R. TUCCILLO, *Art. 9 GDPR*, in A. BARBA, S. PAGLIANTINI (a cura di), *Delle persone*, vol. II, in E. GABRIELLI (diretto da), *Commentario codice civile*, Milano, 2019, 153.

[12] Le finalità perseguibili potranno e dovranno naturalmente avere natura religiosa, culturale, politica, sindacale, sportiva, di istruzione, formazione, tutela dell'ambiente, beneficenza, assistenza sociale o socio-sanitaria, ecc… Sul punto, cfr. ancora R. TUCCILLO, *op. cit.*, 169. È stata l'Autorità Garante della Privacy a chiarire e a circoscrivere, con provvedimenti nn. 3/2016 e 146/2019 l'ambito di applicazione della disposizione *de qua*, sia dal punto di vista soggettivo sia oggettivo.

[13] Anche se lo statuto è spesso generico e le finalità del trattamento, come vedremo (v., *infra*, in questo §), vanno specificate nell'informativa. Quindi, ad esempio, quando l'associazione raccoglie i dati comuni dei suoi associati per inserirli nel libro soci, per inviare a casa la corrispondenza o il giornalino dell'associazione e comunque per averne la reperibilità, o raccoglie i dati dei beneficiari dell'attività per garantire il servizio, non potrà senza l'autorizzazione e/o l'informazione specifica ai soci/beneficiari usare tali dati per scopi diversi da quelli istituzionali: così, non potrà comunicare il nome e l'indirizzo o altre informazioni a terzi per *marketing*, iniziative commerciali o comunque per scopi che non riguardano l'ente.

[14] Il GDPR (art. 12, comma 1) prevede che l'informativa sia concisa, trasparente, comprensibile, facilmente accessibile e di linguaggio semplice e chiaro e sia fornita "per iscritto o con altri mezzi" e anche "se del caso, con mezzi elettronici" e anche oralmente, "se richiesto dall'interessato". L'informativa deve contenere: l'identità e i dati di contatto del titolare del trattamento e, ove applicabi-

«trasparenza e modalità» – detta le regole generali operanti per l'obbligo di informazione agli interessati alla luce del principio di trasparenza espressamente sancito e relativo tanto alla fase prodromica del trattamento, quanto a quella successiva in cui i dati vengano effettivamente trattati. Gli ETS, in forza dell'art. 12 GDPR, saranno così tenuti a fornire informazioni concise, trasparenti, intellegibili e facilmente accessibili, in forma scritta o ancora una volta con mezzi elettronici, purché adeguati alle circostanze e alle modalità di interazione – tra ente titolare del trattamento e interessato – o alle modalità di raccolta delle informazioni medesime.

Con specifico riferimento ai mezzi elettronici, nel caso di utilizzo da parte dell'ente di un sito *internet*, il Gruppo di lavoro Articolo 29 [15] ha raccomandato l'uso di informazioni stratificate che consentano di consultare le sezioni specifiche dell'informativa sulla *privacy*, contestualmente ed in aggiunta ad un unico documento completo in formato digitale al quale gli interessati possano accedere altrettanto facilmente, qualora intendano consultare le informazioni di cui sono destinatari nella loro interezza. Uno degli strumenti di maggiore novità in tema di informazione e di trasparenza è rappresentato proprio dalla possibilità per i titolari di trattamento, e quindi anche per gli ETS, di fornire le informazioni *ex* artt. 13 e 14 GDPR in combinazione con icone standardizzate, presentate elettronicamente e in grado di aumentare la trasparenza, offrendo un quadro facilmente accessibile, intellegibile e chiaro del trattamento previsto.

Per quanto riguarda, poi, i soggetti (ad es. volontari, segretari, personale amministrativo, persone che si occupino del *data entry* nell'anagrafica dei volontari e così via.) che, internamente all'ente, hanno accesso ai dati personali, l'ente (titolare del trattamento) dovrà *ex* art. 29 GDPR istruirli *ad hoc* sulle modalità del trattamento [16]. Il GDPR, diversamente dalla disciplina contenuta nel Codice *Privacy*, non prevede espressamente la figura dell'"incaricato", ma neppure la esclude, là dove fa riferimento, proprio nell'art. 29, a «persone autorizzate al trattamento sotto l'autorità diretta del titolare o del responsabile»: chiunque, all'interno o all'esterno dell'organizzazione, svolga questa attività dovrà essere sempre adeguatamente informato e istrui-

---

le, del suo rappresentante; i dati di contatto del responsabile della protezione dei dati (Data Protection Officer o DPO), ove nominato; le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) (esistenza di un "legittimo interesse del titolare del trattamento o di terzi" che non leda i diritti e le libertà fondamentali dell'interessato), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili. Inoltre, la stessa informativa deve contenere: il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; qualora il trattamento sia basato sul consenso prestato dall'interessato (ai sensi dell'6, comma 1, lett. a e art. 9, comma 2, lett. a del GDPR), l'esistenza del diritto di revocare il consenso in qualsiasi momento, senza però pregiudicare la liceità del trattamento effettuato sulla base del consenso prestato prima della revoca; il diritto di proporre reclamo al Garante della Protezione dei Dati Personali; se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, commi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

[15] Com'è noto, il Gruppo di lavoro "Articolo 29" (Art. 29 WP), poi sostituito dallo *European Data Protection Board* (EDPB), era il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018 (entrata in vigore del GDPR) aveva lo scopo di occuparsi di questioni interpretative relative alla protezione della vita privata e dei dati personali.

[16] Art. 29 GDPR: «il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

to su come trattare i dati. Trattasi di un adempimento di carattere generale, relativo alla formazione dei soggetti per così dire "incaricati" (secondo la vecchia terminologia) ed anche questo chiaramente ispirato ad un altro dei principi fondamentali sanciti dall'art. 5 Reg. UE n. 679/2016 e, in particolare, quelli di «integrità e riservatezza» (lett. f) che per l'appunto impone (nella specie, all'ente) di trattare i dati in modo da garantire anche indirettamente, e cioè attraverso soggetti diversi dall'ente, la medesima sicurezza dei dati e impedire violazioni nel trattamento degli stessi. La sicurezza dei dati non può infatti prescindere da un'accurata istruzione dei soggetti che materialmente trattano i dati personali [17].

Tutti i soggetti per così dire "esterni" all'ente, ossia che trattino o possano trattare dati personali per conto dell'ente stesso (come consulenti, professionisti, altre organizzazioni, soggetti che si occupano della gestione e manutenzione di *software* ecc.) dovranno non soltanto essere istruiti dall'ente del terzo settore, in quanto titolare del trattamento, ma altresì stipulare con quest'ultimo un vero e proprio contratto *ex* art. 28 del Regolamento, che disciplina le modalità con cui devono essere trattati i dati [18]: un contratto scritto, per lo più in forma digitale, dal contenuto predeterminato dalla norma stessa e per effetto del quale il soggetto "esterno" (consulente, professionista, altra organizzazione, soggetto che si occupa della gestione e manutenzione di *software* ecc.) agirà per conto dell'ente del terzo settore titolare del trattamento [19].

Proprio in questi termini, sembra legittimo risolvere l'*impasse* interpretativo scaturente dal combinato disposto degli artt. 28 e 29 GDPR alla cui stregua, rispettivamente, «qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento» con i quali ha l'obbligo di stipulare «un contratto […] *sulla* durata del trattamento, natura e finalità, tipo di dati trattati e categorie di interessati […]» (art. 28) e «il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non istruito in tal senso dal titolare del trattamento» (art. 29). In sostanza, se è vero che il contratto *ex* art. 29 GDPR va stipulato (non con chiunque, ma) soltanto con chi effettui il trattamento per conto dell'ente titolare del trattamento, è altrettanto vero che chiunque abbia accesso ai dati personali, a prescindere dal contratto *ex* art. 29 GDPR, dovrà comunque essere adeguatamente edotto ed istruito dal titolare del trattamento per poter trattare i dati.

---

[17] Sull'argomento, cfr. M. Massimi, *Art. 29 GDPR*, in A. Barba, S. Pagliantini (a cura di), *op. cit*., 574.

[18] Art. 28 GDPR, comma 3: «I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento […]». E. Maio, *Art. 28 GDPR*, in A. Barba, S. Pagliantini (a cura di), *Delle persone*, cit., 566 s. sottolinea come la norma sia strutturata sul modello tedesco (§ 11 BDSG), probabilmente per la puntualità della normativa tedesca rispetto alle altre, garanzia di una maggiore efficienza nella protezione dei dati personali dell'interessato e di una limitata discrezionalità dei soggetti coinvolti nel trattamento dei dati.

[19] Si pensi, a titolo esemplificativo, ad un birrificio con molti dipendenti. Firma un contratto con una società addetta all'elaborazione delle buste paga per pagare gli stipendi. Il birrificio indica a tale società quando deve essere pagato lo stipendio, quando un dipendente lascia l'azienda o ottiene un aumento di stipendio, e fornisce tutti gli altri dati per le buste paga e i pagamenti. La società fornisce il sistema informatico e conserva i dati dei dipendenti. Il birrificio è il titolare del trattamento e la società addetta all'elaborazione delle buste paga è il responsabile del trattamento. Nonostante, infatti, i cambiamenti introdotti dal Nuovo Regolamento UE 2016/679 (GDPR, Regolamento Generale sulla protezione dei dati), le basi normative introdotte dal Codice della *Privacy* (d.lgs. n. 196/2003) rimangono invariate. La terminologia del nuovo Regolamento, da questo punto di vista, si allinea alla normativa nazionale. Le figure coinvolte nel trattamento dei dati sono sempre le stesse: si parla di titolare, responsabile (sostanzialmente corrispondente all'incaricato del trattamento), sia a livello comunitario che a livello nazionale. Il Regolamento definisce, infatti, caratteristiche soggettive e responsabilità del titolare e del responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). La disciplina europea ha tuttavia introdotto alcune novità significative, volte a rafforzare la tutela del diritto alla *Privacy* e, di conseguenza, i diritti degli interessati.

Tutto ciò, sempre e ancora una volta, nel rispetto dei principi generali del Regolamento sanciti dall'art. 5 del GDPR. In particolare, in forza del c.d. principio di "limitazione delle finalità", le ODV, gli ETS, o in generale, le «persone (*da loro*) autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile» (*ex* art. 4, n. 10, GDPR) dovranno raccogliere, trattare ed utilizzare i dati compatibilmente ed esclusivamente per finalità determinate, esplicite e legittime: finalità che, di norma e come già sottolineato, coincideranno con quelle dell'ente stesso indicate nello statuto o nell'atto costitutivo. In tale contesto, il profilo di maggiore criticità attiene alla compatibilità o meno del trattamento effettuato (nella specie) da un ETS con le c.d. finalità ulteriori. Se è vero che gli ETS possono, *ex* art. 6 del codice del terzo settore, esercitare attività secondarie e strumentali rispetto a quelle di interesse generale tipizzate nell'art. 5 CTS, purché esplicitamente individuate nello statuto o nell'atto costitutivo, sembra legittimo fondare anche la valutazione di compatibilità [20] del trattamento per fini ulteriori proprio sul rapporto di strumentalità delle finalità ulteriori rispetto a quelle iniziali. Ed invero l'art. 5, lett. b, GDPR ritiene compatibile con le finalità iniziali «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici» [21].

---

[20] Per stabilire la compatibilità della nuova finalità occorre tenere conto, tra l'altro, di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione: in tal senso, cfr. D. ACHILLE, *Art. 5*, in A. BARBA, S. PAGLIANTINI (a cura di), *Delle persone*, cit., 109. È possibile rinvenire alcune importanti linee guida in merito al compimento della valutazione di compatibilità delle finalità nell'*Opinion* 3/2013 dell'Art. 29 *Data Protection Working Party* – sebbene si tratti di un'*opinion* scritta sotto la vigenza della Direttiva 95/46/CE, è comunque utile ripercorrere i termini del "*compatibility assessment*", coniugandolo con le attuali previsioni del GDPR. In particolare, in tale parere, viene affermato che il (determinante) test di compatibilità debba preferibilmente fondarsi su una valutazione sostanziale (piuttosto che formale, per natura eccessivamente rigida, benché, a prima vista, maggiormente obiettiva e neutrale), la quale, capace di andare oltre agli aspetti meramente formalistici, si basa sulla valutazione dei seguenti (utili e noti) criteri, divenendo, così, un metodo flessibile, pragmatico e maggiormente efficace: il rapporto tra la finalità per la quale i dati sono stati raccolti e la finalità ulteriore di trattamento, sicché l'attenzione deve concentrarsi sul rapporto sostanziale tra le due finalità (originaria ed ulteriore) di trattamento, onde così comprendere se sussiste una situazione in cui l'ulteriore trattamento fosse già (più o meno) implicito nella finalità iniziale ovvero assunto come una fase logica successiva del trattamento in base a tale finalità; in secondo luogo, il contesto in cui i dati sono stati raccolti, e la (ragionevole) aspettativa del soggetto interessato in merito al loro ulteriore utilizzo e al fine di valutare la ragionevole aspettativa del soggetto interessato, è necessario tenere in considerazione la natura del rapporto tra l'interessato e il relativo titolare del trattamento, lo *status* di quest'ultimo nonché la base giuridica su cui si è fondata la finalità di trattamento originaria, onde così comprendere il grado di sorpresa dell'interessato e l'eventuale squilibrio, ai danni dello stesso, nel relativo rapporto; la natura dei dati e l'impatto dell'ulteriore trattamento sul soggetto interessato. Tale terzo fattore esprime un comune approccio, giacché la normativa in parola è stata progettata ed è volta a proteggere le persone fisiche contro l'impatto di un uso improprio ovvero eccessivo dei dati personali: in merito, viene, dunque, ricordato che più sensibili sono le informazioni personali coinvolte, più ristretto è, di conseguenza, l'ambito di un utilizzo compatibile. Infine, rilevano le garanzie applicate dal titolare del trattamento al fine di determinare un trattamento corretto e prevenire un qualsiasi indebito impatto sul soggetto interessato: in merito, il WP 29 ha precisato che la sussistenza di adeguate misure aggiuntive possono essere idonee, in linea di principio, a compensare l'ulteriore finalità di trattamento ovvero il fatto che essa non sia stata chiaramente specificata all'inizio, così come *ex lege* richiesto.

[21] Tale tipo di trattamento, comunque, deve essere realizzato in base ad apposite garanzie, come previste dall'art. 89 GDPR, al fine di tutelare i diritti degli interessati. Le garanzie, ovviamente, sono date dalle misure di sicurezza (tra le quali si può includere la pseudonimizzazione) e il rispetto della minimizzazione dei dati. Il novellato Codice *Privacy* (art. 110-*bis*), poi, stabilisce che l'Autorità di controllo può autorizzare il trattamento ulteriore dei dati per fini di ricerca scientifica o per finalità statistiche da parte di soggetti che svolgano principalmente tali attività, qualora l'informazione agli interessati risultasse impossibile o implicasse uno sforzo sproporzionato, però a condizione che vengano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati, ivi incluse forme preventive di minimizzazione e di anonimizzazione dei dati. Peraltro, il WP 29 ha sottolineato che, in via potenziale, possono sussistere tre differenti scenari: la compatibilità è *prima facie* ovvia e, quindi, un ulteriore trattamento può

Nonostante l'ente titolare del trattamento sia dunque chiamato a prevedere *ex* ante e in modo specifico le finalità cui attenersi nello svolgimento delle operazioni di trattamento, non è escluso lo svolgimento di trattamenti ulteriori per scopi diversi: ciò può avvenire nella misura in cui le finalità ulteriori siano "compatibili" rispetto alle finalità per le quali i dati sono stati inizialmente raccolti [22].

Al riguardo, la formulazione dell'art. 5, lett. b, GDPR risulta "ambigua", dal momento che non è sufficientemente chiaro quali siano le finalità del trattamento "compatibili" rispetto a quelle della raccolta. L'unica certezza chiaramente espressa dal legislatore europeo è, per l'appunto, che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è […] considerato incompatibile con le finalità iniziali» [23]: così, ad esempio, non costituirà trattamento ulteriore quello effettuato a fini di ricerca di dati raccolti per l'attività clinica da parte di un ente di ricovero e cura a carattere scientifico in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta da tale ente rispetto alla ricerca. In caso contrario, e cioè nell'ipotesi di incompatibilità del trattamento ulteriore con le finalità originarie per le quali il trattamento è stato autorizzato, l'ente dovrà agire in virtù di un'autonoma base giuridica ai sensi dell'art. 6 GDPR [24].

Altrettanto dubbia è la natura meramente esemplificativa o tassativa del riferimento alle suddette finalità ulteriori specificamente menzionate dal legislatore europeo come "compatibili". La soluzione di tale quesito non sembra poter prescindere da una lettura dell'art. 5, lett. b, GDPR in combinato disposto con il successivo art. 6, comma 4 e con il considerando n. 50 [25]: sicché l'ente del terzo settore potrà trattare i dati personali per

---

essere ritenuto compatibile, in quanto i dati sono trattati per raggiungere, in un modo consueto, le finalità specificate al momento della raccolta; oppure la compatibilità non è ovvia e, dunque, necessita di un ulteriore analisi per verificare la sussistenza di una connessione tra lo scopo specificato ed il modo in cui i dati vengono successivamente elaborati. In altri termini, gli scopi sarebbero correlati, ma non completamente corrispondenti. Infine, l'incompatibilità è ovvia e i dati vengono elaborati in un modo o per scopi aggiuntivi che una persona ragionevole riterrebbe inaspettati, inappropriati o altrimenti discutibili: il trattamento non soddisfa, senz'altro, le aspettative dell'interessato. L'allegato 4, poi, contiene ulteriori esempi pratici – da casi semplici e diretti a casi più complessi – che illustrano come può essere effettuata una valutazione di compatibilità sostanziale. I vari esempi includono, tra gli altri, l'elaborazione di dati nell'ambito del *marketing*, le telecamere a circuito chiuso, il trasferimento dei risultati della visita medica pre-assunzione, l'uso di algoritmi per prevedere la gravidanza delle clienti dalle abitudini di acquisto, l'uso di posizioni di telefoni cellulari per informare sulle misure di moderazione del traffico, sull'uso dei registri dei nominativi dei passeggeri, sul trattamento dei dati di misurazione intelligente a fini fiscali o per rilevare un uso fraudolento o sull'applicazione della direttiva sulla conservazione dei dati.

[22] Nel pieno rispetto del ben noto principio di *accountability*, l'ente titolare del trattamento sarà poi chiamato a comprovare di aver agito conformemente al principio di finalità, sulla base di un'attenta valutazione in merito alla compatibilità degli scopi ulteriori del trattamento, così come richiesto ai sensi del combinato disposto degli artt. 5, lett. b e 6, comma 4, GDPR. Più precisamente, il GDPR prevede espressamente che sia possibile ampliare le finalità iniziali del trattamento e che la valutazione in merito alla loro "non incompatibilità", ai sensi e per gli effetti dell'art. 6, comma 4, sia rimessa al titolare e a lui soltanto, rientrando nella sua *accountability* l'esser in grado di dimostrare che il trattamento sia in ogni caso avvenuto nel pieno rispetto della normativa applicabile in materia di protezione dei dati personali.

[23] Norma, questa, che va letta in combinato disposto con l'attuale formulazione dell'art. 110-*bis* del d.lgs. n. 196/2003, come da ultimo emendato dal d.lgs. 10 agosto 2018, n. 101, alla cui stregua l'Autorità Garante per la protezione dei dati personali può autorizzare il trattamento ulteriore dei dati per fini di ricerca scientifica o per finalità statistiche da parte di soggetti che svolgano principalmente tali attività, allorché informare gli interessati risultasse impossibile o implicasse uno sforzo sproporzionato e a condizione che vengano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati, ivi incluse forme preventive di minimizzazione e di anonimizzazione dei dati.

[24] Sull'argomento, cfr. F. RESTA, *Art.5*, in RICCIO, SCORZA, BELLISARIO (a cura di), *GDPR e normativa privacy*, Vicenza, 2018, 51 ss. e, in particolare, 58.

[25] Considerando n. 50) del GDPR: «Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali […] L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il

finalità ulteriori, non limitate a quelle di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici, ma ritenute in generale *compatibili* con quelle originarie, alla luce del contesto in cui i dati personali sono stati raccolti e in particolare delle ragionevoli aspettative dell'interessato, della natura dei dati personali, delle conseguenze dell'ulteriore trattamento previsto per gli interessati e, infine, dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto [26].

Alla luce, poi, del principio di "minimizzazione e proporzionalità", anch'esso sancito dall'art. 5 GDPR, le ODV e in generale gli ETS non potranno acquisire informazioni e dati ultronei rispetto a quelli necessari per il raggiungimento dello scopo del trattamento: essi devono cioè assicurarsi che i dati raccolti siano adeguati, pertinenti e non eccedenti rispetto a quanto necessario per il perseguimento delle finalità per cui sono raccolti. Ci si intende riferire, in particolare, all'ipotesi assai frequente nella prassi di un'associazione che sottoponga agli utenti o a coloro che entrano in contatto con l'ente moduli nei quali conferire un numero o tipologie di dati eccessivi rispetto alle finalità (es. nelle richieste di iscrizione alla *newsletter*, o nella domanda di partecipazione ad un evento o a un seminario sono da considerarsi certamente ultronei la residenza, la data di nascita e il codice fiscale, o due recapiti telefonici, ecc.). In tali casi, occorrerà di volta in volta valutare quali siano i dati strettamente indispensabili per fornire il servizio richiesto e sarà certamente possibile, nello stesso modulo (o *format* di iscrizione ad un corso), proporre all'interessato di conferire i dati ulteriori e di fornire il consenso al trattamento per i diversi servizi cui voglia accedere [27].

Considerazioni pressoché analoghe valgono per il principio della c.d. "limitazione della conservazione", alla cui stregua gli ETS, in quanto titolari di trattamento, dovranno conservare i dati per un periodo di tempo non superiore a quello necessario per il raggiungimento delle finalità per cui sono stati raccolti, a meno che la conservazione non avvenga, ancora una volta, per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In siffatto contesto, appare opportuno interrogarsi sulla possibilità per gli ETS di conservare, e conseguentemente trattare, i dati personali dei propri associati anche dopo che essi abbiano lasciato l'ente. Il GDPR, all'art. 9 comma 2 lett. d), come già rilevato, consente l'utilizzo dei dati (anche sensibili) degli *ex* soci senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'associazione e con adeguate garanzie (di protezione dei dati), con divieto però di comunicazione all'esterno (per tale comunicazione ci vuole il consenso specifico dell'*ex* socio) [28]: sicché il trattamento dei

---

trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti di liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenza dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto […]».

[26] L'ETS potrà inoltre trattare i dati per finalità ulteriori anche *incompatibili* rispetto a quelle originarie, purché l'interessato abbia prestato il proprio consenso ovvero il trattamento si basi su un atto legislativo dell'Unione o degli Stati membri, che costituisca una misura necessaria e proporzionata per la salvaguardia, in particolare, degli importanti obiettivi di interesse pubblico generale di cui all'art. 23, comma 1, GDPR.

[27] Ad esempio, chi partecipa ad un corso organizzato da un'associazione acconsentirà facilmente a che il suo indirizzo *mail* sia inserito nella *newsletter* che lo avverta di nuovi eventi formativi.

[28] Peraltro, in applicazione del principio di proporzionalità e minimizzazione dei dati, i dati "trattenuti" dall'associazione dopo l'uscita del socio dovranno però essere strettamente inerenti alle specifiche attività "residue" (es. invio della *newsletter*, convocazione per gli anniversari, ecc.), e quindi potranno, per esempio, ridursi al nominativo e all'indirizzo *mail*. Quanto, poi, alla protezione dei dati in senso stretto, essa è assicurata all'interessato (c.d. *data subject*) attraverso l'esercizio dei diritti indicati dagli articoli da 15 a 22 del GDPR: là dove "soggetti interessati" sono anche gli stessi associati/volontari, e non solo i soggetti esterni all'ETS. In base a tali articoli l'interessato può infatti chiedere al Titolare, cioè all'ente *non profit* di avere conferma che l'ente utilizzi i suoi dati e di

dati degli *ex* soci, ammesso dal Regolamento, ha carattere meramente interno. In particolare, l'Autorità Garante della Privacy [29] ha non solo precisato che, prima di iniziare o proseguire il trattamento, i sistemi informativi e i programmi informatici utilizzati dagli enti devono essere configurati in guisa da ridurre al minimo l'utilizzazione di dati personali identificativi e da escluderne il trattamento ogniqualvolta le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o opportune modalità che permettano di identificare l´interessato solo in caso di necessità; ma ha altresì circoscritto l'ambito di applicazione della disposizione sia dal punto di vista soggettivo, sia oggettivo.

Sotto il primo profilo, il provvedimento chiarisce che il trattamento potrà essere operato da associazioni, organizzazioni assistenziali e di volontariato, fondazioni, comitati, consorzi e organismi senza scopo di lucro: in sostanza, gli enti del terzo settore. Sotto il secondo profilo, il trattamento dovrà perseguire scopi determinati e legittimi di natura religiosa, culturale, politica, sportiva, di formazione e istruzione, tutela e valorizzazione dell'ambiente e del patrimonio culturale, di salvaguardia dei diritti civili, di beneficenza e assistenza sociale o sociosanitaria: in altri termini, tutte quelle attività c.d. di «interesse generale» per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale indicate nel codice del terzo settore, all'art. 5.

Ma il principio di limitazione della conservazione dei dati e l'interrogativo posto, ossia la possibilità o meno per gli ETS di conservare, e conseguentemente trattare, i dati personali dei propri associati anche dopo che essi abbiano – per qualunque ragione o evento – lasciato l'ente, a ben vedere, involge (anche) per gli ETS la più ampia e *vexata quaestio* della gestione del patrimonio digitale per il tempo in cui una persona, nella specie il membro dell'ente, avrà cessato di vivere: questione complessa stante soprattutto l'inadeguatezza degli istituti tradizionali che, seppur adattati alle peculiari caratteristiche del mondo digitale, restano ancorati ad un sistema pensato e sviluppatosi per una realtà ed un contesto socio-economico profondamente diversi e che necessita, quindi, di essere rimeditato alla luce dell'incessante evoluzione digitale, che caratterizza e condiziona ormai la nostra epoca in ogni aspetto, anche quello oltre la morte fisica dell'individuo. Limitandoci in questa sede agli aspetti più strettamente inerenti alla relazione tra digitalizzazione e terzo settore, va osservato come la rilevanza giuridica della questione del trattamento postumo dei dati da parte dell'ETS [30] sia principalmente riconducibile alla circostanza che i dati rappresentano una por-

---

sapere quali siano questi dati; di conoscere l'origine dei dati (cioè come e da chi l'ETS li ha acquisiti), le finalità del trattamento, i soggetti a cui i dati vengono comunicati e il periodo di conservazione dei dati; di rettificare (correggere o integrare) i dati inesatti o incompleti (es. cambio di indirizzo o dello stato civile, aggiornamento del curriculum, ecc.); di cancellare i dati (cd. diritto "all'oblio") quando il trattamento non è più necessario per il raggiungimento delle finalità per cui sono stati raccolti, o in caso di revoca del consenso, o in caso di trattamento illecito o negli altri casi previsti dall'art. 17 GDPR; ottenere una "limitazione del trattamento" nei casi previsti dall'art. 18 GDPR; di poter trasferire i dati ad un altro titolare (diritto "alla portabilità dei dati"); di opporsi al trattamento dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono "motivi particolari" (cioè particolari e valide ragioni: ad esempio se ha presentato domanda di recesso dall'associazione, o se il trattamento, anche se lecito, risulta lesivo della sua dignità o riservatezza); di opporsi al trattamento dei dati svolto per il "*marketing* diretto" (invio di materiale pubblicitario o vendita diretta o compimento di ricerche di mercato o di comunicazione commerciale); di non essere sottoposto ad una decisione basata su un "trattamento automatizzato" di dati (inclusa la cd. profilazione).

[29] Autorizzazione generale n. 3/2016, modificata dal provvedimento n. 146 del 5 giugno 2019, emessa dopo l'entrata in vigore del GDPR ed operante anche con riferimento alle norme in esso contenute: testualmente, «la presente autorizzazione ha efficacia dal 1° gennaio 2017 fino al 24 maggio 2018, tenuto conto che a decorrere dal 25 maggio 2018 sarà applicabile il Regolamento (UE) 2016/679 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) entrato in vigore il 24 maggio 2016, salve le modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia e ferme restando le determinazioni eventualmente adottate dall´Autorità in applicazione del citato Regolamento».

[30] Cfr., sull'argomento, I. MASPES, *Successione digitale, trasmissione dell'*account *e condizioni generali di contratto predisposte*

zione consistente della ricchezza nelle moderne economie [31]. Muovendo cioè dalla considerazione che i dati personali di un "interessato" (*data subject*) sopravvivono oltre la sua vita, per un periodo anche illimitato di tempo, grazie (o a causa) delle attuali tecnologie dell'informazione e della comunicazione, risulta innegabile l'esigenza di un riconoscimento di diritti e poteri di controllo su tali informazioni [32] anche nella fase *post mortem* dell'interessato, quale "prosecuzione" del diritto alla protezione dei dati personali [33]: il quesito allora che si pone attiene non all'*an*, ma al "chi" e in base a quali norme e principi spetterebbe la protezione dei dati nella fase c.d. "post mortale" [34]. Più precisamente, se è vero che con il principio di limitazione della conservazione, sancito dall'art. 5 lett. e), il GDPR consente sia una conservazione prolungata nel tempo dei dati qualora questi, se idonei ad identificare il soggetto interessato, siano trattati per fini di archiviazione nel pubblico interesse, statistici, di ricerca scientifica o storica, sia una protrazione del trattamento dei dati raccolti – là dove sia realizzata e garantita l'impossibilità per chiunque di procedere all'identificazione dell'interessato [35] –, è altrettanto vero che tale principio si scontra innegabilmente con il diritto all'oblio o alla cancellazione dei propri dati che l'interessato può esercitare *ex* art. 17 GDPR [36]. In altri termini, posto che l'ETS possa continuare a trattare i dati dell'*ex* membro defunto, appare doveroso chiedersi se e a chi vada riconosciuta

---

dagli internet services providers, in *I Contratti*, 2020, 5, 583 ss.; G. RESTA, *La "morte" digitale*, in *Dir. inf*., 2014, 907 ss., che sottolinea come la maggior parte dei dati personali digitali sia nella disponibilità dei *providers* e la loro (in)trasmissibilità è normalmente regolata nelle condizioni del contratto di servizio. Si tratta di clausole di contratti *standard* unilateralmente predisposte, spesso di origine americana e tendenzialmente volte ad escludere la trasferibilità dell'*account* e dei suoi contenuti. Più recentemente, ID., *La successione nei rapporti digitali e la tutela postmortale dei dati personali*, in *Contr. e impr*., 2019, 86 ss. V., anche, ZENO ZENCOVICH, *La "datasfera". Regole giuridiche per il mondo digitale parallelo*, in AA.VV., *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, a cura di L. SCAFFARDI, Torino, 2018, 99; C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf*., 2018, 65 ss.; A. VESTO, *Successione digitale e circolazione dei beni* online. *Note in tema di eredità digitale*, Napoli, 2020; A. MAGNANI, *Il patrimonio digitale e la sua devoluzione ereditaria*, in *Vita not*., 2019, 1208 ss.; M. TESCARO, *La tutela postmortale della personalità morale e specialmente dell'identità personale*, in *juscivile*, 2014, 10, 316 ss.

[31] Con riferimento all'ordinamento giuridico italiano, si segnala un primo rilevante intervento legislativo effettuato con il d.lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)". Tale legge contiene una previsione specifica circa il trattamento dei dati personali riguardanti le persone decedute. All'art. 2-*terdecies* è infatti previsto che "i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione". È fatta salva la volontà dell'interessato, purché risulti in modo non equivoco, di vietare l'esercizio di tali diritti. Cfr., sul tema, P. PATTI, F. BARTOLINI, *Digital Inheritance and post mortem data protection: the Italian Refor*m, in *European Review of Private Law*, 2019, 1181 ss.

[32] Ci si intende in particolare riferire a documenti digitali *offline*, dati immessi e conservati nei *social media*, messaggi di posta elettronica e via *chat*, profili *on line* personali e professionali, *accounts*, *files* conservati attraverso servizi di *cloud computing*: si parla al riguardo della c.d. eredità digitale. Sul punto, cfr. G. RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 400 s.

[33] Ancora G. RESTA, *op. ult. cit*., 398, dopo aver sottolineato quanto particolarmente dibattuta nel quadro dell'economia digitale sia la questione circa la "morte digitale" ed il regime dei dati personali digitali nella fase successiva alla morte dell'interessato, parla al riguardo di «*zombie* digitali» i cui dati conservati e trattati da intermediari professionali e quindi sottratti alla disponibilità di eredi e congiunti, sono peraltro oggetto di una riserva contrattuale che ne stabilisce l'intrasmissibilità *mortis causa*.

[34] Così, sempre, G. RESTA, *op. ult. cit.*, 402. In altri termini, si tratta di individuare e trovare un valido appiglio per la protezione postuma degli interessi dell'interessato-defunto.

[35] In tal senso, DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in CUFFARO, D'ORAZIO, RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, 214.

[36] Sull'argomento, cfr. *ex multis* M.A. LIVI, *Art. 17 Reg.UE n. 679/2016*, in A. BARBA, S. PAGLIANTINI (a cura di), *op. cit*., 292 ss. e la ricca bibliografia ivi indicata.

eventualmente la legittimazione ad opporsi a tale perdurante conservazione da parte dell'ente medesimo o, in generale, ad agire per la protezione dei dati personali.

Ed invero, l'art. 2 *terdecies* (rubricato «Diritti riguardanti le persone decedute»), d.lgs. n. 101/2018, emanato per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE n. 679/2016, attribuisce in generale i diritti e i poteri di controllo sui contenuti digitali dell'interessato deceduto, a «chi abbia un interesse proprio, o agisca a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione», salvo diversa disposizione legislativa o divieto scritto, specifico, non equivoco, libero e informato dell'interessato, presentato o comunicato al titolare del trattamento [37]. In conformità, dunque, alla posizione espressa al riguardo dal Gruppo di lavoro WP29 nell'opinione 4/2007 [38] e in termini sostanzialmente analoghi ma più circoscritti rispetto all'art. 13, Codice Privacy [39], l'art. 2-*terdecies*, d.lgs. n. 101/2018 contiene una disciplina non esattamente rispondente ai principi successori *mortis causa* e senz'altro giustificata dall'obiettivo di tutelare coloro ai quali possa derivare pregiudizio dalla "sopravvivenza" di tali dati [40]. Più precisamente, il legislatore italiano sembra aver adottato non tanto un modello "successorio", seppur "anomalo" [41], stante la mancanza sia di un vero e proprio acquisto *mortis causa* sia di "successori" o eredi meramente familiari, quanto piuttosto un meccanismo di «estensione» [42] in capo a terzi della tutela dei diritti dell'interessato, giustificato non soltanto da «ragioni familiari meritevoli di protezione» [43] e in forza dunque di un legame o interesse familiare [44], ma altresì da un «interesse proprio», autonomo e non derivato, oppure da quello «dell'interessato» deceduto, sulla base di un rapporto fiduciario (mandato). In altri termini, non sembra trattarsi di una vicenda acquisitiva "successoria", neppure "anomala", bensì di una legittimazione "straordinaria" [45] ad agire ed esercitare i diritti dell'interessato deceduto, per la protezione *post mortem* dei

[37] Ai sensi dei commi 4 e 5, dell'art. 2-*terdecies* così introdotto, l'interessato ha in ogni momento il diritto di revocare o modificare il divieto e, in ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

[38] In tale opinione, il Gruppo di lavoro W29 ammette il trattamento di dati relativi a defunti allorché la legge nazionale lo consenta, oppure perché onore e immagine siano tutelati anche dopo la morte della persona.

[39] L'art. 13, comma 3, riconosceva in capo a «chiunque (avesse) interesse» il potere di esercitare i diritti de quibus (cancellazione, rettifica e relativa notificazione) sui dati personali concernenti persone decedute.

[40] Sul punto, v. R. RESTUCCIA, *sub art. 13*, in E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH, *La tutela dei dati personali commentario alla L. 675/96*, Padova, 1997, 138.

[41] In tal senso, A. ZACCARIA, *op. cit.*, 23 ss., 72, 79 s., 94 e 261 ss.; A. ZOPPINI, *Le «nuove proprietà» nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, 2000, I, 204 e 244; A. PALAZZO, A. SASSI, *Trattato della successione e dei negozi successori*, 1, *Categorie e specie della successione*, Milano, 2012, 83 ss.

[42] Utilizza tale espressione G. RESTA, *La successione nei rapporti digitali e la tutela postmortale dei dati personali*, cit., 411.

[43] La norma, sebbene in termini più generici, ricalca fortemente gli artt. 7 e 8 cod. civ., per la tutela del diritto al nome e alla cui stregua i rimedi (inibitori e risarcitori) possono essere esperiti «anche da chi, pur non portando il nome contestato o indebitamente usato, abbia alla tutela del nome un interesse fondato su ragioni familiari degne di essere protette» (art. 8 cod. civ.) e a prescindere dal fatto che sia erede oppure no.

[44] Nel Parere 4/2007 sul concetto di dati personali, Articolo 29 Gruppo di lavoro WP29, viene riconosciuto ai legislatori nazionali il potere di estendere le disposizioni delle leggi nazionali sulla protezione dei dati ad alcuni aspetti riguardanti il trattamento dei dati dei defunti, qualora un interesse legittimo lo giustifichi. In altri termini, è compito degli Stati membri stabilire se ed in quale misura il regolamento debba essere applicato alle persone decedute.

[45] Ciò in termini sostanzialmente analoghi alla legittimazione ad agire per l'adempimento dell'onere nella donazione o nel testamento: sul punto, cfr. PROTO-PISANI, *Dell'esercizio dell'azione*, in *Comm. cod. proc. civ.* (diretto da Allorio), Torino, 1973, 1065 ss.; COSTANZA, *Problemi dell'onere testamentario*, in *Riv. dir. civ.*, 1978, II, 313 ss.; G.CAPOZZI, *Successioni e donazioni*, I, Milano, 2002, 494 s. Contro il riconoscimento dell'esercizio di determinati diritti in capo a soggetti viventi a ciò meramente legittimati, si obietta che tale ricostruzione è stata elaborata per assicurare la persistenza di diritti, privi a un certo punto di un titolare, nell'interesse di soggetti che, successivamente, li potranno acquistare, laddove, nel caso in esame non vi sarebbero soggetti che in futuro possano divenire titolari dei diritti della personalità del defunto. Ma la tesi della "legittimazione" appare senz'altro meno artificiosa e critica-

suoi dati personali: legittimazione indipendente dalla titolarità di situazioni giuridiche soggettive [46] ed avente fonte ora in un interesse personale o familiare, ora in un mandato *post mortem* c.d. *exequendum* [47]. Nell'ampia categoria dei legittimati ad esercitare i diritti dell'interessato defunto (nella specie, il membro dell'ETS) saranno perciò compresi non soltanto i congiunti dell'interessato, ma altresì il "mandatario" – quale soggetto incaricato dall'interessato di tutelare la propria identità digitale dopo la morte – e qualunque soggetto che abbia un interesse (patrimoniale o solo morale) alla protezione (in senso ampio) dei dati personali riferiti alla persona deceduta [48]: sicché, a ben vedere, alla luce del combinato disposto degli artt. 5 GDPR e 2 *terdecies*, d.lgs. n. 101/2018, l'ETS non solo potrà – in qualità di titolare del trattamento – continuare a conservare e a trattare i dati personali del membro deceduto (*ex* art. 5 GDPR), ma nulla sembrerebbe escludere che possa altresì ed eventualmente esercitare i diritti dell'interessato defunto in quanto soggetto avente *lato sensu* un interesse alla protezione dei dati personali di un proprio membro deceduto (*ex* art. 2 *terdecies*, d.lgs. n. 101/2018).

3. – L'art. 30 GDPR, poi, prevede per alcuni titolari di trattamento l'obbligo di un Registro delle attività di trattamento: una sorta di "censimento dei trattamenti", predisposto (anche) in formato elettronico, costantemente aggiornato e all'occorrenza esibito per controlli da parte dell'autorità competente, contenente varie informazioni sui trattamenti svolti, tra cui le generalità del titolare, le finalità del trattamento, le categorie di soggetti interessati (*data subjects*) e dei dati personali trattati, i destinatari della comunicazione dei dati, l'eventuale paese straniero o organizzazione internazionale a cui i dati vengono trasferiti, il momento della cancellazione dei dati e, se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

In un siffatto contesto, appare legittimo chiedersi se le ODV e, in generale, gli ETS siano o meno tenuti, in qualità di titolari del trattamento, alla redazione, tenuta e conservazione di tali Registri. Orbene, l'art. 30 GDPR stabilisce che siffatto obbligo non sussiste per gli enti «con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10».

---

bile della successione c.d. "anomala", che implicherebbe regole notevolmente differenti da quelle dettate nel libro II del codice civile con riguardo alle successioni legittime.

[46] Trattasi di un'autonoma legittimazione all'esercizio dei diritti da parte di soggetti portatori di interessi qualificati, diversi da quello al quale si riferiscono i dati. In altri termini, la norma riconosce e prevede una scissione tra legittimazione (all'esercizio dei diritti e dei poteri di controllo) e titolarità dei diritti: sul punto, cfr. Bargelli E., *sub art. 13* (Diritti dell'interessato), in C.M. BIANCA, F.D. BUSNELLI (a cura di), *Tutela della privacy*, *(legge 31dicembre 1996, n. 675)*, in *Nuove leggi civ.*, 1999, 416.

[47] Sull'argomento, cfr. N. DI STASO, *Il mandato* post mortem exequendum, in *Fam. pers. succ.*, 2011, 685; A. PALAZZO, *Le successioni*, Milano, 2000, 53 s. In giurisprudenza, cfr. per tutte Cass., 9 maggio 1969, n. 1584, in *Foro it.*, vol. 92, n. 12, 3193 ss., che ha sancito l'ammissibilità nel nostro ordinamento di un mandato *post mortem exequendum*, in quanto non in contrasto con il divieto posto alla volontà del defunto di operare *post mortem*, relativamente ai beni dell'eredità al di fuori del testamento. Con specifico riferimento al GDPR, si tratta di una nuova applicazione di tale mandato, propria dell'epoca contemporanea: dinnanzi all'imponente massa di dati generati dalla diffusione delle tecnologie informatiche, destinata a sopravvivere al *de cuius*, occorre gestire l'accesso a *blog*, piattaforme, *account* di posta elettronica e *social network* dell'utente dopo il suo decesso.

[48] La "sopravvivenza" e l'«esercizio post mortale» o prosecuzione dei diritti dell'interessato sono pertanto unicamente sorretti dalla *ratio* della protezione dei dati personali, in via diretta e immediata («interesse proprio» o familiare) ovvero indiretta e mediata, dando esecuzione alla volontà dell'interessato deceduto («in qualità di suo mandatario»): così, G. RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, cit., 415.

A tale stregua, saranno tenuti alla redazione del Registro gli ETS titolari di trattamento con 250 o più dipendenti [49]; quanto agli enti titolari con meno di 250 dipendenti, l'art. 30 GDPR contiene un'elencazione delle ipotesi di esenzione dall'obbligo, non del tutto chiara. In particolare, appare fondato ritenere che siano obbligati *ex* art. 30 GDPR gli enti titolari con meno di 250 dipendenti ma i cui trattamenti siano rischiosi per i diritti e le libertà degli interessati: ipotesi, questa, a sua volta assai estesa, perché il Considerando n. 75 del GDPR stabilisce che vi è rischio, ad esempio, quando il trattamento possa comportare discriminazioni o riguardi dati sanitari o "particolari", o ancora se implichi una valutazione della persona o si riferisca a minori o, infine, coinvolga un numero elevato di interessati. Altrettanto dicasi per gli ETS con meno di 250 dipendenti e titolari di trattamenti continuativi o non occasionali, anche se non rischiosi, o aventi ad oggetto dati "particolari" (*ex* sensibili) o giudiziari. Questa interpretazione, avvalorata dal *Working Party Article 29* (oggi *European Data Protection Board*, EDPB), comporta in sostanza l'obbligo del Registro per la maggior parte degli ETS che trattino dati personali per la loro attività, con meno di 250 dipendenti ma i cui trattamenti siano rischiosi per i diritti e le libertà degli interessati, continuativi o non occasionali e, anche se occasionali, riguardino dati "particolari" (*ex* sensibili) o giudiziari [50].

Nell'incertezza della norma, e muovendo dalla considerazione che comunemente i trattamenti e le attività delle ODV e, in generale, degli ETS coinvolgono diritti fondamentali o dati "sensibili", sembra comunque opportuno optare per la predisposizione e la tenuta del Registro, non solo perché l'omissione di siffatto obbligo, là dove si ritenesse sussistente, determinerebbe l'applicazione di una sanzione pecuniaria notevolmente gravosa, ma anche perché il Registro, a ben vedere, può costituire un ottimo strumento di *accountability* o "responsabilizzazione" [51] e di cooperazione con l'Autorità di controllo. Più precisamente, il Registro delle

---

[49] Situazione, peraltro, difficile che si verifichi con riferimento agli enti *non profit* e considerato anche il riferimento specifico ai "dipendenti", si può tendenzialmente escludere che ai dipendenti siano equiparabili i volontari e, quindi, che siano tenuti alla redazione del Registro una ODV o un ETS per il solo fatto di aver 250 volontari o più.

[50] In particolare, il *Working Party Article 29* ha precisato la natura alternativa delle deroghe, ritenendo che sia sufficiente anche una sola delle condizioni previste dall'art. 30 GDPR per determinare l'obbligo di tenuta del registro. Il Garante, poi, ha precisato che si considerano soggetti obbligati le organizzazioni con almeno 250 dipendenti quelle che, anche in presenza di un numero minore di dipendenti, effettuino trattamenti non occasionali o che possano presentare un rischio, anche non elevato, peri diritti e le libertà dell'interessato o trattamenti delle categorie particolari di dati di cui all'art. 9 GDPR. Associazioni, fondazioni e comitati dovranno predisporre e aggiornare il registro ove trattino categorie particolari di dati e/o dati relativi a condanne penali o a reati.

[51] L'innovazione più significativa introdotta dal GDPR è senz'altro rappresentata dal riconoscimento normativo del principio di *accountability*: espressione notoriamente mutuata dai sistemi di *common law* e, come più volte sottolineato in dottrina, difficilmente traducibile se non con uno sforzo ermeneutico complesso e con locuzioni prolisse, oltreché poco efficaci, a tal punto che si preferisce continuare ad utilizzare il termine inglese. Ed invero, la parola *accountability* non esaurisce la propria funzione e il proprio contenuto nella mera "responsabilità", ma include altresì un obbligo di "rendicontazione" o "dimostrazione" «che il trattamento è effettuato conformemente al [...] Regolamento» (art. 24). Più precisamente, l'*accountability* si compone di due voci: "adozione" di misure appropriate ed efficaci per l'adempimento degli obblighi scaturenti dal Regolamento e "dimostrazione" della conformità del trattamento alle norme del GDPR. Obbligo di conformarsi e obbligo di provare la conformità del trattamento rappresentano cioè le due facce della stessa medaglia (*accountability*) in mano al *data controller*, cui è per l'appunto affidato un ruolo "proattivo" nella "valutazione" e nella conseguente "gestione" del rischio connesso al trattamento. Nelle linee guida *Governing the protection of privacy and transborder flows of personal data*, stabilite dalla OECD (*Organization for Economic Cooperation and Development*), il termine *accountability* era già presente nel 1980. In particolare, al § 14 si legge che «*a data controller should be accountable for complying with measures which give effect to the principles stated above. OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation*».

Sul punto, cfr. RICCIO, SCORZA, BELISARIO (a cura di), *op. cit*., 239; G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento Europeo sulla protezione dei dati personali*, cit., 14, nt. 38. Sulla genesi di tale principio, cfr. il Parere del Gruppo di lavoro art. 29 (noto come WP29), intitolato *Opinion 3/2010 on the principle of* accountability e, in dottrina, v. in particolare, RICCIO, SCORZA, BELISARIO (a cura di), *op. cit.,* 239 s.; cfr. G. FINOCCHIARO, *Art. 24*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., 515 s.; ID., *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (diretto da), *Il*

attività di trattamento rappresenta un mezzo utile a dimostrare il rispetto e la *compliance* dei dettami del GDPR, un documento idoneo ad attestare l'avvenuta implementazione di specifici modelli organizzativi, che assicurino l'adeguatezza dei trattamenti dei dati personali, la loro conformità al Regolamento e l'efficacia delle misure adottate. In altri termini, la tenuta del Registro consente una ricognizione delle attività svolte e si colloca in un sistema di governo trasparente, cui risulta ispirato peraltro anche il codice del terzo settore, frutto di un nuovo approccio culturale e organizzativo fondato nel GDPR sul principio per l'appunto di "responsabilizzazione": per tali ragioni, il Garante ne raccomanda la redazione a tutti i titolari in quanto, fornendo piena contezza del tipo di trattamenti svolti, contribuisce non soltanto ad attuare in modo semplice ed accessibile il principio di *accountability*, ma anche perché agevola, al contempo, l'attività di controllo del Garante stesso.

Anche la figura del d.p.o. (*data protection officer*) o r.d.p. (responsabile della protezione dei dati) risulta ispirata al principio di *accountability*, in quanto misura funzionale di autocontrollo degli enti (pubblici e) privati. Trattasi, secondo il Considerando n. 97, di una persona avente «conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati», che esercita un'attività di consulenza e di assistenza nei confronti del titolare del trattamento (e del responsabile), con riferimento a tutti gli obblighi che il GDPR impone. La nomina del d.p.o. consente, cioè, di realizzare un alto livello di *compliance* al Regolamento ed evitare in tal guisa sanzioni scaturenti dalla violazione delle sue prescrizioni.

Ciò posto, appare legittimo interrogarsi sull'obbligatorietà, o mera opportunità, per gli ETS di nominare un d.p.o. Al riguardo, l'art. 37 del GDPR stabilisce che siano obbligati a nominarlo, a parte gli enti pubblici, per quel che rileva ai nostri fini, quelli privati che hanno come attività principale [52] lo svolgimento di «trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala»; o, ancora, gli enti privati, la cui attività principale consista «nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10»: in generale, tutte ipotesi in cui il trattamento dei dati comporti rischi particolarmente alti e tali da imporre la nomina del d.p.o.

---

nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Torino, 2017, 12 ss.; RICCIO, SCORZA, BELISARIO (a cura di), *op. cit*., 61 e 236 ss. Sulla scia dei *fora* internazionali di *data protection*, si sottolinea la portata globale e assai ampia dell'obbligo di responsabilità, c.d. *overarching concept of accountability*. Nel parere n. 3 del 2010 del Gruppo di lavoro art. 29 l'*accountability* viene tradotta come responsabilità, affidabilità, assicurazione, obbligo di rendicontare.

[52] L'art. 37, paragrafo 1, lettere b) e c), del GDPR contiene un riferimento alle «attività principali del titolare del trattamento o del responsabile del trattamento». Nel considerando n. 97, si afferma che le attività principali di un titolare del trattamento «riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria». Secondo il Gruppo di Lavoro Articolo 29, con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento. Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ente per l'assistenza socio-sanitaria consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualunque struttura di questo tipo, tenuta pertanto a nominare un RPD. Si pensi anche ad un'associazione di promozione sociale sportiva che sostiene i valori dello sport, opera per il benessere e la promozione della salute dei cittadini ed è altresì impegnata ad assicurare la corretta organizzazione e gestione delle attività sportive, il rispetto del "*fair play*", la decisa opposizione ad ogni forma di illecito sportivo. L'attività principale dell'associazione è innegabilmente legata in modo inscindibile al trattamento di dati personali: ne consegue che l'associazione dovrà nominare un RPD. D'altro canto, tutti gli enti svolgono determinate attività quali la predisposizione di strutture *standard* di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

Procedendo con ordine, gli ETS saranno obbligati a nominare il d.p.o. là dove il trattamento richieda un monitoraggio regolare e sistematico [53] degli interessati che ricorre, ai sensi del Considerando n. 24, allorché «le persone fisiche siano tracciate su *internet*», come nel caso del *tracking on line* (anche) per scopi comportamentali [54]: monitoraggio da intendersi quale osservazione o controllo, normalmente ma non esclusivamente, di comportamenti e da svolgersi in modo «regolare» e «sistematico», ossia, rispettivamente, continuativo o periodico e «metodico o predeterminato» [55]. Ci si intende, ad esempio, riferire al monitoraggio di dati relativi allo stato di benessere psicofisico e alla salute attraverso dispositivi indossabili, alla localizzazione mediante *apps* su dispositivi mobili, all'utilizzo di telecamere a circuito chiuso.

Inoltre, perché un ETS sia obbligato a nominare il d.p.o. è altresì richiesto che il monitoraggio venga svolto su «larga scala» e, cioè, relativamente ad «una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale», con un'incidenza «su un vasto numero di interessati» potenzialmente e altamente rischiosa. Nel regolamento non si dà alcuna definizione di trattamento su "larga scala", ma è il considerando n. 91 a fornire indicazioni in proposito [56] e se è pressoché impossibile individuare con esattezza la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità, è tuttavia pensabile la specificazione di alcuni *standard* utili a definire puntualmente e/o quantitativamente il concetto di "larga scala", con riguardo ad alcune tipologie di trattamento maggiormente comuni. Ed ancora una volta, è intervenuto il Gruppo di lavoro Articolo 29 che ha contribuito a delineare questi *standard*, sia raccomandando di tener conto di criteri quantitativi e qualitativi quali il numero degli interessati, l'estensione temporale (durata e persistenza) e geografica del trattamento, il volume, il numero e/o le diverse tipologie di dati oggetto di trattamento [57]; sia elencando a titolo esemplificativo alcune ipotesi di trattamento su "larga scala" come quello avente ad oggetto i dati relativi a pazienti e svolto da un ente o istituto di cura; o riguardanti gli spostamenti di utenti di un servizio (per esempio, il loro tracciamento attraverso titoli di viaggio); o ancora quello di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche, ovvero personali da

[53] Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "monitoraggio del comportamento di detti interessati" ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Testualmente, «per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su *internet*, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».

[54] In tal senso, *Article 29 Data Protection Working Party* (oggi *European Data Protection Board*), *Linee guida sui responsabili della protezione dei dati*, adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017, 16/IT, WP 243 rev.01.

[55] Così, *Article 29 Data Protection Working Party*, *Linee guida*, cit., 11. Più precisamente, l'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici. L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia. Altre esemplificazioni di attività indicate dal Gruppo sono il reindirizzamento di messaggi di posta elettronica; attività di *marketing* basate sull'analisi dei dati raccolti; profilazione e *scoring* per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione; programmi di fidelizzazione; pubblicità comportamentale; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

[56] Il considerando in questione vi ricomprende, in particolare, «trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato».

[57] *Article 29 Data Protection Working Party* ha indicato, a titolo esemplificativo come soggetti che svolgono trattamenti su vasta scala, gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione.

parte di un motore di ricerca per finalità di pubblicità comportamentale; oppure il trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici [58].

Alla luce delle considerazioni sin qui svolte, appare quindi legittimo ritenere sussistente l'obbligo di nomina del d.p.o. per quegli Enti del Terzo Settore che, nello svolgimento della loro attività principale, svolgano un monitoraggio sistematico su larga scala dei beneficiari/destinatari della loro attività o compiano un trattamento non occasionale di dati "particolari" (*ex* sensibili) "*o*" [59] di dati giudiziari interconnessi con altri dati personali raccolti per finalità diverse.

4. – In forza ancora una volta del noto principio di *accountability*, gli ETS, in qualità di titolari di trattamento, dovranno garantire un'adeguata sicurezza e protezione dei dati personali, adottando *policies* e procedure idonee al caso concreto, tra le quali vi è sicuramente quella per la gestione di eventuali "*data breach*" [60]. Si tratta di una procedura volta a stabilire *a priori* come affrontare la malaugurata ipotesi di una violazione della sicurezza dei dati [61]: si pensi al caso in cui i dati trattati dall'ente del terzo settore, per errore umano o a seguito di un attacco informatico, vengano accidentalmente persi o comunicati a soggetti non autorizzati.

L'ente del terzo settore dovrà quindi dimostrare di aver adottato e costantemente aggiornato tutte le misure tecniche e organizzative atte a garantire il raggiungimento di un livello di sicurezza adeguato ai rischi: il problema allora non attiene all'*an* bensì al *quomodo* della dimostrazione. Al riguardo, non v'è dubbio che qualunque trattamento informatico di dati non possa ormai prescindere dall'adozione di "misure minime", da quelle fisiche e banali – quali la corretta conservazione dei documenti cartacei contenenti i dati – a quelle tecniche ed informatiche come *password* di accesso, sistemi antivirus e di *backup*, ecc. In generale, il GDPR riconosce e attribuisce al titolare del trattamento il potere di scegliere modalità e strumenti di attuazione delle prescrizioni europee a fronte dell'obbligo di dimostrarne l'adeguatezza rispetto al caso concreto. Pro e contro dunque: da un lato discrezionalità e diritto di scelta, dall'altro incertezza della "bontà" dell'operato e delle valutazioni effettuate fino all'eventuale esame da parte dell'autorità giudiziaria o amministrativa. L'*accountability* segna quindi il passaggio da una tutela *ex post* dei dati, propria della disciplina previgente e operante in funzione rimediale sulle violazioni e sui relativi danni, ad una protezione *ex ante* o preventiva tipica del

[58] D'altro canto, lo stesso considerando prevede in modo specifico che «il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato». Il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo): fra tali estremi si colloca tuttavia un'ampia zona grigia.

[59] Il testo italiano reca già la congiunzione "o", diversamente dal regolamento. Sebbene infatti l'art. 37, paragrafo 1, lettera c), del Regolamento menzioni il trattamento di categorie particolari di dati ai sensi dell'art. 9 e di dati personali relativi a condanne penali e a reati di cui all'articolo 10, nonostante cioè l'utilizzo della congiunzione "e" nel testo, non è apparsa sistematicamente fondata l'applicazione simultanea dei due criteri: il testo, pertanto, è stato più correttamente interpretato e tradotto come se recasse la congiunzione "o".

[60] Per *data breach* o violazione dei dati personali (artt. 4 e 33 GDPR) si intende una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzato o l'accesso ai dati personali. Si tratta quindi della perdita, del danneggiamento o della fuoriuscita di dati o dell'accesso illecito anche indipendente dalla volontà dell'ente (anche la perdita di una chiavetta USB, il furto del PC, la cancellazione di un archivio dati, l'accesso al computer di estranei, ecc.).

[61] La procedura ha il vantaggio di facilitare le valutazioni che, in questo caso, si rendono necessarie per poter poi adempiere agli obblighi previsti dal Regolamento (annotazione della violazione nell'apposito registro, eventuale notifica al Garante e comunicazione agli interessati).

nuovo Regolamento e basata «sull'esame prudenziale di tutte le attività di trattamento»[62] sin dalla fase iniziale. Il parametro fondamentale che deve presiedere all'adempimento degli obblighi scaturenti dal Regolamento sembrerebbe, dunque, la diligenza del *bonus pater familias* (per così dire) "informatico", formula che riassume la misura dello sforzo o impegno "adeguato" richiesto, in questo caso, all'ente in quanto titolare del trattamento per rispettare il Regolamento[63]. L'ETS, in quanto «titolare del trattamento» dovrà «mette(re) in atto misure tecniche e organizzative adeguate[64] per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al [...] Regolamento» (art. 24 GDPR). Il Regolamento affida quindi alla discrezionalità del titolare del trattamento, nella specie l'ente, la decisione sulle misure da adottare: discrezionalità libera ma non illimitata, anzi necessariamente parametrata alle condizioni indicate nello stesso art. 24 GDPR, quali la natura, l'àmbito di applicazione, il contesto e le finalità del trattamento, nonché il rischio di lesione dei diritti e delle libertà delle persone fisiche[65]. In altri termini, non vengono astrattamente specificati rigidi comportamenti, ma viene piuttosto assegnato al titolare il compito di scegliere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali: il tutto nel rispetto delle disposizioni normative e alla luce dei criteri indicati nel GDPR. Il Regolamento, infatti, non prevede un elenco esaustivo né tassativo di "misure adeguate", ma si limita ad indicarne alcune. Ciò significa che l'ente titolare del trattamento potrà mettere in atto non solo le misure adeguate "tipiche", già preconfigurate dal legislatore europeo, ma anche nuove o "atipiche" che non rientrino tra quelle normativamente previste, purché nel rispetto dei requisiti fissati dal Regolamento: il che rappresenta la massima espressione ed estrinsecazione del principio di *accountability* e dell'autonomia riconosciuta al titolare del trattamento.

Prima, però, di procedere ad una sia pur breve illustrazione delle misure tecniche e organizzative suggerite dal Regolamento, appare opportuno soffermarsi sul diverso atteggiarsi dell'*accountability* e dell'onere

---

[62] Così, L. GRECO, *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, cit., 254.

[63] M. RATTI, *op. cit.*, 620, suggerisce che la diligenza richiesta al titolare e al responsabile del trattamento sia "qualificata", stante l'inciso di cui all'art. 82 GDPR, secondo il quale l'evento dannoso non deve essere «in alcun modo» imputabile al danneggiante per liberarsi da responsabilità: di conseguenza, la presenza anche della colpa lieve sarebbe idonea a determinare la sussistenza del nesso materiale tra condotta del titolare danneggiante ed evento dannoso. In generale, sulla nozione e sulle graduazioni della colpa, cfr. in particolare, C. TURCO, *Diritto civile*, I, Torino, 2014, 363 s. La diligenza, quindi, unitamente alla perizia e alla competenza, sembra rappresentare la regola e, al contempo, il criterio di valutazione del comportamento dell'ente e di imputazione della responsabilità, non in base alle capacità possedute dal medesimo, ma secondo un modello oggettivo e astratto, corrispondente a quello ordinario, oltreché in virtù delle caratteristiche e delle esigenze del trattamento in concreto effettuato: pertanto, sembra sufficiente per escludere l'imputabilità e la responsabilità tendenzialmente "colposa" o "soggettiva" la violazione del Regolamento dipendente da un'impossibilità analogamente soggettiva e cioè caratterizzata dall'assenza di colpa o negligenza, pur se collegata a circostanze attinenti alla sfera di controllo e organizzazione del titolare del trattamento (comunque incolpevole).Per converso, un comportamento debitorio immune da colpa o negligenza non impedirebbe un'imputabilità e una responsabilità per colpa senza colpa o oggettiva, che verrà meno solo nel caso in cui la violazione del Regolamento dovuta ad un'impossibilità parimenti oggettiva di adempiere: non solo indipendentemente da colpa o negligenza, ma causata da eventi estranei alla sfera di controllo e di organizzazione (nella specie) del titolare del trattamento e non rientranti nel rischio tipico inerente all'attività svolta dal titolare del trattamento, imprevedibile ed eccezionali (c.d. caso fortuito: si pensi ad es. ad un totale e prolungato *black out* elettrico) ovvero ineludibili ed insuperabili (c.d. forza maggiore).

[64] Il Regolamento richiama molte volte il concetto di "adeguatezza", necessariamente relativo e relazionale, da intendersi come capacità di soddisfare una qualità o un risultato posto come obiettivo. "Adeguatezza" equivale ad "accettabilità" in termini sia tecnici (pertinenza delle misure), sia qualitativi (efficacia della protezione): sul punto, v. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa* Privacy *commentario*, cit., 297.

[65] La valutazione di adeguatezza delle misure va condotta ex ante e in concreto in una prospettiva prognostica e soggetta ad aggiornamenti. I parametri essenziali di tale valutazione forniti dal GDPR sono: natura, àmbito applicativo, contesto e finalità del trattamento, rischi possibili.

probatorio gravante sull'ente in quanto titolare del trattamento, a seconda che questo abbia adottato misure tipiche o, al contrario, innominate. Per le prime sembra legittimo ritenere sussistente una presunzione relativa [66] di conformità al Regolamento, nel senso che il titolare del trattamento dovrà semplicemente provarne l'adozione, non anche il rispetto degli obblighi imposti dal GDPR, valutato *ex ante* dal legislatore europeo; laddove, trattandosi di misure per così dire atipiche o innominate, in quanto non previste nel Regolamento, l'ente titolare del trattamento dovrà dimostrarne non solo l'adozione (l'*an*), ma altresì la conformità ai principi e l'adeguatezza (*quomodo*): il che sembra suggerito dallo stesso art. 24 GDPR che menziona alcune misure quali «i codici di condotta di cui all'art. 40» e i «meccanism(i) di certificazione di cui all'art. 42», definendole «element(i)» atti a «dimostrare il rispetto degli obblighi del titolare del trattamento», ivi inclusa l'adeguatezza delle misure tecniche e organizzative di sicurezza adottate [67].

Tra le «misure tecniche e organizzative adeguate [...] volte ad attuare in modo efficace i principi di protezione dei dati», menzionate dal Regolamento, si colloca anzitutto la "pseudonimizzazione" [68] (art. 25) definita all'art. 4 come insieme di operazioni idonee ad evitare che i dati personali «possano [...] essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Trattasi, in sostanza, di uno strumento in grado di rendere più difficile l'identificazione dell'interessato e la diretta riconducibilità a quest'ultimo delle informazioni personali: al termine del trattamento i dati non potranno più essere ricollegati o riassociati ad una persona determinata se non mediante dati e informazioni ulteriori, oggetto di separata archiviazione e protezione [69]. In termini pratici, la "pseudonimizzazione" maschera l'identità di un soggetto mediante sia la sostituzione di un dato personale, solitamente univoco, con un altro dato per l'appunto "pseudonimo" – anch'esso univoco, ma non immediatamente intellegibile né direttamente identificativo (un codice, un numero di protocollo) [70] – sia la separazione di tali informazioni aggiuntive; *in secundis*, essa consente, in circostanze predefinite, di riassociare il dato alla persona, ossia di risalire all'identità dell'interessato, utilizzando (a ritroso) le informazioni aggiuntive.

Altro strumento normativamente "adeguato" per la protezione dei dati personali è previsto dal medesimo art. 25 ed è individuato con l'espressione *privacy by default*: trattasi di un rimedio volto a proteggere l'interessato dal rischio di perdere consapevolezza o controllo circa l'utilizzo delle proprie informazioni personali [71].

---

[66] *Contra*, G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa* Privacy *commentario*, cit., 63, che riconoscono nelle misure indicate dal Regolamento elementi utili a dimostrare l'adempimento degli obblighi del titolare e, quindi, l'*accountability*, ma non rappresentano presupposti per una vera e propria presunzione legale, neppure relativa, di conformità al GDPR della condotta del titolare.

[67] In senso conforme, G. FINOCCHIARO, *Art. 24*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., 518. Sull'argomento, v. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *op. cit*., 62. Le misure atipiche dovranno in concreto superare una duplice valutazione, relativa alla loro adozione e conformità, e quindi all'adeguatezza, rispetto alle caratteristiche concrete dei dati e del trattamento, nonché al suo impatto e ai rischi che possa determinare per i diritti e le libertà degli interessati.

[68] Il processo di pseudonimizzazione sembra consistere nella formazione di due insiemi parziali di informazioni: il primo raggruppa dati e contiene lo pseudonimo e i dati che permettono l'identificazione; il secondo, complementare al primo, raccoglie pseudonimi e dati personali, senza tuttavia consentire l'identificazione degli interessati. Il processo di pseudonimizzazione consente di riassociare i dati: sul punto, cfr. M. MONTANARI, *Art. 25*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., 535 ss.

[69] Ad esempio, mediante l'utilizzo di criptografia a chiavi simmetriche o asimmetriche.

[70] Al riguardo, cfr. G G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa* Privacy *commentario*, cit., 251 s.: codici "inintellegibili" in luogo della reale identità degli individui.

[71] In realtà, ai sensi dell'art. 25, la protezione dei dati deve essere garantita fin dalla progettazione (c.d. *privacy by design*) e per impostazione predefinita (c.d. *privacy by default*): il titolare è chiamato ad implementare misure in grado di proteggere efficacemente

Adottando tale misura, l'ente titolare garantirà, «per impostazione predefinita» (art. 25) e in ossequio al c.d. principio di "minimizzazione" [72], che siano trattati soltanto i dati personali necessari per ciascuna finalità specifica del trattamento: ciò attraverso l'utilizzo di impostazioni in automatico, scelte, predisposte e preselezionate da parte del titolare del trattamento o di chi costruisce il sistema informatico, in guisa da «garantire scelte di *default* orientate verso soluzioni di massima protezione dei dati» [73].

Come già rilevato [74], anche il registro delle attività di trattamento prescritto dall'art. 30 rappresenta una misura normativamente tipica volta a dimostrare la rispondenza del trattamento posto in essere dal titolare ai dettami del Regolamento. Più precisamente, per provare la piena conformità del trattamento al Regolamento, l'ente titolare (del trattamento) che tenga l'apposito registro riuscirà a rendicontare e comprovare l'adeguatezza, la conformità al Regolamento e l'efficacia delle misure adottate. La rendicontazione *ex* art. art. 30 GDPR non può considerarsi, quindi, un mero adempimento formale, bensì un mezzo tecnico efficace e pertinente per la corretta gestione dei dati personali.

L'art. 35, poi, disciplina la "preventiva valutazione di impatto sulla protezione dei dati personali" (c.d. DPIA o *privacy impact assessment*) che, insieme agli altri mezzi o strumenti sin qui elencati, e in particolare al registro delle attività di trattamento, costituisce un congegno significativo e concreto per garantire e fornire la prova, da parte del titolare, della conformità del trattamento al GDPR. Essa è finalizzata anzitutto a stimare, in relazione alla probabilità e gravità, i rischi per i diritti e le libertà delle persone fisiche a seguito del trattamento di dati; in secondo luogo, la DPIA mira alla definizione delle misure idonee ad escludere o ridurre siffatti rischi. Analogamente al registro delle attività di trattamento, la DPIA – richiesta soltanto per quei trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche – non rappresenta la tappa obbligatoria di un *iter* burocratico, bensì un sistema di gestione del suddetto rischio, utile per "minimizzarlo" o addirittura eliminarlo.

Il Regolamento, inoltre, riconosce efficacia probatoria – circa la conformità del trattamento di dati effettuato dal titolare – ai codici di condotta [75], rispondenti ai requisiti di cui agli artt. 40 e 41. In particolare, la sottoscrizione di un codice costituisce, per espressa disposizione legislativa, elemento atto a dimostrare il rispetto degli obblighi che gravano sul titolare del trattamento e la sussistenza di misure tecniche e organizzative adeguate a garantirne la sicurezza. Com'è intuibile, trattasi di codici di comportamento elaborati con il supporto delle associazioni rappresentative e degli organismi esponenziali delle rispettive categorie, allo scopo di integrare i principi generali della disciplina e di adattarli allo specifico ambito o tipologia di trattamento. La funzione dei codici è infatti attuativa e allo stesso tempo complementare; la loro conformità al GDPR è subordinata alla previsione di meccanismi procedurali mediante i quali l'organismo di controllo vigila sul rispetto dei codici medesimi da parte dei soggetti obbligati. Le disposizioni sui codici di condotta sono stret-

---

i dati personali al momento della progettazione di processi e modelli di trattamento, e a garantire il rispetto del principio di necessità, nel corso dell'esecuzione del trattamento.

[72] Com'è noto, l'art. 5, par. 1, lett. c), impone che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati. Il principio di minimizzazione si compone dunque di due "voci": necessità e pertinenza. La prima consiste nella limitazione del trattamento ai soli dati indispensabili per la realizzazione della finalità o scopo del trattamento; la seconda attiene alla funzionalità del dato rispetto allo scopo perseguito, in base ad un nesso eziologico che deve permanere durante tutto il trattamento. Sul principio di minimizzazione, v. tra gli altri G.M. Riccio, G. Scorza, E. Belisario (a cura di), *op. ult. cit*., 57 s.; D. Achille, *Art. 5*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., 110 s.

[73] Così, L. Greco, *I ruoli: titolare e responsabile*, in G. Finocchiaro (diretto da), *op. cit.*, 256.

[74] V., *supra*, § 4.

[75] Per un approfondimento sul tema, v. in particolare, A.R. Popoli, *Codici di condotta e certificazioni*, in G. Finocchiaro (diretto da), *op. cit*., 367 ss.

tamente correlate a quelle sulla certificazione e sugli organismi privati a ciò abilitati, di cui agli artt. 42 e 43 GDPR. Sulla scia del *risk based approach*, le certificazioni previste dall'art. 42 costituiscono uno strumento a disposizione del titolare del trattamento, nella specie l'ente, per valutare l'adeguatezza degli *standards* adottati. Ai sensi dell'art. 42, «gli Stati membri [...] incoraggiano l'istituzione di meccanismi di certificazione [...] allo scopo di dimostrare conformità al Regolamento dei trattamenti effettuati dai titolari di trattamento». Trattasi di una certificazione, rilasciata direttamente dal Garante – o da organismi di certificazione preventivamente accreditati – a seguito di una procedura volontaria di valutazione di conformità. Orbene, come già sottolineato e analogamente ai codici di condotta, la presenza di una certificazione determina di per sé una presunzione di conformità e adeguatezza degli *standards* adottati dal titolare del trattamento con i parametri del Regolamento.

5. – Come già rilevato [76], le riflessioni sulla relazione tra digitalizzazione, protezione dei dati e terzo settore non possono concludersi senza volgere lo sguardo al Registro Unico Nazionale del Terzo Settore (RUNTS), non solo in quanto registro (per l'appunto) telematico [77], ma anche perché esso – finalizzato ad assicurare principalmente la piena trasparenza degli ETS, da un lato e l'acquisto della qualifica di ETS, dall'altro – solleva un duplice ordine di questioni relative, rispettivamente, all'operatività o meno del GDPR per il trattamento dei dati degli enti raccolti nel RUNTS e alla configurabilità dell'iscrizione nel Registro come pubblicità costitutiva della qualifica di ETS e dell'acquisto della personalità giuridica.

Sotto il primo profilo, secondo il diritto dell'UE, le persone fisiche sono gli unici beneficiari delle norme sulla protezione dei dati. Il GDPR, infatti, definisce "dati personali" tutte quelle informazioni relative «a una persona fisica identificata o identificabile»: il che induce legittimamente a negare protezione ai dati personali di un ente o persona giuridica [78]. La protezione dei dati personali accordata dal GDPR appare cioè un diritto

[76] V., *supra*, § 1.

[77] Il RUNTS, istituito presso il Ministero del Lavoro e delle Politiche Sociali in attuazione degli artt. 45 ss. del Codice del Terzo Settore, è il luogo digitale e telematico in cui reperire le seguenti informazioni sull'Ente del Terzo Settore (ETS): la denominazione, la forma giuridica, la sede legale e le eventuali sedi secondarie, la data di costituzione, l'oggetto dell'attività di interesse generale, il codice fiscale o la partita iva, il possesso della personalità giuridica e il patrimonio minimo, le generalità dei rappresentanti legali, le generalità dei soggetti che ricoprono cariche sociali e tutte le modifiche agli atti fondamentali dell'ente. Inoltre, nel RUNTS saranno riportati i rendiconti o i bilanci d'esercizio e il bilancio sociale. Il RUNTS è composto da sette sezioni, una per ogni tipologia di ETS: organizzazioni di volontariato, associazioni di promozione sociale, enti filantropici, imprese sociali, reti associative, società di mutuo soccorso. Gli aspiranti enti che vogliono iscriversi a una delle sezioni del RUNTS devono essere in possesso di un corredo digitale minimo che comprende l'identità digitale del legale rappresentante (Spid o Cie), la firma digitale e un indirizzo Pec. Sottolinea il particolare impatto dell'adozione del RUNTS, con le implicazioni che tagliano trasversalmente una molteplicità di profili (costituzione, controlli, preservazione dell'autonomia e *accountability* degli ETS; attuazione dell'art. 118 Cost.), M. GORGONI (a cura di), *Codice del terzo settore. Commento al d.lgs. 3 luglio 2017, n. 117* (Seconda edizione aggiornata con il DM 15 settembre 2020), Pisa, 2021; cfr., anche, A. MAZZULLO, *Il nuovo codice del terzo settore. Profili civilistici e tributari*, Torino, 2017; L. GORI, *Terzo settore e Costituzione*, Torino, 2022, 161 ss.; A. FICI, *Profili e principi generali della riforma del Terzo settore*, in AA.VV., *Dalla parte del Terzo settore*, Roma-Bari, 2019, 18 ss.

[78] Da un punto di vista storico-evolutivo, il concetto di "persona", che in base alla Direttiva n. 58/2002 si riteneva operante soltanto per le persone fisiche (cfr. sul punto, *Volker und Markus Schecke GbR* e *Haertmut Eifert v. Land Essen*), era invece stato recepito dal nostro legislatore come ricomprendente anche le persone giuridiche, gli enti e le associazioni (art. 1, lett. c, l. n. 675/1996) e implicante un'estensione dell'ambito di applicazione della disciplina per la tutela dei dati personali anche a soggetti diversi dalle persone fisiche. Con il d.l. n. 201/2011, convertito con l. n. 214/2011, art. 40, il legislatore italiano ha poi eliminato dal Codice per la protezione dei dati personali il riferimento alle persone giuridiche: riferimento che, tuttavia, permaneva nella Direttiva n. 58/2002 (c.d. Direttiva *E-privacy*), relativa al trattamento dei dati personali nel particolare settore delle comunicazioni elettroniche. L'attuale proposta di Reg. UE *E-privacy* prevede esplicitamente l'estensione della tutela ivi prevista alle persone giuridiche, ma in materia di

esclusivo delle persone fisiche, ma non di quelle giuridiche e, quindi, degli ETS: gli artt. 1 e 4 del Regolamento europeo [79] non sembrano lasciare spazio all'estensione della tutela agli enti, sicché i relativi dati – come il nome, la forma, la sede, i contatti – non ricevono protezione in base alla normativa europea. Altrettanto dicasi per il Considerando n. 14 [80], secondo cui «è opportuno che la protezione prevista dal […] regolamento si applichi alle persone fisiche […] Il […] regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche […] compresi il nome e la forma della persona giuridica e i suoi dati di contatto». A tale stregua, i dati degli ETS potranno essere non solo raccolti, ma anche trattati e quindi comunicati a terzi, senza necessità di una base giuridica e, conseguentemente, senza che l'ente possa vantare alcun diritto sui propri dati. Ciò significa che l'ETS non potrà esercitare i diritti (di accesso, rettifica o cancellazione) previsti dal GDPR per gli interessati (persone fisiche) e ai relativi dati non si applicheranno i principi stabiliti dal regolamento europeo: il che non esclude che una persona giuridica possa subire dei danni a seguito di un trattamento di dati, ma semplicemente che, se dovesse accadere, l'ente non potrà avvalersi dei vantaggi e degli strumenti di tutela di cui al GDPR; semmai, esso eventualmente agirà per il risarcimento del danno in base alle norme del codice civile (art. 2043 cod. civ.).

Eppure anche per le persone giuridiche sussistono esigenze di tutela dei dati e si profilano margini di riconoscimento di una speciale protezione di essi, nel diritto vivente e *de iure condendo*. Per quel che concerne il primo ambito, basta citare la causa *Bernh Larsen Holding AS* e altri *v. Norvegia* (2013) [81], in cui tre società norvegesi impugnarono una decisione dell'autorità giudiziaria che ordinava loro di fornire ai revisori dei conti una copia di tutti i dati conservati su un *server* utilizzato congiuntamente. La Corte EDU, sebbene abbia escluso nel caso specifico una violazione delle norme sulla protezione dei dati, ha ammesso in linea di principio che un siffatto ordine e conseguente obbligo per le società ricorrenti costituisca un'ingerenza nella sfera giuridica privata degli enti medesimi ai sensi dell'art. 8 della CEDU [82]. Più precisamente, la Corte non

---

definizione di "dato personale", allo stato, sussiste un mero rinvio al GDPR: sull'argomento, cfr. per tutti, S. MARTINELLI, *Art. 4 GDPR*, in A. BARBA,S. PAGLIANTINI (a cura di), *Delle persone*, cit., 92 ss.

[79] I tre paragrafi dell'art. 1 specificano che la protezione concerne le persone fisiche: le norme del regolamento riguardano la protezione delle "persone fisiche" (§ 1); la finalità del regolamento è quella di dettare norme per la protezione dei diritti e delle libertà fondamentali delle "persone fisiche" (§ 2); la libera circolazione dei dati personali non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche (§ 3). Nell'art. 4, poi, viene specificato il significato di dato personale come «una qualsiasi informazione riguardante una persona fisica identificata o identificabile»: la protezione dei dati personali riguarda dunque innegabilmente le persone fisiche, così escludendo quelle giuridiche.

[80] Eppure la direttiva del 1995 aveva lasciato ampio margine di manovra agli Stati membri in merito all'estensibilità o meno, in sede di recepimento, alle persone giuridiche della normativa sulla *privacy*. L'Italia aveva optato per l'estensibilità e all'art. 4 codice *privacy* definiva il dato personale come «qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione». Successivamente, l'art. 40, comma 2, d.l. n. 201/2011, convertito in l. n. 214/2011, ha abrogato alcune disposizioni del codice *privacy* e l'art. 5 del codice escludeva ora dall'ambito di applicazione del codice medesimo le persone giuridiche, gli enti e le associazioni. Sulla questione, si è espresso poi il Garante della *privacy* (provvedimento del settembre 2012) che decise di mantenere l'applicazione del codice anche alle persone giuridiche. Il Reg. UE, come rilevato nel testo, ha definitivamente ed attualmente escluso l'operatività della *data protection law* per gli enti. Sull'argomento, cfr. *ex multis*, G. LIBERATI BUCCIANTI, *Art. 1 GDPR*, in A. BARBA, S. PAGLIANTINI (a cura di), *Delle persone*, cit., 32 ss.; ZOPPINI, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, in *Riv. dir. civ.*, 2002, 48, 6, 851 ss.; FICI, RESTA, *La tutela dei dati degli enti collettivi: aspetti problematici*, in PARDOLESI (a cura di), *Diritto alla riservatezzae circolazione die dati personali*, Milano, 2003, 375 ss.; RICCI, *La reputazione: dal concetto alle declinazioni*, Torino, 2018, 185.

[81] *Bernh Larsen Holding AS* e altri *v. Norvegia*, n. 24117/08. Cfr. altresì, *Liberty* e altri *v. Regno Unito*, n.58243/00.

[82] Testualmente, art. 8 CEDU (Convenzione Europea dei Diritti dell'Uomo o *ECHR*, *European Convention of Human Rights*), rubricato come «*Right to respect for private and family life*»: «*1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the econom-*

ha negato tutela alle società *tout court*, in quanto persone giuridiche, ma ha trovato nel caso concreto un giusto equilibrio tra il diritto di esse al rispetto e alla protezione dei propri dati, da un lato, e l'interesse pubblico a garantire un'efficiente ispezione ai fini dell'accertamento fiscale, dall'altro: ciò, alla luce di una serie di circostanze concrete, quali l'adozione da parte delle autorità fiscali di tutele efficaci e adeguate contro gli abusi, l'informazione con largo anticipo alle società ricorrenti dell'accertamento fiscale, la possibilità per queste ultime di essere presenti e di poter sollevare osservazioni durante l'intervento in loco, la distruzione del materiale una volta completata la revisione fiscale. Proprio tali circostanze hanno indotto la Corte a ritenere non integrata la violazione dell'art. 8 CEDU nella vicenda sottoposta al suo esame.

L'estensione della tutela alle persone giuridiche ha trovato supporto anche in un noto provvedimento dell'Autorità Garante per la protezione dei dati personali [83], volto a fornire indicazioni in relazione alla disciplina applicabile al trattamento dei dati relativi a persone giuridiche, enti e associazioni. Sia pur con specifico riferimento ai c.d. servizi di comunicazione elettronica e nonostante la definizione di "interessato" nella disciplina a protezione dei dati personali non ricomprendesse già più le persone giuridiche [84], i destinatari delle norme risultavano comunque individuati non in funzione della loro qualifica soggettiva (persone fisiche ovvero giuridiche), bensì di una qualifica ulteriore che ne prescindeva e, segnatamente, quella di "contraente": termine che, proprio a seguito dell'entrata in vigore del d.lgs. n. 69/2012, a far data dal 1° giugno 2012 ha sostituito, nelle disposizioni del Codice, quello precedente di "abbonato".

Analoghe considerazioni, *mutatis mutandis*, potrebbero legittimamente valere per il concetto di "interessato" di cui al GDPR e indurre il legislatore europeo a modificarne la definizione contenuta nell'art. 4 GDPR [85], aggiungendo il riferimento a qualunque "persona (fisica o) giuridica": in altri termini, come il concetto di "abbonato" e poi di "contraente" dei servizi di comunicazione elettronica è stato ritenuto certamente applicabile, anche sulla base di principi comunitari, tanto alle persone fisiche quanto a quelle giuridiche, così il termine "interessato" di cui al GDPR dovrebbe essere esteso anche agli enti in quanto titolari, sia pur con gli opportuni adattamenti [86], di un diritto alla protezione dei propri dati.

De iure condendo, poi, la bozza di Regolamento UE sulla *E-privacy* [87], in senso diametralmente opposto al GDPR, prevede espressamente l'estensione della tutela ivi prevista alle persone giuridiche: e ciò, sin dal § 1 che, nel proclamare il rispetto della *confidentiality* nelle comunicazioni elettroniche, sancisce l'operatività del relativo principio *both to natural and legal persons*, e cioè sia per le persone fisiche sia per quelle giuri-

---

ic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others».

[83] Provvedimento n. 262/2012.

[84] V., *supra*, nt. 76.

[85] Testualmente, art. 4, § 1, GDPR, «*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*».

[86] Com'è noto, tradizionalmente si ritiene che l'ente giuridico abbia capacità giuridica, sebbene non possa essere destinatario di tutti i rapporti o situazioni giuridiche soggettive riferibili alla persona fisica e, segnatamente, di quelli strettamente legati alla natura o alla qualità di persona umana del soggetto, in questo caso *data subject* o interessato, come la protezione di dati *physical*, *physiological*, *genetic* o *mental*; ma può certamente esserlo per quelli di tipo diverso, di natura *economic*, *cultural* o di *social identity*, e così via. L'ente potrebbe così vantare un diritto alla protezione dei dati relativi alla propria denominazione, nazionalità, sede, orientamento politico, ecc…. Sul punto, cfr. per tutti, C. TURCO, *Diritto civile*, I, Torino, 2014, 110 s.

[87] Esattamente, la *Proposal for a Regulation of the European Parliament and of the Council, concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, recentemente modificata con procedimento n. 6087/2021 e al cui § 1 si legge che «*respect for the confidentiality of one's communications is an essential dimension of this right, applying both to natural and legal persons.*».

diche. In siffatto contesto, rileva altresì il § 2a, alla cui stregua le disposizioni del nuovo Reg. *E-privacy* integrerebbero il regolamento (UE) 2016/679 con norme in materie che non rientrano nell'ambito di applicazione del Regolamento (UE) 2016/679, come la tutela dei diritti delle persone giuridiche.

Ma è soprattutto il § 3 della medesima proposta di Regolamento *E-privacy* a condurre verso un concetto di "persona" che ricomprenda anche gli enti e ad ipotizzare fondatamente un'estensione alle persone giuridiche (anche) della tutela relativa al trattamento dei dati personali di cui al GDPR là dove, muovendo dalla necessità di tutelare i dati delle comunicazioni elettroniche degli enti – come segreti aziendali o altre informazioni sensibili di natura economica e/o di valore – con conseguente applicazione delle disposizioni del Regolamento *E– privacy* alle persone giuridiche, esso dispone che, ove necessario, le norme del Regolamento UE 2016/679 debbano operare *mutatis mutandis* anche per quegli utenti finali che sono persone giuridiche: d'altro canto, se così non fosse, rimarrebbero delle "zone grigie" riguardanti i dati di una persona giuridica, fonti di legittimi dubbi interpretativi. Si pensi al caso in cui il nome di una persona fisica (come il titolare di un'azienda) sia compreso nella denominazione dell'ente, oppure all'ipotesi in cui i dati raccolti riguardino sia persone fisiche sia giuridiche (come accade nelle *email* aziendali), o ancora ai trattamenti automatizzati di dati personali, nei quali risulta difficile distinguere tra dati relativi a persone fisiche e quelli relativi a persone giuridiche [88].

Sotto il secondo profilo [89], poi, relativo alla natura giuridica dell'iscrizione di un ente nel RUNTS, ai sensi dell'art. 4 CTS [90], l'iscrizione al RUNTS è requisito indispensabile perché un ente acquisti la qualifica di Ente del Terzo Settore (ETS) e, conseguentemente, sia assoggettato alla disciplina dettata dal CTS [91]: da qui, la configurazione dell'iscrizione nel Registro come pubblicità costitutiva della qualifica di ETS e dell'acquisto della personalità giuridica, come confermato dal decreto di attuazione del CTS (art. 7, comma 1, d.m. n. 106/2020).

Tuttavia, il CTS non ha abrogato né le disposizioni del libro primo del codice civile in materia di enti *non profit*, né quelle contenute nel d.P.R. n. 361/2000 sul registro delle persone giuridiche e a tali enti è ricono-

---

[88] In questi casi, per esempio, il WP29 (Gruppo di lavoro articolo 29) ha invitato ad utilizzare i criteri di "contenuto", "scopo" e "risultato" per stabilire se le informazioni personali si riferiscano o meno alla persona giuridica.

[89] È noto come, istituendo il Registro Unico nazionale del terzo settore, il legislatore abbia inteso realizzare i numerosi auspici da tempo formulati, ispirati ad un'esigenza di riordino e costituenti parte di un'istanza più generale di disponibilità dei dati e completa trasparenza, ispirata a quella cultura dell'*accountability* invocata dal GDPR. Sul punto, cfr. F. Bosetti, *op. cit.*, 401 ss. Possono iscriversi al RUNTS le organizzazioni di volontariato (ODV), le associazioni di promozione sociale (a.p.s.), gli enti filantropici, le reti associative, le associazioni riconosciute o non riconosciute, le società di mutuo soccorso che non hanno l'obbligo di iscrizione nel Registro delle Imprese, le fondazioni e gli altri enti di carattere privato diversi dalle società e costituiti per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale mediante lo svolgimento, in via esclusiva o principale, di una o più attività di interesse generale in forma di azione volontaria o di erogazione gratuita di denaro, beni o servizi, o di mutualità o di produzione o scambio di beni o servizi.

[90] Testualmente, «sono enti del Terzo settore le organizzazioni di volontariato, le associazioni di promozione sociale, gli enti filantropici, le imprese sociali, incluse le cooperative sociali, le reti associative, le società di mutuo soccorso, le associazioni, riconosciute o non riconosciute, le fondazioni e gli altri enti di carattere privato diversi dalle società costituiti per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale […] ed iscritti nel registro unico nazionale del Terzo settore»: l'iscrizione, quindi, è *conditio sine qua non* per la qualifica di ETS.

[91] Gli ETS, con l'iscrizione al RUNTS, saranno tenuti al rispetto di vari obblighi riguardanti la trasparenza nei bilanci, i rapporti di lavoro e i relativi stipendi, l'assicurazione dei volontari, la destinazione degli eventuali utili, ma potranno accedere anche ad una serie di esenzioni e vantaggi economici previsti dalla riforma. Le soluzioni *software* e gli strumenti telematici dovrebbero garantire una gestione completa e trasparente dell'ente e del mondo *non profit*: dal tesseramento, alla contabilità, ai volontari e ai donatori, alle attività, convocazioni e verbali. Il d.m. n. 106/2020 ha integrato il CTS individuando le procedure che dovranno seguire gli enti per iscriversi al RUNTS.

sciuta la facoltà di non iscriversi o di non trasmigrare al RUNTS e quindi di continuare ad operare nella veste di associazione, fondazione o comitato soggetto alle norme del codice civile e del d.P.R. Allo stesso tempo, però, l'art. 22 CTS contempla un procedimento "agevolato" per le associazioni e le fondazioni che, attraverso l'iscrizione al RUNTS, mirino ad ottenere sia la qualifica di ETS, sia – in deroga alle disposizioni del d.P.R. n. 361/2000 – la personalità giuridica [92]. Secondo parte della dottrina [93], il regime del riconoscimento della personalità giuridica contemplato dal CTS e avente carattere "normativo" si differenzierebbe da quello previsto dal d.P.R. n. 361/2000 di natura "concessoria" in quanto conseguente «ad un provvedimento amministrativo di carattere discrezionale […] all'esito di una verifica sulla meritevolezza dello scopo dell'ente e della congruità dei mezzi predisposti per perseguirlo»: il che susciterebbe, in base a tale orientamento, dubbi in ordine alla costituzionalità della scelta del CTS di mantenere in vita il doppio binario per il riconoscimento della personalità giuridica agli ETS (iscrizione nel Registro delle persone giuridiche, da una parte e iscrizione al RUNTS, dall'altra).

A ben vedere, già il citato d.P.R. n. 361/2000 – preso atto del vasto fenomeno delle "formazioni sociali" e in piena coerenza con il dettato costituzionale (art. 2 Cost.) – ha segnato il significativo mutamento di prospettiva rispetto all'abrogata disciplina codicistica (art. 12 cod. civ.) e il riconoscimento, pur spettando sempre all'autorità a ciò preposta, è stato pressoché svuotato del suo contenuto "concessorio" e discrezionale [94]. In particolare, esso può legittimamente considerarsi di tipo eminentemente "normativo" e «determinato» dall'iscrizione dell'ente nel registro delle persone giuridiche [95] disposta (e non concessa) dall'autorità competente sulla base di un controllo preventivo (non di merito o sostanziale della fisionomia dell'ente, ma) meramente formale della sola possibilità e liceità dello scopo perseguito e della consistenza del patrimonio destinato alla sua realizzazione. Consequenziale a tale tipo di riconoscimento è il regime di pubblicità dichiarativa cui sono sottoposte le persone giuridiche, atto per l'appunto a rendere opponibili ai terzi elementi, atti e fatti indicati nel relativo registro [96].

Analoghe considerazioni, *mutatis mutandis*, sembrano fondatamente valere per l'acquisto della personalità giuridica a seguito di iscrizione nel RUNTS, fondata sulla mera verifica della sussistenza dei requisiti richiesti per la costituzione di un'associazione, fondazione o ente del terzo settore. Sembra deporre, in tal senso, lo stesso tenore complessivo delle regole dettate dal CTS riguardo all'iscrizione nell'apposito registro e, in particolare, sia l'art. 101 alla cui stregua «il requisito dell'iscrizione al Registro unico nazionale del Terzo

[92] Testualmente, art. 22, comma 1, CTS, «le associazioni e le fondazioni del Terzo settore possono, in deroga al decreto del Presidente della Repubblica 10 febbraio 2000, n. 361, acquistare la personalità giuridica mediante l'iscrizione nel registro unico nazionale del Terzo settore ai sensi del presente articolo».

[93] R. CATALANO, *Il Registro Unico Nazionale ed il riconoscimento*, in D. DI SABATO, O. NOCERINO (a cura di), *Il Terzo settore. Profili critici della riforma*, Napoli, 2018, 49.

[94] Il riconoscimento degli enti senza scopo di lucro, prima del d.P.R. n. 361/2000 che ha per l'appunto innovato sotto tale aspetto la disciplina codicistica delle persone giuridiche contenuta nell'abrogato art. 12 cod. civ., era di tipo *concessorio*. Esso veniva rimesso alla valutazione discrezionale dell'autorità governativa (Governo o Prefetti), che poteva per l'appunto "concederlo" o meno con decreto (d.P.R. o prefettizio) sulla base di un preventivo controllo di merito o sostanziale della fisionomia dell'ente (organizzazione, mezzi patrimoniali, importanza e rilevanza dello scopo, ecc.): evidente retaggio storico dell'atteggiamento di sfavore del legislatore verso gli enti non di profitto. Al riguardo, cfr. C. TURCO, *op. cit.*, 115.

[95] Trattasi in entrambi i casi (Registro delle persone giuridiche e RUNTS) di una funzione o efficacia costituiva analoga a quella dell'iscrizione della società per azioni nel registro delle imprese *ex* art. 2331, comma 1, cod. civ., secondo il quale, in termini sostanzialmente equipollenti al d.P.R. n. 361/2000 e al d. m. n. 106/2020 di attuazione del CTS, «con l'iscrizione nel registro, la società acquista la personalità giuridica». Si tratta di pubblicità e di un'efficacia *costitutiva* in quanto non serve unicamente ad amplificare e rendere opponibile ai terzi un atto e/o rapporto già di per sé efficace *inter partes*, bensì a modificare la realtà giuridica preesistente "creando" essa stessa, sul piano degli effetti, una nuova situazione giuridica inerente ad un atto e/o rapporto.

[96] In tal senso, C. TURCO, *Diritto civile*, I, Torino, 2014, 115.

settore […], nelle more dell'istituzione del Registro medesimo, si intende soddisfatto da parte delle reti associative e degli enti del Terzo settore attraverso la loro iscrizione ad uno dei registri attualmente previsti dalle normative di settore»; sia l'art. 22, comma 1 *bis* [97], che prevede la sospensione – e non la perdita – di efficacia della personalità giuridica acquistata ai sensi del d.P.R. n. 361/2000 per quelle associazioni e fondazioni che ottengano, nel rispetto dei requisiti indicati dal CTS, l'iscrizione nel RUNTS e fintanto che questa sia mantenuta: il che induce legittimamente a ritenere – anche alla luce del *nomen iuris* e della lettera del testo che parla di effetto "costitutivo" dell'iscrizione (art. 7 d. m. n. 106/2020) – l'equipollenza (se non coincidenza) tra le due forme di riconoscimento della personalità giuridica (che altrimenti potrebbero coesistere), anche sul piano degli effetti giuridici. In particolare, l'art. 52 CTS disciplina espressamente l'opponibilità ai terzi degli atti ivi trascritti soltanto dopo la relativa pubblicazione nel Registro stesso, a meno che l'ente provi che i terzi ne erano a conoscenza. Trattasi, nondimeno, di una di quelle ipotesi di pubblicità dichiarativa *sui generis* [98], in quanto l'opponibilità-inopponibilità non risulta basata, come di norma, sulla c.d. scienza legale della trascrizione/iscrizione, a prescindere dalla conoscenza effettiva o meno del terzo, ma è legata alla prova che il terzo sia comunque e per altra via venuto a conoscenza di un certo atto o fatto, che, in caso di effettiva conoscenza, gli sarà ugualmente opponibile nonostante l'omessa pubblicità nella forme dovute.

In siffatto contesto, volto ad escludere che il CTS evochi una categoria o tipologia di personalità giuridica diversa da quella del d.P.R. n. 361/2000, si colloca altresì l'art. 22, comma 7, là dove espressamente prevede l'operatività per gli ETS personificati del generale principio alla cui stregua le persone giuridiche godono di autonomia patrimoniale perfetta [99]: anche per il CTS, quindi, l'autonomia patrimoniale perfetta rappresenta l'effetto fisiologico e più rilevante del riconoscimento dell'ETS come persona giuridica e della sua conseguente sottoposizione ad un regime di pubblicità che, oltre a rendere opponibili ai terzi i fatti e/o gli atti (struttura, organizzazione, vicende) oggetto di quest'ultima, pone i creditori dell'ente in grado di conoscerne la consistenza patrimoniale.

D'altra parte, non appare tuttavia condivisibile l'affermazione per cui il CTS avrebbe introdotto uno statuto generale dettato per gli ETS, dotati o meno di personalità giuridica, ed operante indipendentemente dall'acquisto della personalità giuridica [100]: ciò, in quanto, se è vero che l'iscrizione al RUNTS si configura come una libera scelta degli enti *non profit* che vogliano avvantaggiarsi delle agevolazioni fiscali e della legislazione speciale introdotta per il terzo settore, è altrettanto vero che essa è *conditio sine qua non* per l'acquisto della qualifica di ETS e per l'operatività della relativa disciplina tra cui il riconoscimento della

[97] Comma inserito dall'art. 6, comma 1, lett. b), d.lgs. 3 agosto 2018, n. 105, a decorrere dall'11 settembre 2018, ai sensi di quanto disposto dall'art. 35, comma 1, del medesimo d.lgs. n. 105/2018.

[98] Si pensi, ulteriormente, al caso del difetto di notificazione al debitore ceduto della cessione del credito, cui può ovviarsi con la dimostrazione che il debitore, che è "terzo" rispetto al negozio di cessione intercorso tra creditore cedente e cessionario, fosse comunque «a conoscenza dell'avvenuta cessione» (art. 1264 cod. civ.); oppure quello della revoca o della modifica della procura con cui un soggetto attribuisce ad un altro il potere di rappresentarlo, che «devono essere portate a conoscenza dei terzi con mezzi idonei» e, in mancanza, saranno nondimeno opponibili a quei terzi che si provi le conoscessero «al momento della conclusione del contratto» con il rappresentante (art. 1396 cod. civ.); o ancora all'art. 2448 cod. civ., sugli effetti della pubblicazione nel registro delle imprese, alla cui stregua «gli atti per i quali il codice prescrive l'iscrizione o il deposito nel registro delle imprese sono opponibili ai terzi soltanto dopo tale pubblicazione, a meno che la società provi che i terzi ne erano a conoscenza».

[99] Testualmente, art. 22, comma 7, CTS, «nelle fondazioni e nelle associazioni riconosciute come persone giuridiche, per le obbligazioni dell'ente risponde soltanto l'ente con il suo patrimonio».

[100] In tal senso, R. CATALANO, *Il Registro Unico Nazionale ed il riconoscimento della personalità giuridica agli Enti del Terzo Settore*, cit., 50, che conclude affermando che la generale disciplina contenuta nel CTS definisce il regime giuridico cui sottostanno tutti gli enti qualificabili come ETS, siano essi personificati o no, in ragione dell'attività esercitata e dell'iscrizione al RUNTS ovvero, in regime transitorio, agli altri previgenti registri speciali.

personalità giuridica. Ai sensi dell'art. 22, comma 1, infatti, «le associazioni e le fondazioni del Terzo settore possono acquistare la personalità giuridica mediante l'iscrizione nel registro unico nazionale del Terzo settore» e, *ex* art. 7, comma 1, d.m. n. 160/2020, «l'iscrizione nel RUNTS ha altresì effetto costitutivo della personalità giuridica».

In altri termini, alla luce di un'attenta lettura del dettato normativo, gli enti *non profit* potranno essere riconosciuti o meno come persone giuridiche, ma acquisteranno necessariamente la personalità giuridica – oltreché la qualifica di ETS – a seguito di iscrizione nel RUNTS: sicché ci saranno associazioni o fondazioni non iscritte al RUNTS e tuttavia già dotate di personalità giuridica, perché iscritte nell'apposito registro delle persone giuridiche, ma non sembrano pensabili ETS, così qualificabili perché iscritti al RUNTS, privi di personalità giuridica. Ragionando diversamente – e cioè limitando il riconoscimento della personalità giuridica a seguito di iscrizione nel RUNTS alle sole associazioni e fondazioni che trasmigrino nel RUNTS – non solo si determinerebbe uno scollamento ed un'ingiustificata disparità di trattamento giuridico tra ETS e RUNTS, da una parte e associazioni e fondazioni che trasmigrano nel RUNTS, dall'altra, ma si svuoterebbe altresì la stessa *ratio* della riforma del terzo settore che è quella del riordino e della razionalizzazione delle norme in materia di enti *non profit*, mediante l'emanazione di una disciplina unitaria ed organica di tale settore, anche e soprattutto atta a semplificare il sistema di registrazione con l'istituzione di un registro unico nazionale: *ratio* che non potrebbe realizzarsi se, diversamente dal registro delle persone giuridiche di cui al d.P.R. n. 361/2000, il RUNTS determinasse l'acquisto soltanto della qualifica di ETS e non anche della personalità giuridica per tutti gli enti che chiedano ed ottengano l'iscrizione nel medesimo. Ed è in tal senso che va letto l'art. 48 CTS sul «contenuto» dell'iscrizione là dove elenca tra le «informazioni» che «devono risultare per ciascun ente» nel RUNTS anche l'*eventuale* «possesso della personalità giuridica»: tale informazione va più correttamente intesa come richiesta per quegli enti già personificati ai sensi del d.P.R. n. 361/2000 che vogliano acquisire la qualifica di ETS e per i quali l'efficacia dell'iscrizione nei registri delle persone giuridiche di cui al d.P.R. n. 361/2000 è sospesa fintanto che sia mantenuta l'iscrizione nel registro unico nazionale del Terzo settore (art. 22, comma 1-*bis*, CTS).

Più precisamente, per gli ETS già in possesso di personalità giuridica, l'iscrizione al RUNTS comporterà la sospensione (non cancellazione) dal registro delle persone giuridiche e, nel caso di successiva eventuale cancellazione dal RUNTS, tale originario riconoscimento riacquisterà efficacia. Per quanto riguarda i nuovi richiedenti ETS, il controllo di legalità ai fini dell'iscrizione è affidato al notaio che, in caso di valutazione positiva, richiederà l'iscrizione dell'ente nel RUNTS e, una volta iscritto, l'ente acquisterà la personalità giuridica e l'autonomia patrimoniale perfetta [101]. Soltanto nel secondo caso, l'iscrizione nel RUNTS avrebbe effetto "costitutivo" non solo relativamente all'acquisizione della qualifica di ente del Terzo settore (e della fruizione dei benefici previsti dal Codice e dalle vigenti disposizioni in favore degli ETS), ma altresì della personalità giuridica: ai sensi dell'art. 7 del recente d.m. n. 106/2020, infatti, «nei casi previsti dall'art. 22, commi 1, 2 e 3 del Codice, l'iscrizione nel RUNTS ha altresì effetto costitutivo della personalità giuridica». Rimane fuori il comma 1-*bis* dell'art. 22 CTS relativo alle associazioni e fondazioni già in possesso della personalità giuridica: posto che non sembra possa trattarsi di una dimenticanza, l'esclusione del comma 1-*bis* parrebbe dettata non da una diversa efficacia tra i due tipi di riconoscimento della personalità giuridica, ma

[101] In altri termini, il RUNTS ha due binari paralleli per il suo popolamento iniziale: uno partito il 23 novembre 2021 che prevede il trasferimento delle organizzazioni di volontariato e delle associazioni di promozione sociale già iscritte nei rispettivi Registri regionali alla data del 22 novembre 2021 e l'altro, avviato il 24 novembre 2021, cui possono accedere gli Enti del Terzo settore di nuova costituzione o di nuova iscrizione.

più correttamente dalla superfluità di una "doppia" personalità giuridica e dall'obiettivo di evitare che i due sistemi, "vecchio" (registro delle persone giuridiche, di cui al d.P.R. n. 361/2000) e "nuovo" (RUNTS, introdotto con il CTS) si sovrappongano inutilmente. In altri termini, con l'art. 7, comma 1, d.m. n. 106/2020 e l'omessa menzione del comma 1-*bis* dell'art. 22 CTS, il legislatore ha inteso essenzialmente rendere coerente il sistema, escludendo scientemente che l'iscrizione nel RUNTS determini (e sia presupposto per) l'acquisto della personalità giuridica in capo ad enti (associazioni e fondazioni del terzo settore) che già la possiedono ai sensi del d.P.R. n. 361/2000.