

RIVISTA TRIMESTRALE
DELLA SCUOLA DI PERFEZIONAMENTO
PER LE FORZE DI POLIZIA

Periodico trimestrale
di Dottrina, Legislazione e Giurisprudenza

Anno 2026, n. 1

SOMMARIO

Parte I – Interventi	Pag.	5
Vincenzo Modeo – <i>intervento del Direttore della Scuola di Perfezionamento per le Forze di Polizia tenuto il 3 febbraio 2026 in occasione della cerimonia di apertura dell’anno accademico 2025-2026.</i>	»	7
Matteo Piantedosi – <i>intervento del Ministro dell’Interno tenuto il 3 febbraio 2026 in occasione della cerimonia di apertura dell’anno accademico 2025-2026.</i>	»	10
Francesco Giorgino – <i>Università LUISS Guido Carli. “Il ruolo della comunicazione e del marketing istituzionale per accrescere il valore percepito delle Forze di Polizia”. Prolusione tenuta il 3 febbraio 2026 in occasione della cerimonia di apertura dell’anno accademico 2025-2026.</i>	»	14
Parte II – Articoli e Saggi	»	25
Alessandro Salvemini – <i>“Digitalizzazione e innovazione nella gestione delle risorse umane nel pubblico impiego in Italia”.</i>	»	27
Paolo Iafrate – <i>“La tutela dei minori stranieri non accompagnati tra innovazioni legislative e limiti applicativi”.</i>	»	37
Giuseppe Giliberti, Antonio Di Mauro, Daniele Soffietti, Laura Crimaldi, Elena Luperto, Diego Abbatiello – <i>“Lawful access e prove digitali nell’ecosistema globale: limiti giuridici, sfide tecnologiche e modelli di cooperazione”.</i>	»	58
Parte III – Voci dall’Aula	»	75
Filippo Vanni – <i>“L’approccio amministrativo per il contrasto al crimine. La soluzione adottata dall’Italia e quella proposta dall’Unione europea”.</i>	»	77
Daniela Gregorio – <i>“Problematiche nascenti dalla tutela della privacy per l’espletamento di attività investigative da parte delle Forze di Polizia e della Polizia Giudiziaria”.</i>	»	116
Parte IV – Documenti, Normativa e Giurisprudenza di interesse	»	193
Nunzio Mario Tritto – <i>“Aspetti finanziari e contabili delle gestioni straordinarie degli enti sciolti per infiltrazioni e condizionamenti di tipo mafioso”.</i>	»	195

Parte I
Interventi

Intervento del Direttore della Scuola di Perfezionamento per le Forze di Polizia tenuto il 3 febbraio 2026 in occasione della cerimonia di apertura dell'anno accademico 2025-2026

di Vincenzo Modeo

Sig. Ministro dell'interno, Sig. Ministro della Giustizia, Signora Sottosegretario, Sig. Capo della Polizia-Direttore Generale della Pubblica Sicurezza, Signori Comandanti Generali, Autorità tutte, signori Docenti, cari frequentatori, gentili ospiti, un sentito ringraziamento per la vostra partecipazione a questa manifestazione con la quale si dà il formale avvio alle attività didattiche 2025/2026 della Scuola di Perfezionamento.

Quest'anno la nostra riflessione inaugurale si arricchisce grazie al contributo del Prof. Francesco Giorgino, che ringrazio per la sua disponibilità nonostante i concomitanti importanti impegni professionali di questi ultimi giorni. Nella sua prolusione dal titolo "Il ruolo della comunicazione e del *marketing* istituzionale per accrescere il valore percepito delle Forze di polizia" il prof. Giorgino evidenzierà alcuni nodi essenziali per il futuro delle istituzioni della sicurezza come la creazione e gestione del valore delle istituzioni di sicurezza nei differenti contesti ordinari ed emergenziali.

Ci troviamo oggi nell'Auditorium della Scuola di Perfezionamento per le Forze di polizia, dedicato al Prefetto Carlo Mosca, già decano del corpo decente e padre del coordinamento, nonché grande testimone di valori e modello di comportamento per tutti noi.

Nel corso degli anni, anche grazie al grande impegno e alla professionalità di chi mi ha preceduto, questa Scuola ha saputo costruire e consolidare un prestigio riconosciuto sia a livello nazionale che internazionale, diventando un punto di riferimento per la formazione avanzata delle Forze di polizia. Un prestigio che non nasce per caso, ma che è il risultato di una visione lungimirante, di una costante ca-

pacità di rinnovarsi e di un investimento continuo sulla qualità della didattica e sul valore delle persone.

La nostra Scuola ha sempre interpretato la formazione non come semplice trasmissione di saperi e prassi consolidate, ma come anticipazione delle sfide future. Ha saputo leggere in anticipo i cambiamenti della società, l'evoluzione delle minacce alla sicurezza, l'impatto delle nuove tecnologie e delle trasformazioni culturali, adattando i propri percorsi formativi a un contesto in continua e rapida evoluzione.

È proprio questa attenzione al futuro – unita al rispetto delle tradizioni e dei valori fondanti delle Amministrazioni qui rappresentate – che ha consentito alla Scuola di Perfezionamento di affermarsi come luogo di eccellenza, capace di formare professionalità moderne, consapevoli, flessibili e pronte ad affrontare scenari complessi, ordinari ed emergenziali.

Senza trascurare l'aspetto internazionale che negli ultimi mesi ha visto aggiungere come *partner* istituzionale della Scuola, la *Naif Arab University for Security Sciences di Ryad*, della quale proprio in questi giorni ospitiamo una delegazione per un corso sulla *leadership* e l'organizzazione dei grandi eventi, a testimonianza che anche realtà così lontane si trovano al tempo stesso così vicine.

In questa sede, come in poche altre, si percepisce con chiarezza che la sicurezza non è soltanto un insieme di procedure operative, ma un bene comune, un valore che si rinnova attraverso la formazione, la disciplina, la responsabilità e l'impegno quotidiano di ciascuno.

Questo grazie *in primis* ad una peculiarità preziosa: riunire competenze, saperi e identità operative differenti provenienti da tutte le Forze di polizia.

Interforze non è una parola formale, ma un metodo di lavoro, una prospettiva culturale prima ancora che organizzativa.

Lavorare guardando divise diverse significa offrire ognuno il proprio valore aggiunto, ognuno la propria formazione che in questa sede si mettono a fattor comune per creare un capitale professionale che nessuna amministrazione potrebbe mettere in campo da sola.

Significa prepararsi a un mondo in cui le minacce alla sicurezza sono sempre più ibride, interconnesse, veloci.

E dove solo la cooperazione permette risposte efficaci.

Tuttavia il valore del nostro impegno non si misura solo nei risultati operativi, ma anche nel rafforzamento della fiducia dei cittadini, condizione indispensabile per un Paese sicuro, libero e coeso. E a questo scopo serve equilibrio, capacità critica, gestione delle emozioni, etica professionale e spirito di servizio.

Il nostro mandato formativo non si può esaurire nella mera trasmissione di conoscenze, dovrà invece accompagnare la complessità mutevole della nostra epoca, essere multidisciplinare e tendere al dialogo con la società, ponendo come base i concetti di sicurezza e legalità.

Viviamo un'epoca attraversata da sfide sempre nuove: la transizione digitale, le minacce *cyber*, le vulnerabilità sociali, la pressione informativa, i rischi globali che diventano locali in poche ore.

Per fronteggiare tutto ciò servono: competenze tecnologiche avanzate, capacità di decisione rapida, cooperazione interistituzionale nonché internazionale, una solida cultura dei diritti e delle regole.

La nostra Scuola vuole essere esattamente questo: un laboratorio di innovazione, un presidio di pensiero, un luogo in cui prepararci non solo ai compiti di oggi, ma anche alle sfide di domani, per noi operatori della sicurezza.

Ringrazio pertanto tutti voi per la partecipazione alla cerimonia di inaugurazione dell'anno accademico 2025-2026.

Intervento del Ministro dell'Interno tenuto il 3 febbraio 2026 in occasione della cerimonia di apertura dell'anno accademico 2025-2026

di Matteo Piantedosi

Autorità, Docenti e Allievi,

questa cerimonia rappresenta uno dei momenti più alti della vita delle istituzioni che rappresentiamo, perché qui si investe sul capitale umano chiamato a garantire la sicurezza del Paese.

Ho ascoltato con estrema attenzione le riflessioni di grande spessore del Prof. Francesco Giorgino, che si inseriscono pienamente nel dibattito sul rapporto tra comunicazione, valore percepito e funzione pubblica delle istituzioni.

Considerazioni che mettono a fuoco un aspetto che riguarda molto da vicino anche il mondo della sicurezza: oggi non basta semplicemente svolgere bene il proprio compito, è necessario anche renderne comprensibile il valore.

Per le Forze di polizia il *marketing* istituzionale non è consenso, ma legittimazione.

Non deve essere e non è mera visibilità, ma riconoscibilità del valore pubblico.

Questa Scuola è il luogo dove si forma la *leadership* della sicurezza pubblica. Qui non si costruiscono soltanto competenze tecniche, ma visione, responsabilità, capacità di governo della complessità.

Viviamo una fase storica nella quale la velocità della circolazione delle notizie ha reso la sicurezza un tema quotidiano di confronto collettivo.

Interventi complessi e di grande valore possono restare quasi invisibili, mentre singoli episodi isolati possono dominare la scena informativa. Basti pensare a quanto accaduto lo scorso sabato a Torino, documentato dalle immagini riprese dai tanti giornalisti e cineoperatori presenti.

La prevenzione, invece, non genera titoli, non produce immagini. Pur essendo la forma più alta di successo per la collettività, raramente fa notizia, perché coincide con eventi che non accadono.

È esattamente questo lo spazio di cui parlava il Prof. Giorgino: quello tra valore prodotto e valore percepito.

Uno spazio che non può essere lasciato al caso ma che va governato con linguaggi appropriati, con responsabilità istituzionale.

Le Forze di polizia proteggono persone, intervengono nelle emergenze, contrastano la criminalità, presidiano il territorio, garantiscono diritti.

Ma nella società della comunicazione “continua”, il valore prodotto non coincide sempre con il valore riconosciuto.

Se non viene spiegato, reso leggibile, rischia di non essere compreso e, quindi, di non generare fiducia, soprattutto quella duratura.

La comunicazione istituzionale incide direttamente sulla percezione di sicurezza che, oggi, è sempre più il risultato dell’incontro tra ciò che le istituzioni fanno e ciò che i cittadini comprendono di quell’azione.

Quando questo incontro è efficace, la sicurezza si rafforza.

La comunicazione istituzionale, in questo senso, non può limitarsi a informare.

Deve saper spiegare, contestualizzare, dare senso.

Deve essere sobria, autorevole, coerente. Non per costruire consenso, ma per costruire fiducia.

È una responsabilità che riguarda tutti i livelli dell’azione pubblica ma assume un valore particolare nell’ambito della sicurezza.

Contrastare le diverse forme e modalità con cui opera la criminalità organizzata, significa anche rendere visibile la presenza dello Stato, far percepire che le istituzioni sono affidabili, presenti e più forti di qualsiasi potere mafioso.

In questo contesto, la comunicazione diventa uno strumento di emancipazione civile.

Raccontare il lavoro quotidiano delle Forze di polizia, spiegare il senso delle indagini, valorizzare l’impegno sul territorio contribuisce a rafforzare il legame tra Stato e comunità, a rompere l’isolamento sociale che spesso favorisce il radicamento dei fenomeni criminali.

Un discorso analogo vale per la minaccia terroristica, che utilizza la comunicazione come una delle proprie armi principali.

Il terrorismo si nutre di paura, di messaggi simbolici destinati a destabilizzare le società democratiche.

In questo caso, la risposta istituzionale non può essere soltanto operativa ma deve essere anche comunicativa, capace di informare

senza allarmare, di rassicurare senza minimizzare, di trasmettere l'immagine di istituzioni ferme, vigili e coordinate.

La dimensione comunicativa è centrale anche nella sicurezza cibernetica, che rappresenta una delle sfide più complesse del presente.

Gli attacchi informatici e le campagne di disinformazione non colpiscono soltanto infrastrutture e sistemi tecnologici, ma la credibilità delle istituzioni e la tenuta dei processi democratici.

In questi casi, tempestività e chiarezza nella comunicazione sono parte integrante della risposta di sicurezza.

I flussi migratori, le trasformazioni economiche, il disagio sociale, le tensioni urbane richiedono politiche complesse e scelte difficili, ma il modo in cui queste ultime vengono raccontate incide direttamente sulla percezione di sicurezza e la coesione sociale.

Pensiamo poi al contrasto alla violenza di genere, ai reati contro i minori, ai fenomeni di odio e discriminazione. In questi ambiti, una efficace comunicazione delle istituzioni può rafforzare la fiducia delle vittime e incoraggiare la denuncia.

Guardiamo anche alla dimensione digitale. Una parte crescente della reputazione delle istituzioni si forma *online*. Narrazioni parziali, contenuti decontestualizzati e disinformazione possono riflettersi profondamente sulla percezione dell'attività delle Forze di polizia.

Una riflessione la impone anche il contesto internazionale, che rende ancora più evidente quanto la sicurezza interna sia legata alla capacità dello Stato di comunicare con chiarezza le proprie scelte.

C'è infine un tema decisivo, anch'esso evocato dal Prof. Giorgino nel suo intervento: il rapporto con i giovani.

Una parte fondamentale del valore percepito delle Forze di polizia si costruisce prima del bisogno e prima dell'emergenza, nel modo in cui le nuove generazioni comprendono la sicurezza e la legalità.

I giovani oggi conoscono le istituzioni soprattutto attraverso narrazioni indirette e canali digitali.

Per questo è fondamentale la componente educativa, culturale e formativa alla quale ha fatto riferimento il Prof. Giorgino.

La sicurezza deve essere spiegata come condizione di libertà, non solo come controllo.

La cultura della legalità deve essere trasmessa come valore condiviso, non come imposizione: ogni progetto nelle scuole, ogni incontro con gli studenti, ogni iniziativa di educazione civica è un investimento sulla sicurezza futura.

Dove cresce la cultura della legalità, cresce la sicurezza reale. E cresce anche il valore percepito delle istituzioni.

Questo non è *marketing* nel senso superficiale del termine.

È costruzione di fiducia nel tempo.

È educazione civica applicata alla sicurezza.

In questo quadro, risulta evidente come la comunicazione non possa essere improvvisata.

Essa richiede competenza, consapevolezza del ruolo istituzionale e formazione.

Tutto questo chiama in causa direttamente il ruolo della Scuola di Perfezionamento per le Forze di Polizia che non è soltanto un luogo di alta formazione tecnica, ma uno spazio nel quale il coordinamento diventa cultura professionale condivisa.

Qui si forma una *leadership* interforze che supera le logiche di appartenenza e rafforza l'unità dell'azione pubblica.

Qui si formano dirigenti capaci di comprendere il valore delle parole, dei gesti, dei silenzi; capaci di guidare donne e uomini non solo con l'autorità formale, ma con l'esempio, la coerenza e la credibilità.

Inaugurare un nuovo anno accademico significa investire sulla qualità della formazione pubblica.

Agli allievi che oggi iniziano questo percorso dico che da voi lo Stato si aspetta competenza ed equilibrio.

In ogni scelta, in ogni parola, in ogni comportamento, contribuirete a costruire o a indebolire la fiducia dei cittadini.

Ricordate che l'autorevolezza non nasce dalla distanza, ma dal sapere, dalla coerenza e dalla capacità di comunicare il senso del servizio pubblico.

Un ringraziamento sentito va al Direttore della Scuola, al corpo docente e a tutto il personale che, con professionalità e dedizione, rendono possibile questo percorso di eccellenza all'interno di un istituto che, per qualità, organizzazione e prestigio, costituisce un *unicum* a livello europeo, con un'offerta didattica sempre più proiettata verso una dimensione internazionale.

Concludo rivolgendo a tutti i corsisti gli auguri di un anno di confronto e di crescita professionale, invitandoli a fare tesoro di questa esperienza e a tradurla in un agire sapiente e illuminato nelle future sedi di servizio.

Dichiaro ufficialmente aperto l'Anno Accademico 2025-2026 della Scuola di Perfezionamento per le Forze di Polizia.

“Il ruolo della comunicazione e del *marketing* istituzionale per accrescere il valore percepito delle Forze di Polizia”.

di Francesco Giorgino*

Buongiorno a tutti e grazie!

Per me è un grande onore poter svolgere la prolusione alla cerimonia dell'inaugurazione dell'anno accademico 2025-2026 della Scuola di perfezionamento per le Forze di Polizia sul tema “Il ruolo della comunicazione e del *marketing* istituzionale per accrescere il valore percepito delle Forze di Polizia”. Titolo che, pur essendo stato deciso alcune settimane fa, ha assunto negli ultimi giorni una ancor più evidente rilevanza per i noti episodi di violenza subiti da poliziotti, carabinieri, finanzieri a Torino sabato scorso. A voi rappresentanti delle forze dell'ordine va, come cittadino prima ancora che come giornalista e professore della Luiss, la mia più profonda gratitudine per quello che fate. È convinta la solidarietà per gli attacchi che avete subito. Mi auguro che nel Paese non ci siano mai più ambiguità.

Ho avuto modo di dire ieri sera aprendo la prima puntata della terza edizione del programma di Rai 1, XXI Secolo, che prendere a martellate un uomo in divisa significa prendere a martellate lo Stato e le istituzioni. E questo non è accettabile. L'auspicio che formulo è che in Parlamento si trovi al più presto un'intesa tra maggioranza e opposizioni dopo l'autorevole appello rivolto a tutte le forze politiche dal Presidente del Consiglio, Giorgia Meloni.

Saluto il Ministro dell'Interno Matteo Piantedosi, il Ministro della Giustizia Carlo Nordio, il Sottosegretario agli Interni Vanda Ferro, il Capo della Polizia e Direttore Generale della Pubblica Sicurezza, Pre-

* Professore dell' Università LUISS Guido Carli. Prolusione tenuta il 3 febbraio 2026 in occasione della cerimonia di apertura dell'anno accademico 2025-2026.

fetto Vittorio Pisani e il Dirigente generale di Pubblica Sicurezza, Vincenzo Massimo Modeo, Direttore della Scuola di Perfezionamento per le Forze di Polizia. Lo ringrazio per avermi voluto qui stamane: questo contesto formativo valorizza l'attività interforze e il gioco di squadra tra tutti coloro che operano in un settore strategico per la tenuta democratica del Paese, come la sicurezza.

Saluto, altresì, il Comandante Generale della Guardia di Finanza, Generale di Corpo d'Armata Andrea De Gennaro e il Vice Comandante Generale dell'Arma dei Carabinieri, Marco Minicucci, le autorità tutte.

La mia prolusione si svilupperà in due parti. La prima è dedicata ai processi di creazione e gestione del valore "delle" e "per" le istituzioni di sicurezza, in ottica di implementazione delle conoscenze e competenze comunicative dei vari corpi di polizia. Il concetto di "formazione continua e perfezionamento", in ambiti specifici come sicurezza e giustizia, è stato sostituito da quelli di "formazione permanente" e di "perfezionamento strutturale", attesi i molteplici cambiamenti in atto per via della contestuale presenza di fattori endogeni ed esogeni. Tra questi ultimi ci sono sicuramente la consapevolezza della *iper*-complessità delle società *post*-moderne, a partire dal superamento del rapporto lineare di causa ed effetto, ma anche a partire dal rapporto non sempre equilibrato tra rappresentazione e percezione, dalla presa d'atto della rilevanza dell'ipotesi socio-tecnica e di quella deterministica, sugellata in economia dalla Scuola di Toronto: l'innovazione non si limita ad accompagnare i cambiamenti sociali, ma li determina. Dal profondo.

A tal proposito, dovremmo sempre ricordarci che l'innovazione è anzitutto "di processo". Cambiare il *modus operandi*, avendo contezza di quanto e di come si può essere più incisivi e performanti nel contesto sociale, non è operazione semplice, anche se talvolta doverosa.

La seconda parte della mia relazione è dedicata, invece, ad un'interpretazione (in chiave generale) dei concetti di sicurezza e legalità, inclusa la differenza che passa tra l'agire in una condizione ordinaria e l'agire, invece, in una condizione emergenziale.

La parola chiave della prima parte di questa mia prolusione è "*valore*". Valore per lo Stato e per le singole istituzioni. Valore per i cittadini. Valore per la società nel suo complesso.

La mia analisi si poggia, sostanzialmente, su due gambe: una di metodo e una di merito.

La prima è quella che consente di ricercare forme di equilibrio dinamico, ma pur sempre di equilibrio, tra il *valore reale* e il *valore percepito* dei *brand* pubblici, considerando le molte differenze presenti tra le due variabili, specie in termini di misurabilità e di KPI, ovvero di *key performance indicator*.

In linea generale si deve annotare che ci si trova spesso di fronte a organizzazioni che hanno un valore reale superiore al proprio valore percepito, con la conseguenza che si rendono necessari interventi finalizzati a colmare *deficit* quantitativi e qualitativi di comunicazione e *marketing* istituzionale. In qualche caso, invece, capita che i *brand* abbiano un valore percepito superiore al valore reale per effetto di attività di *doping comunicativo* che, tuttavia, alla prova dei fatti non si traducono né in risultati concreti, né in evidenze empiriche degne di nota.

Muoversi in direzione dell'allineamento tra il valore reale e il valore percepito dei *brand* pubblici significa ricorrere a strumenti ermeneutici di matrice multi ed interdisciplinare. Strumenti che sappiano restituire il senso dell'interazione (sempre più sistematica) tra il settore pubblico e il settore privato nel fermento dei molteplici cambiamenti sociali. La cultura della collaborazione tra le istituzioni politiche, economiche, finanziarie, della sicurezza, sociali da un lato e i cittadini e i corpi intermedi operanti nella società tardo-moderna dall'altro è una scelta obbligata.

Le grandi trasformazioni nascono dalla stabilità degli ecosistemi. La soluzione è l'azione collettiva, a maggior ragione in un contesto connotato dall'interazione continua (centrifuga più che centripeta) tra sistemi e sottosistemi sociali, tra il piano globale e quello territoriale, tra la geopolitica e la geoeconomia. Stiamo parlando di un contesto dentro il quale, in ottica di valorizzazione del sistema Paese, i cittadini possono trovare nuove e significative opportunità di legittimazione e di protagonismo sociale, ma sempre dentro una cornice che rafforzi l'idea della sicurezza e delle responsabilità individuali e collettiva, ovvero la consapevolezza delle conseguenze sugli altri del proprio agire (anche di quello comunicativo), come direbbe il sociologo e filosofo Max Weber.

Sul piano più tecnico, occorre evidenziare che sono importanti due aspetti: uno di metodo ed uno di merito.

Quello di metodo ha a che fare con il presidio delle traiettorie che ibridano la funzione comunicazione, quella di *media relationship management* e quella di *marketing* istituzionale delle diverse organizzazioni pubbliche, comprese le forze dell'ordine. In Luiss abbiamo elaborato la teoria del MICS (acronimo che sta per *Marketing, Information, Communication Systems*).

Ho sempre detto: si scrive M-I-C-S, ma si pronuncia MIX (con la x finale), per dare proprio l'idea della contaminazione di queste soluzioni finalizzate alla creazione e alla gestione del valore. Se guardiamo allo specifico di queste attività lato emittenti del processo comunicativo, per dirla con uno dei padri fondatori dei *media studies*, ovvero Harold Lasswell, è evidente che sono tante le differenze esistenti tra chi fa *marketing* pubblico, chi fa comunicazione istituzionale e chi fa informazione secondo le regole del giornalismo, ovvero in base a competenze tematiche, tecnologiche, espressive, relazionali (conoscenza dei pubblici), deontologiche. Se ci poniamo, invece, nell'ottica dei fruitori dei contenuti che viaggiano all'interno della *platform society*, come lo studioso olandese di scienze sociali van Dijk definisce questo elemento della contemporaneità, beh allora diventa più difficile distinguere ciò che è esito di processi di *marketing*, da ciò che è frutto di meccaniche esecutive tipiche della comunicazione e dell'informazione. La miscela, a ben vedere, può essere una criticità per gli utenti, ma nel contempo è anche un'opportunità per chi deve definire e identificare il valore pubblico, per chi deve crearlo e gestirlo nel tempo, persino per chi deve talvolta rigenerarlo, come accade in caso di questioni reputazionali aperte più di pertinenza del privato che del pubblico.

Questa visione olistica e non molecolare (che è essa stessa questione ontologica della formazione permanente e del perfezionamento strutturale) riconduce tutte le attività, pur nella diversificazione funzionale, al perseguimento di obiettivi ambiziosi e lungimiranti.

Lo dico con chiarezza. La parola "*marketing*" non è incompatibile con le istituzioni, tanto più con le espressioni "sicurezza pubblica" e "Forze di polizia". Stiamo parlando di *marketing* pubblico, etichetta con la quale nella letteratura scientifica ci si riferisce anzitutto alle azioni di creazione e gestione del valore poste in essere dal settore pubblico per massimizzare, a beneficio dei cittadini ma anche di tutte le organizzazioni nazionali o territoriali, quelle iniziative in grado di intercettare gli interessi della collettività. Definito in questo modo, il *marketing* istituzionale comporta una chiara correlazione con la comunicazione pubblica, al fine di aumentare il valore percepito in questo caso di Polizia, Carabinieri, Guardia di Finanza, Polizia Penitenziaria e non solo quello reale davanti all'intero Paese.

Come nel *marketing* aziendale, anche in quello istituzionale, si promuove l'ascolto del cittadino per creare e gestire dinamiche interattive tra chi rappresenta l'offerta di sicurezza e legalità e chi sviluppa la domanda di accesso a questa tipologia di servizio pubblico, giu-

risdizione inclusa, dalla quale dipendono poi conseguenze capaci di svilupparsi in più direzioni.

È la parola *cittadino*, nella sua ampiezza semantica ad essere presa in considerazione: cittadino-consumatore; cittadino-utente; cittadino-elettore; cittadino-attore economico; cittadino-attore sociale. Ci si poggia su tre elementi chiave: *relazione, conoscenza e tecnologia*. Più le istituzioni si pongono il problema della propria efficienza e trasparenza, più è necessario ricorrere a relazioni autentiche e sistematiche con i cittadini. La Pubblica Amministrazione ha ormai il dovere di monitorare l'accesso dei cittadini ai servizi, di fornirgli assistenza continua, di registrare ed analizzare il suo gradimento per ciò che fa. Le logiche legate alla digitalizzazione hanno reso questi processi non solo imprescindibili, ma anche più agevoli, moltiplicando i varchi di accesso da parte degli utenti ed aumentando i *touch point* con le istituzioni.

In questa prima chiave interpretativa del *marketing* istituzionale, possiamo far rientrare anche tutte le azioni di *public branding*, ovvero il processo di strutturazione e gestione di una "marca pubblica" (o con valenza pubblica) che parte dell'epistemologia ha sviluppato soprattutto in relazione allo specifico dei singoli territori.

A tal fine, si ricordi che l'introduzione della figura del *social media* e *digital manager* della Pubblica Amministrazione è rilevante per due motivi. Il primo: può migliorare, come dicevo poco fa, i rapporti tra istituzioni e cittadini. Il secondo: può sviluppare di più e meglio strategie efficaci di *marketing* pubblico. Non dimentichiamoci che la dimensione non privata è costituita da dinamiche di accessibilità, inclusività, espansività, misurabilità, adattabilità. Ecco perché la figura del *social media* e il *digital manager* delle istituzioni, specie di quelle "della" e "per" la sicurezza, se supportato da giuste conoscenze e competenze, può svolgere un ruolo chiave. Nell'interesse di tutti.

Fin qui il metodo. Per quanto riguarda il merito, invece, non si può non evidenziare il cambio radicale di postura di gran parte degli *stakeholder* delle istituzioni. In linea generale possiamo dire che siamo passati dalla fase del *cittadino passivo* a quella del cittadino *iper-attivo* e *inter-attivo*. Il contributo che i cittadini, infatti, danno alle istituzioni si sviluppa attraverso la consapevolezza delle differenze di ordine tecnico legate proprio alle dinamiche di co-creazione del valore.

Si inserisce qui la gestione delle strategie di *reputation management*, che anche per il pubblico valgono quanto i risultati ottenuti attraverso il ricorso a KPI di tipo quantitativo e soprattutto tangibili. Le

istituzioni hanno bisogno di posizionarsi nella società (a volte di ri-posizionarsi) in base ai *valori* che coltivano e trasmettono, secondo la propria *identità* e il ruolo che si ritagliano nella sfera pubblica mediata anche in funzione di mappa concettuale, di *problem solver* e in quanto destinatari di *trust* (fiducia) da parte della società. Le azioni quotidiane e i contenuti comunicativi sono il tramite tra le organizzazioni e le persone, a patto che non siano troppo autoreferenziali.

Altro elemento fondamentale nella gestione dei contenuti comunicativi per finalità di *public brand management* è quello correlato alle esigenze di autenticità dei messaggi, alla trasparenza dell'agentività pubblica, al funzionamento del meccanismo dello *stakeholder engagement*: essere performanti nella creatività comunicativa, nello *storytelling*, nella raggiungibilità dei diversi *target*, ma sempre rimanendo istituzionali, autentici, alla portata di tutti. Rassicuranti e competenti.

È una grande sfida, se consideriamo che tutto ciò deve avvenire nell'ambito della supervisione costante delle logiche di orizzontalizzazione di quelle dinamiche che nel secolo scorso erano dal punto di vista comunicativo esclusivamente verticali. Erano, cioè, solo *one to many*. La leva della *user experience*, del resto, attiva meccanismi virtuosi, allineando la sicurezza percepita a quella reale e viceversa.

Il ricorso alle scienze sociali agevola la gratificazione di questi bisogni ermeneutici, sviluppa strategie performanti, collocando soprattutto le istituzioni lungo l'asse diacronico "passato-presente-futuro". È un tema sociologico quest'ultimo.

Se da un lato bisogna contrastare la sistematica delegittimazione ideologica del passato e di alcuni dei suoi simboli, come per esempio vorrebbe la *cancel culture*, dall'altro bisogna vivere il presente con maggiore consapevolezza e con l'intento di cominciare a governare non tanto i *futuri possibili*, quanto i futuri più *probabili*. Una sfida dal sapore agostiniano che, tuttavia, deve vedere insieme pubblico e privato.

Vengo ora alla seconda parte della mia relazione che come dicevo in apertura è dedicata all'esame (a grandi linee) dei concetti di sicurezza e legalità e alla differenza che passa tra l'agire in una situazione ordinaria e l'agire in una situazione emergenziale.

Operare in emergenza significa farsi carico da un lato delle reazioni che possono essere innescate da situazioni imprevedibili e impreviste, dall'altro della neutralizzazione, o quanto meno del ridimen-

sionamento, dell'effetto di panico diffuso che spesso si propaga alla velocità della luce in situazioni percepite dai cittadini come pericolose. La comunicazione emergenziale con i vecchi e i nuovi *media* consiste nell'uso di canali e codici, messaggi e contesti utili a diffondere rapidamente, *real time*, informazioni cruciali durante situazioni di crisi, come per esempio disastri naturali o incidenti, fatti criminosi, epidemie, ecc. Lo scopo è quello di informare, di allertare, di coordinare la risposta delle autorità e della comunità, facilitando così il flusso delle informazioni fondamentali e limitando al massimo i pericoli per i cittadini.

La comunicazione in emergenza è un processo di grande importanza che richiede messaggi chiari, tempestivi, trasparenti, coinvolgenti, adattati ai singoli destinatari per gestire situazioni critiche, coordinare i soccorsi e avvertire il pubblico, con l'obiettivo di ridurre il disorientamento e la paura attraverso piani predefiniti, strumenti adeguati e un linguaggio che guidi all'azione nel modo più corretto possibile.

La comunicazione emergenziale, come dimostra la tragica vicenda del Covid e della strage di capodanno a Crans Montana, così come in passato abbiamo visto in ambito di lotta alla mafia, alla criminalità organizzata e al terrorismo (nazionale e internazionale), e come stiamo vedendo in queste ore con il terrorismo urbano (come lo ha definito il Ministro Piantedosi) rappresenta un processo complesso che coinvolge emisfero cognitivo, emozionale, comportamentale, relazionale.

È un contesto nel quale la gestione delle criticità è fondamentale per prendere decisioni rapide e soprattutto corrette. Decisioni che contengano i danni, salvino vite umane, preservando la funzionalità delle istituzioni.

Tempestività, reattività, precisione, partecipazione ai cittadini dei rischi e pericoli reali, assicurazione sono aspetti sui quali conviene appoggiarsi. È nella condizione emergenziale più che in quella ordinaria che il valore percepito di un'organizzazione pubblica può allinearsi a suo valore reale, accrescendo il peso specifico di quell'istituzione nella società e riducendo le possibili distorsioni rappresentative.

Come accennavo prima, viviamo in un'epoca in cui la percezione della realtà vale più della realtà stessa. Tendiamo ad agire non sempre in base alla fattualità delle cose, ma in base al modo in cui esse vengono rappresentate nella sfera pubblica mediata, come la chiama lo studioso anglosassone Thompson.

Il tema è particolarmente significativo in relazione alla percezione di sicurezza e, naturalmente, anche del suo opposto e contrario, ovvero la percezione di insicurezza.

Spesso i *media* (vecchi e nuovi) raccontano storie di violenze, di aggressioni, episodi di micro e macro criminalità, a volte da parte di insospettabili, di giovani incensurati che mai avremmo collocato nella sfera del male e che pure si muovono senza scrupoli, senza regole e senza remore.

La sicurezza è uno dei bisogni primari dell'essere umano. È come il bisogno di mangiare, di bere, di respirare, di dormire. Lo psicologo statunitense Maslow ce lo insegna fin dal secolo scorso con la sua piramide, la piramide di Maslow appunto: bisogni fisiologici alla base; bisogni di sicurezza al gradino più sù; e poi, andando verso l'alto della piramide, bisogni di appartenenza, bisogni di stima e di autorealizzazione. La motivazione è il motore che consente all'intera filiera del comportamento umano di evolversi, a metà strada tra razionalità ed emozionalità. E la motivazione alla sicurezza non va data per scontata. Al contrario, va sollecitata. Va costruita ogni giorno, attraverso grandi e piccoli gesti.

In queste ore mi sono richiesto quale sia il vero significato della parola "sicurezza", pensando alle persone, ai gruppi ed alla società nella sua completezza.

Su un punto concordano quasi tutti gli studiosi del tema. La sicurezza è quella condizione che ci rende (o che ci fa sentire) esenti da pericoli. I pericoli, infatti, sono l'altra faccia della medaglia. Più si avverte la loro presenza, più tendiamo ad avere paura di essere vulnerabili, di subire le conseguenze di questo stato di cose e diventare vittime, anche se potenziali, di qualcosa che ci spaventa. È anche questo il motivo che ci porta a far coincidere l'idea di sicurezza con la possibilità di eliminare gran parte dei rischi, rendendo meno pesanti e gravi i danni che inevitabilmente si producono. Il rischio, non dimentichiamolo, è un concetto probabilistico. È la probabilità, cioè, che accada quello che non vorremmo mai che accadesse.

La sicurezza non si fonda solo sulla repressione e voi me lo insegnate. Al contrario, trova la sua legittimazione soprattutto nella prevenzione, dunque nella capacità di eliminazione parziale o totale dei danni, dei rischi e dei pericoli. È un concetto che vale sempre: per la sicurezza pubblica, per quella stradale, per quella alimentare, per quella informatica, per la sicurezza del e sul lavoro e per la più vasta sicurezza sociale. Alla base c'è sempre e comunque il combinato disposto di prevenzione e repressione. La seconda, talvolta, è al servizio della prima, dovendo la giustizia e, dunque, l'accertamento delle responsabilità individuali, innescare meccanismi di erogazione di sanzioni giu-

ridiche e sociali che siano di monito agli altri, che coltivino il proprio valore simbolico e non solo quello sostanziale.

Del resto, i latini, facendo grande risparmio lessicale e semantico, scelsero due sole parole per definire la sicurezza: "*sine cura*". Ovvero senza preoccupazione. In fondo è questo ciò che noi cittadini chiediamo allo Stato e alle altre persone: vivere senza troppe preoccupazioni e, quindi, vivere in modo sicuro.

Definita la sicurezza, chiediamoci per pochi secondi cosa sia la legalità. Se consultiamo il vocabolario, possiamo subito notare che questa voce del dizionario della lingua italiana corrisponde soprattutto alla necessità che l'agire degli esseri umani sia conforme alla legge, ovvero al complesso di norme e disposizioni che vengono emanate per regolamentare i comportamenti degli individui nella sfera pubblica. Legge con la L maiuscola, facendo riferimento a quella piramide che parte dalla norma più importante, la nostra Costituzione, per poi arrivare a leggi nazionali, regionali e a regolamenti di vario tipo.

La legge serve a stabilire delle regole a cui tutti devono attenersi. Le norme ci comunicano due cose: cosa possiamo e cosa non possiamo fare; a quali conseguenze andiamo incontro se commettiamo qualcosa che non avremmo potuto fare o a qualcosa che rappresenta un illecito. È a questo punto che nasce una domanda chiave: perché se la legalità è un principio così lineare e così chiaro, ci sono persone che agiscono nella sfera familiare, nella sfera locale, nella sfera nazionale e internazionale in violazione alla legge? Insomma, perché ci sono persone che non rispettano le norme e commettono reati, a volte anche gravi, muovendosi in direzione opposta a quanto prevedono e prescrivono la legge?

Nel quarto capitolo della Genesi viene raccontata la storia di Caino che uccide il fratello Abele per invidia, perché Dio aveva preferito il raccolto di Abele (dedito alla pastorizia) a quello di Caino (che praticava l'agricoltura). La deviazione dalla linea retta, insomma da ciò che è giusto fare (nell'esempio biblico l'amore fraterno), risale dunque alla notte dei tempi. È nella fragilità della natura umana sbagliare, peccare, violare la norma, a partire da quella morale. Basta questa spiegazione? Certamente no, ma è un punto di partenza interessante.

Allargando di un po' lo sguardo, si può dire che la nostra è una società nella quale la cultura del "noi" è stata sostituita dalla cultura dell'"io": ci interessa far valere le nostre ragioni subito, sempre e comunque, magari senza guardare alle ragioni degli altri. Spesso ragioniamo solo con la nostra testa e non anche con la testa e il cuore degli altri. La nostra è una società nella quale si sta sviluppando un'idea

sbagliata della libertà: una cosa è agire, sapendo che la mia libertà finisce dove inizia la libertà degli altri, altra è agire pensando che la nostra libertà valga sempre e comunque, indipendentemente dagli altri, fornendoci la licenza di fare qualsiasi cosa.

Questo modello di società finisce per creare, anche involontariamente, i presupposti perché attecchiscano comportamenti sbagliati, perché si sviluppino egoismi, prevaricazioni, perché non si rispettino le regole. In questo terreno crescono piante che a volte si raddrizzano e piante (tante, troppe) che invece sono destinate a crescere storte.

La cultura della legalità, che significa soprattutto rispetto delle regole, si impara fin da bambini. Quando nasciamo e cresciamo, cominciamo fin da subito a relazionarci con gli altri: prima i genitori, poi i nostri parenti stretti, gli insegnanti, i coetanei, quello che viene definito "altro generalizzato". Dunque, i primi modelli da seguire per imparare a crescere secondo la cultura della legalità, dobbiamo individuarli nella famiglia e nella scuola, nelle cosiddette "agenzie educative". Educare alle regole, ai valori, al sapersi comportare bene con gli altri.

In questo ragionamento dobbiamo coinvolgere anche i mezzi di comunicazione, la televisione, la radio, i quotidiani, i *social network* dai quali riceviamo a volte modelli positivi e a volte molto negativi che si diffondono grazie alle logiche virali. È opportuno separare il grano buono da quello cattivo. Nelle scuole, da un po' di tempo, sono entrati programmi educativi finalizzati a spiegare l'importanza della cultura della legalità e della giustizia, in chiave di sicurezza collettiva ed è importante che siate voi a segnalarne gli aspetti salienti, mantenendo la vostra centralità sul tema.

Mi avvio alla conclusione con l'ultima domanda: da quali basi dobbiamo partire o ripartire? Almeno da due basi.

La prima. Riconoscere l'importanza delle leggi e osservarle nella vita di tutti i giorni: la legalità non è solo un insieme di divieti e prescrizioni, ma anche partecipazione attiva alla vita di una comunità. La seconda. Avere rispetto degli altri. La parola "rispetto" significa non solo "non fare agli altri ciò che non vorresti fosse fatto a te", ma anche "fai agli altri ciò che vorresti fosse fatto a te" e "ama il prossimo tuo come te stesso", come prova l'evoluzione testamentaria in ambito evangelico.

Rispettare gli altri e se stessi è la più importante delle rivoluzioni da mettere in atto, subito. Importante come la rivoluzione del buon senso. Servono cultura, conoscenza, responsabilità. Serve ricordarci tutti i giorni che non esistono solo diritti, ma anche doveri.

I diritti nascono dai doveri. E non viceversa.

Grazie per la vostra attenzione!

Parte II
Articoli e Saggi

“Digitalizzazione e innovazione nella gestione delle risorse umane nel pubblico impiego in Italia”.

Trasformazione Digitale, Competenze e Sfide Organizzative

di Alessandro Salvemini*

Abstract

Il presente articolo analizza il processo di digitalizzazione nella gestione delle risorse umane (HRM) all'interno del pubblico impiego italiano, con particolare attenzione alle trasformazioni normative, organizzative e tecnologiche intercorse nel periodo 2020–2025. Attraverso una rassegna sistematica della letteratura e l'analisi delle principali riforme legislative — tra cui il Piano Nazionale di Ripresa e Resilienza (PNRR) e le riforme Brunetta e Madia — lo studio esamina come le pubbliche amministrazioni italiane stiano adottando strumenti digitali per ottimizzare la selezione del personale, la valutazione della *performance*, la formazione continua e il lavoro agile. I risultati evidenziano opportunità significative in termini di efficienza operativa e trasparenza, nonché persistenti criticità legate al divario digitale, alla resistenza al cambiamento organizzativo e all'inadeguatezza delle competenze digitali di alcuni dipendenti pubblici. Lo studio offre implicazioni pratiche per *policy maker* e dirigenti pubblici impegnati nella modernizzazione della PA.

Parole chiave: digitalizzazione, gestione delle risorse umane, pubblica amministrazione, PNRR, lavoro agile, e-HRM, riforma della PA

* Primo Dirigente di Polizia penitenziaria, titolato Scuola di perfezionamento Forze di Polizia, direttore Divisione I – Corpo di Polizia penitenziaria della Direzione generale del personale del DAP.

This dissertation analyzes the process of digitalization in human resource management (HRM) within the Italian public sector, with a particular focus on the regulatory, organizational and technological changes that have taken place between 2020 and 2025. Through a systematic review of the relevant literature and an analysis of the main legislative reforms — including the National Recovery and Resilience Plan (PNRR) as well as the Brunetta and Madia reforms — this thesis describes how Italian public administrations are adopting digital tools to optimize staff recruitment, performance evaluation, constant training and smart working. The findings highlight significant opportunities in terms of operational efficiency and transparency, as well as persistent difficulties linked to the digital gap, resistance to organizational change and the deficiency of digital skills among some civil servants. This study provides for practical suggestions addressed to policymakers and public managers engaged in the modernization of the Public Administration.

Keywords: digitalization, human resource management, public administration, PNRR, smart working, e-HRM, PA reform

1. Introduzione

La pubblica amministrazione italiana si trova oggi al centro di una profonda trasformazione digitale che investe, in modo trasversale, tutti i processi organizzativi e gestionali. In questo scenario, la gestione delle risorse umane – tradizionalmente caratterizzata da elevata regolamentazione, rigidità procedurale e scarsa propensione all’innovazione – è chiamata a ridefinire i propri modelli operativi alla luce delle nuove tecnologie digitali e delle istanze di modernizzazione provenienti tanto dal contesto sovranazionale quanto dall’interno del sistema istituzionale nazionale.

Il Piano Nazionale di Ripresa e Resilienza (PNRR), approvato nel 2021, ha allocato risorse significative per la digitalizzazione della PA, individuando nella modernizzazione delle pratiche di HRM uno dei pilastri fondamentali per il rilancio della competitività del sistema pubblico italiano. Parallelamente, la pandemia da COVID-19 ha agito da acceleratore involontario, imponendo l’adozione massiva del lavoro agile e accelerando la transizione verso sistemi elettronici di gestione del personale (e-HRM).

Il presente contributo si propone di: (I) ricostruire il quadro normativo e istituzionale della digitalizzazione dell’HRM pubblico italiano; (II) analizzare le principali dimensioni applicative degli strumenti digitali nella gestione del personale; (III) identificare le criticità strut-

turali che ne limitano la piena implementazione; (IV) proporre qualche spunto di riflessione per una *governance* efficace del cambiamento digitale nelle amministrazioni pubbliche.

2. Quadro teorico e rassegna della letteratura

Il concetto di e-HRM (*electronic Human Resource Management*) è stato elaborato in letteratura come l'insieme di pratiche, politiche e strutture organizzative che utilizzano canali *web-based* per implementare e supportare i processi di gestione delle risorse umane (Ruel *et al.*, 2004; Bondarouk & Ruel, 2009). Nella sua accezione più ampia, l'e-HRM comprende non solo la semplice automazione dei processi amministrativi, ma anche la trasformazione strategica del ruolo della funzione HR all'interno delle organizzazioni pubbliche.

2.1. *New Public Management e digitalizzazione*

Il paradigma del *New Public Management* (NPM), affermatosi a partire dagli anni Ottanta del Novecento, ha introdotto nella gestione pubblica principi e strumenti tipici del settore privato, tra cui la valutazione della *performance*, la competizione per merito e la flessibilità gestionale (Hood, 1991; Pollitt & Bouckaert, 2011). La digitalizzazione dell'HRM pubblico si iscrive in questo filone di ricerca come evoluzione naturale e tecnologicamente mediata delle istanze di modernizzazione amministrativa.

La letteratura recente ha evidenziato come la *Digital Era Governance* (DEG), teorizzata da Dunleavy *et al.* (2006), rappresenti un paradigma complementare al NPM, in grado di valorizzare le potenzialità integrative e reintegrative delle tecnologie digitali per il rinnovamento delle strutture amministrative. In tale prospettiva, la digitalizzazione dell'HRM non è meramente strumentale, ma concorre alla ridefinizione delle relazioni organizzative, dei processi decisionali e dei modelli di responsabilità.

2.2. *Il contesto italiano: specificità e vincoli*

Il sistema del pubblico impiego italiano presenta caratteristiche strutturali che condizionano significativamente i processi di innovazione digitale. Tra queste, si segnalano l'elevata frammentazione isti-

tuzionale (con circa 32.000 enti pubblici di diversa natura e dimensione), la persistente dicotomia tra amministrazioni centrali e locali, la complessità del quadro normativo di riferimento e la storica debolezza della cultura manageriale nella PA (Ongaro, 2009; Borgonovi, 2018).

Studi recenti (Capano & Lippi, 2021; Dente & Coletti, 2011) hanno documentato come le riforme della PA italiana tendano a produrre esiti non ottimali per via di meccanismi di *path dependency*, della capacità di resistenza delle burocrazie consolidate e dell'instabilità del sistema politico-istituzionale. Tali dinamiche si riverberano inevitabilmente sui processi di digitalizzazione dell'HRM, determinando velocità di adozione diseguali tra enti e tra livelli di governo.

3. Il Quadro Normativo della digitalizzazione dell'HRM pubblico

Il processo di digitalizzazione della gestione del personale pubblico in Italia ha preso avvio con il Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005), che ha definito i principi fondamentali della transizione digitale e istituito le basi normative per l'adozione di sistemi informativi integrati nelle pubbliche amministrazioni. Da allora, il quadro normativo si è progressivamente arricchito di successive stratificazioni legislative.

3.1. Le riforme Brunetta e Madia (2009 e 2015)

Il D.Lgs. n. 150/2009 (cd Riforma Brunetta) ha introdotto un sistema organico di misurazione e valutazione della *performance* individuale e organizzativa, prevedendo l'utilizzo di sistemi informatici per la raccolta e l'elaborazione dei dati di *performance*. Successivamente, la legge n. 124/2015 (cd Riforma Madia) ha ulteriormente razionalizzato il sistema, promuovendo, tra l'altro, la dematerializzazione dei procedimenti amministrativi e l'adozione di sistemi di gestione documentale digitale.

3.2. Il PNRR e la strategia nazionale per la PA digitale

Il Piano Nazionale di Ripresa e Resilienza (2021) ha destinato alla digitalizzazione della PA circa 6,7 miliardi di euro, di cui una quota rilevante è indirizzata al potenziamento delle competenze digitali dei dipendenti pubblici e allo sviluppo di piattaforme integrate di gestio-

ne del personale. La Missione 1, Componente 1 del PNRR, denominata “Digitalizzazione, Innovazione e Sicurezza nella PA”, ha identificato tre assi prioritari: la modernizzazione dell’infrastruttura digitale, lo sviluppo delle competenze e la riforma dei processi della PA.

In tale contesto, il Dipartimento della Funzione Pubblica ha adottato il Piano Integrato di Attività e Organizzazione (PIAO), che dal 2022 sostituisce una pluralità di documenti programmatici e introduce un approccio integrato alla pianificazione delle risorse umane, della *performance* e dell’organizzazione amministrativa.

4. Dimensioni applicative della digitalizzazione dell’HRM

4.1. *Reclutamento e selezione digitale*

La digitalizzazione dei processi di selezione del personale pubblico ha conosciuto una significativa accelerazione a partire dal 2021, con l’introduzione di procedure concorsuali semplificate e la possibilità di svolgere prove selettive in modalità telematica (d.l. n. 80/2021). Il portale InPA (Infrastruttura Nazionale per la PA), operativo dal 2022, ha centralizzato l’offerta di opportunità di impiego pubblico e ha introdotto strumenti di *matching* digitale tra profili professionali e fabbisogni delle amministrazioni.

Studi empirici condotti su un campione di 45 amministrazioni centrali (Ferrara & Greco, 2023) evidenziano come l’adozione di sistemi di *Applicant Tracking System* (ATS)¹ abbia ridotto in media del 35% i tempi di espletamento delle procedure concorsuali, con significativi risparmi di risorse amministrative. Tuttavia, permangono criticità legate all’accessibilità digitale per fasce di popolazione a bassa alfabetizzazione informatica e alla standardizzazione eccessiva dei profili ricercati.

4.2. *Valutazione della performance e People analytics*

L’adozione di sistemi digitali per la valutazione della *performance* rappresenta uno degli ambiti di maggiore innovazione nell’HRM pub-

1 I sistemi ATS (*Applicant Tracking System*) sono *software* utilizzati dalle aziende per automatizzare e gestire l’intero processo di selezione del personale, dallo *screening* dei CV fino all’assunzione.

blico italiano. I *People analytics* — intesi come l'applicazione di tecniche di analisi dei dati alle risorse umane — offrono potenzialità significative per il monitoraggio in tempo reale degli indicatori di *performance* individuale e organizzativa, per l'identificazione di *pattern* comportamentali e per il supporto alle decisioni manageriali.

L'ANAC (Autorità Nazionale Anticorruzione) e il Dipartimento della Funzione Pubblica hanno promosso l'adozione di *dashboard* digitali integrate nel sistema PIAO per la visualizzazione e il monitoraggio dei dati di *performance*, favorendo una cultura della trasparenza e della rendicontazione basata sui dati. Tuttavia, la capacità effettiva di utilizzare tali strumenti in chiave strategica rimane disomogenea tra le diverse amministrazioni e non esistono studi attendibili che attestino quale e quanta importanza effettiva tali dati abbiano nella valutazione della *performance*. La cultura della rendicontazione ancorata a dati omogenei e verificabili sconta ancora, purtroppo, il limite della progressione non sempre meritocratica nel pubblico impiego italiano, per cui, quale che sia la *performance* certificata e verificata, mediamente il dipendente pubblico progredirà nel suo percorso di carriera, almeno fino al limite consentito dal rispettivo ordinamento, per il solo trascorrere del tempo.

4.3. Formazione e sviluppo professionale digitale

La Scuola Nazionale dell'Amministrazione (SNA) ha avviato una significativa riorganizzazione della propria offerta formativa in chiave digitale, sviluppando piattaforme di *e-learning* e percorsi di formazione mirati per i dipendenti pubblici. Il progetto "*Syllabus*", promosso dal Dipartimento della Funzione Pubblica, ha definito un *framework* di competenze digitali per la PA articolato in cinque livelli e cinque aree tematiche, fornendo alle amministrazioni uno strumento standardizzato per la mappatura e lo sviluppo delle competenze digitali del personale.

4.4. Lavoro agile e gestione digitale della presenza

La pandemia da COVID-19 ha imposto una sperimentazione di massa del lavoro agile nella PA italiana: nel picco dell'emergenza sanitaria (aprile 2020), circa 1,8 milioni di dipendenti pubblici erano in modalità *smart working*, a fronte di circa 30.000 pre-pandemia (ISTAT, 2020). Questa transizione forzata ha accelerato l'adozione di piattafor-

me collaborative, strumenti di gestione digitale della presenza e sistemi di monitoraggio remoto della produttività.

Il d.l. n. 80/2021 e le successive Linee Guida del Ministro per la Pubblica Amministrazione hanno istituzionalizzato il lavoro agile come modalità ordinaria di svolgimento della prestazione lavorativa, prevedendo che le amministrazioni adottino Piani Organizzativi del Lavoro Agile (POLA) integrati nel PIAO. La gestione digitale del lavoro agile richiede lo sviluppo di nuove competenze manageriali, legate alla *leadership* a distanza e alla valutazione per obiettivi anziché per presenze.

5. Criticità e barriere all'implementazione

Nonostante i progressi registrati, il processo di digitalizzazione dell'HRM pubblico italiano si confronta con criticità strutturali di varia natura, che ne limitano l'efficacia e la diffusione omogenea.

Ci si confronta, innanzitutto, con un significativo divario digitale interno. Ricerche condotte da Formez PA (2022) evidenziano come il 42% dei dipendenti pubblici presenti competenze digitali inferiori al livello base definito dal *framework* europeo DigComp, con variazioni significative tra generazioni e tra aree geografiche.

È nota, altresì, una particolare resistenza organizzativa al cambiamento da parte di un apparato burocratico, a tratti sovradimensionato, che rappresenta uno dei principali ostacoli all'adozione di sistemi digitali di HRM; tale resistenza è spesso alimentata da timori relativi alla riduzione dell'autonomia discrezionale.

Non va sottovalutata, ancora, la particolare frammentazione infrastrutturale della PA italiana. La coesistenza di sistemi informativi eterogenei e non interoperabili rappresenta un ostacolo sistemico alla digitalizzazione integrata dell'HRM. Una ricerca condotta su un campione di 200 comuni italiani (Penati & Rizzi, 2024) ha rilevato la presenza di oltre 340 applicativi diversi per la gestione del personale, con elevati costi di manutenzione e scarsa capacità di integrazione.

Infine, vengono in rilievo rilevanti questioni di *privacy* e protezione dei dati. L'adozione di sistemi di *People analytics* solleva questioni critiche relative al trattamento dei dati personali dei dipendenti pubblici, alla luce del GDPR (Reg. UE 2016/679) e del Codice *Privacy* nazionale. Il bilanciamento tra le esigenze di monitoraggio organizzativo e i diritti individuali dei lavoratori costituisce un'area di crescente tensione giuridica e organizzativa.

6. Riflessioni per una *Governance* efficace della digitalizzazione HRM

Sulla base dell'analisi condotta, è possibile formulare alcune riflessioni operative per le amministrazioni pubbliche impegnate nel processo di digitalizzazione dell'HRM.

1. Investimento sistematico nelle competenze digitali. Le amministrazioni dovrebbero adottare piani pluriennali di sviluppo delle competenze digitali, articolati per profili e livelli, con sistemi di incentivazione del personale che partecipa ai percorsi formativi.
2. Adozione di piattaforme interoperabili. La scelta di soluzioni tecnologiche per l'HRM digitale dovrebbe privilegiare la conformità agli *standard* di interoperabilità definiti dall'AgID, favorendo l'integrazione tra sistemi e la riduzione della frammentazione applicativa.
3. Approccio partecipativo al cambiamento organizzativo. Il successo delle trasformazioni digitali nell'HRM pubblico richiede processi partecipativi di *change management*, che coinvolgano i dipendenti nelle fasi di progettazione e implementazione dei nuovi strumenti, riducendo le resistenze e aumentando il senso di responsabilità.
4. *Framework* etico per i *People analytics*. Le amministrazioni dovrebbero dotarsi di linee guida etiche per l'uso dei dati del personale, definendo con chiarezza i limiti del monitoraggio, le finalità del trattamento dei dati e i meccanismi di tutela dei lavoratori, in dialogo con le rappresentanze sindacali.

7. Conclusioni

Il presente articolo ha esaminato il processo di digitalizzazione dell'HRM nel pubblico impiego italiano, evidenziando sia le opportunità che le sfide connesse a questa trasformazione. I risultati dell'analisi suggeriscono che la digitalizzazione dell'HRM pubblico è un processo complesso, multidimensionale, multisistemico e non lineare, che non può essere ridotto alla mera adozione di strumenti tecnologici, ma richiede un'azione sinergica su più piani: normativo, organizzativo, culturale e professionale.

L'esperienza italiana si inserisce in un contesto europeo di progressiva convergenza verso modelli di *digital government*, pur

mantenendo specificità strutturali che ne condizionano i ritmi e le modalità di attuazione. Il PNRR ha offerto un'opportunità storica per accelerare la modernizzazione della PA, ma la sua efficacia dipenderà in larga misura dalla capacità delle amministrazioni di sviluppare competenze digitali diffuse, adottare un approccio strategico al cambiamento organizzativo e costruire ecosistemi digitali integrati e interoperabili.

Futuri approfondimenti dovranno indagare gli effetti di lungo periodo della digitalizzazione dell'HRM sui livelli di benessere organizzativo, sulla qualità dei servizi pubblici erogati e sull'attrattività della PA come datore di lavoro per le nuove generazioni di professionisti digitalmente nativi.

Bibliografia

- BONDAROUK T. – RUEL H., *Electronic human resource management: Challenges in the digital era*, International Journal of Human Resource Management, vol. 20 (n.3), 505–514, 2009.
- BORGONOV E., *Principi e sistemi aziendali per le amministrazioni pubbliche*, Egea, 2018.
- CAPANO G. – LIPPI A., *Decentralization, policy capacities, and varieties of first health response to the COVID-19 outbreak: evidence from three regions in Italy*, Journal of European Public Policy, vol. 28 (n.8), 1–22, 2021.
- DENTE B. – COLETTI P., *Measuring Governance in Urban Innovation*, RE.PUBLIC@POLIMI pubblicazioni di ricerca del Politecnico di Milano, 2, 59– 84, 2011.
- DUNLEAVY P. – MARGETTS, H. – BASTOW S. – TINKLER J., *Digital Era Governance: IT corporations, the state, and e-government*, Oxford University Press, 2006.
- FERRARA M. – GRECO L., *E-recruitment nella PA italiana: Efficienza e criticità*, Rivista di Diritto del Lavoro, vol. 45 (n.2), 213–238, 2023.
- FORMEZ PA, *Rapporto sulle competenze digitali per la pubblica amministrazione italiana*, Dipartimento della Funzione Pubblica, 2022.
- HOOD C., *A public management for all seasons?*, Public Administration, vol. 69 (n.1), 3–19, 1991.
- ISTAT, *Lavoro e conciliazione dei tempi di vita. Rapporto annuale 2020*, 2020.
- ONGARO E., *Public management reform and modernization*, Edward Elgar, 2009.
- PENATI A. – RIZZI G., *Frammentazione informatica nella PA locale: Costi e opportunità di integrazione*, Economia Pubblica, vol. 51 (n.1), 45–72, 2024.
- POLLITT C. – BOUCKAERT G., *Public management reform: A comparative analysis*, Oxford University Press, 2011.
- RUEL H. – BONDAROUK T. – LOOISE J. K., *E-HRM: Innovation or irritation?*, Management Revue, vol. 15 (n.3), 364–380, 2004.

“La tutela dei minori stranieri non accompagnati tra innovazioni legislative e limiti applicativi”.

di Paolo Iafrate*

Abstract

Il contributo analizza il sistema di protezione dei minori stranieri non accompagnati (MSNA) in Italia, alla luce delle innovazioni legislative e delle persistenti criticità applicative. Muovendo dalla definizione di MSNA come categoria caratterizzata da una “doppia vulnerabilità” – derivante dalla minore età e dalla condizione di straniero – l’elaborato ricostruisce il quadro normativo internazionale, europeo e nazionale, con particolare attenzione alla legge n. 47/2017 (cd Legge Zampa), che ha rappresentato la prima disciplina organica in Europa in materia. Attraverso un approccio comparativo e l’esame della giurisprudenza della Corte europea dei diritti dell’uomo, lo studio si concentra su tre ambiti: il sistema di accoglienza, le procedure di accertamento dell’età e la conversione del permesso di soggiorno al compimento della maggiore età. Vengono evidenziati i progressi introdotti dalla riforma del 2017, quali il divieto di collocamento in strutture per adulti, l’approccio multidisciplinare nell’accertamento dell’età e l’equiparazione dei diritti dei MSNA ai minori italiani. L’analisi evidenzia, da un lato, il ruolo suppletivo della giurisprudenza nel ripristinare *standard* di tutela elusi a livello normativo o amministrativo; dall’altro, la frammentarietà dell’approccio europeo e l’assenza di strumenti vincolanti specificamente dedicati ai MSNA. In conclusione, si auspica l’adozione di una direttiva europea che armonizzi le garanzie sostanziali e procedurali delle politiche migratorie e minorili.

* Professore titolare di “normativa nazionale ed europea” presso l’Università degli Studi di Roma “Tor Vergata”.

This paper analyses the system for the protection of unaccompanied foreign minors in Italy, in the light of legislative innovations and ongoing difficulties in implementing the law. Starting with the definition of unaccompanied foreign minor as a group characterized by a “dual vulnerability”, i.e. their status of minors and foreigners, the paper outlines the international, European and national legal framework, with a special focus on Law No. 47/2017 (the so-called Zampa Act), which was the first comprehensive piece of legislation on the subject in Europe.

Comparing and examining the case law of the European Court of Human Rights, this paper deals with three areas: the reception system, age assessment procedures, and the conversion of residence permits upon coming of age.

Emphasis is placed on the improvements introduced by the 2027 reform, such as the ban on placing unaccompanied foreign minors in facilities for adults, the multidisciplinary approach to age assessment, and the treatment of unaccompanied foreign minors on an equal footing with Italian minors.

The analysis stresses the supplementary role of case law in restoring standards of protection that have been circumvented at the legislative or administrative level while showing the fragmented nature of the European approach and the lack of binding instruments specifically designed for unaccompanied foreign children. In short, the paper calls for the adoption of a European directive to harmonize the substantive and procedural safeguards under migration and child protection policies.

Introduzione

Il fenomeno dei Minori Stranieri Non Accompagnati, d’ora inanzi MSNA, in questi anni ha subito una crescita importante, tale da suscitare notevole attenzione a livello internazionale ed europea.

La presenza di MSNA è divenuta numericamente sempre più consistente nel territorio europeo, ponendo sempre più la necessità di strutturare interventi atti a determinare sistemi di protezione in grado di assicurare effettiva tutela dei diritti dei minori coinvolti.

Ebbene, la qualifica di “minori” prima che di “stranieri non accompagnati” che ha invitato il legislatore ad allontanarsi da un’ottica adulto-centrica nelle misure di protezione degli stessi.

La definizione di MSNA fa riferimento a soggetti minori di età, dunque persone non giuridicamente in grado di prendersi cura dei propri interessi, non aventi cittadinanza italiana o dell’Unione Europea che si trovano per qualsiasi causa nel territorio dello Sta-

to o che è altrimenti sottoposto alla giurisdizione italiana, privi di assistenza e di rappresentanza da parte dei genitori o di altri adulti per loro legalmente responsabili in base alle leggi vigenti nell'ordinamento considerato¹.

Conseguentemente, ciò che contraddistingue la loro vulnerabilità è la mancanza di accompagnamento, e non dunque lo stato di abbandono, da parte del nucleo familiare; in molti casi, infatti, i minori mantengono relazioni stabili con le famiglie presenti nei paesi d'origine e lo stesso viaggio da loro intrapreso è giustificato dalla necessità di contribuire al fabbisogno giornaliero della stessa.

La categoria dei MSNA comprende una "doppia" vulnerabilità: l'una attinente alla minore età e alla assenza di riferimenti sul territorio nazionale; l'altra relativa alla condizione giuridica di stranieri.² Il diritto internazionale e nazionale considera ragazzi e ragazze al di sotto dei diciotto anni vulnerabili per non aver ancora raggiunto il completo sviluppo psico-fisico, emotivo e cognitivo, e riconosce loro il diritto a protezione e salvaguardie speciali, in particolare, ma non solo, se non sono accompagnati o se sono separati dalla loro famiglia³.

Infine, un aspetto della situazione attuale dell'accoglienza dei MSNA è rappresentato dalla diffusa "cultura dell'emergenza" (o della "straordinarietà") che si continua a mostrare come modo unico per affrontare una condizione strutturale delle migrazioni nel Paese.

Nel caso dei MSNA, alla vulnerabilità tipica dei minorenni si aggiungono una serie di altri fattori, oggettivi e soggettivi, esterni ed intrinseci, variamente intrecciati tra loro⁴.

È riconosciuto che nessun individuo giunto di recente in un ambiente sconosciuto – e tanto meno un MSNA – sia in grado di

1 Legge n. 47/2017, art. 2, co. 1. Secondo la giurisprudenza della Corte di Cassazione, rientrano in tale definizione anche i minori affidati di fatto a parenti entro il quarto grado, in quanto questi minori, pur essendo assistiti, sono comunque privi di rappresentanza (ordinanza 9199/2019 Corte Cass.).

2 FRA (European Union Agency for Fundamental Rights), "Children in Migration in 2019", p. 3 reperibile in https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-children-in-migration_en.pdf: "Children in migration are more vulnerable than adults, particularly when they are unaccompanied. Their vulnerability makes them more exposed to violence, exploitation and trafficking in human beings, as well as physical, psychological and sexual abuse".

3 TOMASI M., *Verso la definizione di uno statuto giuridico dei minori stranieri non accompagnati in Europa? Modelli astratti e concreti di tutela della vulnerabilità*, in *Rivista AIC*, 1, 2020.

4 AMATO A. – MACK G., "Neanche per andare al bagno riuscivo a comunicare" – *Potersi esprimere ed essere ascoltati: un'indagine pilota tra i minori stranieri non accompagnati*, in *Diritto, Immigrazione e Cittadinanza*, 3, 2021.

compiere scelte ragionate e ipotizzare in modo coerente e razionale le opzioni possibili⁵.

La sussistenza delle criticità descritte – unitamente alle condizioni di fragilità che la scelta migratoria, prima, e l'arrivo, dopo, inevitabilmente determinano evidenza come i MSNA necessitino di adeguate misure di accompagnamento, protezione e accoglienza, al fine di favorire le condizioni idonee alla realizzazione di percorsi di accoglienza efficaci, che possano dunque all'origine arginare il fenomeno degli allontanamenti volontari⁶.

L'Unione Europea non ha attivato strumenti normativi specifici per la tutela dei MSNA e non c'è dunque nessuna differenza tra lo *status* giuridico di un MSNA e quello di un minore migrante richiedente asilo. Infatti, la loro tutela viene garantita attraverso il rispetto degli *standard* europei fissati in materia di asilo, immigrazione e tratta.

Di conseguenza, non è possibile individuare un eguale livello di tutela dei MSNA comune ed equivalente tra gli Stati membri, e la disciplina europea può dirsi frammentata sul punto.

Proprio tale assenza di una prospettiva di armonizzazione rende arduo il compito dell'interprete nell'individuazione dei diritti sostanziali e processuali riferibili a dei profili di complessa vulnerabilità come *supra* definita.

La gestione dei MSNA per i governi europei poiché solleva questioni legate ai diritti dell'infanzia, al fenomeno migratorio, al diritto di asilo e alla cooperazione internazionale.

A tal proposito, per una migliore comprensione del tema dei MSNA è opportuno comprendere come i flussi migratori hanno inciso nei diversi Stati UE, specialmente quelli direttamente coinvolti nel controllo delle frontiere.

Al riguardo, il contributo prenderà in considerazione lo studio e l'analisi della gestione (e protezione) dei MSNA in paesi di frontiera quali Italia, al fine di individuare il rispettivo quadro legislativo nazionale e le criticità applicative.

Lo scopo del presente contributo sarà, infatti, quello di comparare soluzioni e approcci adottati negli Stati membri nel dare contenuto al *best interest of the child*, e valutare dunque l'impatto delle politiche legislative e della prassi sui diritti fondamentali dei MSNA.

5 Per un maggior approfondimento, <https://www.istitutoeuroarabo.it/DM/minori-sulla-carta-adulti-nella-vita-leggere-i-bisogni-e-le-competenze-dei-msna/>

6 DI LELLA F., *I minori stranieri non accompagnati tra vulnerabilità e resilienza*, in *Famiglia*, 2019, p. 3.

1. Inquadramento legislativo internazionale ed europeo dei MSNA

Le fonti normative che disciplinano lo *status* dei MSNA sono molteplici e la normativa non è sempre organica.

A livello internazionale, la stessa Convenzione sui Diritti del Fanciullo del 1989 contiene delle disposizioni relative alla disciplina dei minori non accompagnati⁷.

Al riguardo tra i principi generali della Convenzione troviamo: il principio di non discriminazione (art. 2) e il principio del preminente interesse del minore (art. 3), come evidenziato nei *General Comments* del Comitato sui Diritti dell'Infanzia.

Il combinato disposto degli artt. 2 e 3 della Convenzione, in particolare, pone in evidenza il principio guida dell'argomento in questione: il «superiore interesse» del minore migrante deve essere, preminente in tutte le decisioni che riguardano queste persone (art. 3.1).

In tal senso il *General Comment* No. 6 (2005) sul Trattamento dei Minori non Accompagnati o Separati che si trovino fuori dal proprio paese, detta una definizione di questo *status*⁸.

7 L'articolo 22, il quale stabilisce che "Gli Stati parti adottano misure adeguate affinché il fanciullo il quale cerca di ottenere lo statuto di rifugiato, oppure è considerato come rifugiato ai sensi delle regole e delle procedure del diritto internazionale o nazionale applicabile, solo o accompagnato dal padre o dalla madre o da ogni altra persona, possa beneficiare della protezione e della assistenza umanitaria necessarie per consentirgli di usufruire dei diritti che gli sono riconosciuti della presente Convenzione e dagli altri strumenti internazionali relativi ai diritti dell'uomo o di natura umanitaria di cui detti Stati sono parti. A tal fine, gli Stati parti collaborano, nelle forme giudicate necessarie, a tutti gli sforzi compiuti dall'Organizzazione delle Nazioni Unite e dalle altre organizzazioni intergovernative o non governative competenti che collaborano con l'Organizzazione delle Nazioni Unite, per proteggere e aiutare i fanciulli che si trovano in tale situazione e per ricercare i genitori o altri familiari di ogni fanciullo rifugiato al fine di ottenere le informazioni necessarie per ricongiungerlo alla sua famiglia. Se il padre, la madre o ogni altro familiare sono irrimediabilmente, al fanciullo sarà concessa, secondo i principi enunciati nella presente Convenzione, la stessa protezione di quella di ogni altro fanciullo definitivamente oppure temporaneamente privato del suo ambiente familiare per qualunque motivo".

Altre disposizioni, poi, vengono in rilievo: l'art. 12 che stabilisce il diritto del minore di essere ascoltato e di essere partecipe nelle decisioni che lo riguardano; l'art. 19 che pone in capo agli Stati l'obbligo di adottare le misure atte a tutelare il fanciullo contro ogni forma di violenza, di oltraggio o di brutalità fisiche o mentali, di abbandono o di negligenza, di maltrattamenti o di sfruttamento, compresa la violenza sessuale; gli art. 24, 27, 28, 29 e 31 che riconoscono il diritto alla vita, alla sopravvivenza, allo sviluppo personale, alla salute, al tempo libero e allo svago e al perseguimento di un adeguato *standard* di vita; art. 18 e 20 che dettano l'obbligo di nominare un legale rappresentante o un cd "*guardian*" per il minore.

8 "*Unaccompanied children*" (also called *unaccompanied minors*) are children, as defined in article 1 of the Convention, who have been separated from both parents and other relatives and are not

Inoltre, l'art. 22 della Convenzione, introduce il dovere degli Stati membri di garantire protezione adeguata e assistenza umanitaria ai minori stranieri richiedenti asilo, accompagnati o non accompagnati, attraverso misure connotate nel senso della stabilità.

Queste previsioni normative sono integrate dal Commento Generale n. 6, approvato nel 2005 dal Comitato ONU sui diritti dell'infanzia, esplicitamente rivolto anche alla situazione dei minori non accompagnati che include una serie di raccomandazioni rivolte agli Stati su come implementare gli obblighi contenuti nell'art. 22 e interpretare l'intero testo e spirito della Convenzione⁹.

La Corte Interamericana dei Diritti dell'Uomo (CIDH)¹⁰ nel contesto dei diritti e delle garanzie dei minori migranti e/o bisognosi di protezione internazionale ha osservato che i minori detengono i diritti umani di tutti gli esseri viventi e godono di diritti speciali derivati dal loro *status* a cui corrispondono specifici doveri familiari, sociali e statali¹¹. Ebbene, definito il minore straniero, l'esame delle regole applicabili all'ingresso, al soggiorno e alla tutela dei minori stranieri possono essere affrontati da diversi ambiti di riflessione. Il primo aspetto concerne l'individuazione della categoria del minore straniero e la distinzione interna tra minori accompagnati dai genitori o da "adulti per loro responsabili" e minori stranieri non accompagnati: si tratta di stabilire, in generale, a quali soggetti si applichi l'articolata disciplina dettata per regolare il fenomeno individuale e collettivo dell'immigrazione adolescenziale¹². Il secondo aspetto richiama l'individuazione della normativa applicabile alle differenti categorie di soggetti¹³. L'ultimo, attiene all'individuazione dell'autorità, nazionale o estera, amministrativa o giudiziaria,

being cared for by an adult who, by law or custom, is responsible for doing so. 8. "Separated children" are children, as defined in article 1 of the Convention, who have been separated from both parents, or from their previous legal or customary primary caregiver, but not necessarily from other relatives. These may, therefore, include children accompanied by other adult family members. 10. If not otherwise specified, the guidelines below apply equally to both unaccompanied and separated children".

9 Glossario EMN Migrazione e asilo, Edizione Idos, Roma, giugno 2011, p. 29.

10 *Ibidem*, p. 181.

11 Opinione Consultiva de la Corte Interamericana dei diritti umani, OC-21/14 de 19 agosto 2014 a richiesta di Argentina, Brasile, Paraguay e Uruguay.

12 CORDIANO A., *The best interest of unaccompanied foreign child e gli istituti del diritto minorile: un caso di convergenze (quasi) parallele*, in *Dir. succ. Famiglia*, 2018, p. 409 ss.

13 TARZIA G., *"La Tutela del minore straniero nel sistema legislativo italiano"*, in *Diritto di famiglia e minorile*, Wolters Kluwer, Seconda edizione, 2017, p. 361.

competente a porre in essere quelle azioni di sostegno, promozione, cura e tutela che la normativa prevede¹⁴.

2. La tutela dei MSNA in Italia: dati e legislazione

In Italia la Direzione Generale dell'Immigrazione e delle politiche di integrazione censisce i dati sui Minori Stranieri Non Accompagnati nella banca dati istituita ai sensi dell'art. 4 del regolamento n. 535/1999¹⁵.

Secondo i dati riportati, i minori stranieri non accompagnati (MSNA) censiti in Italia al 31 dicembre 2025 sono 17.011: si tratta in maggioranza di maschi (88,63%) e hanno per la maggior parte 17 anni (53,52%), 16 anni (20,36%) e 15 anni (6,62%); arrivano soprattutto da Egitto (5.159 minori), Ucraina (2.963), Bangladesh (1.703), Gambia (1.114) e Tunisia (932), mentre le Regioni che ne accolgono di più sono la Sicilia (3.324 minori, il 21,56% del totale), la Lombardia (2.074, il 13,45%), Campania (1.775, l'11,55%) l'Emilia-Romagna (1.156, il 7,50%) e il Lazio (936, il 6,07%)¹⁶.

I diritti dei minori stranieri non accompagnati e le procedure riguardanti l'arrivo e la permanenza nel territorio nazionale sono disci-

14 Cfr. *Condición Jurídica y Derechos Humanos del Niño. Opinión Consultiva OC-17/02 de 28 de agosto de 2002. Serie A No. 17, párr. 42.*

15 Si rimanda al seguente link: <https://www.lavoro.gov.it/temi-e-priorita/immigrazione/focus-on/minori-stranieri/pagine/rapporti-di-approfondimento-sulla-presenza-dei-msna-in-italia>. Rispetto alla distribuzione per età dei minori presenti prima del 2025, permane una minore concentrazione dei minori di età superiore ai 16 anni a favore dei minori con età inferiore, motivata dal peso della distribuzione per età della popolazione dei minori ucraini presenti in Italia, che al contrario delle altre cittadinanze, ha un'incidenza di oltre il 50% dei minori nella fascia d'età inferiore a 16 anni. L'analisi dei dati degli ingressi per Paese di origine ha evidenziato delle concentrazioni rispetto alle modalità di ingresso dei minori in Italia.

16 *Report* statistici sulla presenza dei Minori Stranieri Non Accompagnati in Italia del Ministero del Lavoro e delle Politiche Sociali, i *Report* sono realizzati in ottemperanza a quanto previsto dall'art. 33 del Testo Unico Immigrazione nonché dall'art. 2, comma 2 del d.p.c.m. n. 535/1999. I *Report*, predisposti a partire dai dati censiti dalla Direzione Generale, analizzano le principali caratteristiche dei minori non accompagnati presenti nel territorio italiano, prestando particolare attenzione all'evoluzione del fenomeno in termini quantitativi e qualitativi, attraverso il confronto per i diversi indicatori di analisi con i dati dei periodi precedenti, <https://analytics.lavoro.gov.it/t/PublicSIM/views/PresenzadeiMinoristranierinonaccompagnatiinItalia/PresenzadeiMinoristranierinonaccompagnatiinItalia?%3Aembed=y&%3Aiid=5&%3AisGuestRedirectFromVizportal=y>; <https://analytics.lavoro.gov.it/t/PublicSIM/views/PresenzadeiMinoristranierinonaccompagnatiinItalia/PresenzadeiMinoristranierinonaccompagnatiinItalia?%3Aembed=y&%3Aiid=5&%3AisGuestRedirectFromVizportal=y>.

plinati in parte da specifiche norme relative ai MSNA come il D.Lgs. n. 142/15 (Attuazione della direttiva 2013/33/UE recante norme relative all'accoglienza dei richiedenti protezione internazionale), nonché dalla direttiva 2013/32/UE, recante procedure comuni ai fini del riconoscimento e della revoca dello *status* di protezione internazionale che ha definito altresì il sistema di accoglienza per i MSNA¹⁷.

Tuttavia, il confronto con le prassi applicative ha evidenziato la persistenza di alcune criticità che privano i minori di una adeguata tutela anche a causa di un percorso burocratico-amministrativo complesso.

3. Legge n. 47/2017: analisi di una riforma

La legge 7 aprile 2017 n. 47, cd Legge Zampa, dedicata ai minori stranieri non accompagnati, ha previsto tutta una serie di interventi strutturali a favore dei minori presenti sul territorio italiano, riconoscendo la loro vulnerabilità e la titolarità di appositi diritti.

Al fine di individuare luci e ombre dell'attuale legislazione italiana in materia, è necessario far riferimento ad alcune disposizioni, concentrandosi in particolar modo su tre aspetti principali: il sistema d'accoglienza, l'accertamento dell'età e la conversione del titolo di soggiorno.

Tutti questi aspetti sono stati oggetto di modifica del decreto legislativo n. 133/2023 (convertito in legge 1 dicembre 2023, n. 176), che ha suscitato preoccupazione a causa della possibile riduzione degli *standard* di tutela dei diritti fondamentali dei MSNA, come enunciato da studiosi e operatori non solo legali, ma anche dei medici legali incaricati della procedura di accertamento dell'età¹⁸.

La legge n. 47/2017 è la prima normativa in Europa dedicata alla realizzazione di un sistema organico di protezione per i minori

17 Il D.Lgs. 18.8.2015, n. 142 denominato «Attuazione della direttiva 2013/33/UE, recante norme relative all'accoglienza dei richiedenti protezione internazionale, nonché della direttiva 2013/32/UE, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale», completa il recepimento delle principali norme di revisione del sistema europeo comune in materia di asilo, ed è in vigore dal 30 settembre 2015. Gli articoli 17, 18 e 19 sono specificamente dedicati ai minori stranieri, accompagnati e non accompagnati.

18 In particolare, si rinvia al seguente *link*: <https://www.simlaweb.it/accertamento-eta-questione-medico-legale/>; IAFRATE P. – BALSÌ M., *La tutela dei minori stranieri non accompagnati tra progressi e regressioni*, Osservatorio Romano sulle Migrazioni, Ventesimo Rapporto, edito dal Centro Studi e Ricerche IDOS in collaborazione e con il supporto dell'Istituto di Studi Politici San Pio V. Edizioni IDOS Roma, giugno 2025, pp. 132-135.

stranieri non accompagnati. In Italia, per il suo approccio sistematico e innovativo, questa può essere considerata una vera e propria riforma della materia.

L'art. 1 della legge definisce l'ambito di applicazione, riconoscendo innanzi tutto ai minori stranieri non accompagnati la titolarità dei diritti in materia di protezione dei minori a parità di trattamento con i minori di cittadinanza italiana o dell'Unione. Uno dei presupposti fondamentali è la sostanziale equiparazione, quanto alle tutele applicabili, del minore straniero non accompagnato ai minori italiani o dell'Unione Europea¹⁹.

La prima fase d'accoglienza prevede l'inserimento nelle strutture governative di prima accoglienza per le esigenze di soccorso e di protezione immediata, istituite con decreto del Ministro dell'interno per il tempo strettamente necessario. Nella seconda fase, è previsto il ruolo degli Enti locali attraverso il sistema SAI (Sistema Accoglienza Integrazione).

L'art. 4, legge 47/17 interviene sull'art. 19, D.Lgs. 142/15, con alcune modifiche: riduce a 45 (a seguito della ulteriori modifiche introdotte dalla legge n. 50/2023) i 60 giorni previsti dall'art. 19, co. 1, D.Lgs. 142/15 di permanenza nelle strutture di prima assistenza e accoglienza dei minori stranieri non accompagnati, stabilendo altresì che la procedura di identificazione debba terminare entro 10 giorni; prevede che le strutture governative di prima accoglienza debbano essere destinate solo a minori stranieri non accompagnati, escludendo la permanenza in strutture miste in cui siano presenti anche adulti.

Al riguardo, occorre considerare che la maggior parte dei MSNA è attualmente accolta nelle strutture convenzionate con gli enti locali, e dunque tali sistemi di accoglienza determinano una forte eterogeneità delle politiche sociali e socio-educative, proprio a causa dell'assenza di un unico modello sociale di riferimento a livello locale.

In relazione alla procedura di identificazione e accertamento dell'età, può dirsi come entrambe costituiscano senza dubbio il passaggio più importante per garantire o negare l'accesso alle misure di tutela e protezione. Un eventuale errore in questa fase può determinare l'esclusione del MSNA dal complessivo sistema di tutela e protezione o respingimenti, espulsioni e ingiustificati trattenimenti.

19 CASONE C., *Brevi disposizioni in merito alla Legge 47/2017: luci ed ombre*, in *Diritto, Immigrazione e Cittadinanza*, 2, 2017.

La procedura di accertamento dell'età si presenta quindi come permanentemente in bilico «tra tutela e controllo e in sostanza tra inclusione e esclusione»²⁰.

La fase del accertamento dell'età include il colloquio sociale, la visita pediatrica auxologica, la valutazione psicologica o neuropsichiatrica, in base ad un criterio di invasività progressiva. Ebbene, se, all'esito di ciascuna fase o stadio della procedura risultano certi gli elementi in ordine alla minore età dell'interessato, non si procede ad accertamenti successivi. In base alla normativa, un unico esame può essere sufficiente all'identificazione come minorenni, ma non sufficiente ad identificare l'interessato come maggiore di età (ad es. radiografia polso-mani, radiografia dell'arcata dentaria etc).

L'accertamento deve essere condotto in un ambiente idoneo e adeguato, da professionisti appositamente formati e con il supporto di un mediatore culturale ove necessario, utilizzando modalità meno invasive possibili e rispettose dell'età presunta, del sesso e dell'integrità fisica e psichica; non devono essere eseguiti esami socio-sanitari che possano compromettere lo stato psico-fisico della persona e si deve tenere in considerazione l'origine etnica e culturale del minore (D.Lgs. 24/14 art. 4, d.p.c.m. n. 234 art. 1).

La verifica dell'età richiede un'attenta regolazione dell'interazione tra autorità di polizia e autorità giudiziaria, la diffusione di protocolli di collaborazione con strutture socio-sanitarie in grado di effettuare l'accertamento con metodo multidisciplinare e la determinazione degli aspetti procedurali di dettaglio. Al riguardo, occorre richiamare il Protocollo multidisciplinare per la determinazione dell'età dei MSNA del 9.7.2020²¹, che contiene linee guida e disposizioni utili per un corretto accertamento dell'età dei MSNA.

Per converso, i procedimenti volti all'attribuzione dell'età ai minori stranieri non accompagnati possono durare fino ad un anno²².

20 BENVENUTI M., *Dubito, ergo iudico: le modalità di accertamento in Italia dei MSNA*, in *Diritto, Immigrazione e Cittadinanza*, 1, 2022; IAFRATE P., *Lo status giuridico del minore straniero non accompagnato*, in (a cura di) Garante dell'Infanzia e dell'Adolescenza della Regione Lazio. Avv. Jacopo Marzetti, *Tutori volontari per minori stranieri non accompagnati*, vol. 1, 2018, pp. 149-182, Santarcangelo di Romagna, Maggioli.

21 Disponibile al seguente link: <https://www.statoregioni.it/media/2751/p3-cu-atto-rep-n-73-9lug2020.pdf>.

22 FIORE O., *Minori stranieri non accompagnati: dalla tutela alla diffidenza. il cambiamento di prospettiva nelle riforme contenute nel d.l. 133/2023*, in *Diritto, Immigrazione e Cittadinanza*, 1, 2024.

A ciò si aggiunga che, nel tentativo dei Tribunali per i Minorenni di ridurre le pendenze, si è assistito talvolta all'assunzione di provvedimenti superficiali, carenti di istruttoria e fondati esclusivamente sull'esito degli esami clinici, in contrasto non solo con il Protocollo multidisciplinare per la determinazione dell'età dei minori stranieri non accompagnati richiamato, ma con l'art. 19-*bis*, co. 6, D.Lgs. 142/2015.

All'identificazione e all'accoglienza è correlato quello dell'integrazione socio-lavorativa dei MSNA, in relazione alla conversione del permesso di soggiorno per minore età in studio, lavoro autonomo o subordinato. L'integrazione, dovrebbe rappresentare il "naturale sviluppo" del percorso migratorio, quindi anche indice di politiche migratorie efficaci.

Il sistema normativo vigente, all'art. 32 del TU, D.Lgs. 286/1998 prevede che al compimento della maggiore età possa essere rilasciato un permesso di soggiorno per motivi di studio o accesso al lavoro ai minori stranieri, compresi i MSNA, affidati ai sensi dell'art. 2, legge n. 184/83 ovvero sottoposti a tutela, previo parere della Direzione generale dell'immigrazione e delle politiche di integrazione del Ministero del lavoro o ancora (quando non sottoposti a tutela o affidamento) che siano stati ammessi per un periodo non inferiore a due anni in un progetto di integrazione sociale e civile gestito da un Ente pubblico o privato riconosciuto. Tuttavia, tale disposizione è stata oggetto di modifica del decreto legislativo 133/2023 convertito in legge 176/2023, le cui conseguenze sembrerebbero ledere i diritti costituzionalmente garantiti.

4. Il d.l. 133/2023: dal progresso legislativo all'approccio securitario

L'art. 5 d.l. n. 133 del 2023 conv. in legge 176/2023 introduce una serie di novità riguardanti i tre punti *supra* esposti, dunque accoglienza, identificazione, e conversione del permesso di soggiorno.

Per quanto concerne l'accoglienza, viene previsto che in caso di momentanea indisponibilità di strutture ricettive temporanee il Prefetto può disporre la provvisoria accoglienza del minore di età non inferiore a sedici anni in una sezione dedicata nei centri e strutture per adulti per un periodo comunque non superiore a novanta giorni.

Sul punto, tuttavia, preme precisare come la Corte Europea dei Diritti dell'Uomo abbia già condannato l'Italia per violazione dell'art. 3 della CEDU nel caso di minorenni stranieri non accompagnati collocati presso strutture per adulti, caratterizzate da sovraffollamento, carenza di operatori e precarie condizioni igienico-sanitarie.

Nel recente caso *Darboe e Camara c. Italia* la Corte di Strasburgo ha condannato l'Italia proprio per le condizioni di accoglienza di un minorenne; la Corte, infatti, ha verificato che le autorità italiane hanno illegittimamente ritenuto che il sig. Darboe fosse maggiorenne, tramite esami medici relativi all'accertamento dell'età anacronistici e non affidabili, in contrasto con quanto dichiarato dallo stesso ricorrente, così mancando di nominare un tutore che ne avesse la rappresentanza e impedendogli di presentare la richiesta di protezione internazionale. Inoltre, l'erronea determinazione dell'età del ricorrente ne aveva determinato la collocazione nel centro di accoglienza per adulti di Cona, noto per la condizione di sovraffollamento estremo, di violenza diffusa e per le gravi carenze igienico-sanitarie, per più di quattro mesi. Alla luce di tali accertamenti, la Corte ha valutato che fossero stati violati il diritto al rispetto della vita privata e familiare del sig. Darboe (art. 8 della Convenzione) ed il divieto di sottoposizione a trattamenti inumani e degradanti (art. 3 della Convenzione). La Corte sottolinea che l'estrema vulnerabilità dei minori è un elemento fondamentale da considerare attentamente unitamente alla loro condizione di richiedenti asilo che deve essere garantita con tutti i mezzi appropriati.

Il ricorso è stato ritenuto ammissibile poiché la Corte ha altresì constatato l'inesistenza, all'interno dell'ordinamento italiano, di rimedi giudiziali effettivi (art. 13 della Convenzione) per agire contro le condizioni di vita all'interno delle strutture di accoglienza, nonché contro gli errati accertamenti dell'età di minorenni, considerati alla stregua di maggiorenni.

Nonostante la rilevante e significativa pronuncia in tema, le violazioni dell'Italia in relative al sistema di accoglienza dei MSNA permangono²³, fino a includere accertamento di illegittimo trattenimento di minori in violazione anche del divieto espresso dal D.Lgs. 142/2015. Infatti, ciò che avviene sistematicamente presso alcuni luoghi di frontiera italiani (quali Crotone, Lampedusa, Pozzallo, Hot-spot di Contrada Cifali e Taranto) è il trattenimento generalizzato di MSNA ivi accolti, che non possono lasciare il centro e sono costretti a una condizione di totale isolamento.

La Corte Europea dei Diritti Umani, con la decisione del 23 novembre 2023 resa nel procedimento n. 47287/17 (caso A.T. ed altri c.

23 Sul punto, <https://www.asgi.it/famiglia-minori/minori-stranieri-non-accompagnati-dopo-la-condanna-della-cedu-le-violazioni-permangono/>.

Italia), ha condannato l'Italia per avere detenuto illegalmente nel *hot-spot* di Taranto diversi minori stranieri non accompagnati (art. 5, parr. 1, 2 e 4 della Convenzione europea dei diritti dell'uomo), per avere utilizzato trattamenti inumani e degradanti nel predisporre le loro misure di accoglienza (art. 3 della Convenzione), per non aver nominato un tutore né aver fornito loro alcuna informazione sulla possibilità di ricorrere in giudizio avverso tale condizione (art. 13 della Convenzione, in relazione all'art. 3). Il Governo italiano sarà tenuto, altresì, a risarcire i ricorrenti per il danno loro causato.

La CEDU ha condannato nuovamente l'Italia ordinando al Governo italiano l'immediato trasferimento dal centro di accoglienza Sant'Anna di Isola Capo Rizzuto (Crotone) di un minore trattenuto dal 24 giugno 2023 in condizioni materiali degradanti.

A tal proposito, va sottolineato che il principio secondo il quale nessuno può essere esposto al rischio di trattamenti inumani o degradanti ha carattere assoluto e non risulta pertanto derogabile neppure in tempo di guerra, circostanza che rende del tutto comprensibile la statuizione della Corte Europea riguardo l'eventuale violazione dell'articolo 3 della CEDU.

La stessa Corte ritiene che non può “che ribadire la sua consolidata giurisprudenza secondo la quale, dato il carattere assoluto dell'articolo 3, le difficoltà derivanti dall'accresciuto afflusso di migranti e richiedenti asilo, in particolare per gli Stati che costituiscono le frontiere esterne dell'Unione europea, non esonerano gli Stati membri del Consiglio d'Europa dai loro obblighi ai sensi di tale disposizione”²⁴.

24 Sentenza Darboe e Camara, § 169, § 182; Corte eur. dir. uomo, J.A. e altri c. Italia, n. 21329/18, 30 giugno 2023 e Corte eur. dir. uomo, A.B. c. Italia, n. 13755/18, 19 ottobre 2023. Entrambi i casi riguardano alcuni migranti trattenuti per diversi giorni nel cd *hotspot* di Lampedusa, Contrada Imbriacola, accertando una violazione dell'art. 3 CEDU in relazione alle condizioni del centro e dell'art. 5, §§ 1, 2 e 4 CEDU in relazione all'illegittima privazione della libertà personale, oltre che dell'art. 13 CEDU con riferimento alla mancata previsione di adeguati strumenti di tutela; Sentenza del 31 agosto 2023 (caso M. A. c. Italia) Ricorso n. 70583/17 - Causa C c. Italia, § 49, § 50. La ricorrente aveva trascorso quasi otto mesi in questo centro di accoglienza per adulti ed era stato trasferito in un centro adattato all'accoglienza di minori solo in seguito all'applicazione di una misura provvisoria (art. 39 del regolamento della Corte) indicata dalla CEDU. Le sue precedenti richieste di trasferimento erano rimaste senza risposta nonostante la sua particolare vulnerabilità data la sua minoranza e gli abusi sessuali di cui era stata vittima in Ghana, poi in Libia, conseguentemente la Corte europea dei diritti dell'uomo ha concluso per una violazione dell'articolo 3 della CEDU (diritto a non essere sottoposto a trattamenti disumani e trattamenti degradanti).

Al riguardo, la disposizione così modificata dal D.Lgs. 133/2023²⁵ presenterebbe, dunque, profili di incostituzionalità con riferimento agli artt. 3 e 117, comma 1, della Costituzione Italiana, quest'ultimo per la violazione degli obblighi internazionali derivanti dagli artt. 26 e 37 della Convenzione ONU sui diritti del fanciullo, approvata dall'Assemblea Generale delle Nazioni Unite il 20.11.1989 e ratificata dall'Italia il 27.5.1991 con la legge n. 176.

Il D.Lgs. 133/2023 prevede che *“in caso di arrivi consistenti, multipli e ravvicinati, a seguito di attività di ricerca e soccorso in mare, di rintraccio alla frontiera o nelle zone di transito [...], di rintraccio sul territorio nazionale a seguito di ingresso avvenuto eludendo i controlli di frontiera”*. Visti i presupposti applicativi particolarmente ampi, sussiste il rischio concreto che proprio la procedura derogatoria diventi la modalità standardizzata di effettuazione dell'accertamento dell'età.

Tale attività viene affidata dal d.l. 133/2023 alle forze dell'ordine, che, nei casi appena descritti, possono scegliere di avvalersi delle modalità derogatorie, potendo così disporre, nell'immediatezza, *“lo svolgimento di rilievi antropometrici o di altri accertamenti sanitari, anche radiografici, volti all'individuazione dell'età”*.

Una volta concluso l'accertamento gli operanti dovranno redigere un verbale contenente il resoconto delle attività svolte, l'esito degli esami effettuati e l'indicazione del margine di errore, contro il quale l'interessato potrà fare ricorso, entro soli cinque giorni dalla consegna del documento; si tratta, tuttavia, di un tempo insufficiente per un'effettiva difesa, tenendo conto delle condizioni in cui la disposizione troverà applicazione: in frontiera, nell'immediatezza del rintraccio, in *hotspot* o centri di prima accoglienza. Ebbene, il tempo esiguo entro il quale impugnare il provvedimento risulterebbe lesivo degli artt. 24, 113 e 117 della Costituzione, nonché in violazione degli obblighi internazionali derivanti dall'art. 13 CEDU (Convenzione Europea dei Diritti dell'Uomo) e 47 della CDFUE (Carta Fondamentale dei diritti dell'Unione Europea). La modifica in esame, dunque, non garantirebbe una tutela giurisdizionale effettiva ed un concreto accesso agli strumenti di impugnazione.

25 ROMEO F., *Migration phenomena and protection of unaccompanied foreign minors in light of the innovations introduced by the legislative decree n. 133/2023*, in *Actualidad Jurídica Iberoamericana* N° 20, febrero 2024, pp. 184-205; BRAUZZI F. – SODANO V., *Indagine sui bisogni evolutivi dei MSNA*, Approfondimento n. 19, febbraio 2024, Osservatorio Nazionale sui diritti dei minori stranieri non accompagnati, p. 3, https://www.cespi.it/sites/default/files/osservatori/allegati/approf_19_indagine_sui_bisogni_evolutivi_dei_msna.pdf

Inoltre, un'ulteriore criticità è rappresentata dal fatto che dopo la presentazione del ricorso contro il verbale relativo all'accertamento dell'età, non è prevista la sospensione automatica di ogni procedimento amministrativo e penale conseguente all'identificazione come maggiorenne. Per converso nella procedura ordinaria, l'interessato va trattato ad ogni effetto come minorenni fino alla decisione sul reclamo, senza bisogno di uno specifico provvedimento dell'Autorità Giudiziaria che lo preveda.

L'ultimo profilo da affrontare riguarda la conversione del permesso di soggiorno da minore età a motivi di studio e di lavoro²⁶.

Il decreto legislativo 133/2023 dispone infatti che: *“la verifica dei requisiti per il rilascio del permesso di soggiorno per motivi di lavoro subordinato o di lavoro autonomo di cui al comma 1-bis è demandata ai professionisti di cui all'articolo 1 della legge 11 gennaio 1979, n. 12, ovvero alle organizzazioni dei datori di lavoro comparativamente più rappresentative sul piano nazionale alle quali il datore di lavoro aderisce o conferisce mandato. Al sopravvenuto accertamento dell'assenza dei requisiti di cui al primo periodo, consegue la revoca del permesso di soggiorno e di ciò viene data notizia al pubblico ministero competente”*.

La disposizione attribuisce, dunque, una funzione pubblica che presenta caratteri di discrezionalità importanti a soggetti privati che non hanno le competenze per svolgerla, in violazione dell'art. 97 Cost., in base al quale i pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione²⁷.

Inoltre, risulta manifesta la violazione degli artt. 3 e 117, comma 1, della Costituzione, quest'ultimo per la violazione dell'art.

26 Per ciò che riguarda il rilascio del parere positivo da parte della Direzione generale dell'Immigrazione e delle politiche di integrazione per la conversione del pds dei MSNA al diciottesimo anno di età si rimanda a: IAFRATE P., *La Conversione dei permessi di soggiorno per i minori stranieri non accompagnati neomaggiorenni a seguito dell'entrata in vigore della legge 50/2023*, in ADiM Blog, *Analisi & Opinioni*, agosto 2023 p. 5; Save the Children, *«Gli effetti psicologici della migrazione sui minori migranti: quale impatto?»*, 10 giugno 2025.

27 La Corte di Cassazione, con le ordinanze 28161 e 28162 del 6 ottobre 2023 (in *www.altalex.it*), seppur nell'ambito di questioni sottoposte alla disciplina previgente, ha chiarito, in relazione all'abrogazione della norma in commento, che “in ogni caso, il diritto al rispetto della vita privata e familiare non solo è rimasto in vita nell'art. 5, comma 6, TUI, ma continua ad essere tutelato dall'art. 8 CEDU e rientra in quel “catalogo aperto” dei diritti fondamentali (cfr. Cass. Sez. U., 24413/2021) connessi alla dignità della persona e al diritto di svolgere la propria personalità nelle formazioni sociali, tutelati dagli artt. 2, 3, 29, 30 e 31 Cost., trovando dunque il suo fondamento in fonti sovraordinate rispetto alla legislazione ordinaria”.

10 della Convenzione OIL (Organizzazione Internazionale del Lavoro) n. 143 del 24 giugno 1975, sulle migrazioni in condizioni di abuso e promozione delle parità di opportunità e di trattamento dei lavoratori migranti, ratificata con legge 10 aprile 1981, n. 158. Difatti appare irragionevole la disparità di trattamento tra stranieri neomaggiorenni che richiedano la conversione del permesso per minore età in permesso per lavoro e stranieri già maggiorenni che richiedano la conversione nel medesimo titolo di un permesso diverso da quello per minore età²⁸.

Conclusioni

In altri termini, l'intero percorso di protezione dei MSNA comprende una fase amministrativa ed una giudiziaria: la presenza di MSNA a qualunque titolo sul territorio pone, tuttavia, un problema di cura prima ancora che di giurisdizione.

Il principio ispiratore delle politiche legislative è quello del *best interest of the child*, il quale si configura, da un lato, dal punto di vista sostanziale, nel senso che il minore ha il diritto di essere considerato (dunque, ascoltato) quando viene adottata una misura che lo riguarda, affinché i suoi migliori interessi siano stati valutati per giungere ad una soluzione.

Nel contempo, si tratta di un principio generale di carattere interpretativo, in modo che se una disposizione giuridica può essere interpretata in più di un modo, si deve scegliere per l'interpretazione tutela al meglio l'interesse superiore del minore.

Inoltre, una terza dimensione richiama la condizione di "norma di procedura" che questo principio ha, nel senso che il processo decisionale dovrà includere una stima delle possibili ripercussioni (positive o negative) della decisione sui MSNA.

Nel corso degli anni, il quadro normativo attorno all'accoglienza e alla protezione di MSNA si è sviluppato seguendo le tendenze ed è cambiato diverse volte per far fronte alle sfide del fenomeno in Italia e nel contesto europeo.

28 FIORE O., *op. cit.*; CeSPI Osservatorio MSNA, Approfondimento n. 20/marzo 2024, *Monitoraggio normativo. L'accoglienza dei MSNA in Europa ed Italia: quadro attuale e prospettico*, p. 16, https://www.cespi.it/sites/default/files/osservatori/allegati/approf._20_monitoraggio_normativo_msna_2023.pdf.

Il quadro normativo italiano ha seguito l'esempio delle direttive internazionali e dell'Unione Europea, in altre situazioni ha adottato sistemi innovativi prima di altri paesi, come nel caso della cd Legge Zampa.

Tuttavia, le decisioni di condanna della CEDU nei confronti dell'Italia confermano il quadro allarmante del trattenimento generalizzato dei MSNA e le relative precarie condizioni di accoglienza che sistematicamente vedono violati i loro diritti e risultano così privi di adeguata tutela in diversi luoghi di frontiera italiani.

Non stupisce, dunque, il contenuto della raccomandazione del Comitato Economico e Sociale Europeo del 2020²⁹, il quale esorta l'UE a sviluppare un approccio coerente e armonizzato alla protezione dei minori stranieri non accompagnati in Europa, esprimendo preoccupazione per la situazione di questa categoria di minori, che sono tra i soggetti più vulnerabili nel contesto della migrazione e, dunque esposti a un rischio più elevato di violazione dei loro diritti fondamentali.

Il rischio che si prospetta è che dietro l'ideale condiviso della realizzazione dei *best interest of the child* con riferimento a persone che versano in una condizione di "doppia vulnerabilità", si sviluppino linee di tendenza discordanti, talvolta più e talvolta meno rispettose dello stesso³⁰.

Inoltre, concentrarsi sul caso dei MSNA permette di esplorare un fenomeno che è quantitativamente significativo, ma anche di valutare le politiche e le pratiche nei campi dell'inclusione, dell'educazione, della formazione, del capitale sociale, delle relazioni, dell'autonomia e della coesione sociale, e dunque del futuro stesso del paese coinvolto nell'accoglienza³¹.

29 Parere del Comitato economico e sociale europeo sul tema «Protezione dei minori migranti non accompagnati in Europa» (parere d'iniziativa) (2020/C 429/04). Lo stesso Comitato riporta che i MSNA sono presenti in tutti gli Stati membri dell'UE, ma nel 2019 il 60% di tutti i MSNA è stato registrato in quattro paesi (Grecia, Germania, Belgio e Paesi Bassi). Nel 2019 13.800 richiedenti asilo che avevano presentato domanda di protezione internazionale nei 27 Stati membri dell'Unione europea sono stati considerati minori non accompagnati. Nell'UE i MSNA rappresentavano il 7% di tutti i richiedenti asilo di età inferiore ai 18 anni, e la maggior parte di essi (85%) era di sesso maschile. Due terzi avevano 16 o 17 anni (ossia 9.200 persone), quelli di 14 o 15 anni rappresentavano il 22% dei minori non accompagnati (3.100 persone) e, infine, quelli di età inferiore ai 14 anni l'11% (1.500 persone). https://www.conibambini.org/wp-content/uploads/sala-stampa/2025/06/Openpolis.it_17-giugno-1.pdf; PICUM, *Children's rights in the 2024 Migration and Asylum Pact*, Ottobre 2024, p. 21, <https://picum.org/wp-content/uploads/2024/10/PICUM-Analysis-Children-Rights.pdf>.

30 TOMASI M., *op. cit.*

31 CASADO PATRICIO E., *El capital social de los menores extranjeros no acompañados y jóvenes extutelados*, in *Revista Hispana para el analisis de redes sociales*, 3, 2022; FOSCHINO BARBARO M. G., *Salute mentale di MSNA: tra vulnerabilità e resilienza*, 2019, p. 22.

Infine, anche il ruolo della giurisprudenza all'interno di tale dinamica, definita come "una funzione di ri-equalizzazione fondamentale", in una duplice prospettiva: tra principi internazionali e sovranazionali e disciplina nazionale, fino a surrogare eventuali lacune presenti a livello legislativo attraverso una attuazione diretta dei richiamati principi, da un lato; tra quadro normativo e prassi attuative, garantendo l'effettiva applicazione degli *standard* previsti a livello normativo, dall'altro³².

Come appare evidente, il *best interest of the child*, ai fini della sua stessa implementazione, necessita di strategie di cooperazione interna (dunque, tra enti locali, regioni o comunità autonome) ed europeo e internazionale.

È indispensabile riconsiderare anche il ruolo – ora marginale – dell'Unione europea³³ nella protezione dei MSNA; effettivamente, anche a causa dell'assenza di un quadro giuridico preciso che gli Stati membri si trovano ad affrontare grandi difficoltà nel gestire il problema dei minori stranieri non accompagnati in modo concertato e coerente.

Come abbiamo visto all'interno dell'Unione Europea non sono uniformi le normative che definiscono il modo in cui devono essere trattati e i procedimenti a cui sono soggetti (determinazione dell'età, tutori, diritti, ecc.), le criticità riscontrate sono comunque simili e un inasprimento della legislazione di uno Stato accentuerebbe le disparità tra le stesse normative UE coinvolte nel medesimo fenomeno³⁴.

Ebbene, appare auspicabile, che venisse fornito un punto di vista europeo – non più in termini di *soft-law* – sul tema dei MSNA, che possa vincolare maggiormente gli Stati a garantire la protezione adeguata a tale categoria di soggetti vulnerabili nel pieno rispetto dei loro diritti fondamentali.

In tal modo si ridurrebbe anche il rischio che l'obiettivo di tutela dei minori, in virtù della logica dei bilanciamenti di interesse, pur dichiarato e perseguito in una prospettiva multilivello, possa cedere di fronte a esigenze sistematicamente considerate prioritarie come la difesa e il controllo dei confini.

In altri termini è necessario ripensare il fenomeno alla luce di una diversa formulazione funzionale al *best interest of the child*.

32 PENASA S., *L'accertamento dell'età dei minori stranieri non accompagnati: quali garanzie? Un'analisi comparata e interdisciplinare*, in *Federalismi.it*, 2, 2019.

33 DELUIGI R. – DI RUSCIO M. – RINALDI A., *Handle with care. Tuning into plural biographical pathways in community care, system for unaccompanied foreign minors*, in (a cura di) BIANCHI L. – CATARCI M. – RICCARDI V., *QTimes webmagazine* - Anno XVII - n. 2, 2025, Anicia Editore, pp. 167-178.

34 LÓPEZ ULLA J. M., *Razones para una Directiva europea sobre menores extranjeros no acompañados y juventud migrante*, in *Revista de Derecho Comunitario Europeo*, 73, 2022.

Bibliografia

- AMATO A. – MACK G., *“Neanche per andare al bagno riuscivo a comunicare” – Potersi esprimere ed essere ascoltati: un’indagine pilota tra i minori stranieri non accompagnati*, in *Diritto, Immigrazione e Cittadinanza*, 3, 2021.
Per un approfondimento, si rimanda al link: <https://www.istitutoeuroarabo.it/DM/minori-sulla-carta-adulti-nella-vita-leggere-i-bisogni-e-le-competenze-dei-msna/>.
- BENVENUTI M., *Dubito, ergo iudico: le modalità di accertamento in Italia dei MSNA*, in *Diritto, Immigrazione e Cittadinanza*, 1, 2022.
- CASADO PATRICIO E., *El capital social de los menores extranjeros no acompañados y jóvenes extutelados*, in *Revista Hispana para el analisis de redes sociales*, 3, 2022.
- CASCONI C., *Brevi disposizioni in merito alla Legge 47/2017: luci ed ombre*, in *Diritto, Immigrazione e Cittadinanza*, 2, 2017.
- CORDIANO A., *The best interest of unaccompanied foreign child e gli istituti del diritto minorile: un caso di convergenze (quasi) parallele*, in *Dir. succ. Famiglia*, 2018, p. 409 ss.
- DELUIGI R. – DI RUSCIO M. – RINALDI A., *Handle with care. Tuning into plural biographical pathways in community care, system for unaccompanied foreign minors*, in (a cura di) BIANCHI L. – CATARCI M. – RICCARDI V., *QTimes webmagazine - Anno XVII - n. 2*, 2025, Anicia Editore, pp. 167-178.
- DI LELLA F., *I minori stranieri non accompagnati tra vulnerabilità e resilienza*, in *Famiglia*, 2019.
- FIORE O., *Minori stranieri non accompagnati: dalla tutela alla diffidenza. il cambiamento di prospettiva nelle riforme contenute nel d.l. 133/2023*, in *Diritto, Immigrazione e Cittadinanza*, 1, 2024.
- FOSCHINO BARBARO M. G., *Salute mentale di MSNA: tra vulnerabilità e resilienza*, 2019, p. 22, in *CISMAI*, <https://cismai.it/assets/uploads/2019/10/Requisiti20minimi20Salute20mentale20dei20MSNA.pdf>
- FRA (European Union Agency for Fundamental Rights), *“Children in Migration in 2019”*, reperibile in https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-children-in-migration_en.pdf

- *Glossario EMN Migrazione e asilo*, Edizione Idos, Roma, giugno 2011 pp. 29 e 181.
- IAFRATE P., *Lo status giuridico del minore straniero non accompagnato*, in (a cura di) Garante dell'Infanzia e dell'Adolescenza della Regione Lazio. Avv. Jacopo Marzetti, *Tutori volontari per minori stranieri non accompagnati*, vol. 1, 2018, pp. 149-182, Santarcangelo di Romagna, Maggioli S.p.A. Editore.
- IAFRATE P., *Tutela e accoglienza dei minori stranieri non accompagnati in Francia, Grecia e Italia*, in *Famiglia*, 2020.
- IAFRATE P., *La Conversione dei permessi di soggiorno per i minori stranieri non accompagnati neomaggiorenni a seguito dell'entrata in vigore della legge 50/2023*, in *ADiM Blog, Analisi & Opinioni*, agosto 2023.
- IAFRATE P. – BALSÌ M., *La tutela dei minori stranieri non accompagnati tra progressi e regressioni*, Osservatorio Romano sulle Migrazioni, *Ventesimo Rapporto*, edited by Centro Studi e Ricerche IDOS in collaborazione e con il supporto dell'Istituto di Studi Politici San Pio V. Edizioni IDOS Roma, giugno 2025, pp.132-135.
- LÓPEZ ULLA J. M., *Razones para una Directiva europea sobre menores extranjeros no acompañados y juventud migrante*, in *Revista de Derecho Comunitario Europeo*, 73, 2022.
- Opinione Consultiva de la Corte Interamericana dei diritti umani, OC-21/14 de 19 agosto 2014 a richiesta di Argentina, Brasile, Paraguay e Uruguay.
- PENASA S., *L'accertamento dell'età dei minori stranieri non accompagnati: quali garanzie? Un'analisi comparata e interdisciplinare*, in *Federalismi.it*, 2, 2019.
- ROMEO F., *Migration phenomena and protection of unaccompanied foreign minors in light of the innovations introduced by the legislative decree n. 133/2023*, in *Actualidad Jurídica Iberoamericana* N° 20, febrero 2024, pp. 184-205.
- TOMASI M., *Verso la definizione di uno statuto giuridico dei minori stranieri non accompagnati in Europa? Modelli astratti e concreti di tutela della vulnerabilità*, in *Rivista AIC*, 1, 2020.
- TARZIA G., *“La Tutela del minore straniero nel sistema legislativo italiano”*, in *Diritto di famiglia e minorile*, Wolters Kluwer, Seconda edizione, 2017, p. 361.

Sitografia

- <https://www.asgi.it/famiglia-minori/minori-stranieri-non-accompagnati-dopo-la-condanna-della-cedu-le-violazioni-permangono/>
- <https://www.lavoro.gov.it/temi-e-priorita/immigrazione/focus-on/minori-stranieri/pagine/rapporti-di-approfondimento-sulla-presenza-dei-msna-in-italia>
- <https://www.simlaweb.it/accertamento-eta-questione-medico-legale/>

“*Lawful access* e prove digitali nell’ecosistema globale: limiti giuridici, sfide tecnologiche e modelli di cooperazione”.

di Giuseppe Giliberti*, Antonio Di Mauro**, Daniele Soffietti***,
Laura Crimaldi****, Elena Luperto*****, Diego Abbatiello*****

Abstract

Il contributo analizza l’evoluzione del dibattito sul “*lawful access*” nell’ecosistema digitale contemporaneo, caratterizzato dalla globalizzazione dei servizi di comunicazione elettronica, dalla diffusione della crittografia *end-to-end* e dalla crescente extraterritorialità dei dati.

Dopo aver ricostruito il quadro normativo e giurisprudenziale dell’Unione europea, con particolare riferimento alla giurisprudenza della Corte di giustizia in materia di *data retention* e accesso ai dati, il lavoro esamina le principali criticità operative connesse alla disponibilità delle prove digitali e ai conflitti di giurisdizione.

L’analisi comparata dei modelli europeo, statunitense e britannico evidenzia differenti bilanciamenti tra esigenze investigative e tutela dei diritti fondamentali.

Infine, alla luce delle più recenti evoluzioni internazionali, vengono prospettate soluzioni di *governance* del dato digitale fondate su cooperazione multilaterale, infrastrutture tecnologiche condivise e modelli di “*privacy by design*” in ambito investigativo¹.

* Primo Dirigente della Polizia di Stato.

** Maggiore Arma dei Carabinieri.

*** Commissario Capo Polizia di Stato.

**** Capitano Arma dei Carabinieri RF.

***** Commissario Capo Polizia di Stato.

***** Tenente Guardia di Finanza.

1 Sul punto, *ex multis*, GILIBERTI G., *Privacy e sicurezza*, in *Polizia Moderna*, settembre 2025.
<https://poliziamoderna.poliziadistato.it/articolo/35368c03f93c64c4795167759>.

This paper analyzes the evolution of the debate on “lawful access” in the contemporary digital ecosystem, characterized by the globalization of electronic communication services, the widespread adoption of end-to-end encryption, and the increasing extraterritoriality of data.

After reviewing the EU’s legal and case law framework—with particular reference to the case law of the Court of Justice regarding data retention and access to data—this study examines the main operational challenges related to the availability of digital evidence and conflicts of jurisdiction.

A comparative analysis of the European, U.S. and British models reveals different balances between investigative needs and the protection of fundamental rights.

Finally, in light of the latest international developments, solutions for digital data governance are being proposed. They are based on multilateral cooperation, shared technological infrastructure, and “privacy by design” models in the investigative context.

1. Trasformazione digitale e crisi del modello tradizionale di accesso alle prove²

La progressiva smaterializzazione delle comunicazioni, la diffusione dei servizi di messaggistica istantanea e l’archiviazione dei dati in infrastrutture *cloud* distribuite su scala globale hanno attribuito al dato digitale un ruolo centrale nelle indagini penali contemporanee, determinando, al contempo, un significativo incremento delle criticità connesse alle attività di accertamento e repressione dei reati.

Se in passato l’azione investigativa si confrontava prevalentemente con operatori nazionali di telecomunicazioni, oggi una quota rilevante delle comunicazioni elettroniche è gestita da *provider* privati operanti su scala transnazionale, spesso stabiliti in ordinamenti extraeuropei³.

2 I risultati dello studio condotto sono stati compendati in CURTOTTI D. – RIZZI V. – NOCERINO W. – RUSSITTO A. – GILIBERTI G. – SCARPA G., *Piattaforme criptate e prove penali*, in *Sist. pen.*, 6/2023, p. 173; RIZZI V. – RUSSITTO A. – GILIBERTI G. – SCARPA G. – CURTOTTI D. – NOCERINO W., *Piattaforme criptate e prova penale. L’etere digitale alla sfida del codice di rito*, in *Polizia Moderna*, agosto-settembre 2023.

3 Sul punto, *ex multis*, BAJOVIC V. – CORIC V., *Encrochat and Sky ecc Data as Evidence*, cit., p. 260; CURTOTTI D. – RIZZI V. – NOCERINO W. – RUSSITTO A. M. – GILIBERTI G. – SCARPA G., *Piattaforme criptate e prova penale*, cit., p. 196; NOCERINO W., *L’acquisizione della messaggistica su sistema criptati: intercettazioni o prova documentale?*, in *Cass. pen.*, 2023, p. 2801.

Tale trasformazione ha prodotto una crescente divaricazione tra la dimensione territoriale della giurisdizione e la natura globale dei servizi digitali, imponendo alle autorità nazionali di acquisire dati detenuti in altre giurisdizioni, con conseguenti difficoltà legate al conflitto di leggi, alla cooperazione giudiziaria internazionale e alla tempestività delle risposte investigative.

Queste criticità risultano ulteriormente accentuate dalla diffusione della crittografia *end-to-end*, che impedisce ai fornitori di servizi di accedere al contenuto delle comunicazioni degli utenti. Sebbene tale evoluzione tecnologica rafforzi la tutela della riservatezza e la sicurezza delle comunicazioni, essa incide in modo significativo sulla possibilità per le autorità di acquisire prove digitali anche in presenza di un legittimo provvedimento autorizzativo.

Il fenomeno, noto nel dibattito internazionale come “*going dark*”, evidenzia la crescente tensione tra esigenze di sicurezza pubblica e protezione dei diritti fondamentali⁴.

In questo contesto si colloca il tema del *lawful access*, espressione con cui si fa riferimento all'accesso legittimo ai dati da parte delle autorità pubbliche per finalità di prevenzione, accertamento e repressione dei reati.

La questione si configura oggi come uno dei nodi più delicati del rapporto tra esigenze investigative, tutela dei diritti fondamentali e ridefinizione dei confini della sovranità statale nell'ambiente digitale.

Il presente contributo si propone di analizzare in chiave critica l'evoluzione normativa e giurisprudenziale del *lawful access*, con particolare riferimento al contesto dell'Unione europea e alle principali dinamiche di cooperazione internazionale, al fine di valutare se gli strumenti attualmente disponibili siano idonei a garantire un equilibrio effettivo tra efficacia investigativa e tutela dei diritti fondamentali nell'ecosistema digitale contemporaneo.

2. Il *lawful access* nel diritto UE: definizione, quadro normativo e limiti giurisprudenziali

L'espressione *lawful access* non è oggetto di una definizione normativa univoca nel diritto dell'Unione europea. In termini ge-

⁴ FINOCCHIARO G., *La protezione dei dati personali*, Bologna, Il Mulino, ult. ed., p. 145 ss.

nerali, essa viene utilizzata per indicare la possibilità per le autorità pubbliche competenti, in particolare quelle di *law enforcement* e giudiziarie, di accedere legittimamente ai dati digitali detenuti da soggetti pubblici o privati per finalità di prevenzione, accertamento e repressione dei reati.

Sotto il profilo penal-processuale, il *lawful access* si configura come una categoria funzionale riconducibile ai mezzi di ricerca della prova e, più in generale, ai poteri di acquisizione probatoria dell'autorità giudiziaria e della polizia giudiziaria.

La sua emersione è strettamente connessa alla trasformazione digitale delle evidenze probatorie e alla crescente dipendenza delle indagini penali da dati detenuti da soggetti terzi, spesso stabiliti in ordinamenti diversi da quello procedente.

In dottrina è stato evidenziato come tale nozione debba essere distinta sia dalle forme di sorveglianza di massa indiscriminata, sia da pratiche di accesso ai dati prive di adeguata base legale. L'elemento qualificante del *lawful access* non risiede, infatti, nella mera utilità investigativa del dato, bensì nella conformità dell'accesso a una base giuridica chiara, precisa e prevedibile, nonché nel rispetto dei principi di necessità e proporzionalità dell'ingerenza.

In assenza di tali presupposti, l'accesso ai dati rischia di tradursi in una forma di sorveglianza incompatibile con i principi dello Stato di diritto.

Nel dibattito europeo, il concetto è frequentemente associato al fenomeno del cosiddetto "*going dark*", ossia alla crescente difficoltà per le autorità investigative di accedere a dati rilevanti a causa della diffusione della crittografia *end-to-end*, dell'utilizzo di servizi *over-the-top* e della frammentazione geografica dell'archiviazione dei dati.

Tuttavia, l'espansione degli strumenti di accesso solleva rilevanti questioni di compatibilità con i diritti fondamentali garantiti dal diritto dell'Unione, in particolare con quelli sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea.

In tale contesto, la giurisprudenza della Corte di giustizia dell'Unione europea ha progressivamente delineato un sistema di principi volto a circoscrivere rigorosamente le condizioni di legittimità dell'accesso ai dati.

Il *lawful access* si inserisce, pertanto, in un quadro normativo multilivello, nel quale interagiscono discipline eterogenee, tra cui la protezione dei dati personali, la cooperazione giudiziaria in materia

penale, la regolazione delle comunicazioni elettroniche e la disciplina delle prove digitali in ambito transfrontaliero.

Pur in assenza di un atto normativo unitario dedicato specificamente all'accesso ai dati per finalità di *law enforcement*, è possibile individuare un sistema coerente di principi e regole che ne definiscono presupposti, limiti e garanzie.

Un primo asse normativo è rappresentato dalla disciplina della protezione dei dati personali in ambito penale, in cui assume rilievo centrale la direttiva (UE) 2016/680⁵, la quale impone che ogni trattamento, e dunque anche ogni forma di accesso ai dati, sia fondato su una base giuridica chiara, persegua finalità determinate e rispetti i principi di necessità, proporzionalità e minimizzazione⁶.

La direttiva richiede, inoltre, l'introduzione di adeguate garanzie procedurali e di controlli affidati ad autorità indipendenti.

Accanto a tale disciplina, il regolamento (UE) 2016/679 (GDPR) contribuisce a definire lo *standard* europeo di protezione dei dati personali, incidendo in via indiretta anche sull'accesso ai dati detenuti dai *provider* digitali.

Analogamente, la direttiva 2002/58/CE (*e-Privacy*) continua a rappresentare un riferimento essenziale in materia di comunicazioni elettroniche, stabilendo il divieto generale di intercettazione, sorveglianza e conservazione dei dati, salvo eccezioni previste dalla legge e giustificate da esigenze di sicurezza pubblica e repressione dei reati.

Sul piano della cooperazione giudiziaria, l'Unione europea ha progressivamente introdotto strumenti volti a facilitare l'acquisizione transfrontaliera delle prove digitali⁷.

In tale prospettiva si colloca la direttiva 2014/41 sull'ordine europeo di indagine⁸, cui si affianca il più recente pacchetto *e-Evidence* (regolamento (UE) 2023/1543 e direttiva (UE) 2023/1544), che consente alle autorità giudiziarie di rivolgersi direttamente ai fornitori di ser-

5 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, art. 5.

6 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016.

7 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, art. 15, par. 1.

8 Ricostruiscono il dibattito, DANIELE M., *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite*, in *Sist. pen.*, 12/2023; LORENZETTO E., *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale*, in *Cass. pen.*, 2024, p. 182; LUDOVICI L., *I criptofonini: sistemi informatici criptati e server occulti*, in *Sist. pen.*, 3/2023, p. 420.

vizi stabiliti o rappresentati in un altro Stato membro, superando le inefficienze dei tradizionali strumenti di assistenza giudiziaria⁹.

Il quadro normativo così delineato è profondamente inciso dall'elaborazione giurisprudenziale della Corte di giustizia, che ha costruito un sistema di garanzie particolarmente rigoroso¹⁰.

La sentenza *Digital Rights Ireland* ha rappresentato il punto di svolta, sancendo l'incompatibilità con il diritto dell'Unione dei regimi di conservazione generalizzata e indiscriminata dei dati di traffico¹¹.

Tale orientamento è stato successivamente consolidato nelle pronunce *Tele2 Sverige*¹², *Ministerio Fiscal*¹³, *La Quadrature du Net*¹⁴, *Prokuratuur*¹⁵ e

9 CAMALDO L., *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *Diritto penale contemporaneo*, 27 maggio 2014; ARMADA I., *The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?*, in *New Journal of European Criminal Law*, 2015, p. 8 ss.; BELFIORE R., *The European Investigation Order in Criminal Matters: Developments in Evidence-gathering across the EU*, in *European Criminal Law Review*, 2015, p. 312 ss.; JURKA R., *Movement of evidence in the European Union: Challenges for the European Investigation Order*, in *Baltic Journal of Law & Politics*, 2016, p. 56 ss.

10 Cfr. Cass., Sez. Un., 14 giugno 2024, n. 23755, cit.; Cass., Sez. Un., 14 giugno 2024, n. 23756, cit. Per i primi commenti, si vedano, DANIELE M., *La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera*, cit.; GUAGLIARDI G., *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?*, in *Giur. pen.*, 2024, 6, p. 1; PIGNATA S., *Le Sezioni unite sull'utilizzabilità della messaggistica criptata acquisita mediante ordine europeo di indagine*, in *Penale. Diritto e procedura*, 1 luglio 2024; SPANGHER G., *Le Sezioni Unite precisano le condizioni di utilizzabilità della messaggistica dei criptofonini*, in *Dir. e giust.*, 18 giugno 2024; Id., *Criptofonini: le sentenze delle Sezioni Unite*, in *Giust. insieme*, 20 giugno 2024. Per un esame delle questioni rimesse alle Sezioni unite e del delicato tema della sicurezza globale, SPANGHER G., *Criptofonini: sono "in gioco" diritti fondamentali*, in *Cass. pen.*, 2024, p. 173.

11 Corte di giustizia, 8 aprile 2014, cause riunite C293/12 e C594/12, *Digital Rights Ireland Ltd e Kärntner Landesregierung e a.*; FINOCCHIARO G., op. cit., p. 245 ss.; MANTELERO A., *Data retention e diritti fondamentali nel diritto dell'Unione europea*, in *Riv. it. dir. pubbl. com.*, 2017, p. 923 ss.; PIZZETTI F., *La Corte di giustizia e la data retention: verso un nuovo standard europeo di tutela*, in *Dir. inform.*, 2014, p. 689 ss.

12 Corte di giustizia, 21 dicembre 2016, cause riunite C203/15 e C698/15, *Tele2 Sverige AB e Secretary of State for the Home Department*; POLLICINO O. – BASSINI M., *La Corte di giustizia e il difficile equilibrio tra sicurezza e privacy*, in *Federalismi.it*, 2017, p. 1 ss.

13 Corte di giustizia, 2 ottobre 2018, causa C207/16, *Ministerio Fiscal*.

14 Corte di giustizia, 21 dicembre 2016, cause riunite C203/15 e C698/15, *Tele2 Sverige AB e Secretary of State for the Home Department*; POLLICINO O. – BASSINI M., *La Corte di giustizia e il difficile equilibrio tra sicurezza e privacy*, in *Federalismi.it*, 2017, p. 1 ss.

15 Corte di giustizia, 2 marzo 2021, causa C746/18, *H.K. c. Prokuratuur*; CAIANIELLO M., *Accesso ai tabulati e controllo giurisdizionale nel diritto dell'Unione*, in *Cass. pen.*, 2022, p. 1450 ss.

*SpaceNet*¹⁶, nelle quali la Corte ha ribadito il divieto di *data retention* generalizzata e ha delineato i presupposti di legittimità delle misure di accesso ai dati.

In particolare, la Corte ha affermato la necessità di limitare la conservazione e l'accesso ai dati a ipotesi circoscritte, fondate su criteri oggettivi, temporalmente limitate e sottoposte a controllo preventivo da parte di un'autorità indipendente¹⁷.

È stato inoltre precisato che il livello di tutela deve essere modulato in base alla natura dei dati, richiedendo condizioni più stringenti per quelli maggiormente invasivi, quali i dati di traffico e di localizzazione.

La giurisprudenza più recente conferma tale impostazione, evidenziando come anche l'accesso ai dati relativi agli indirizzi IP possa integrare un'ingerenza grave nei diritti fondamentali, qualora consenta di ricostruire aspetti significativi della vita privata degli utenti.

Nel complesso, emerge un modello europeo di *lawful access* fortemente garantito, nel quale il principio di proporzionalità assume un ruolo centrale nella valutazione della legittimità delle misure di accesso ai dati¹⁸.

Tale evoluzione ha inciso in modo significativo sugli ordinamenti nazionali, generando una crescente tensione tra l'approccio garantista imposto dal diritto dell'Unione e le esigenze operative delle autorità investigative, sempre più confrontate con una riduzione del bacino informativo disponibile.

3. Dalla territorialità del dato alla globalizzazione: trasformazioni strutturali del *lawful access*

Il concetto di *lawful access* si sviluppa storicamente nell'ambito delle tecniche di intercettazione delle comunicazioni, quale strumento volto a consentire alle autorità investigative di acquisire informazioni rilevanti ai fini dell'accertamento dei reati nel rispetto delle garanzie di legge. In tale contesto, esso si configurava come un meccanismo

16 Corte di giustizia, 20 settembre 2022, cause riunite C793/19 e C794/19, *SpaceNet AG e Telekom Deutschland GmbH*; ZICCARDI G., *Data retention e accesso ai dati: gli ultimi approdi della Corte di giustizia*, in *Sistema penale*, 2024, p. 1 ss.

17 POLLICINO O. – BASSINI M., *La Corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto penale contemporaneo*, 2017.

18 BASSINI M., *Sicurezza pubblica e diritti fondamentali nello spazio digitale europeo*, in *Federalismi. it*, 2024, p. 1 ss.

normativamente stabile, fondato su tre presupposti essenziali: la territorialità delle infrastrutture di comunicazione, l'esistenza di obblighi legali di cooperazione in capo agli operatori di rete e la concreta disponibilità tecnica dei dati richiesti.

Questo assetto ha a lungo garantito un equilibrio tra esigenze investigative e tutela dei diritti fondamentali, anche grazie alla previsione di rigorosi presupposti autorizzativi e di controlli giurisdizionali.

L'avvento delle comunicazioni digitali e la progressiva diffusione di *Internet* hanno tuttavia determinato una trasformazione profonda di tale paradigma.

A partire dagli anni Duemila, il traffico comunicativo degli utenti si è progressivamente spostato dalle reti telefoniche tradizionali verso servizi di comunicazione elettronica basati su protocollo *Internet*, gestiti da fornitori globali spesso privi di una presenza giuridicamente rilevante nei singoli ordinamenti nazionali.

Tale evoluzione ha inciso in modo significativo sull'effettività degli strumenti di *lawful access*, segnando il passaggio da un modello fondato sulla disponibilità diretta del dato a uno caratterizzato da una crescente dipendenza da soggetti terzi.

Un primo elemento di discontinuità è rappresentato dalla distinzione tra accesso al contenuto delle comunicazioni e accesso ai dati di traffico (metadati).

Se nel modello tradizionale entrambe le categorie risultavano generalmente disponibili presso gli operatori di telecomunicazioni, nell'ecosistema digitale la disponibilità delle informazioni dipende in larga misura dalle scelte tecniche e commerciali dei *provider*.

Ne deriva uno spostamento del baricentro del *lawful access* dal piano strettamente giuridico a quello dell'architettura tecnologica dei servizi.

Un ulteriore fattore di complessità è rappresentato dalla dissociazione tra il luogo di commissione del reato, quello dell'autorità procedente e quello di conservazione del dato.

L'architettura di *Internet* determina infatti una costante delocalizzazione delle informazioni, che possono essere archiviate su *server* ubicati in Stati diversi, incidendo sui tradizionali criteri di collegamento territoriale del diritto processuale penale. In tale contesto, il dato informatico sfugge a una localizzazione univoca: il *server* può trovarsi in uno Stato, il *provider* avere sede in un altro e l'utente operare in un terzo ordinamento¹⁹.

19 SARTOR V. G., *Il diritto dell'informatica giuridica*, Bologna, Il Mulino, ult. ed., p. 233 ss.; BASINI M., op. cit., p. 102 ss.

Questa frammentazione rende problematica l'individuazione della giurisdizione competente e della legge applicabile, sollevando questioni di sovranità e di rispetto del principio di non ingerenza. Gli strumenti tradizionali di cooperazione giudiziaria internazionale²⁰ si sono rivelati, in molti casi, inadeguati rispetto alle esigenze investigative contemporanee, caratterizzate da rapidità e volatilità del dato.

Da qui l'emergere di modelli alternativi che consentano alle autorità giudiziarie di rivolgersi direttamente ai fornitori di servizi stabiliti o rappresentati in altri ordinamenti.

Tuttavia, tali meccanismi pongono delicati problemi sistematici, in quanto attenuano il ruolo dello Stato di esecuzione e riducono i margini di controllo preventivo da parte delle sue autorità.

Le criticità risultano ancora più evidenti quando il *provider* è stabilito al di fuori dell'Unione europea, poiché l'accesso ai dati dipende dalla cooperazione volontaria dell'operatore o dall'attivazione di strumenti convenzionali, con il rischio di conflitti tra ordinamenti²¹.

Il problema dell'extraterritorialità dei dati costituisce, pertanto, uno snodo centrale del sistema di accesso alle prove digitali, incidendo sia sulla scelta degli strumenti normativi sia sulla definizione delle garanzie applicabili e imponendo un coordinamento sempre più stretto tra dimensione nazionale, unionale e internazionale.

Accanto ai profili di localizzazione del dato, il *lawful access* incontra ulteriori limiti strutturali legati alla concreta disponibilità delle informazioni digitali. In particolare, due fattori incidono in modo determinante sull'effettività dell'accesso: la diffusione della crittografia forte e i vincoli derivanti dalla disciplina della *data retention*.

La crittografia *end-to-end* rappresenta oggi uno dei principali strumenti di protezione della riservatezza delle comunicazioni elettroniche, consentendo che il contenuto dei messaggi sia accessibile esclusivamente ai soggetti comunicanti.

Tale tecnologia impedisce ai *provider* di accedere ai dati in chiaro e rende, in molti casi, tecnicamente inesigibili i provvedimenti di intercettazione.

20 Regolamento (UE) 2023/1543 del Parlamento e Consiglio del 12 luglio '23; Direttiva (UE) 2023/1544 del Parlamento e Consiglio del 12 luglio 2023.

21 MANES V. – LASAGNI G., *Le prove elettroniche nel processo penale europeo*, Milano, Giuffrè, 2020, p. 157 ss.; FALLETTI E., op. cit., p. 61 ss.

Nel modello tradizionale, infatti, l'operatore era in grado di accedere ai contenuti delle comunicazioni, consentendo l'esecuzione degli ordini dell'autorità giudiziaria.

Con l'introduzione della crittografia *end-to-end*, il *provider* non detiene più le chiavi di cifratura e l'intercettazione in transito perde di efficacia, determinando una significativa riduzione della capacità investigativa.

Tale fenomeno è ulteriormente accentuato dall'utilizzo, da parte delle organizzazioni criminali, di dispositivi di comunicazione criptata dedicati, caratterizzati da elevati *standard* di sicurezza e da sistemi avanzati di protezione dei dati. In questi casi, l'acquisizione diretta delle comunicazioni risulta impraticabile e l'attività investigativa si orienta verso l'accesso ai dati archiviati nei *server*, spesso distribuiti su scala globale.

L'accesso a tali informazioni presenta, tuttavia, rilevanti criticità giuridiche e tecniche: da un lato, l'intervento su infrastrutture collocate all'estero; dall'altro, l'acquisizione di grandi volumi di dati, non sempre pertinenti alle indagini, con conseguenti problemi di selezione, analisi e tutela dei diritti fondamentali.

Sul piano giuridico, la diffusione della crittografia impone un delicato bilanciamento tra esigenze di sicurezza e tutela dei diritti fondamentali. Se da un lato essa rappresenta uno strumento essenziale per la protezione della vita privata e della sicurezza informatica, dall'altro lato può determinare una significativa riduzione dell'accessibilità alle informazioni rilevanti ai fini investigativi.

A tale problematica si affianca quella relativa alla durata degli obblighi di conservazione dei dati.

La giurisprudenza della Corte di giustizia²² ha infatti escluso la compatibilità con il diritto dell'Unione di regimi di conservazione generalizzata e indiscriminata, determinando una tensione strutturale tra l'esigenza di limitare l'ingerenza nella sfera privata e la necessità di disporre di dati storici per la ricostruzione dei fatti.

In ambito penal-processuale, ciò si traduce nel rischio concreto di perdita della prova digitale.

22 Corte di giustizia, 8 aprile 2014, cause riunite C293/12 e C594/12, *Digital Rights Ireland Ltd e Kärntner Landesregierung e a.*; FINOCCHIARO G., op. cit., p. 245 ss.; MANTELERO A., *Data retention e diritti fondamentali nel diritto dell'Unione europea*, in *Riv. it. dir. pubbl. com.*, 2017, p. 923 ss.; PIZZETTI F., *La Corte di giustizia e la data retention: verso un nuovo standard europeo di tutela*, in *Dir. inform.*, 2014, p. 689 ss.

Le istituzioni europee hanno finora evitato di imporre obblighi generalizzati di indebolimento della crittografia, consapevoli dei rischi sistemici connessi all'introduzione di meccanismi di accesso privilegiato. Le soluzioni prospettate nel dibattito internazionale evidenziano criticità rilevanti: i sistemi di accesso generalizzato, come le *backdoor* o il *key escrow*, comportano vulnerabilità strutturali, mentre strumenti come il *client-side scanning* sollevano rischi di sorveglianza preventiva.

Le soluzioni maggiormente compatibili con il modello europeo appaiono quelle di tipo mirato, come il cosiddetto *lawful hacking*, che consente l'acquisizione dei dati intervenendo direttamente sul dispositivo dell'indagato, pur presentando profili di elevata intrusività.

Nel complesso, la combinazione tra globalizzazione dei dati, diffusione della crittografia e restrizioni alla *data retention* riduce significativamente l'area delle informazioni effettivamente accessibili alle autorità giudiziarie, configurando una delle principali sfide del *lawful access* nell'ecosistema digitale contemporaneo.

4. Crittografia e disponibilità del dato: il bilanciamento tra sicurezza e diritti fondamentali

Il rapporto tra *lawful access* e crittografia evidenzia una tensione strutturale tra esigenze di sicurezza pubblica, sicurezza informatica e tutela dei diritti fondamentali. Tale tensione rappresenta uno degli snodi centrali dell'attuale dibattito in materia di accesso alle prove digitali.

Le soluzioni di carattere sistemico, quali l'introduzione di *backdoor* o di meccanismi generalizzati di *key escrow*, presentano criticità rilevanti sotto il profilo della proporzionalità, risultando difficilmente compatibili con gli *standard* di tutela delineati dall'ordinamento europeo. In particolare, esse comportano il rischio di vulnerabilità strutturali delle infrastrutture digitali, esponendo i sistemi a possibili abusi e compromettendo la fiducia degli utenti nei servizi di comunicazione.

Diversamente, le soluzioni di tipo mirato, tra cui il cosiddetto *lawful hacking*, pur caratterizzate da un elevato grado di intrusività, appaiono maggiormente coerenti con un modello fondato sul principio di proporzionalità, in quanto consentono di circoscrivere l'interferenza ai soli soggetti sottoposti a indagine, preservando al contempo la sicurezza complessiva dell'ecosistema digitale e garantendo la possibilità di un controllo giurisdizionale puntuale.

In tale prospettiva, la disponibilità del dato si configura oggi come uno dei principali fattori critici del *lawful access*: la combinazione tra diffusione della crittografia avanzata e restrizioni alla *data retention*, così come delineate dalla giurisprudenza della Corte di giustizia dell'Unione europea, determina una significativa riduzione delle informazioni effettivamente accessibili alle autorità giudiziarie.

Ne deriva l'esigenza di individuare soluzioni normative e tecniche idonee a preservare un nucleo minimo di effettività dell'azione investigativa, senza compromettere il livello elevato di tutela dei diritti fondamentali richiesto dall'ordinamento unionale, in un contesto in cui l'equilibrio tra sicurezza e libertà assume una dimensione sempre più complessa e dinamica.

5. Modelli normativi a confronto: *e-Evidence* europeo, *CLOUD Act* e sistema britannico

Nel contesto europeo, la principale risposta normativa alle criticità dell'accesso transfrontaliero alle prove digitali è rappresentata dal cosiddetto pacchetto *e-Evidence*, composto dal regolamento (UE) 2023/1543 e dalla direttiva (UE) 2023/1544.

Il regolamento introduce due strumenti principali: l'ordine europeo di produzione, finalizzato all'acquisizione di dati già conservati entro termini particolarmente stringenti (dieci giorni, ridotti a otto ore nei casi di emergenza), e l'ordine europeo di conservazione, volto a imporre ai prestatori di servizi la preservazione temporanea dei dati digitali in vista di una successiva richiesta. L'elemento innovativo risiede nella possibilità per le autorità giudiziarie di uno Stato membro di rivolgersi direttamente ai fornitori di servizi stabiliti o rappresentati in un altro Stato membro, superando le inefficienze dei tradizionali strumenti di assistenza giudiziaria.

La disciplina distingue tra categorie di dati e prevede condizioni più rigorose per quelle maggiormente invasive, in linea con i principi di necessità e proporzionalità elaborati dalla giurisprudenza della Corte di giustizia. La direttiva (UE) 2023/1544, funzionale all'effettiva operatività del sistema, impone ai prestatori di servizi digitali di designare un rappresentante legale nell'Unione, così da garantire l'esecuzione degli ordini anche nei confronti di operatori *extra-UE*²³.

23 BIARELLA L., *Cooperazione penale e prove digitali: modifica ai Regolamenti UE*, in www.diritto.it, 10 febbraio 2026.

Il nuovo regime, pur rappresentando un significativo avanzamento nella modernizzazione del *lawful access*²⁴, non elimina le criticità derivanti dalla globalizzazione dei servizi digitali. Permangono, infatti, possibili conflitti tra gli obblighi di consegna previsti dal diritto dell'Unione e le limitazioni imposte dagli ordinamenti di Stati terzi. A tal fine, il legislatore europeo ha previsto un meccanismo procedimentalizzato di gestione del conflitto di leggi, che attribuisce all'autorità giudiziaria il compito di valutare la sussistenza e la rilevanza del contrasto normativo.

Resta, inoltre, un limite strutturale legato alla disponibilità tecnica del dato: il regolamento non può imporre la produzione di informazioni che il *provider* non detiene, come nel caso delle comunicazioni protette da crittografia *end-to-end*.

Nel sistema statunitense, l'accesso ai dati investigativi è fortemente influenzato dal *Fourth Amendment*, che tutela i cittadini da perquisizioni e sequestri irragionevoli.

L'elaborazione giurisprudenziale ha sviluppato il criterio della "ragionevole aspettativa di *privacy*", ma la cosiddetta *third-party doctrine* ha storicamente ridotto la protezione per i dati affidati a soggetti terzi, ampliando i margini di intervento delle autorità investigative.

Il quadro normativo si è evoluto a partire dallo *Stored Communications Act* del 1986 fino all'adozione del *CLOUD Act* del 2018, che ha introdotto un principio di extraterritorialità fondato sul controllo del dato da parte del *provider*, indipendentemente dalla sua localizzazione fisica. Il sistema consente inoltre la conclusione di accordi bilaterali per l'accesso diretto ai dati tra autorità e operatori, privilegiando l'efficienza investigativa, pur esponendosi a criticità in termini di conflitti di legge e tutela dei diritti fondamentali²⁵.

Il Regno Unito ha sviluppato un modello particolarmente incisivo, fondato sull'*Investigatory Powers Act* del 2016, successivamente aggiornato nel 2024.

Tale sistema si caratterizza per l'ampiezza dei poteri investigativi, bilanciata da un articolato meccanismo di autorizzazione "a doppia chiave", che prevede sia l'intervento dell'autorità politica sia il controllo giudiziario.

24 TABASCO G., *L'acquisizione transfrontaliera delle prove elettroniche*, in *Riv. Processo penale e giustizia*, 4/2025, p. 965 ss., specifica che sotto il profilo delle garanzie difensive, il pacchetto assicura che il valore probatorio dei dati sia valutato nel rispetto del giusto processo.

25 VENEGONI A., *Crittografia e poteri investigativi*, in *Cass. pen.*, 2021, p. 3140 ss.

La normativa britannica impone obblighi di conservazione dei metadati e di cooperazione tecnica a carico dei fornitori di servizi, rafforzati da una significativa estensione extraterritoriale fondata sul criterio della fruibilità del servizio nel territorio nazionale.

Il sistema è sottoposto al controllo di un'autorità indipendente, l'*Investigatory Powers Commission*, chiamata a garantire il rispetto dei principi di legalità, necessità e proporzionalità.

Le più recenti riforme evidenziano una transizione verso modelli di *intelligence* preventiva e analitica, con un rafforzamento delle capacità operative e una crescente integrazione tra dimensione tecnologica e giuridica.

Tuttavia, tali sviluppi pongono interrogativi rilevanti in ordine alla compatibilità con gli *standard* sovranazionali di protezione dei diritti fondamentali.

Dal confronto tra i tre modelli emerge come il *lawful access* costituisca una questione non solo tecnica, ma eminentemente politica, riflettendo differenti bilanciamenti tra sicurezza e libertà, tra effettività dell'azione penale e tutela della sfera privata, nonché tra sovranità statale e cooperazione internazionale.

In tale contesto, la natura transnazionale dei dati rende sempre più difficile l'applicazione di strumenti giuridici fondati su logiche territoriali.

Ne deriva la crescente centralità della cooperazione internazionale, sia attraverso accordi bilaterali sia mediante strumenti multilaterali, quali la Convenzione di Budapest e il relativo Secondo Protocollo addizionale.

Tuttavia, anche tali strumenti presentano limiti: gli accordi bilaterali, pur garantendo maggiore rapidità, rischiano di frammentare il sistema, mentre gli strumenti multilaterali, sebbene assicurino maggiore uniformità, risultano spesso caratterizzati da maggiore complessità e minore tempestività.

In definitiva, la sfida futura non risiede tanto nell'espansione dei poteri di accesso su base nazionale, quanto nella costruzione di un modello di *governance* internazionale del dato digitale, capace di coniugare efficacia investigativa, tutela dei diritti fondamentali e cooperazione tra Stati in un contesto tecnologico in continua e crescente complessità.

6. Verso un paradigma globale: cooperazione tecnologica e *governance* del dato digitale

Il Simposio di Londra del marzo 2025 ha rappresentato un momento di svolta nel dibattito internazionale sul *lawful access*, segnan-

do il progressivo superamento della tradizionale contrapposizione tra autorità inquirenti e fornitori di servizi digitali e delineando un modello orientato alla cooperazione strutturata su scala globale. In tale sede è stata evidenziata l'inadeguatezza dei sistemi di cooperazione bilaterale, ritenuti non più idonei a operare in un ambiente digitale caratterizzato da elevata volatilità del dato e da una marcata frammentazione geografica.

Elemento centrale del confronto è stato il concetto di "giurisdizione del flusso", volto a riflettere la necessità di adeguare gli strumenti investigativi alla dinamicità delle minacce cibernetiche. In questa prospettiva, il *lawful access* viene progressivamente reinterpretato non come mera espressione di un potere statale, ma come un nucleo essenziale di effettività dell'azione investigativa, da preservare nel rispetto degli *standard* di tutela dei diritti fondamentali.

Tra le proposte più innovative emerse nel corso dei lavori si segnala l'ipotesi di istituzione di una *Digital Clearing House* (DCH) internazionale, concepita come piattaforma tecnologica condivisa per la gestione delle richieste di accesso ai dati.

Tale infrastruttura, configurata come uno "sportello unico" gestito congiuntamente da autorità giudiziarie e Forze di polizia, si propone di razionalizzare e rendere più efficiente il flusso delle richieste, superando le criticità dei modelli basati su relazioni bilaterali.

L'architettura ipotizzata si fonda sull'utilizzo di tecnologie di tipo *distributed ledger*, idonee a garantire la tracciabilità e l'immutabilità delle operazioni, rafforzando l'affidabilità e l'integrità dell'evidenza digitale lungo l'intero ciclo di vita probatorio.

In tale contesto, la piattaforma assumerebbe la funzione di infrastruttura fiduciaria, volta a standardizzare le procedure e a rendere trasparente l'esecuzione degli ordini di produzione dei dati.

Particolare attenzione è stata dedicata alle implicazioni derivanti dalla diffusione della crittografia *end-to-end*.

Le soluzioni prospettate si orientano verso approcci che evitino l'indebolimento dei sistemi di sicurezza, privilegiando invece tecnologie avanzate, quali la crittografia omomorfica, che consente l'elaborazione dei dati senza necessità di decrittazione.

Tale approccio permetterebbe, almeno in via teorica, di coniugare esigenze investigative e tutela della riservatezza, limitando l'accesso ai soli risultati dell'analisi.

Ulteriore profilo emerso riguarda la necessità di adottare protocolli di sicurezza *post-quantum*, al fine di garantire la tenuta nel tempo

dell'evidenza digitale rispetto all'evoluzione delle capacità computazionali. In questa prospettiva, la preservazione dell'integrità e della utilizzabilità processuale dei dati assume una dimensione prospettica, legata allo sviluppo tecnologico futuro.

Le innovazioni tecnologiche richiedono, inoltre, un adeguamento dei modelli organizzativi.

In particolare, è stata prospettata l'evoluzione delle tradizionali figure di collegamento verso modelli più avanzati di cooperazione interforze, fondati su competenze specialistiche nella gestione della sovranità del dato e nella mediazione tra ordinamenti.

Tali figure sarebbero chiamate a operare all'interno di strutture permanenti di coordinamento, con funzioni di facilitazione e integrazione operativa.

Nel complesso, le riflessioni emerse delineano un passaggio da un modello reattivo e frammentato a un sistema integrato e proattivo, nel quale l'efficacia del *lawful access* dipende sempre più dall'interazione tra innovazione tecnologica, coordinamento istituzionale e cooperazione internazionale.

7. Verso un modello sistemico di sicurezza digitale: prospettive e proposte di riforma

L'analisi svolta evidenzia come il *lawful access* si collochi oggi al centro di una trasformazione profonda, determinata dall'evoluzione tecnologica e dalla globalizzazione dei servizi di comunicazione elettronica.

In tale contesto, il modello tradizionale di accesso ai dati deve ritenersi ampiamente superato.

Ne deriva una significativa riduzione della disponibilità immediata del dato investigativo, dovuta sia a limiti di natura tecnica – in particolare connessi alla diffusione della crittografia *end-to-end* – sia a criticità giuridiche, quali i conflitti di giurisdizione e le difficoltà di esecuzione delle misure nei confronti di fornitori stabiliti in Stati terzi.

Il percorso ricostruttivo fin qui delineato trova nel Simposio di Londra del marzo 2025 un punto di sintesi che assume rilevanza non solo teorica, ma anche operativa e strategica, evidenziando la necessità di superare l'attuale frammentazione degli strumenti normativi e dei modelli di cooperazione.

In tale prospettiva, appare necessario delineare un modello sistemico di sicurezza digitale fondato su direttrici di intervento coordinate.

In primo luogo, si impone l'esigenza di promuovere un quadro normativo multilaterale in materia di accesso alle prove digitali, idoneo a superare la frammentazione derivante dagli accordi bilaterali.

L'adozione di un trattato globale sull'*e-Evidence*, eventualmente nell'ambito delle Nazioni Unite o attraverso un'evoluzione della Convenzione di Budapest, consentirebbe di introdurre *standard* comuni fondati su un principio di reciprocità garantista, riducendo il rischio di conflitti di giurisdizione e di fenomeni di *forum shopping* investigativo.

In secondo luogo, si prospetta la necessità di sviluppare infrastrutture tecnologiche condivise a livello internazionale.

In tale ottica, l'istituzione di un *hub* tecnologico interforze permanente, ispirato al modello della *Digital Clearing House*, potrebbe favorire la standardizzazione e la tracciabilità delle richieste di accesso ai dati. L'adozione di tecnologie avanzate per la gestione della catena di custodia digitale consentirebbe di rafforzare le garanzie di integrità, verificabilità e trasparenza dell'attività investigativa.

In terzo luogo, emerge l'esigenza di promuovere un approccio di "*privacy by design*" in ambito investigativo, volto a integrare sin dalla fase di progettazione dei sistemi tecnologici soluzioni compatibili con l'accesso legittimo ai dati, senza compromettere la sicurezza complessiva delle infrastrutture digitali.

In tale prospettiva, assumono particolare rilievo gli investimenti in tecnologie avanzate, quali la crittografia omomorfa e i sistemi di sicurezza *post-quantum*, che consentono di coniugare esigenze investigative e tutela dei diritti fondamentali.

In definitiva, le riflessioni sviluppate, anche alla luce delle prospettive emerse nel Simposio di Londra, evidenziano la necessità di una evoluzione del ruolo delle istituzioni e degli operatori della sicurezza.

Il coordinamento interforze è chiamato ad assumere una funzione sempre più strategica, non solo sul piano operativo, ma anche quale presidio dell'equilibrio tra efficacia dell'azione investigativa e tutela dei diritti fondamentali nell'ambiente digitale²⁶.

Il *lawful access* si configura, pertanto, come uno dei principali ambiti nei quali si misura la capacità degli ordinamenti contemporanei di governare l'innovazione tecnologica, preservando i valori fondamentali dello Stato di diritto²⁷.

26 POLLICINO O., *Recuperare la sovranità nell'era delle piattaforme*, Milano, EGEA, 2023, p. 205 ss.

27 Sul punto, *ex multis*, GILIBERTI G., *Privacy e sicurezza*, in *Polizia Moderna*, settembre 2025.

Parte III
Voci dall'Aula

“L’approccio amministrativo per il contrasto al crimine. La soluzione adottata dall’Italia e quella proposta dall’Unione europea”.

di Filippo Vanni*

*“Egredi studenti,
forse l’egregio signor Sciascia con cui comincia la vostra lettera
voleva essere un segno di distanza; ma io vi ricordo che la parola egregio,
ormai usurata e banale, originariamente indica una distinzione
che mi piace ed accetto: l’essere fuori dal gregge.
E vi rispondo dunque chiamandovi con sentimento egregi:
speranza ed augurio che veramente lo siate [...]”.*

*Ricordate che la mafia è violenza, la mafia è negazione del diritto:
non la si può combattere con la violenza e con la negazione del diritto
senza rischiare che il cittadino, tra le due parti,
scelga quella che appare più forte”.*

L. Sciascia, lettera a studenti

Premessa

Per ragioni storiche che sono ancora indagate e su cui non vi sono univoci approdi, certa parte della criminalità italiana si è negli anni trasformata – a differenza di quanto accaduto in altri Stati europei dove è rimasta destrutturata – in crimine organizzato di tipo mafioso. Personalmente sono propenso a considerare che tale “evolu-

* Colonnello dell’Arma dei Carabinieri, già frequentatore del XL Corso di Alta Formazione presso la Scuola di Perfezionamento per le Forze di Polizia.

zione" sia stata strettamente legata alle modalità con cui è nato il nostro Stato unitario, all'atteggiamento aggressivo e impositivo di alcune aree del Paese rispetto ad alcune regioni del sud, che ha determinato la nascita di un sentimento di sfiducia verso le nascenti istituzioni statali, a tutto vantaggio delle consorterie criminali locali che invece si sono dimostrate capaci di garantire ordine e, in un certo senso, persino un embrione di amministrazione della giustizia.

Quando vi era più bisogno di affidabilità da parte delle istituzioni chiamate a far rispettare la legge, dunque, sono mancati i riferimenti essenziali degli attori pubblici a questo preposti per mandato, rafforzando una gestione parallela e informale dell'"*enforcement*" delle regole poste a base della convivenza civile. Infatti, la caratteristica comune alle tre principali organizzazioni criminali mafiose nazionali è sempre stata quella di riuscire a trasformare i propri interessi in valori, al fine di ottenere l'approvazione di parti numericamente sempre più rilevanti della società civile. Lo sviluppo di queste moderne "Gorgoni", apparentemente seducenti ma cariche di conseguenze terribili per chi ne fosse stato irretito, è stato probabilmente sottovalutato dapprincipio da parte delle Forze di polizia e dell'autorità giudiziaria nelle fasi iniziali di gemmazione, cosicché, rafforzandosi e irrobustendosi progressivamente, hanno reso infine evidente la loro effettiva e temibile esistenza ma allo stesso modo difficilissimo il loro decisivo contrasto. Oggi appare del tutto chiaro che la lotta ai fenomeni criminali di tipo mafioso non possa prescindere dalla comprensione della loro "funzione" territoriale, prima ancora che della loro struttura organizzativa: un passaggio, questo, senza il quale appare difficile, laddove non impossibile, contrastarli coi "soli" strumenti del diritto.

Sui limiti del processo penale per il contrasto del crimine organizzato di tipo mafioso

Nonostante le indiscutibili evoluzioni della normativa penale, con particolare riferimento alle fattispecie per il contrasto delle associazioni criminali anche di tipo mafioso, la struttura e i riti del processo presentano alcune limitazioni intrinseche quando si tratta di contrastare efficacemente tali gravi manifestazioni antisociali.

Uno dei principali problemi connessi con lo strumento del processo è la sua "natura reattiva". Esso, infatti, si attiva evidentemente solo "a valle" di un reato commesso e appreso dall'autorità giudiziaria, di polizia giudiziaria o da quelle che alla prima hanno obbligo di riferire. Tuttavia, la

criminalità organizzata opera spesso in modi che minimizzano la visibilità, la tracciabilità dei reati e la capacità di ricerca delle relative fonti di prova, sfruttando reti comunicazione peculiari e segrete tra gli associati, il vincolo associativo e la forza di intimidazione e di assoggettamento che costituiscono gli elementi costitutivi della fattispecie *ex art. 416-bis* Codice penale.

In tale quadro, una difficoltà significativa è costituita dall'onere probatorio. Nel processo penale, infatti, l'accusa deve dimostrare la colpevolezza "oltre ogni ragionevole dubbio" ed è facile comprendere come nei contesti di criminalità organizzata raccogliere prove sufficienti per soddisfare questo *standard* possa essere estremamente difficile, date le peculiari caratteristiche e la complessità strutturale di questa forma di criminalità, nonché la complessità di raccogliere fonti di prova testimoniali robuste e attendibili¹.

Per affrontare queste sfide, l'Italia, negli anni, ha sviluppato e implementato un *parterre* di strumenti di carattere "amministrativo" denominato misure di prevenzione, rivolte sia alla persona che al patrimonio, con l'intento originario di completare e rafforzare la risposta dello Stato alla minaccia mafiosa.

Queste misure sono progettate infatti per essere più flessibili rispetto al processo penale tradizionale, riposando su *standard* probatori decisamente più blandi, ancorati ad una (possibilmente solida) base indiziaria ma non alle fonti di prova tipiche del processo. Le misure patrimoniali, in particolare, mirano a colpire il cuore economico delle organizzazioni anche di tipo mafioso, interrompendo i flussi finanziari che alimentano e sostengono l'attività criminale e riuscendo in tal modo a intaccare la loro capacità operativa senza dover attendere l'esito delle lunghe e complesse procedure penali.

L'integrazione delle misure preventive nel quadro giuridico italiano ha dunque rappresentato dalla sua nascita una risposta necessaria e complessa a un fenomeno come quello mafioso, che non poteva essere combattuto efficacemente solo con mezzi tradizionali. Queste misure rappresentano ancora oggi un approccio proattivo, complementare al processo, per il depotenziamento delle organizzazioni criminali².

1 Seguire le transazioni finanziarie, in questo quadro, è il vero strumento per tentare di vincere uno scontro da sempre asimmetrico contro il potere mafioso, giacché sul piano penale "non ci saranno mai prove sufficienti, il silenzio degli onesti e dei disonesti lo proteggerà sempre". Così SCIASCIA L., *Il giorno della civetta*.

2 In un'ottica di lungo termine, evidentemente, la lotta alla mafia richiede un impegno costante da parte di tutte le componenti della società civile, incluse tutte le istituzioni centrali e territoriali, il settore privato e i cittadini. La trasparenza, l'efficienza amministrativa e la

CAPITOLO I

Le misure di prevenzione nell'ordinamento italiano

1. La genesi delle misure di prevenzione

Come si è detto, le misure di prevenzione costituiscono, nel nostro ordinamento giuridico, un binario parallelo rispetto al più noto sistema processuale penale e sono disciplinate da regole specifiche, di gran lunga meno garantiste rispetto a quelle che disciplinano il processo e la fase di indagine preliminare.

La tempistica impiegata dal sistema giudiziario per infliggere condanne definitive e la sempre crescente importanza data dagli organi inquirenti all'individuazione e al sequestro ai fini di confisca dei patrimoni ottenuti commettendo delitti, ha reso sempre più interessante ed investigativamente remunerativo l'utilizzo del "binario" delle misure di prevenzione, in particolar modo di quelle di carattere patrimoniale³.

A premessa, si rappresenta che l'attività legislativa degli anni 2008 e 2009 ha determinato la creazione di una piattaforma normativa basata su tre corpi: la legislazione originaria contenuta nel provvedimento quadro n. 1423 del 1956 (che *ab origine* ha introdotto le misure di prevenzione), la legge n. 575 del 1965 (che contiene disposizioni contro la criminalità mafiosa) e da ultimo la legge n. 152 del 1975 (cd legge Reale), nata in un'epoca molto particolare della storia della nostra Repubblica, che contiene le disposizioni che più interessano in questa sede agli articoli 18, 19, 20, così come modificati dal cd "provvedimento sicurezza" dell'anno 2008 (d.l. n. 92/2008).

Ora, se già in materia esisteva il cd "doppio binario", che sanciva la sostanziale indipendenza del procedimento penale da quello di prevenzione, dal 2008 la strada del procedimento di prevenzione si è ulteriormente sdoppiata con la separabilità di fatto del procedimento che irroga la misura di prevenzione personale da quello che decreta la misura patrimoniale.

L'art. 19 della legge Reale prevedeva che le disposizioni relative alle misure di prevenzione patrimoniali contenute nella legge antimafia n. 575/1965 si applicano "...anche alle persone indicate nell'articolo 1,

partecipazione attiva dei cittadini sono elementi cruciali per costruire una cultura di legalità e di fiducia nello Stato nel suo complesso.

3 Per un approfondimento sul tema, VANNI F., *Modifiche alla disciplina delle Misure di Prevenzione Patrimoniali: un altro binario nel doppio binario*, su www.filodiritto.com, 24 giugno 2010.

numeri 1) e 2) della legge 27 dicembre 1956, n. 1423". Competente all'istruzione della pratica di prevenzione, secondo la deroga introdotta dal "pacchetto sicurezza 2008", è il Procuratore della Repubblica del circondario nel quale dimora il soggetto proposto; rimane la competenza del procuratore distrettuale solo per i soggetti indiziati di appartenere a sodalizio criminale di tipo mafioso.

La legge n. 125/2008, di conversione del citato provvedimento-sicurezza, ha tuttavia previsto anche l'abrogazione di una parte dell'altra fondamentale norma in materia di lotta alla criminalità mafiosa ed organizzata in genere: la legge n. 55 del 1990, che all'art. 14 recitava: "salvo che si tratti di procedimenti di prevenzione già pendenti alla data di entrata in vigore della presente legge, da tale data le disposizioni della legge 31 maggio 1965 n. 575, concernenti le indagini e l'applicazione delle misure di prevenzione di carattere patrimoniale..." di cui alla normativa quadro antimafia (legge n. 575 del 1965), si applicano oltre che agli indiziati di appartenere a sodalizi criminali di tipo mafioso, anche ai soggetti "... indicati nel numero 2) del primo comma dell'art. 1 della legge 27 dicembre 1956 n. 1423 ..." solo nella misura in cui abbiano tratto profitto dai delitti previsti e puniti dagli artt. 600, 601, 602, 629, 630, 644, 648-bis e *ter* Codice penale e dal contrabbando di T.L.E. (ovvero riduzione o mantenimento in schiavitù o in servitù, tratta di persone, acquisto e alienazione di schiavi, estorsione, sequestro di persona a scopo di estorsione, usura, riciclaggio, impiego di denaro beni o altra utilità di provenienza illecita e contrabbando di tabacchi lavorati esteri).

In sostanza questa norma introduceva una disposizione di carattere limitativo riguardo all'applicazione delle misure di prevenzione patrimoniali, consentendone la proposta su soggetti "a pericolosità generica" solo se avessero tratto i loro illeciti profitti dalla serie di reati sopra menzionati (lasciando ovviamente salva l'applicazione delle misure patrimoniali di cui agli artt. 2-bis e *ter* della legge n. 575/1965 a tutti i soggetti connotati dalla cd "pericolosità qualificata", ovvero indiziati di far parte di sodalizi criminali mafiosi).

Con tale abrogazione, è tornato vigente l'art. 19 della legge Reale che, come detto, estende a tutti i "genericamente pericolosi" di cui all'art. 1 nn. 1 e 2 della legge 1423/1956 l'applicabilità delle misure di prevenzione patrimoniale una volta riservate ai soli mafiosi dalla legge antimafia del 1965⁴.

4 Sul punto è chiarissima la Corte di cassazione, sez. I penale, n. 6000/2009: l'art. 14 della legge 55/1990 era speciale rispetto alla più generica portata dell'art. 19 della legge Reale

Ciò posto, dunque, i soggetti destinatari della severa normativa in materia di prevenzione patrimoniale sono quelli catalogati nelle prime due categorie di cui all'art. 1 della legge n. 1423/1956: "coloro che debba ritenersi, sulla base di elementi di fatto, che siano abitualmente dediti a traffici delittuosi" e "coloro che per condotta ed il tenore di vita debba ritenersi, sulla base di elementi di fatto, che vivano abitualmente, anche in parte, con i proventi di attività delittuose".

Nei confronti di questa duplice categoria di soggetti, abrogata la limitazione posta dall'art. 14 della legge n. 55/1990, sono quindi proponibili le misure di prevenzione patrimoniali da richiedere ad opera del Procuratore della Repubblica del circondario entro il quale dimora il proponendo.

Un altro intervento molto significativo in materia, sempre dovuto al citato pacchetto sicurezza 2008, è l'inserimento del comma 6-*bis* nell'art. 2-*bis* della legge antimafia del 1965. Una modifica di portata rilevante: "le misure di prevenzione personali e patrimoniali possono essere richieste e applicate *disgiuntamente*, e per le misure di prevenzione patrimoniali, *indipendentemente* dalla pericolosità sociale del soggetto proposto per la loro applicazione al momento della richiesta della misura di prevenzione...".

La prima parte del nuovo comma costituisce senz'altro una novità normativa, ma non una novità applicativa, perché l'orientamento giurisprudenziale già si era diretto nel senso di un'applicazione disgiunta delle due misure. La novità assoluta è un'altra: le misure di prevenzione patrimoniali possono essere richieste ed applicate indipendentemente dalla pericolosità sociale del soggetto proposto al momento della richiesta. Entrambe queste innovazioni sono poi state recepite in pieno dal vigente Codice delle leggi antimafia.

All'interno di questo secondo binario "preventivo" si crea dunque un'ulteriore facilitazione applicativa che consente di prescindere dal significativo requisito dell'attuale pericolosità sociale del proposto. La pericolosità sociale deve essere certamente accertata, ma non è necessario che essa sia ancora in essere (la non necessaria attualità vale

n. 152/1975. La legge n. 55/1990, sostiene la Suprema Corte, si poneva dunque in rapporto derogatorio quale *lex specialis posterior*, rispetto alla legge Reale citata, che aveva certamente il compito di "... restringere il margine di operatività delle misure di prevenzione patrimoniali ... concentrando l'attività di indagine sui casi più gravi...". Con l'entrata in vigore del provvedimento sicurezza 2008, e la conseguente abrogazione dell'art. 14, non può che rivivere nella sua pienezza – conclude la Corte – l'operatività della norma generale, che non è mai stata modificata o abrogata.

esplicitamente solo per le misure di prevenzione patrimoniali, poiché le personali continuano a pretendere – anche col vigente assetto normativo – l’attualità del pericolo per la sicurezza pubblica).

Invero, è stato rilevato in dottrina come da quando è divenuta possibile l’applicazione disgiunta delle due tipologie di misure, quelle personali hanno finito per perdere quella non trascurabile utilità marginale prima correlata alla conseguente richiesta di un provvedimento patrimoniale⁵; se ne desume quindi come il legislatore, con tali innovativi provvedimenti, abbia voluto spostare il suo interesse dalla *pericolosità del soggetto* alla *pericolosità del patrimonio*.

Un cenno a parte merita la distanza che la legge, prima, e la giurisprudenza, poi, hanno posto tra gli “elementi indiziari” richiesti per giungere a un’affermazione di responsabilità penale e gli “elementi di fatto” richiesti dalla legge quadro sulle misure di prevenzione del 1956, dal momento che i secondi si sottraggono – proprio per il diverso “binario” seguito dai due procedimenti – alle tre note regole processuali per la valutazione degli elementi di prova: l’art. 192 Codice di procedura penale, che richiede indizi gravi, precisi e concordanti (ovvero consistenti, correlati con il fatto da provare e convergenti tra loro) e il riscontro esterno alle dichiarazioni di collaboratori di giustizia o chiamanti in correità a conferma dell’attendibilità del racconto. A tale ultimo riguardo, va precisato che l’assunzione di queste dichiarazioni non esonera comunque il giudice della prevenzione dall’ordinario vaglio di attendibilità e credibilità cd “intrinseca” (dunque diversa dalla ricerca dei riscontri esterni), che costituisce presupposto necessario a determinare il valore probatorio del narrato⁶.

Un rapido esame, sempre in quest’ambito, merita l’utilizzabilità degli elementi acquisiti nell’indagine penale all’interno del procedimento di prevenzione. Statuisce in proposito Cassazione sez. unite penali 9 aprile 2010 n. 13426, traendo spunto dal caso specifico dell’utilizzabilità di intercettazioni telefoniche ed ambientali di procedimenti penali, che solo gli atti che possono fare legittimamente ingresso nel processo penale possono essere fruibili nel procedimento di prevenzione.

Così, come nel caso esaminato dalla Suprema Corte, intercettazioni processualmente non utilizzabili perché autorizzate in vio-

5 CATENACCI M., *Le misure personali di prevenzione fra “critica” e “progetto”: per un recupero dell’originaria finalità preventiva*, in *Rivista italiana di diritto e procedura penale*, fasc. 2, 1° giugno 2017, p. 526.

6 Tra le altre, si vedano Cass. n. 20160/2011 e n. 49853/2013.

lazione dell'art. 268 Codice di procedura penale, siccome tacciate di "patologica inutilizzabilità", non possono fare legittimo ingresso nel procedimento preventivo. Ergo, possono trarsi dal procedimento penale tutti gli elementi che si ritengono utili alla finalità di prevenzione, purché non siano stati acquisiti in violazione di legge. Un passaggio testuale della sentenza sarà ancora più chiarificatore: "...A proposito, poi, della "fenomenologia" della inutilizzabilità [...] la giurisprudenza di questa Corte ha in più occasioni teso a distinguere tra una inutilizzabilità "patologica", quale è quella che deriva dalla violazione di divieti probatori, ed una inutilizzabilità definita "fisiologica", in quanto correlata alle caratteristiche del processo ed alla distinzione tra atti delle indagini e prove dibattimentali [...]. È evidente che per quest'ultima non si pongono problemi di sorta circa la possibilità di "utilizzare", come elementi di valutazione e di giudizio, anche gli atti delle indagini ai fini del processo di prevenzione, posto che i "limiti" sono soltanto interni ed esclusivi al procedimento penale [...]"

Il vero tratto distintivo che qualifica l'autonomia del procedimento di prevenzione dal processo penale va intravisto nella diversa "grammatica probatoria" che deve sostenere i rispettivi giudizi: una diversità, però, che, proprio in quanto riferita esclusivamente al "modo d'essere" degli elementi di apprezzamento del "merito", non incide affatto sulla legittimità delle acquisizioni, a prescindere - evidentemente - dalla sede in cui le stesse siano operate. La prova inutilizzabile, ad esempio perché acquisita in violazione dell'art. 188 del codice di rito, non può "proiettarsi" sul terreno della prevenzione, al pari di qualsiasi altra ipotesi di prova "illegale", in quanto assunta in contrasto con i divieti di legge.

Questo si deve tenere ben presente quando si argomenta sul concetto di "autonomia" dei procedimenti.

In merito ai beni che possono essere oggetto di possibile sequestro e confisca va precisato che il legislatore in tema di misure di prevenzione non parla di illecita provenienza, ma di *illegittima* provenienza. In tema di confisca come misura di sicurezza ai sensi dell'abrogato art. 12-*sexies* del d.l. n. 306/1992⁷, possono formare oggetto del provvedimento "...denaro, beni o altre utilità di cui il condannato non può giustificare la provenienza e di cui, anche per interposta persona fisica o giuridica, risulta essere titolare o avere la disponibilità a qualsiasi

⁷ Oggi confluito nell'art. 240-*bis* Codice penale.

titolo in valore sproporzionato al proprio reddito, dichiarato ai fini delle imposte sul reddito, o alla propria attività economica”.

Nessun arco temporale di riferimento, dunque, e nessun nesso di pertinenzialità che possa fermare l'apprensione del patrimonio illecitamente accumulato con la citata misura di sicurezza.

Nel procedimento di prevenzione la giurisprudenza, nel merito, non è sempre stata uniforme. Hanno argomentato vari tribunali che l'affinità tra la confisca speciale prevista dal citato art. 12-*sexies* e la confisca quale misura di prevenzione antimafia all'epoca prevista dall'art. 2-*ter* della legge n. 575 del 1965 consentirebbe di concludere che quest'ultimo modello sia stato largamente mutuato dall'art. 12-*sexies*; con la sentenza Montella (Cass. Sez. Unite penali n. 920/2003) la Suprema Corte ha appunto ribadito che l'art. 12-*sexies* citato configura "... una misura di sicurezza atipica con funzione anche dissuasiva parallela all'affine misura di prevenzione antimafia introdotta dalla legge del 1965 n. 575”.

Secondo questo orientamento, quindi, va considerato irrilevante sia il nesso di pertinenzialità tra i beni in sequestro ed il compendio indiziario a fondamento della misura di prevenzione, che il rapporto di connessione temporale tra l'attività criminale e l'acquisizione dei beni oggetto del provvedimento reale (nel senso anche Corte Cass. Sez. Unite n. 29022/2001).

Queste informazioni di storia legislativa sono utili a comprendere da quali basi è nato il Codice delle leggi antimafia, che oggi costituisce il testo compilativo (e in parte innovativo) che contiene l'intero apparato di prevenzione. Per concludere, un brevissimo cenno anche alla legge n. 646 del 1982, meglio nota come “Rognoni – La Torre”, secondo cui (art. 16) il procuratore della Repubblica del luogo dove le operazioni debbono essere eseguite, può autorizzare gli ufficiali di polizia giudiziaria ad intercettare comunicazioni o conversazioni telefoniche, quando lo ritenga necessario al fine di controllare che le persone nei cui confronti sia stata applicata una delle misure di prevenzione previste dall'articolo 3 della legge 27 dicembre 1956, n. 1423, non continuino a porre in essere attività o comportamenti analoghi a quelli che hanno dato luogo all'applicazione della misura di prevenzione (norma poi interamente confluita nel Codice antimafia).

Siamo dunque in presenza di una variante delle ccdd “intercettazioni preventive”, già autorizzabili ad esempio per la prevenzione dei delitti commessi con finalità di terrorismo ed eversione. Come per le preventive, infatti, in carenza di un provvedimento autorizzativo giurisdizionale, “... Gli elementi acquisiti attraverso le intercettazioni

possono essere utilizzati esclusivamente per la prosecuzione delle indagini e sono privi di ogni valore ai fini processuali”.

Le registrazioni debbono essere trasmesse al procuratore della Repubblica che ha autorizzato le operazioni, il quale dispone la distruzione delle registrazioni stesse e di ogni loro trascrizione, sia pure parziale” (art. 16 legge citata e ora art. 78 del D.Lgs. n. 159/2011).

Ciò nondimeno, anche tenendo ben presente l’insanabile vizio di inutilizzabilità che geneticamente affligge questo tipo di ascolti, ne è evidente la valenza investigativa, che va ad arricchire il ricco panorama di indizi, elementi di fatto e metodi per la loro ricerca del lungo alternativo “binario” delle misure di prevenzione.

2. Le misure del Codice delle leggi antimafia. Fondamento costituzionale e funzione parasanzionatoria e restitutiva

Con la legge 13 agosto 2010, n. 136 il Governo è stato delegato ad emanare un decreto legislativo recante il Codice delle leggi antimafia e delle misure di prevenzione, con il compito di effettuare una completa ricognizione delle norme antimafia di natura penale, processuale e amministrativa, nonché la loro armonizzazione e coordinamento anche con la nuova disciplina dell’Agenzia nazionale per l’amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata. Il decreto adottato è suddiviso in quattro diversi libri: - Libro I: Le misure di prevenzione; - Libro II: La documentazione antimafia; - Libro III: Le attività informative ed investigative nella lotta contro la criminalità organizzata. L’amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata; - Libro IV: Modifiche al codice penale e alla legislazione penale complementare.

Occorre a questo punto riflettere su cosa debba intendersi per “prevenzione”, termine che ricorre per oltre 150 volte nel testo del Codice delle leggi antimafia (D.Lgs. n. 159/2011), ma di cui non viene data alcuna definizione. In dottrina è stato rilevato come la prevenzione, e così la repressione, riguardi tutti gli istituti predisposti dall’ordinamento per evitare che un comportamento contrario alla legge si verifichi o si ripeta⁸. In questo senso, dalla lettura combinata degli artt. 4 e 8 del Codice si potrebbe ricavare che la prevenzione consista nell’e-

8 FURFARO S., *La prova nel processo di prevenzione: lineamenti*, in *Archivio Penale*, 2022, n. 1.

sigenza di scongiurare, attraverso le prescrizioni dell'art. 8, la reiterazione dei delitti presupposto di cui all'art. 4.

Dopo la nota sentenza CEDU De Tommaso c. Italia del 23 febbraio 2017 in materia di misure di prevenzione, invero si è parlato di una prima "crepa" nel sistema, in relazione alla segnalata incompatibilità delle misure di prevenzione con i principi sovranazionali, con specifico riguardo ai casi di cd "pericolosità generica", ovvero sia quella pericolosità fondata sul giudizio probabilistico che il soggetto possa concretamente compiere in futuro azioni delittuose.

La Corte costituzionale, tuttavia, poco tempo dopo ha ribadito che la confisca di prevenzione "[...] *in assenza di connotati afflittivi ulteriori*" rispetto all'ablazione di un arricchimento illecito, ha un valore meramente ripristinatorio dello *status quo ante*, ovvero precedente all'illecita acquisizione del bene⁹.

Al riguardo, anche convenendo sul fatto che di diritto penale non si tratta e che quella forma di confisca "ripristina" anziché "punire", la compressione di diritti costituzionalmente presidiati consiglia di individuare un livello di garanzie proporzionato alla gravità degli effetti prodotti.

Per vero, non vi è chi non noti il silenzio serbato dalla stessa Costituzione alla materia della prevenzione dei reati e alla loro compatibilità coi diritti e le libertà. Le misure *ante delictum* hanno sempre dimostrato una grande duttilità applicativa, venendo per questo utilizzate per reprimere il fenomeno del brigantaggio, prima, ed alcune forme di dissenso politico, poi. Successivamente, con l'avvento del fascismo, fu fatto largo uso di strumenti di prevenzione quali l'ammonizione e il domicilio coatto, come strumenti "integrativi" del sistema repressivo penale.

La prima volta che la Corte costituzionale ha scritto di "*misura amministrativa finanziaria a carattere restitutorio e riparatorio*" lo ha fatto con riguardo alla confisca dei beni "totale e senza eccezione" a carico di gerarchi fascisti e di coloro che si erano resi responsabili di collaborazionismo con l'invasore tedesco¹⁰. (Anche) in quel caso, la Consulta ha dichiarato infondata la questione, giacché la misura in sindacato manifestava "chiaramente la sua natura non penale attraverso i caratteri" attribuiti dalla legge, "che si riassumono essenzialmente nell'applicabilità della confisca anche dopo l'estinzione del reato e anche in confronto degli eredi".

⁹ C.Cost. n. 24/2019.

¹⁰ C.Cost. n. 29/1961 e n. 46/1964.

Ciò nondimeno, dopo queste pronunce, la stessa Corte arrivò a dichiarare l'illegittimità costituzionale della legge quadro sulle misure di prevenzione (la già citata n. 1423 del 1956) nella parte in cui ne consentiva l'applicazione ai cd "proclivi a delinquere"¹¹. L'aspetto interessante riguarda il perimetro costituzionale ritenuto violato, ovvero gli artt. 13 e 25 Cost.: "in coerenza con le precedenti decisioni di questa Corte, va ribadito che la legittimità costituzionale delle misure di prevenzione in quanto limitative, a diversi gradi di intensità, della libertà personale è necessariamente subordinata all'osservanza del principio di legalità e alla esistenza della garanzia giurisdizionale. Si tratta di due requisiti ugualmente essenziali ed intimamente connessi, perché la mancanza dell'uno vanifica l'altro"¹². Si potrebbe considerare che questa sia stata la prima e ultima volta in cui, implicitamente, la Consulta abbia riconosciuto le misure di prevenzione come misure "assimilabili" a quelle di carattere penale. La Corte, infatti, non si è mai più pronunciata in questo senso, anzi – assieme alla Corte di cassazione – ha *hic hinde* considerato esplicitamente tali strumenti come misure amministrative.

Dunque, se per alcuna dottrina e per la giurisprudenza¹³ deve individuarsi nell'art. 25, comma 3, Cost. il fondamento del potere di prevenzione da parte dello Stato è certamente l'art. 27 Cost. a rimanere per anni al di fuori della disciplina delle misure di prevenzione. Difettando di un comportamento giuridicamente illecito da porre alla base, e caratterizzandosi quindi per una finalità esclusivamente preventiva, le misure in esame non appaiono in nessun modo contaminate dalla prospettiva rieducativa¹⁴.

Con la nota sentenza n. 364/1988, riferita all'inescusabilità dell'ignoranza della legge penale, la Corte costituzionale ha integrato il

11 C.Cost. n. 177/1980.

12 E ancora: "l'intervento del giudice (e la presenza della difesa, la cui necessità è stata affermata senza riserve) nel procedimento per l'applicazione delle misure di prevenzione non avrebbe significato sostanziale [...] se non fosse preordinato a garantire, nel contraddittorio tra le parti, l'accertamento di fattispecie legali predeterminate".

13 ZUFFADA E., in *disCrimen* del 17 settembre 2021, secondo cui, peraltro, "la 'timidezza' mostrata negli anni dalla Corte costituzionale lasci intravedere [...] l'estrema cautela nel valutare i profili di (in)costituzionalità di misure che, nel corso del tempo, sono "rifiorite" come efficaci strumenti antimafia". Per la giurisprudenza, si veda C.Cost. n. 27/1959 e 177/1980. Nell'opinione dei giudici costituzionali le misure di sicurezza condividono con le misure di prevenzione il loro "oggetto", e cioè la pericolosità sociale del soggetto destinatario.

14 Di "canone inverso rispetto ai principi di colpevolezza e di rieducazione di cui all'art. 27 Cost." parla BRIZZI F., *Dalla prevenzione bellica a quella riparativa*, Key editore, p. 87.

disposto dell'art. 5 Codice penale ponendo un limite alla concezione dell'"illuministica maestà della legge", per garantire agli individui di essere chiamati a rispondere penalmente solo per azioni da essi controllabili e mai per comportamenti realizzati nella non colpevole e, pertanto, inevitabile ignoranza del precetto. Dunque, con l'espressione "responsabilità penale personale" deve intendersi "responsabilità per un fatto umano, proprio, tipico, offensivo e *colpevole*", talché "comunque si intenda la funzione rieducativa della pena, essa postula almeno la colpa dell'agente"¹⁵.

Come argomentato da parte della dottrina¹⁶, in relazione a queste considerazioni sulle finalità ultime dell'art. 27 Cost., occorrerebbe a questo punto domandarsi se tali finalità possano coesistere con due previsioni del citato Codice antimafia, ovvero l'art. 19 (indagini patrimoniali) e l'art. 26 (intestazione fittizia), laddove il primo prevede che le indagini patrimoniali debbano estendersi anche nei confronti dei congiunti del proposto e di coloro che vi hanno convissuto nell'ultimo quinquennio, mentre il secondo inverte l'onere di provare che non si tratti di intestazione fittizia di beni in caso di trasferimenti e intestazioni – anche a titolo oneroso – attuati a favore di congiunti, parenti e affini nei due anni antecedenti alla proposta di misura¹⁷.

Ora, dalla presunzione di non colpevolezza discende sull'accusa l'onere di provare la sussistenza di tutti gli elementi costitutivi di un reato; ma qui, come si è detto, non siamo in presenza di illeciti penali ma di misure di carattere amministrativo. A questo riguardo soccorre una pronuncia della Suprema Corte¹⁸ che riprende le parole di un giu-

15 Secondo il giudice costituzionale "a nulla varrebbe, in sede penale, garantire la riserva di legge statale, la tassatività delle leggi, ecc., quando il soggetto fosse chiamato a rispondere di fatti [...] in relazione ai quali non è in grado, senza la sua benché minima colpa, di ravvisare il dovere di evitarli nascente dal precetto". Per un approfondimento sul tema, VANNI F., *Responsabilità penale d'impresa*, Pintore, Torino, p. 63 ss.

16 F. Brizzi, cit., p. 88 ss.

17 Invero, come meglio specificato *infra*, la giurisprudenza di legittimità ha evidenziato come a carico del proposto residuerebbe non un *onere probatorio* quanto un *onere giustificativo* della legittima provenienza dei beni; il rapporto esistente tra queste particolari persone e il proposto costituisce una "circostanza di fatto significativa", "un lecito criterio interpretativo della situazione di fatto" (che non comporterebbe illegittime inversioni dell'onere della prova) della potenziale e informale disponibilità dei beni da parte del destinatario della misura, specialmente laddove il terzo familiare sia sprovvisto di effettiva capacità economica (Cass., S.U., 2 febbraio 2015 n. 4880; Cass. n. 5184/2016 e n. 17743/2014).

18 Cass. Pen. Sez. III, sent. 5 aprile 2018, n. 15126 in tema di violazioni urbanistiche.

dice portoghese della CEDU: secondo il magistrato non ci si può accontentare del *nomen iuris* attribuito dal legislatore a determinati istituti, laddove tale qualificazione formale risulti diversa dalla sostanza espressa dall'istituto stesso. Proprio nella già citata sentenza De Tommaso c. Italia questo giudice ebbe a esprimersi apertamente nel senso di una “*frode delle etichette*”. Misure coercitive anche solo parzialmente svincolate da un fatto tipico sono infatti accettabili “solo a condizione che ad essere limitata sia la sola libertà dal cui esercizio può a sua volta ragionevolmente concretizzarsi il potenziale danno sociale da cui è scaturita la specifica prognosi di pericolosità”¹⁹.

In una recentissima sentenza²⁰, la Corte costituzionale ha dichiarato illegittima la presunzione di pericolosità per chi, già soggetto a misura di prevenzione, abbia scontato – sospesa la misura – meno di due anni di carcere. L'art. 14, comma 2-ter del Codice antimafia, colpito dalla pronuncia, aveva infatti reintrodotto tale presunzione quando la sospensione della misura collegata allo stato di detenzione dell'interessato fosse inferiore a due anni. Secondo la Consulta, non c'è ragione per ritenere che nell'arco di un biennio la personalità dell'individuo “non possa subire significative modificazioni, quando si tratti di un individuo detenuto in esecuzione di una pena, e dunque sottoposto a un trattamento che per vincolo costituzionale è finalizzato alla sua rieducazione”. Dunque, nella lettura della Corte, la norma confligge anche col principio della finalità rieducativa della pena scandito dall'art. 27, 3° comma, della Costituzione e queste considerazioni sulla necessaria ri-verifica della pericolosità sociale all'avvenuta espiazione della pena costituisce un ulteriore, tenue ma significativo aggancio del principio costituzionale in argomento con questo complesso apparato di misure amministrative.

3. Regole procedurali

È ampio in Italia l'elenco di coloro – specialmente tra quanti sono “addetti ai lavori” – che, nell'esercizio delle proprie funzioni pubbliche, ritengono il sistema della prevenzione antimafia uno strumento

19 Così CATENACCI M., cit. “Oltre questo limite di proporzione, il richiamo a concrete o supposte esigenze di difesa sociale preventiva assume in realtà l'aspetto di una vera e propria truffa delle etichette”.

20 C.Cost. n. 162/2024.

complesso, severo, di grande impatto, ma fondamentalmente equilibrato, e in ogni caso rispettoso del dettato costituzionale²¹.

Tra le ragioni poste a base di queste considerazioni vi è la giurisdizionalizzazione delle misure personali più afflittive e di tutte le misure patrimoniali²², con i correlati tre gradi di giudizio e senza che si attui quello che certa dottrina qualifica come inversione dell'onere della prova²³. Per vero, il procedimento di prevenzione non ha ancora oggi un proprio autonomo statuto processuale e continua a uniformarsi a un paradigma snello, ossia il rito camerale *ex artt.* 127 e 666 Codice di procedura penale.

Proprio recentemente la Corte di cassazione ha puntualizzato che le misure di prevenzione non implicano un "giudizio di colpevolezza", pertanto il giudice della prevenzione ben può utilizzare le emergenze di un procedimento penale pendente o concluso, prescindendo dalle conclusioni cui è pervenuto il giudice penale²⁴, ma con il limite che i fatti storici sintomatici della pericolosità del proposto non siano stati smentiti in sede di cognizione penale.

Com'è noto, l'indagine di prevenzione nasce dalla raccolta di elementi indiziari (dunque non certamente di fonti di prova) che portino al ragionevole convincimento che il soggetto sia/stato pericoloso e che parte del patrimonio accumulato sia di origine illecita (o per meglio dire, *non lecita*). A tale ultimo riguardo è utile ricordare come il sequestro e la confisca di prevenzione hanno ad oggetto beni nella disponibilità diretta o indiretta del proposto, di cui si assume l'*illegittima* provenienza. Dunque, non soltanto laddove questi siano il frutto di attività illecite (o del loro reimpiego), ma anche laddove il loro valore risulti sproporzionato al reddito dichiarato o all'attività economica svolta. Dunque, con specifico riguardo al "riparto del carico probatorio", le Sezioni Unite hanno ribadito

21 "Un istituto che, per quanto carico di ambiguità, è fornito di una propria, indiscutibile razionalità politico-criminale e che, proprio per questo, ha sempre avuto un forte radicamento sia nella prassi che nella stessa teoria della difesa sociale". Così CATENACCI M., cit.

22 Vale a dire la confisca (normalmente preceduta dal sequestro), l'amministrazione giudiziaria di beni e aziende e il controllo giudiziario di queste ultime.

23 V. *supra*. Di "Paragiurisdizione" parla CORDERO F., *Procedura penale*, cap. XXII: "è un ibrido la giurisdizione cosiddetta volontaria: dei giudici esercitano poteri amministrativi; forme processuali tutelano gli interessati, garantendo che l'atto sia conforme ai requisiti; ma tale vaglio non costituisce accertamento nel senso forte; possibili, quindi, dei *bis in idem*. È materia aperta all'*happening* normativo [...]".

24 Così da ultimo Cass. n. 31549/2019.

che l'onere della prova sulla sproporzione tra beni e reddito nonché sulla loro illegittima provenienza incombe indiscutibilmente sulla parte pubblica e deve essere la risultante di un processo dimostrativo "ragionevole e plausibile".

Dunque, a carico del proposto residuerebbe non un onere probatorio quanto un "onere giustificativo" della legittima provenienza dei beni²⁵; per questo, argomenta la Corte, sostenere che il denaro provenga dall'elargizione di un terzo senza spiegarne le ragioni equivarrebbe a tentare di aggirare l'onere di allegazione. Parimenti, l'accertamento della disponibilità in capo al proposto di beni formalmente intestati a terzi opera diversamente per il coniuge, i figli e i conviventi rispetto a tutte le altre persone (artt. 19 e 26 del Codice delle leggi antimafia). Secondo la giurisprudenza di legittimità, il rapporto esistente tra queste particolari persone e il proposto costituisce una "circostanza di fatto significativa", "un lecito criterio interpretativo della situazione di fatto" (che non comporterebbe illegittime inversioni dell'onere della prova) e della potenziale e informale disponibilità dei beni da parte del destinatario della misura, specialmente laddove il terzo familiare sia sprovvisto di effettiva capacità economica²⁶.

Nonostante la costruzione investigativa riposi sempre e soltanto su una base indiziaria (nel senso di "conclusioni più o meno probabili su qualcosa", davanti alle quali il giudice "calcola le probabilità"²⁷), e per l'accertamento della natura pericolosa della persona o del patrimonio non si cerchi una dimostrazione "al di là di ogni ragionevole dubbio", in molti sostengono che le previsioni costituzionali poste a presidio della libertà personale apparirebbero comunque garantite. Per converso, in relazione al diritto di proprietà *ex art. 42 Cost.*, che evidentemente è oggetto di compressioni da parte delle misure di prevenzione patrimoniale, si deve considerare che, a differenza del diritto alla libertà personale che è assoluto, quella tutela costituzionale trova limiti nel fatto che la proprietà deve svolgere una "funzione sociale", ovvero non può essere esercitata in modo tale da ledere l'interesse collettivo. Il legislatore può dunque limitare, conformare e incidere sul diritto di proprietà privata. D'altra parte, potrebbe essere difficilmente considerata compatibile coi

25 Cass., S.U., 2 febbraio 2015 n. 4880.

26 Cass. n. 5184/2016 e n. 17743/2014.

27 CORDERO F., cit., p. 572 ss.

limiti posti dalla Carta alla libertà di iniziativa economica privata un'attività di impresa che utilizzi proventi illeciti o ne consenta il reimpiego, oppure realizzi finalità criminali.

In merito alla valutazione degli indizi, come si è avuto modo di accennare, l'art. 192 Codice di procedura penale li esige "gravi, precisi e concordanti", trascrivendo una formula già presente nell'art. 2729 Codice civile. In tale quadro, anche le dichiarazioni del correo – foss'anche collaboratore di giustizia – "contano nella misura in cui le avallino riscontri esterni"²⁸. In assenza di tali riscontri, queste dichiarazioni, che non potrebbe mai avere legittimo ingresso nel processo penale, possono invece essere efficacemente utilizzate all'interno del procedimento di prevenzione, così come possono essere vagliati gli elementi risultanti dal giudizio penale conclusosi con un patteggiamento ovvero anche una pronuncia di proscioglimento, diversa dall'assoluzione nel merito²⁹. Del resto, la possibilità di valorizzare nella prevenzione circostanze che emergono anche da pronunce liberatorie risulta fisiologicamente dalla "mancanza di correlazione tra le misure di prevenzione e la consumazione dei reati"³⁰.

Invero, vi è una sola ipotesi per cui *ex lege* viene meno l'autonomia del procedimento preventivo in caso di statuizione del giudice penale: la condanna a pena condizionalmente sospesa, che in nessun caso può costituire di per sé sola motivo per l'applicazione di misure di prevenzione ai sensi dell'art. 166 Codice penale. La ragione, piuttosto evidente, risiede nel fatto che ove il giudice penale concedendo la sospensione abbia già formulato una prognosi favorevole al soggetto, in mancanza di elementi ulteriori il proposto non potrà essere ritenuto pericoloso da parte del giudice della prevenzione.

Piuttosto recentemente la Corte costituzionale ha affermato che le misure di prevenzione, pur non avendo natura punitiva, "intanto possono considerarsi legittime, in quanto rispettino i requisiti cui l'art. 13 Cost. subordina la liceità di ogni restrizione alla libertà personale, tra i quali vanno in particolare sottolineate la riserva assoluta

28 Così Cordero F., cit., che richiama C.Cass. SU 18 febbraio 1988. "Formula ovvia, se la intendiamo nel senso che esigano vagli particolarmente cauti, estesi a ogni circostanza utile, perché questi narranti non vanno creduti sulla parola" (*ibidem*).

29 Cass. n. 31549/2019. Nel senso anche C.Cost. n. 24/2019, secondo cui "l'esistenza di una sentenza di proscioglimento nel merito per un determinato fatto impedisce, alla luce anche del disposto dell'art. 28, comma 1, lett. b) [D.Lgs. n. 159/2011], che esso possa essere assunto a fondamento della misura".

30 Cass. n. 111/2018.

di legge (rinforzata, stante l'esigenza di predeterminazione legale dei «casi e modi» della restrizione) e la riserva di giurisdizione". Le fa eco la giurisprudenza di legittimità³¹, ritenendo che non sia "discutibile che si tratti di procedimento giurisdizionale, sottoposto al rispetto di principi fondamentali del processo penale e qualificato come tale dall'intervento decisionale di autorità giudicante terza rispetto alle parti, dalla contestazione di una forma specifica di pericolosità e dalla formulazione di precisa «proposta» nel rispetto dei principi di legalità e tassatività della stessa".

Per questo, discorso a parte deve essere fatto sulla rilevanza procedimentale del "sospetto". Nel giudizio di prevenzione, condizione sufficiente e necessaria a legittimarne l'applicazione è che l'attività criminosa risulti da evidenze che la legge indica come "elementi di fatto", siano essi tassativi e determinati come pure fatti sintomatici in quanto collegati a dati certi. Mai, tuttavia, da meri sospetti. A questo riguardo, con la sentenza n. 2 del 1956, la Corte costituzionale, nell'enunciare già allora l'obbligo della garanzia giurisdizionale per ogni provvedimento limitativo della libertà personale, ha argomentato sul netto rifiuto del "sospetto" come presupposto per l'applicazione dei provvedimenti di prevenzione, legittimi in quanto motivati da fatti specifici³². Tale assunto è poi stato fatto proprio anche dalla giurisprudenza di legittimità³³, secondo cui "il giudizio di pericolosità, in un'ottica costituzionalmente orientata, si fonda sull'oggettiva valutazione di fatti sintomatici collegati ad elementi certi e non su meri sospetti, senza alcuna inversione dell'onere della prova a carico del proposto".

A fianco del rifiuto del sospetto come base legittima per un'istruttoria di prevenzione, si consideri infine che lo stesso requisito di pericolosità, per uniforme giurisprudenza, non deve essere desunto da fatti remoti: sono infatti irrilevanti le pregresse manifestazioni di pericolosità sociale ove non si riscontrino, al momento dell'applicazione della misura personale, questi sintomi rivelatori della persistenza del soggetto in comportamenti antisociali³⁴.

31 Cass. Sez. I, 6 luglio 2016, n. 49180.

32 "Per intanto ci basti considerare che c'è una sola cosa più irredimibile della mafia: il sospetto. L'irredimibilità del sospetto proietta le presunte colpe dei padri tra le generazioni".

Così BARBANO A., *L'inganno: antimafia. Usi e soprusi dei professionisti del bene*, p. 34.

33 Cass. n. 30974/2018.

34 Per tutte, C.Cass. Sez. I, n. 499/1992 e Sez. I, n. 3866/1991.

Passando all'esame del tema della prova, va rilevato che nel procedimento di prevenzione non è previsto il cd "doppio fascicolo": non esiste quindi un fascicolo del pubblico ministero processualmente distinto da quello del tribunale. Ne discende direttamente che sono utilizzabili per la decisione anche gli elementi di prova non formati nel contraddittorio, compresi quelli derivanti dalle indagini difensive (ad eccezione delle prove patologicamente inutilizzabili, ovvero formate in violazione di divieti probatori³⁵). Nella prassi, non sono rare le deleghe di indagine alla polizia giudiziaria da parte del tribunale, necessarie a colmare necessità probatorie su richieste di sequestro o confisca³⁶. Si tratta di indagini riservate per le quali è esclusa la partecipazione dell'interessato, a meno che non si compiano atti che richiedono l'assistenza difensiva. Certamente, una volta istaurato il contraddittorio, l'interessato ha diritto di esaminare gli atti ottenuti e controdedurre.

In tema di contraddittorio, solo dopo il 2017 (con la legge n. 161) la normativa sulle misure di prevenzione ha previsto una *contestazione* degli elementi dedotti a carico del proposto, disponendo che l'avviso contenga la "concisa esposizione dei contenuti della proposta". La Corte di cassazione ha avuto modo di chiarire che non vi è violazione del diritto di difesa laddove il o i fatti attorno a cui ruota il procedimento di prevenzione, ovvero "gli accadimenti idonei a sostenere la valutazione di pericolosità", "sia portato a conoscenza dell'interessato [...] con concreta possibilità di controdeduzione"³⁷.

Come accennato, per l'applicazione delle misure (sia personali che patrimoniali) opera il rito camerale *ex art. 666* Codice di procedura penale, al quale c'è un esplicito rinvio nel Codice delle leggi antimafia, ad eccezione della misura del controllo giudiziario delle aziende, per cui si rinvia al procedimento in camera di consiglio *ex art. 127* Codice di procedura penale.

La principale differenza riguarda il potere istruttorio del giudice, laddove l'art. 666 gli attribuisce la facoltà – se occorre – di assumere prove in udienza, nel rispetto del contraddittorio, conferendo dunque alla disposizione una connotazione in parte inquisitoria³⁸. Tale scarna

35 Quali, ad esempio, le dichiarazioni accusatorie indirette, rese in violazione dell'art. 195, comma 7, Codice di procedura penale, ove resti non identificata la fonte conoscitiva diretta.

36 Di "potere dell'ufficio giudicante dalla chiara connotazione inquisitoria" parla FRANCOLINI G., *Sistema Penale*, fascicolo 10/2020, p. 17.

37 Cass. n. 32032/2013.

38 Nel senso, FRANCOLINI G., cit.

disciplina ha creato alcuni problemi nella prassi applicativa laddove, in caso di escussione di “soggetti informati su fatti rilevanti per il procedimento”³⁹ essi non assumono formalmente la qualità di “testimoni” e di conseguenza non vengono loro sempre rivolti gli avvisi previsti dal codice di rito, coi relativi dubbi sulle conseguenze in caso di dichiarazioni reticenti o false.

Infine, la giurisprudenza di legittimità ha argomentato che non è necessario che l’assunzione di queste prove dichiarative avvenga in contraddittorio tra le parti, “essendo sufficiente che al proposto sia consentito, mediante l’esame degli atti, la piena conoscenza del loro contenuto e il diritto di controdedurre”⁴⁰.

4. Breve *focus* sull’interdittiva antimafia del prefetto

In materia di interdittiva del prefetto, comunque qualificabile quale provvedimento di natura cautelare preventiva per la tutela dell’ordine economico *ex* artt. 84 e seguenti del Codice delle leggi antimafia, il Consiglio di Stato è intervenuto più volte enunciando il principio del “*più probabile che non*”, tipico degli strumenti preventivi, che fa da contraltare a quello del “ragionevole dubbio” di stampo processuale penale⁴¹. Tale regola integra un criterio di giudizio di tipo empirico-deduttivo, ben integrabile con dati di comune esperienza resi dall’osservazione di fenomeni sociali (quali quello mafioso), che certifica “l’estraneità del sistema delle informazioni antimafia da qualsiasi logica penalistica di certezza probatoria raggiunta al di là del ragionevole dubbio”, giacché simile logica “vanificherebbe la finalità anticipatoria dell’informazione antimafia, che è quella di prevenire un grave pericolo e non già di punire, nemmeno in modo indiretto, una condotta penalmente rilevante”⁴². In virtù della sua funzione di massima anticipazione della soglia di prevenzione, che colpisce il *rischio* di infiltrazione e non il *tentativo*, la misura di prevenzione dell’interdittiva prefettizia richiede “soltanto” la sussistenza di “elementi sintomatico-presuntivi dai quali – secondo un giudizio prognostico lata-

39 Art. 7, comma 8, D.Lgs. n. 159/2011.

40 Cass., sez. VI, 19 luglio 2017, n. 40552.

41 *Ex multis*, CdS n. 1743/2016, n. 5214/2017, 2343/2018 e 4938/2018.

42 Così CdS n. 2343/2018.

mente discrezionale – sia deducibile il pericolo di ingerenza della criminalità organizzata”⁴³.

Quanta distanza dalla definizione di prova, come “segno sensibile del fatto da provare”, che impone rilevanza, compiuta valutazione e deve riflettere “solo i dati conformi alle regole”⁴⁴.

La comunicazione e l’informazione antimafia (liberatoria o interdittiva) hanno la durata stabilita dall’art. 86 del relativo Codice, ovvero sei e dodici mesi; tuttavia, il semplice decorso del tempo non determina la cessazione automatica degli effetti della misura, giacché ne conseguono ulteriori accertamenti per verificare il proseguire della cd “contiguità mafiosa”. In questo senso, la giurisprudenza, ad oggi, è univoca⁴⁵. In sostanza, la valutazione del rischio infiltrativo già effettuata dal prefetto, pur dovendo tener conto degli elementi sopravvenuti, non può conoscere soluzione di continuità che non dipenda da fatti nuovi oggettivamente capaci di rendere irrilevanti e inefficaci i precedenti elementi indiziari di infiltrazione mafiosa⁴⁶. Dunque, l’aggiornamento del provvedimento interdittivo richiede la sopravvenienza di fatti nuovi rispetto a quelli in origine valutati dall’autorità prefettizia e tali da dimostrare la recisione di legami, rapporti, amicizie o cointeressenze con soggetti organici o contigui alle associazioni mafiose, nonché una comprovata “presa di distanza” da contesti criminali⁴⁷.

La principale ragione per cui la Corte costituzionale ha sin qui sempre salvato l’istituto dell’informazione interdittiva risiede principalmente nel fatto che esso si pone a tutela dell’ordine pubblico economico e della libera concorrenza delle imprese. In tale quadro, non vi sarebbe contrasto con l’art. 41 Cost. poiché il provvedimento si qualifica come “atto ripristinatorio” della libera concorrenza. Ciò nondimeno, diverse critiche sono state mosse all’istituto dell’informazione interdittiva (specialmente quella cd “generica” ex art. 84, comma 4, lett. d) ed e) del Codice delle leggi antimafia, dai presupposti decisa-

43 Ancora CdS n. 2343/2018. “D’altro lato, detti elementi vanno considerati in modo non unitario e non atomistico, cosicché ciascuno di essi acquisti valenza nella sua connessione con gli altri”.

44 CORDERO F., cit., p. 595. “Our law excludes evidence of many matters which in life outside the courts sensible peoples take into consideration when making decisions” (R. v. Turner, 1975, citato da F. Cordero).

45 CdS n. 7002/2011; n. 292/2012; n. 4602/2015.

46 Così SALAMONE V., presidente dal TAR Campania, nello studio *L’efficacia temporale delle interdittive antimafia e le procedure di revisione. Si tratta veramente di un “ergastolo imprenditoriale”?*, 3 maggio 2023.

47 CdS n. 896/2019.

mente indeterminati), qualificato come un vero e proprio “ergastolo imprenditoriale”, con potenziale impatto anche sul buon andamento della pubblica amministrazione in termini di possibilità e opportunità di contrarre. Basti pensare che, quando emerge la sussistenza di un eventuale tentativo di infiltrazione mafiosa, i soggetti destinatari del provvedimento non possono stipulare, approvare o autorizzare contratti o subcontratti, né autorizzare, rilasciare o comunque consentire concessioni e erogazioni. Tutto questo, salva la revoca del provvedimento da parte dell'autorità che lo ha emesso oppure in caso di contenzioso favorevole presso il TAR competente.

Al netto dell'individuazione dei cd “reati spia”, non esiste inoltre una vera e propria tipizzazione delle condizioni poste alla base del provvedimento. Per questo, nel richiamare il citato principio del “più probabile che non”, il Consiglio di Stato ha ricordato alcuni elementi che devono essere considerati nel corso dell'istruttoria prefettizia, tra cui:

- provvedimenti sfavorevoli del giudice penale (cautelari o di merito);
- sentenze di proscioglimento o assoluzione;
- misure di prevenzione;
- vicende personali del proposto, rapporti parentali e derivazione delle risorse economiche;
- contatti, rapporti, conoscenza, amicizie e frequentazioni;
- vicende anomale nella formale struttura dell'impresa o nella sua concreta gestione (verificate, ad esempio, a seguito di accesso ai cantieri);
- condivisione di un sistema di illegalità per ottenere benefici (tra cui la mancata denuncia dei reati di estorsione).

Ci sia consentita a questo punto una provocatoria invasione nel campo della filosofia del diritto, laddove è nato il concetto teorico del “diritto penale del nemico”⁴⁸. Gli individui sarebbero infatti suddivisi in due categorie: le persone “giuridiche” e quelle “non giuridiche”. Solo alle prime sarebbero riservate tutte le garanzie dello stato di diritto; di conseguenza il diritto penale si ergerebbe contro le seconde quale strumento di prevenzione verso gli individui pericolosi, applicandosi ben prima della commissione del fatto delittuoso e anticipando così di molto la soglia dell'intervento penale. Tale riflessione (non basata su assunti di politica del diritto, bensì su elementi di filosofia del diritto)

⁴⁸ La teoria (*Feindstrafrecht*) fu elaborata dallo studioso tedesco Gunther Jakobs negli anni '80 del secolo scorso.

pone una demarcazione netta tra *essere* e *dover essere*. L'inflizione della pena al cittadino (o delinquente normale) può consolidare nuovamente il suo essere persona *giuridica*; invece, di fronte a un nemico che dedica stabilmente la sua vita a strutture criminali, "la ri-affermazione della persona *giuridica* attraverso la pena rimane un'aspettativa *infinitamente controfattuale*"⁴⁹. È importante che il nostro apparato di prevenzione nazionale si presenti ed evolva in modo tale da allontanarsi il più lontano possibile da queste categorie filosofiche.

Nonostante l'introduzione di alcune importanti innovazioni legislative a garanzia del proposto, quali quella del contraddittorio (a richiesta dell'interessato), la prevenzione collaborativa e il controllo giudiziario, è un fatto che la Corte europea dei diritti dell'uomo si pronuncerà a breve sull'interdittiva antimafia "generica" del prefetto che, emessa sulla base di presupposti vaghi e imprecisati, non garantirebbe vincoli alla discrezionalità dell'autorità governativa né la prevedibilità degli eventuali provvedimenti da questa adottati⁵⁰. La questione appare delicata alla luce delle previsioni costituzionali che, come noto, consentono l'ingresso della giurisprudenza sovranazionale nell'ordinamento attraverso gli artt. 117 (in modo diretto, per le pronunce della Corte di giustizia UE) e 11 (in modo indiretto, previo ricorso alla Consulta, per quelle della CEDU).

5. Possibili prospettive di riforma

Tornando alle riflessioni rese in premessa, lo strumento del processo penale – coi suoi ordinari istituti tesi al contrasto delle ordinarie forme di criminalità e devianza – si è negli anni dimostrato insufficiente a contrastare le più pervicaci, violente e aggressive forme di criminalità organizzata di tipo mafioso, e soprattutto a intaccarne le illecite e gigantesche forme di accumulo patrimoniale. Questa è la principale

49 Argomenta su questa teoria BRUNETTI P., *Diritto penale del nemico: una lettura critica dei presupposti filosofici*, in *Penale – Diritto e Procedura* del 29 maggio 2020. Tutto questo legittimerebbe la richiamata anticipazione della soglia dell'intervento penale, rendendo accettabile l'uso della coercizione e finanche della tortura.

50 "L'assoluta indeterminatezza delle condizioni che possono consentire al prefetto di emettere un'informativa antimafia "generica" appare davvero poco sostenibile in un ordinamento democratico che rifugga da antichi spettri di diritto di polizia e di "pene" del sospetto e voglia ancorare qualsiasi provvedimento restrittivo a basi legali precise e predeterminate". Così BRIZZI F., *L'interdittiva antimafia nell'alveo della sanzione penale?*, su *www.ius.giuffre.it*, 19 agosto 2024.

ragione alla base della nascita, dello sviluppo e del successo delle misure di prevenzione: un apparato che, “per quanto carico di ambiguità”⁵¹, possiede una propria e innegabile razionalità politico-criminale e un forte radicamento negli organi investigativi, giudiziari e amministrativi specialmente in alcune aree del Paese.

Per questi motivi, lo sforzo che dovrà essere richiesto al legislatore, prima ancora che alla giurisprudenza, è quello di individuare alcuni correttivi nel breve periodo che puntino a risolvere le maggiori criticità e ad allineare gli istituti della prevenzione antimafia al dettato costituzionale e alle regole del diritto sovranazionale, prima di eventuali interventi – dagli epiloghi incerti – delle diverse corti nazionali, europee ed internazionali.

Si fa riferimento, in primo luogo, alla necessità di mettere a fuoco e centrare appieno il requisito costituzionale della legalità e tassatività nella descrizione delle condotte che danno luogo a compressione di diritti fondamentali, ridefinendo i presupposti della “pericolosità” che legittimano il ricorso alle misure di prevenzione. In secondo luogo, si reputa necessario intervenire sulla fase del procedimento allineandolo ai principi del cd “giusto processo” di cui all’art. 111 Cost., a cui nessun esercizio di giurisdizione dovrebbe potersi sottrarre. Infine, sarebbe decisamente opportuno riportare l’insieme dei soggetti destinatari all’originaria “purezza”, eliminando i recenti emendamenti che vi hanno annoverato gli indiziati dei reati più vari (dalla violenza in occasione di manifestazioni sportive, ai maltrattamenti verso familiari o conviventi, agli atti persecutori), favorendo un processo degenerativo dell’istituto verso ipotesi di repressione alternative al diritto e al processo penale⁵².

Sul fronte dell’informazione interdittiva del prefetto, per concludere, non si crede che allo stato sia più rinviabile un intervento che chiarisca in modo definitivo che il decorso del termine indicato dalla legge quale durata complessiva del provvedimento e dei suoi effetti (12 mesi) porti *automaticamente* alla cessazione della misura, fatta salva la rivalutazione dell’autorità prefettizia che, attraverso un nuovo atto positivo, ne rinnovi i contenuti⁵³.

51 Così, CATENACCI M., cit., p. 4.

52 Per un approfondimento su questi temi, si veda nuovamente CATENACCI M., cit., p. 5.

53 Allo stato, come indicato nel paragrafo precedente, la giurisprudenza è granitica nell’affermare che l’aggiornamento del provvedimento interdittivo richiede la sopravvenienza di fatti nuovi rispetto a quelli in origine valutati dall’autorità prefettizia e tali da dimostrare la recisione di legami, rapporti, amicizie o cointeressenze con soggetti organici o contigui alle associazioni mafiose.

CAPITOLO II

Una visione europea: l'approccio amministrativo per il contrasto al crimine grave e organizzato

1. Il problema dello scambio di informazioni di polizia per finalità amministrative e del riconoscimento transfrontaliero delle decisioni di prevenzione

I documenti dell'Unione europea hanno iniziato a considerare in modo onnicomprensivo e strategico il tema della criminalità organizzata a partire dal 2008. A quell'anno, infatti, risale la decisione-quadro della Commissione sul tema, poi approvata dal Consiglio in formato Ministri dell'interno⁵⁴. Il contrasto alla criminalità organizzata è infatti uno dei temi di materia penale, insieme alla lotta al terrorismo e al traffico di stupefacenti, che più si presta ad essere oggetto di strumenti normativi internazionali; per vero, nell'ambito degli Stati membri – con la pregevole eccezione dell'Italia – prima di allora non era presente alcuna costruzione penalistica capace di aggredire il fenomeno in modo sufficientemente severo. Da quel lontano 2008 l'Unione, in uno sforzo sempre maggiore di comprensione di questa complessa manifestazione criminale, si è progressivamente dotata di strumenti di analisi e di *policy* che ogni cinque anni confluiscono nelle periodiche "Strategie dell'UE per la lotta alla criminalità organizzata". L'ultima è quella relativa al quinquennio 2021-2025⁵⁵, e prende finalmente atto di come questo tipo di criminalità rappresenti una minaccia considerevole per i cittadini, le imprese, le istituzioni statali e l'economia dell'Unione nel suo complesso, giacché i gruppi criminali organizzati, "*presenti in tutti gli Stati membri*", sono principalmente mossi da interessi incentrati sui profitti, si dedicano normalmente e contemporaneamente a una pluralità di fenomeni criminali e usano il prodotto di un'attività illecita per finanziare l'espansione in altri settori.

Per agevolare la creazione di un efficace sistema comune di contrasto, nei suoi documenti di settore la Commissione chiarisce come sia essenziale potersi avvalere di un efficace sistema di scambio e di accesso tempestivo alle informazioni all'interno dello spazio comune

54 Decisione n. 2008/841/GAI del Consiglio del 24 ottobre 2008.

55 COM(2021) n. 170 *final*, approvata dal Consiglio con doc. n. 8085/21.

di libertà, sicurezza e giustizia (peraltro, come noto, generalmente caratterizzato dall'assenza di controlli alle frontiere interne). Per questo fine, vengono richiamati gli strumenti oggi in vigore e invitati gli Stati membri a farne il più largo uso possibile:

- Sistema Informativo Schengen (SIS), consultato 4 miliardi di volte nel solo anno 2020, ottenendo più di 200 mila riscontri positivi, con possibilità di scambio di dati biometrici, immagini del volto e profili DNA;
- scambio di informazioni investigative nell'ambito del cd "quadro di Prüm"⁵⁶, che consente alle autorità di contrasto dei 27 di scambiare attraverso un *router* centralizzato a livello UE i dati delle impronte digitali, delle patenti di guida, del DNA, dei cd *police records* e dei dati di immatricolazione dei veicoli delle persone di interesse operativo sulle quali sono condotte indagini;
- PNR (*Passenger Name Record*) e API (*Advanced Passenger Information*), ovvero le informazioni sui passeggeri ad alto rischio dei voli aerei *intra* ed *extra* Schengen⁵⁷;
- Codice di cooperazione di polizia, approvato con la direttiva (UE) 2023/977, che consente alle agenzie di *law enforcement* degli Stati membri di scambiare rapidamente informazioni sulle indagini in corso per tutti i reati afferenti al mandato di Europol, attraverso il canale di comunicazione sicuro di proprietà UE "SIENA"⁵⁸.

In tale quadro appare evidente come la cooperazione internazionale tra le diverse autorità di contrasto sia necessaria a smantellare reti criminali oggi sempre più transnazionali, ricorrendo anche al supporto delle agenzie unionali che operano nel dominio "Giustizia e Affari interni", tra cui – in prima battuta – Europol ed Eurojust, nonché di Interpol.

Fatta questa premessa e volendo considerare adeguatamente tutti i progressi fatti da parte dei singoli Stati membri e delle istituzioni unionali nel loro complesso – soprattutto in tema di consapevolezza del fenomeno –, è necessario ora trattare degli sforzi ancora da compiere e di tutti gli spazi che è ancora necessario colmare per

⁵⁶ Regolamento (UE) n. 982/2024.

⁵⁷ Informazioni che comprendono, oltre ai dati anagrafici, il posto a sedere sul vettore, la rotta, eventuali scali e presenza di bagagli.

⁵⁸ *Secure Information Exchange Network Application*.

potenziare la capacità investigativa, di contrasto e di aggressione patrimoniale delle Forze di polizia. Infatti, al netto delle attività di tipo giudiziario, è emerso con prepotente evidenza come le consorterie criminali organizzate che operano a livello transfrontaliero sfruttino – tra l’altro – la mancanza di informazioni a disposizione delle autorità amministrative del Paese di destinazione delle attività illecite per creare società, acquisire permessi, partecipare a gare d’appalto e, quindi, infiltrarsi nell’economia legale. Invero, condividere le informazioni a livello internazionale per questo scopo è difficilissimo, ove non addirittura impossibile, poiché le leggi nazionali di settore non sono normalmente scritte per finalità di cooperazione internazionale; inoltre, il riconoscimento reciproco transfrontaliero delle decisioni amministrative non è ancora stato normato a livello unionale e si deve quindi far riferimento, caso per caso, a forme di cooperazione bilaterale tra Stati membri dagli esiti e dalle tempistiche incerti. In una parola, *non esiste ad oggi una cornice giuridica comune che consenta lo scambio di informazioni di polizia per finalità amministrative*.

In questo senso, un primo avvicinamento formale a questa tematica è stato tentato durante la seconda edizione del *Law Enforcement Forum* tenutosi a L’Aja il 31 marzo 2022, promosso dall’Italia con il supporto di Europol, nel corso del quale è stata affrontata la necessità di proteggere i fondi dell’Unione europea messi a disposizione per i Piani nazionali di ripresa e resilienza dalle infiltrazioni della criminalità organizzata, offrendo come *best practice* l’esperienza italiana maturata nei controlli amministrativi antimafia nel settore degli appalti pubblici e proponendo come soluzione l’interdizione dei partecipanti ai lavori mediante una misura sanzionatoria amministrativa.

Tale approccio (ribattezzato poi “*approccio amministrativo*” per la prevenzione e il contrasto dell’infiltrazione della criminalità nell’economia legale) è stato promosso nell’ambito dei 27 Stati membri attraverso l’ENAA, l’*European Network on Administrative Approach*⁵⁹, col nome di “*Italian Initiative*” ed ha come ultimo fine la ricerca di un quadro giuridico unionale condiviso che regolamenti gli scambi di dati investigativi per scopi amministrativi.

59 www.administrativeapproach.eu. Questo *network* europeo è stato costituito a seguito delle Conclusioni del Consiglio UE del 5 novembre 2010 ed è copresieduto dallo Stato membro che ha la presidenza di turno del Consiglio unitamente a un rappresentante della Commissione europea.

Al netto del supporto italiano alle iniziative di scambio di informazioni di tipo amministrativo, in ambito unionale è opportuno citare l'esperienza maturata da Belgio, Paesi Bassi e Germania che – da qualche anno – hanno dato vita alla rete EURIEC (*Euro-regional Information and Expertise Centre*), mirando a promuovere una forma di collaborazione amministrativa transfrontaliera contro la criminalità organizzata⁶⁰.

A tal fine, sono state costruite reti e piattaforme di discussione per sensibilizzare l'opinione pubblica sull'approccio amministrativo contro la criminalità organizzata internazionale e per offrire supporto in casi operativi reali. Ciò consente agli esperti dei Paesi partecipanti di collegarsi più rapidamente ad alcune banche dati amministrative che sono state rese interoperabili (anagrafe della popolazione residente, anagrafe dei rapporti finanziari, camera di commercio, catasto, dati sull'assistenza sociale) e di agire su tre principali aree:

- avviare modifiche alla legislazione e ai regolamenti a livello nazionale ed europeo;
- proseguire lo sviluppo di piattaforme di consultazione condivise;
- aumentare la consapevolezza della necessità di scambiare informazioni a fini amministrativi a livello internazionale.

2. I primi esperimenti normativi unionali: il regolamento UE 2018/1805 e la direttiva UE 2024/1260. Breve *focus* sulla Convenzione ONU di Palermo

Come già richiamato, la legislazione eurounitaria presenta ancora oggi problemi applicativi che riguardano principalmente la definizione del concetto di criminalità organizzata e l'esecuzione all'estero delle misure di prevenzione patrimoniali, che condizionano sensibilmente l'effettività dell'azione antimafia intrapresa anche dalle autorità italiane. Circa il primo problema, la già citata decisione-quadro 2008/841/GAI si concentra prevalentemente sulle *condotte* che contribuiscono alle attività di un'organizzazione criminale, ma non fornisce una definizione condivisa di criminalità organizzata: in sintesi essa valorizza il *contrasto* del fenomeno, stimolando la co-

⁶⁰ <https://euriec.eu/en/about>.

operazione tra Stati membri e agenzie. In merito al secondo aspetto problematico, si osserva che l'UE ha affrontato il tema – peraltro in modo non del tutto definitivo – solo col recente Regolamento 2018/1805 relativo al riconoscimento reciproco delle decisioni di sequestro e confisca emesse all'esito di un procedimento di natura non penale. Si tratta di tutte quelle ipotesi di confisca anche non correlate a una condanna (*non-conviction based confiscation*), applicate all'esito di una procedura relativa al patrimonio (cd *actio in rem*). In particolare, il “considerando” n. 13 estende l'applicazione del provvedimento a tutte le decisioni di congelamento e confisca emesse “nel quadro” di un procedimento in materia penale e “contempla altri tipi di provvedimenti emessi in assenza di una condanna definitiva, [...] benché tali provvedimenti possano non esistere nell'ordinamento giuridico di uno Stato membro”. Per converso, però, precisa che i provvedimenti di sequestro e confisca “emessi nel quadro di procedimenti in materia civile o amministrativa” rimangono esclusi dall'ambito di applicazione della norma. Si è, dunque, in presenza di un problema applicativo del Regolamento a misure ablative esterne al processo penale, come le misure di prevenzione patrimoniali italiane.

Molto più recentemente, con uno sforzo culturale prima ancora che legislativo, gli Stati membri hanno approvato la direttiva 2024/1260 in materia di sequestro, confisca e potenziamento degli *asset recovery office* nazionali, pubblicata in gazzetta ufficiale il 2 maggio dell'anno scorso, che invita gli Stati ad adottare le misure necessarie a procedere *sempre* alla confisca dei beni strumentali al reato per cui si procede o ad esso connessi direttamente o indirettamente, anche se trasferiti strumentalmente a terzi, nei casi in cui un procedimento penale sia stato avviato ma non sia stato possibile portarlo a conclusione a causa di una o più di queste circostanze: fuga, malattia o decesso dell'imputato, decorso dei termini di prescrizione del reato. Con particolare riguardo alla confisca nei confronti dei terzi, il provvedimento precisa che gli organi giurisdizionali nazionali devono poter accertare che essi sapevano o avrebbero dovuto sapere che il trasferimento degli *asset* aveva lo scopo di evitare la confisca (tra gli esempi viene richiamato il caso della vendita o donazione nei riguardi di parenti o affini).

Questa direttiva, che costituisce certamente uno sforzo apprezzabile nell'ambito del cd “diritto dell'intervento patrimoniale”, si presenta con tutta evidenza molto lontana dalla forza e dal vigore del quadro normativo italiano in materia che – è il caso di ricordarlo – con-

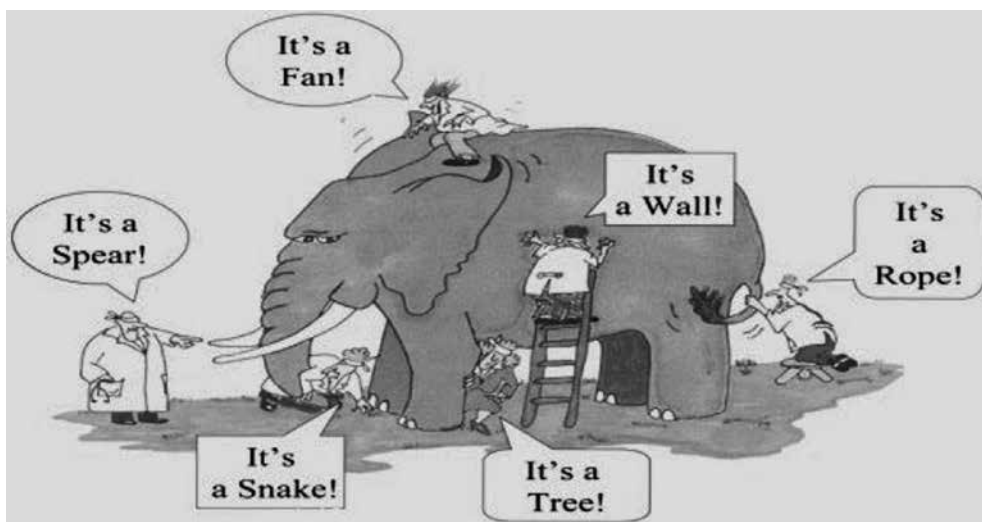
templa ipotesi di confisca senza condanna da circa 40 anni. E comunque, in ogni caso, lascia irrisolto il nodo del riconoscimento reciproco dei provvedimenti *amministrativi* di ablazione patrimoniale.

Dunque, a quest'ultimo riguardo, si ritiene opportuno fare un breve approfondimento dei contenuti della Convenzione ONU di Palermo contro la criminalità organizzata transnazionale del 2000 che presenta elementi di modernità ed efficacia ancora assenti nel contesto delle leggi dell'Unione. A ben vedere sono tre i pilastri su cui poggia il valore aggiunto della Convenzione, vale a dire l'ampiezza del suo ambito oggettivo di applicazione (che copre la criminalità organizzata ma anche i reati gravi transnazionali puniti con un massimo di almeno quattro anni di reclusione), l'elevato numero di Stati che vi hanno aderito (ben 189 su 193 Paesi ONU) e l'incisività delle obbligazioni che impone. L'art. 13 della Convenzione, infatti, impegna gli Stati-parte ad una intensa cooperazione internazionale ai fini della confisca. Precisamente, lo Stato-parte, che abbia ricevuto da un altro una richiesta di confisca di "proventi di reato, beni, attrezzature o altri strumenti" situati sul suo territorio, dovrà presentarla "nella più ampia misura possibile nell'ambito del suo ordinamento giuridico interno" alle sue autorità competenti al fine di ottenere un provvedimento di confisca nazionale. Tali obblighi prescindono del tutto dall'esistenza di una condanna e dalla natura penale del procedimento nel quale viene emesso l'ordine di confisca: si richiede soltanto che tale provvedimento abbia ad oggetto "proventi" derivanti dai reati previsti dalla Convenzione, o beni di valore corrispondente, ovvero "beni, attrezzature e altri strumenti utilizzati o destinati ad essere utilizzati per la commissione di reati" previsti dalla Convenzione⁶¹.

Si può concludere, quindi, che attraverso la Convenzione di Palermo sia possibile richiedere e ottenere l'esecuzione all'estero del sequestro e della confisca di prevenzione.

61 Come dedotto da ACCILI SABBATINI M. A. – BALSAMO A., *Verso un nuovo ruolo della convenzione di Palermo nel contrasto alla criminalità organizzata*, in *Diritto Penale Contemporaneo* n. 12/2018, "questa conclusione è agevolmente desumibile dal tenore letterale dell'art. 13, che richiama esclusivamente la nozione di confisca contenuta nell'art. 2 della Convenzione, la quale, a sua volta, "include – laddove applicabile – l'ipotesi della *forfeiture*" (cioè il prototipo della categoria della *non-conviction based confiscation*) e "indica la definitiva ablazione di beni a seguito di decisione del tribunale o di altra autorità competente", senza alcuna specificazione in ordine alla natura penale o extrapenale della decisione".

3. *The blind men and the elephant*. L'approccio amministrativo: l'idea italiana e la sponda olandese



Questa immagine evocativa rappresenta visivamente la parabola indiana dei sei uomini ciechi e dell'elefante: una storia che illustra come diverse prospettive possano portare a visioni parziali e incomplete di una realtà complessa. Secondo il racconto originale, infatti, ognuno degli uomini era convinto che la propria descrizione fosse corretta e non riuscirono mai a mettersi d'accordo su come fosse realmente un elefante, giacché per natura ognuno tende ad autorappresentarsi la realtà in base alla propria percezione.

Questa raffigurazione rende in effetti plasticamente che cosa può accadere agli organi investigativi quando si imbattono in forme criminali organizzate ma difettano di considerare i singoli episodi criminali come il prodotto di una sola e organizzata strategia.

Mosse da questa consapevolezza, le autorità italiane hanno da tempo avviato confronti e dibattiti nell'ambito di diversi gruppi di lavoro del Consiglio dell'Unione europea, al fine di presentare alle autorità di *law enforcement* degli altri Stati membri la strategia di approccio olistico e onnicomprensivo che a queste latitudini si ha del crimine organizzato, senza trascurarne gli aspetti di aggressione patrimoniale.

In sintesi, lo sforzo fatto è stato quello di spingere i nostri *partner* a considerare i singoli delitti sui quali si indaga come il possibile portato di azioni policriminali riferibili a specifiche organizzazioni criminali. Pro-

tabilmente grazie alla sensibilità maturata nell'ambito del già citato progetto EURIEC, i Paesi Bassi per primi hanno compreso l'importanza del tema sollevato dall'Italia e hanno sottoscritto col nostro Paese un *non-paper* che è stato posto a base dei diversi contatti bilaterali con gli altri Stati membri per presentare loro questo nuovo modello di contrasto al crimine grave e organizzato: il cosiddetto "approccio amministrativo".

Il *non-paper*, partendo dalla consapevolezza dell'urgenza di prevedere una modalità condivisa di scambio di informazioni di polizia per finalità amministrative, definisce l'approccio amministrativo come l'insieme delle misure di controllo, di confisca e di prevenzione per il contrasto del crimine grave. Tra la prime si ricorda il controllo delle licenze per attività commerciali a rischio di infiltrazioni mafiose; tra le misure di confisca si possono citare quella per equivalente e quella non basata sulla condanna penale (cd confisca *prater probationem delictum*) che – come definitivamente chiarito dalla giurisprudenza in occasione dell'esame del panorama normativo italiano – non ha uno scopo sanzionatorio bensì una finalità "ripristinatoria" della libera concorrenza e del libero mercato, mentre tra le misure di prevenzione si richiamano ad esempio gli obblighi di formazione per le professioni ritenute a rischio di corruzione.

In linea generale, tra i vantaggi dell'approccio amministrativo si possono citare la sua maggiore rapidità ed efficienza rispetto alle misure penali, la flessibilità che gli consente di adattarsi alle diverse tipologie di crimine nonché la possibilità di attuarlo in chiave preventiva, senza dover necessariamente attendere il reato e il correlato danno alle persone offese e alla collettività.

Partendo da queste premesse, il *non-paper* italo-olandese propone ai suoi destinatari di:

- sviluppare e utilizzare l'approccio amministrativo nelle indagini e massimizzare il ricorso alla Rete europea sull'approccio amministrativo (ENAA);
- esaminare, con un gruppo più ristretto di Stati membri interessati, in che misura la direttiva (UE) 2023/977 sullo scambio di informazioni tra autorità di indagine⁶² possa essere la strada da seguire per agevolare lo scambio di informazioni di polizia per scopi amministrativi. Tale provvedimento, per sua espressa previsione, mira a rafforzare il contrasto ma anche la *prevenzione* dei reati, il che parrebbe consentire di farvi

⁶² Richiamata sopra, paragrafo 2.1.

rientrare tutte quelle attività messe in campo dalle autorità di polizia al di fuori del formale perimetro di un procedimento penale. Il *non-paper* precisa che l'Italia e i Paesi Bassi sarebbero pronti a formare una tale coalizione con gli altri Stati membri interessati;

- invitare la Commissione a esaminare la fattibilità e il valore aggiunto di proporre una base giuridica nuova per gli scopi descritti, laddove il ricorso alla citata direttiva non sia ritenuta una soluzione percorribile.

Dal canto suo, l'Italia ha avviato proficue iniziative bilaterali per dimostrare in modo mirato ad alcuni Stati membri l'utilità di ricorrere a questo strumento. È il caso dell'Austria e della Francia, coi quali sono stati sottoscritti protocolli rispettivamente per lo scambio di informazioni di polizia per il controllo amministrativo dei cantieri del "*Brenner basis tunnel*" e della tratta ferroviaria ad alta velocità "*Torino-Lione*", funzionale all'adozione di misure interdittive in presenza di condizionamenti di tipo mafioso verso le imprese appaltatrici.

L'Unione europea come noto è una macchina particolarmente complessa. Essa agisce secondo uno schema di priorità di massima che è dettato in linea generale dal programma adottato dalla Commissione europea all'atto del suo insediamento e modella la sua azione nel corso del quinquennio sulla base delle sensibilità evidenziate da parte degli Stati membri sui diversi settori di intervento. Il tema dell'approccio amministrativo non fa eccezione a queste regole. Per far sì che l'Unione lo consideri sempre più un'efficace strada da seguire per contrastare le attività criminali organizzate è necessario alzare il livello di interesse sul tema attuando senza sosta intense bilaterali tra Stati e agendo in modo divulgativo nell'ambito dei diversi gruppi di lavoro del Consiglio.

Il lavoro sin qui svolto dall'Italia sul tema sta effettivamente dando i suoi frutti: per ultimo, il documento "*Il futuro del diritto penale dell'UE. Relazione della Presidenza*" dello scorso dicembre⁶³, frutto della sintesi delle discussioni orali e scritte tra le delegazioni dei 27 Stati membri, inserisce tra le priorità strategiche per il prossimo futuro la revisione della decisione-quadro sulla criminalità organizzata (ormai datata 17 anni fa), ma anche il ricorso all'approccio amministrativo per il contrasto al crimine. In Europa un argomento ha dignità

63 Doc. n. 15763/2024 del 4 dicembre 2024, la cui redazione è stata avviata dalla presidenza belga del Consiglio UE e conclusa da quella ungherese nel dicembre dello scorso anno.

di discussione, approfondimento e finanziamento solo nella misura in cui esso è presente nei documenti di *policy* unionali: la presenza di un riferimento all'*administrative approach* all'interno della richiamata relazione della Presidenza è quindi senza dubbio un primo grande risultato per orientare la macchina burocratica eurounitaria verso la direzione voluta dal nostro Paese.

Nella primavera dello scorso anno l'Italia ha compiuto un altro piccolo passo avanti. Tra i principali gruppi di lavoro consiliari in materia di sicurezza vi è il CO.S.I. (Comitato permanente per la cooperazione operativa in materia di sicurezza interna), presieduto per l'Italia dal Vicedirettore generale della Pubblica sicurezza con delega al coordinamento delle Forze di polizia⁶⁴. A seguito di serrate intese con la presidenza belga del Consiglio, in attività nel primo semestre 2024, si è riusciti a dedicare all'approccio amministrativo un punto dell'ordine del giorno della riunione CO.S.I. del 9 aprile. Un fatto tutt'altro che scontato se si considerano le differenti sensibilità ancora esistenti sul tema e il prevedibile scetticismo di alcuni Paesi rispetto alla reale importanza del tema del contrasto "amministrativo" della criminalità grave e organizzata. Come si è detto, in UE un problema esiste se è scritto nei documenti: sotto l'attenta direzione e revisione del nostro Paese, il Belgio ha prodotto un documento di seduta dedicato proprio all'*administrative approach*⁶⁵.

Si tratta di un testo molto completo che inquadra perfettamente il tema e i suoi indubbi vantaggi nella gestione della politica criminale, considerando necessario integrare il principio "*follow the money*" con misure di carattere amministrativo che prevengano l'infiltrazione delle organizzazioni malavitose nell'economia legale.

In tale quadro, seguendo le priorità indicate nella *roadmap* dell'Unione per il contrasto al traffico di droga e al crimine organizzato, è necessario che gli Stati membri comprendano il ruolo chiave che possono esercitare (anche) le autorità amministrative nella prevenzione dei reati. Il documento dedica poi una sezione all'esperienza di EURIEC (*Euro-regional Information and Expertise Centre*) che, come richiamato in questo stesso capitolo, supporta lo scambio di informazioni amministrative per il contrasto del crimine tra Belgio, Paesi Bassi e Germania. È decisamente sentita la necessità di estendere a molti altri Stati questa possibilità di scambio, sebbene i problemi alla base di tale esigenza sia-

64 Incarico ricoperto dal pref. Stefano Gambacurta.

65 Doc. n. 7743/2024.

no ancora irrisolti, mancando una strategia e una modalità comune per l'esecuzione materiale di tali scambi informativi. Infatti, per lo scambio di informazioni criminali per finalità amministrative mancano punti di contatto ufficiali all'interno degli Stati membri nonché – in molti casi – anche le stesse basi giuridiche per poter avviare attività in questo senso.

Pertanto, riprendendo i contenuti e il suggerimento del *non-paper* italo-olandese, il documento della presidenza ritiene utile esplorare la possibilità di prevedere adeguate modifiche alla recentissima direttiva sullo scambio di informazioni tra agenzie di *law enforcement* (n. 2023/977), a seguito di un adeguato studio di fattibilità da parte della Commissione europea.

Da parte italiana, tale *way forward* è stata ritenuta assolutamente convincente e strategica, poiché valorizzerebbe uno strumento normativo moderno come la direttiva recentemente negoziata, sui cui hanno fatto convergenza gli interessi di tutti gli Stati membri. L'essenziale, tuttavia, è che il sistema che sarà ipotizzato per lo scambio di informazioni criminali per finalità amministrative lasci salve le differenze esistenti negli ordinamenti dei vari Stati per valorizzare l'uso effettivo di queste informazioni. In alcuni Paesi nordeuropei (Olanda e Belgio *in primis*), infatti, i poteri di uso "cogente" di tali informazioni (un vero e proprio potere di *enforcement*) è rimesso alle autorità amministrative locali, tra cui i sindaci. In Italia, evidentemente, sarebbe prediletta una soluzione "*law enforcement driven*", che lasci alle Forze di polizia e agli Uffici territoriali del Governo la facoltà di fare uso di queste informazioni per la prevenzione e il contrasto.

Nell'ambito del dibattito che ne è seguito è interessante notare le conclusioni riportate dalla Commissione europea, che non ha mancato di segnalare come diversi Stati membri dispongano già di quadri normativi ben sviluppati in cui le autorità locali sono autorizzate a utilizzare strumenti amministrativi per prevenire l'infiltrazione criminale nelle imprese legali. In altri Stati membri, invece, l'approccio amministrativo è ancora poco sviluppato, giacché essi non dispongono ancora dell'infrastruttura giuridica necessaria a condividere le informazioni rilevanti con le autorità pubbliche. Nel 2023, l'ENAA⁶⁶ ha presentato una *roadmap* sul tema, divulgando gli esempi operativi forniti dall'Italia, dai Paesi Bassi, dal Belgio e dalla Svezia e raccomandando di procedere facendo innanzitutto il punto sugli

66 *European Network on Administrative Approach*.

strumenti disponibili e diffondendo le buone pratiche a livello di autorità amministrative e di *law enforcement* locali. In aggiunta, l'Italia ha lanciato un progetto pilota sullo scambio di informazioni a fini amministrativi nell'ambito della cooperazione operativa di polizia, utilizzando il canale di comunicazione SIENA di Europol. Nel prossimo futuro, la Commissione valuterà attentamente i risultati delle diverse iniziative in campo e si è infine dichiarata pronta a esplorare la fattibilità di una nuova cornice normativa unionale che disciplini lo scambio di informazioni a fini amministrativi.

Quest'ultimo punto toccato dall'esecutivo UE è essenzialmente il nodo della questione: sulla base degli esperimenti pilota portati avanti dall'Italia, la maggior parte degli Stati membri ingaggiati a livello bilaterale per lo scambio di informazioni hanno chiarito che, in mancanza di un chiaro quadro normativo europeo di settore, le legislazioni nazionali ostano a una simile condivisione informativa. Su sei Stati ingaggiati (Belgio, Paesi Bassi, Germania, Svizzera⁶⁷, Malta, Austria), solo due hanno positivamente replicato alle richieste italiane (Malta e Svizzera)⁶⁸.

La missione dell'Italia a Bruxelles nei prossimi mesi sarà quindi quella di continuare a sensibilizzare gli Stati membri e le istituzioni comunitarie sul tema, facendo affidamento sulle prossime presidenze di turno con una maggiore sensibilità nel contrasto alla criminalità organizzata, al fine di spianare finalmente la strada a una proposta normativa della Commissione che colmi l'attuale vuoto normativo. Quindi, si rivelerà vincente agire con attività di sensibilizzazione ad alto livello – in prima battuta tramite la Rappresentanza permanente d'Italia presso l'UE – al fine di garantire una rapida approvazione della nuova proposta legislativa da parte dei due co-legislatori europei, il Consiglio e il Parlamento.

L'Italia dovrà agire con passione, facendo valere sui tavoli unionali tutta la propria indiscussa autorevolezza da *top player* in materia di tutela della sicurezza interna, evitando che il trascorrere del tempo

67 La Svizzera, pur non essendo formalmente un membro dell'UE, è stata ingaggiata come "Stato associato Schengen".

68 Qui di seguito, a titolo di esempio, si riporta la risposta fornita dalla Polizia federale del Belgio: "*Although the requested information should be handed over towards the Italian police forces, our national legislation does not allow the usage of these police and judicial information for the purposes of administrative measures, even when it should be taken by a police force or authority. Due to these restrictions and a lack of a European legal framework, we regret that we cannot yet respond to your request on a Belgian legal basis*".

e le innumerevoli, importanti e diverse questioni che occupano i Governi sui tavoli del Consiglio possano oscurare l'interesse su un tema così importante per un effettivo contrasto delle forme più aggressive e pervicaci di criminalità economica.

Parafrasando Stendhal, se è vero che le azioni ispirate da una vera passione mancano raramente di produrre il loro effetto, è pur vero che il percorso è appena agli inizi e nel grande "condominio" europeo ogni attore è portatore di interessi nazionali diversi, e sarà necessario convincere per vincere: *"la luna di pomeriggio nessuno la guarda, ed è quello il momento in cui avrebbe più bisogno del nostro interessamento, dato che la sua esistenza è ancora in forse"*⁶⁹.

69 CALVINO I., *Palomar*.

Bibliografia

- ACCILI SABBATINI M. A. – BALSAMO A., *Verso un nuovo ruolo della convenzione di Palermo nel contrasto alla criminalità organizzata*, in *Diritto Penale Contemporaneo* n. 12/2018.
- BARBANO A., *L'inganno: antimafia. Usi e soprusi dei professionisti del bene*.
- BRIZZI F., *Dalla prevenzione bellica a quella riparativa*, Key editore.
- BRIZZI F., *L'interdittiva antimafia nell'alveo della sanzione penale?*, su www.ius.giuffre.it, 19 agosto 2024.
- BRUNETTI P., *Diritto penale del nemico: una lettura critica dei presupposti filosofici*, in *Penale – Diritto e Procedura* del 29 maggio 2020.
- CALVINO I., *Palomar*.
- CATENACCI M., *Le misure personali di prevenzione fra "critica" e "progetto": per un recupero dell'originaria finalità preventiva*, in *Rivista italiana di diritto e procedura penale*, fasc. 2, 1° giugno 2017.
- CORDERO F., *Procedura penale*.
- FRANCOLINI G., *Sistema Penale*, fascicolo 10/2020.
- FURFARO S., *La prova nel processo di prevenzione: lineamenti*, in *Archivio Penale*, 2022, n. 1.
- SALAMONE V., *L'efficacia temporale delle interdittive antimafia e le procedure di revisione. Si tratta veramente di un "ergastolo imprenditoriale"?*, 3 maggio 2023.
- SCIASCIA L., *Il giorno della civetta*.
- VANNI F., *Modifiche alla disciplina delle Misure di Prevenzione Patrimoniali: un altro binario nel doppio binario*, su www.filodiritto.com, 24 giugno 2010.
- VANNI F., *Responsabilità penale d'impresa*, Pintore editore, Torino.
- ZUFFADA E., in *disCrimen* del 17 settembre 2021.

Sitografia

- <https://administrativeapproach.eu/>
- <https://delegates.consilium.europa.eu/index.html>

- <https://euriec.eu/en/about>
- <https://www.filodiritto.com>
- www.ius.giuffre.it

“Problematiche nascenti dalla tutela della *privacy* per l’espletamento di attività investigative da parte delle Forze di Polizia e della Polizia Giudiziaria”.

di Daniela Gregorio*

Introduzione

La scoperta e la massiva diffusione degli elaboratori elettronici ha posto, soltanto a partire da qualche decennio, il problema della protezione dei dati personali. L’evoluzione tecnologica, che ha introdotto la possibilità di conservazione ed elaborazione delle informazioni, ha imposto ai giuristi l’obbligo di confrontarsi con le ricadute e le implicazioni che tali attività potrebbero produrre sulla potenziale lesione dell’immagine pubblica degli individui e la nascita di pregiudizi e discriminazioni, che possono originarsi a causa di un trattamento illegittimo di dati personali.

Tali preoccupazioni diventano ancora più pressanti rispetto ai trattamenti dei dati di particolare delicatezza, quali quelli inerenti alle attività di polizia, poiché possono potenzialmente incidere sulla tutela di diritti e libertà fondamentali individuali, ma anche della collettività, che le forze dell’ordine sono chiamate a proteggere.

La tutela dell’ordine e della sicurezza pubblica, infatti, può comportare la necessità di disapplicare le regole che normalmente disciplinano il trattamento dei dati personali e ciò può portare con sé timori che non possono e non devono essere liquidati con il luogo comune “chi non ha nulla da nascondere, non ha nulla da temere”.

Il diritto alla *privacy*, *melius* alla protezione dei dati personali, diventa, pertanto, una questione ineludibile con cui devono confrontarsi

* Vice Questore della Polizia di Stato, già frequentatrice del XL Corso di Alta Formazione presso la Scuola di Perfezionamento per le Forze di Polizia.

non solo i soggetti privati, ma anche le pubbliche amministrazioni, comprese quelle la cui missione istituzionale è, appunto, assicurare la tutela dell'ordine e della sicurezza, che costituisce, a sua volta, lo strumento per la protezione di un complesso di diritti fondamentali che, in questo modo, ottengono la propria espressione e manifestazione.

Le esigenze di sicurezza, infatti, non devono essere intese come preminenti in termini assoluti rispetto alla protezione della sfera privata dei cittadini, ma anzi è necessario ragionare secondo la logica per la quale la tutela del diritto alla *privacy* non deve essere avvertita soltanto da coloro che hanno qualcosa da nascondere, poiché, in via di principio, ciò equivarrebbe a dire, ad esempio, che non ci si deve curare della libertà di espressione solo perché non si ha nulla da dire: la protezione dei diritti e delle libertà fondamentali non è abdicabile o applicabile soltanto se e quando si avverte la compressione delle stesse, in un contesto di mancata tutela.

In definitiva, *privacy* e protezione dei dati personali sono presidi di democrazia e libertà quanto la Pubblica Sicurezza che rimane – anch'essa – un imprescindibile prerequisito per il godimento di tutti i diritti inviolabili ed è, pertanto, in questa chiave che occorre cercare un sapiente *bilanciamento* tra le diverse istanze, in modo da attuare “un gioco a somma zero”, ovvero un'interazione dove il ‘guadagno’ di un soggetto è perfettamente bilanciato dalla ‘perdita’ della controparte e viceversa, a seconda della situazione di fatto che si presenta di volta in volta.

Questa è la strada tracciata dal legislatore europeo e nazionale, sebbene i molteplici riflessi delle scelte, che la società attuale sta in questi giorni facendo, complici le evoluzioni tecnologiche di recente emersione, vanno meditati con particolare attenzione, valutato che le risposte, che verranno date, influenzeranno il nostro futuro per gli anni a venire.

CAPITOLO I

Il trattamento dei dati personali: le fonti normative, l'ambito di applicazione e le disposizioni di carattere generali

1. Le origini della *privacy* e della protezione dei dati personali

Il diritto alla riservatezza e il diritto alla protezione dei dati personali fanno riferimento a distinti interessi afferenti alla sfera della

persona umana; sebbene, infatti, siano utilizzati spesso in maniera indifferenziata, il diritto alla *privacy* riguarda la libertà *negativa* di non subire interferenze o intrusioni da parte di terzi nella propria vita privata, mentre il diritto alla protezione dei dati personali si esprime nella libertà *positiva* di esercitare un controllo sul flusso delle informazioni relative al singolo individuo¹.

Il diritto alla *privacy* (*right to be let alone*) nasce negli Stati Uniti nel 1890 (Warren e Brandeis²) a seguito della diffusione della stampa rotativa, che consentiva una stampa rapida e molteplice dei giornali e la divulgazione veloce delle notizie attinenti alla sfera privata³; esso è inteso come diritto ad impedire che possano essere divulgate, anche a mezzo stampa, informazioni personali in assenza del consenso dell'interessato, a meno che la persona o la notizia siano di pubblico interesse. La finalità del diritto di *privacy*, dunque, è quella di tutelare la persona fisica dall'indebita curiosità altrui e dalla diffusione illegittima di notizie attinenti alla sfera privata.

Il diritto alla protezione della sfera privata dalle ingerenze altrui è stata riconosciuta per la prima volta dalla Dichiarazione Universale dei Diritti Umani, approvata e proclamata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948: all'art. 12 è previsto, infatti, che «nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».

Successivamente, la Convenzione Europea dei Diritti dell'Uomo (CEDU), adottata dal Consiglio d'Europa il 4 novembre 1950 ed entrata in vigore nel 1953, ha statuito all'art. 8⁴ che «ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla

1 Si tratta della lettura che in Italia è stata sostenuta originariamente in RODOTÀ S., *La privacy tra individuo e collettività*, in *Politica del diritto*, 1975, p. 547.

2 WARREN S. D. – BRANDEIS L. D., *The Right to Privacy*, in *Harvard Law Review*, IV, 1890.

3 BRUNO G., *Diritto alla privacy: la storia e l'evoluzione*, in *Diritto.it*, 2023.

4 Rubricato «Diritto al rispetto della vita privata e familiare».

prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

Da ultimo, la Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza il 7 dicembre 2000 e diventata giuridicamente vincolante in tutti gli Stati membri dell'U.E. dal 1° dicembre 2009 con il Trattato di Lisbona, statuisce all'art. 7 che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

La medesima Carta, in verità, al seguente art. 8, relativo alla «protezione dei dati di carattere personale», riconosce alla protezione dei dati di carattere personale una tutela indipendente rispetto agli altri diritti fondamentali, stabilendo che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Il diritto alla riservatezza e il diritto alla protezione dei dati di carattere personale, oltre ad essere stati riconosciuti formalmente nell'ambito di Carte internazionali di tutela dei diritti fondamentali della persona umana, sono stati disciplinati da una pluralità di fonti giuridiche, mediante atti normativi in costante evoluzione, differenti per qualità e posizione nella gerarchia, con conseguente stratificazione delle disposizioni, che rende necessaria un'analisi comparata e sistematica.

L'esigenza di tutelare la libertà *positiva* di esercitare un controllo sul flusso delle informazioni relative al singolo individuo sorge, inevitabilmente, a seguito dei mutamenti che la tecnica induce nella vita quotidiana, individuale e collettiva, vale a dire a seguito della diffusione massiva dei *personal computer*, che hanno consentito l'immagazzinamento e l'elaborazione automatizzata di una grande quantità di dati con il conseguente pericolo di divulgazione indebita dei predetti dati.

La tutela della protezione dei dati assurge, pertanto, al rango di terreno elettivo per saggiare la tenuta del diritto rispetto alla tecnica, in modo da riportare l'uomo al centro di uno sviluppo tecnologico, che potrebbe, in caso contrario, condizionare in modo negativo la vita quotidiana, tradendo la sua funzione strumentale al miglioramento della qualità della stessa. È necessario, pertanto, garantire una costan-

te e aggiornata lettura del dato fattuale, della realtà coeva, per definire in maniera repentina le regole di trattamento dei dati personali⁵.

La natura di diritto 'moderno' si evince anche dall'assenza di una disposizione all'interno della Costituzione italiana, tuttavia si tratta di un diritto assoluto della personalità che tutela, in generale, le vicende strettamente personali, prive di un rilievo socialmente apprezzabile per i terzi, contro ingerenze non giustificate da interessi pubblici preminenti, consentendo all'interessato di controllare la diffusione dei propri dati personali e di reagire di fronte a comportamenti illegittimi da parte di coloro che tali dati trattano.

La Corte costituzionale, di conseguenza, sin dalla sentenza n. 139 del 26 marzo 1990, esprimendosi in relazione all'art. 9, comma 2, del decreto legislativo 6 settembre 1989, n. 322⁶, impugnato in via principale, ha ricondotto la tutela della riservatezza e la protezione dei dati personali nell'ambito dei principi a tutela della *privacy* individuale, che ha affermato essere diffusi, pressoché in forma analoga, in tutti gli ordinamenti giuridici delle nazioni più civili⁷.

Più recentemente, nel dichiarare incostituzionale l'obbligo di pubblicare *on-line* i dati personali sul reddito e sul patrimonio dei diri-

5 Particolarmente illuminante può essere considerata la lettura del "Considerando" 6 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, che fotografa la situazione fattuale che il legislatore ha affrontato: «La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali».

6 Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400.

7 Specificamente, in tale pronuncia, la Corte ha sostenuto che la *ratio* di tali principi «sta nel prevenire qualsiasi rischio che i dati raccolti siano conosciuti all'esterno nel loro riferimento nominativo o individuale ovvero in modo tale che siffatto riferimento possa esser ricostruito pur in presenza di dati anonimi e/o aggregati. Lo scopo di tale principio è duplice, in quanto, senza siffatte garanzie, da un lato, le statistiche potrebbero risultare non veridiche e, dall'altro lato, potrebbero essere messi in pericolo beni individuali strettamente connessi al godimento di libertà costituzionali e, addirittura, di diritti inviolabili. Per tali motivi, il legislatore delegato ha stabilito in modo preciso e rigoroso il divieto di diffondere o di comunicare all'esterno del Servizio statistico nazionale i dati individuali o quelli comunque riferibili a soggetti individuali».

genti pubblici diversi da quelli che ricoprono incarichi apicali, la Corte costituzionale⁸ ha delineato, in maniera efficace e aderente all'attuale stato del pensiero giuridico, il fondamento costituzionale del diritto alla riservatezza dei dati personali (cd diritto alla *privacy*), evidenziando come esso costituisca un risvolto del diritto fondamentale all'intangibilità della sfera privata⁹. Secondo il Giudice costituzionale, gli artt. 2, 14 e 15 Cost. garantiscono la copertura di garanzia del diritto *de quo*, nel senso che la tutela del domicilio e della corrispondenza potrebbe anche essere letta come strumento per la tutela di un bene giuridico ulteriore, costituito dalla riservatezza.

2. Le fonti normative

Il legislatore nazionale ha affrontato per la prima volta la questione soltanto nel 1996, con la legge n. 675, concernente la «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali», in attuazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il quadro normativo è, poi, stato completamente sostituito con il decreto legislativo 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali», entrato in vigore il 1° gennaio 2004, che è tuttora vigente, sebbene sia stato modificato e parzialmente abrogato da atti normativi successivi.

Nel dettaglio, si fa riferimento al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (cd *General Data Protection Regulation* – GDPR), 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, divenuto obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri dell'Unione europea dal 25 maggio 2018.

8 Cfr. sentenza n. 20 del 23 gennaio 2019.

9 Tale prospettiva è stata colta, fra gli altri, da ARENA G., *La tutela della riservatezza nella società dell'informazione*, in AA.VV., *Scritti in onore di Pietro Virga*, I, Milano, 1994, p. 70 e p. 76 ss. che valorizza il rilievo costituzionale della libertà di circolazione delle informazioni e da BARETTONI ARLERI A., *Trasparenza amministrativa e tutela della privacy*, in (a cura di) AMOROSINO S., *Le trasformazioni del diritto amministrativo. Scritti degli allievi per gli ottanta anni di Massimo Severo Giannini*, Milano, 1995, p. 27, che nota una significativa differenza sul modo di concepire la tutela della *privacy* a seguito dell'affermarsi della regola della circolazione dei dati.

Il GDPR costituisce l'asse portante del nuovo sistema di regole sulla protezione dei dati personali, applicabile a qualsiasi trattamento, sia nel settore pubblico, sia nel settore privato, la cui base giuridica si ritrova nell'art. 16 del TFUE¹⁰, che attribuisce alla competenza europea la materia in oggetto, affidando alla procedura legislativa ordinaria la disciplina in materia di protezione dei dati personali e riconoscendo agli Stati nazionali la facoltà di prevedere limitazioni ai principi in esso contenuti in determinati casi¹¹.

L'entrata in vigore del Regolamento (UE) 2016/679 ha innalzato i livelli di protezione delle persone fisiche rispetto al trattamento dei dati personali e responsabilizzato i titolari dei trattamenti stessi, rendendo, a tal fine, necessario l'adeguamento del già vigente Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

La natura di fonte del diritto direttamente applicabile nel territorio degli Stati membri ha comportato, pertanto, che si rendesse necessario un atto normativo del legislatore nazionale di armonizzazione dell'ordinamento giuridico, che ha trovato espressione nel decreto legislativo 10 agosto 2018, n. 101, il quale, come anticipato, ha prodotto una serie di modificazioni (attraverso l'inserimento di nuove disposizioni o la correzione di quelle previgenti) e abrogazioni delle disposizioni incompatibili del cd Codice della *privacy* del 2003¹².

10 Articolo 16 TFUE (*ex* articolo 286 del TCE): «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea».

11 L'adozione del GDPR è stata prevista nella Comunicazione della Commissione europea «Salvaguardare la *privacy* in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo», del 25 gennaio 2012, ove si precisa che nel nuovo mondo digitale è diritto di chiunque avere il controllo effettivo delle proprie informazioni personali, essendo stata riconosciuta come diritto fondamentale in Europa dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e dall'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE). In tal senso la riforma della protezione dei dati, poi attuata con il GDPR, ha puntato proprio all'introduzione di un quadro normativo globale, coerente, solido e moderno per la protezione dei dati nell'Unione europea.

12 Il Codice della *privacy*, a seguito degli ultimi interventi legislativi, è stato denominato «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679 del Parlamento Europeo e

Contestualmente al GDPR, nella medesima data del 27 aprile 2016, il legislatore europeo ha adottato la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio; tale direttiva doveva essere recepita entro il 6 maggio 2018, pertanto il legislatore nazionale ha provveduto mediante il decreto legislativo 18 maggio 2018, n. 51.

Con tale atto normativo sono state, quindi, riscritte le regole concernenti il trattamento di dati personali effettuato per «ragioni di giustizia penale» e per «finalità di polizia», che sono subentrate allo speciale sistema regolatorio definito in precedenza dal Codice della *privacy* (le cui specifiche disposizioni sono state espressamente abrogate) e che costituiscono il fondamentale riferimento normativo per i trattamenti effettuati per «finalità di polizia», quelli cioè direttamente correlati con lo svolgimento dei compiti di tutela dell'ordine e della sicurezza pubblica, di prevenzione e repressione dei reati.

In questo specifico settore, tuttavia, trova ancora applicazione il decreto del Presidente della Repubblica del 15 gennaio 2018, n. 15, concernente il «Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia».

3. Finalità, oggetto e ambito di applicazione della protezione

Il Regolamento europeo sulla protezione dei dati (GDPR) si pone due obiettivi:

- 1) garantire un livello coerente ed elevato di protezione per gli individui con riguardo ai propri dati personali e
- 2) assicurare la libera circolazione di tali dati nell'ambito dell'Unione.

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».

Si tratta di due aspetti strettamente correlati, in quanto la protezione dei diritti della persona è l'obiettivo da perseguire soprattutto quando il dato personale circola e diventa strumento di potenziale lesione delle prerogative individuali; dall'altra parte, il fine di salvaguardia della persona fisica deve essere integrato con l'esigenza di regolamentazione del mercato, poiché è evidente che la circolazione del dato afferisce a situazioni economicamente rilevanti, in quanto elemento necessario dello sviluppo e del progresso economico.

Per entrambi i profili è necessario rilevare che la tutela non può essere assoluta, in quanto il diritto alla protezione dei dati (strumentale alla tutela delle persone) deve sopportare affievolimenti (ovvero rischi consentiti), ma anche il diritto alla circolazione dei dati deve sopportare condizioni limitanti, dunque, non si può parlare di una prerogativa individuale piena e assoluta, esercitabile *erga omnes*, ma, al pari di tutti i diritti, anche quelli inviolabili, va considerata alla luce della sua funzione sociale e va contemperata con altri diritti fondamentali o interessi generali, in ottemperanza al principio di proporzionalità¹³.

È necessario, in ogni caso, considerare che il legislatore europeo è ben consapevole del fatto che la disciplina del trattamento dei dati personali involve la tutela di tutti «[...] i diritti e le libertà fondamentali [...]» riconosciuti alle «[...] persone fisiche [...]», pertanto non soltanto il «diritto alla protezione dei dati personali», ma anche il diritto al rispetto della vita privata e familiare, la libertà di pensiero, la libertà d'informazione, ecc., che dalla protezione dei dati ottengono tutela mediata.

Per quanto concerne l'*ambito di applicazione materiale*, le disposizioni del GDPR si applicano «[...] al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi¹⁴», con la precisazione che l'archivio debba intendersi come

13 Si valuti, in particolare, quanto statuito dal "Considerando" 4 del GDPR, che recita: «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

14 Vds. art. 2, paragrafo 1, GDPR e art. 1, comma 2, D.Lgs. 18 maggio 2018, n. 51.

un insieme strutturato di dati personali accessibili secondo criteri determinati¹⁵, laddove il ricorso a strumenti elettronici di immagazzinamento dei dati è per sua natura ‘strutturato’. Il GDPR, tuttavia, precisa che è esclusa l’applicazione della disciplina giuridica al trattamento realizzato «da una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico», quindi senza una connessione con un’attività commerciale o professionale¹⁶.

Va sottolineato che permane uno spazio valutativo discrezionale circa la “destinazione in archivio”, cui potrebbe corrispondere un’ambiguità applicativa. Sul punto è necessario rimettersi al prudente apprezzamento del titolare del trattamento, dell’Autorità di controllo e, in caso di contenzioso, del Giudice.

Riguardo all’*ambito di applicazione territoriale*, il GDPR prevede tre ipotesi di applicazione della normativa *de qua*:

1. qualora il trattamento sia effettuato nelle attività poste in essere da uno stabilimento di un titolare del trattamento o di un responsabile del trattamento operanti nell’Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell’Unione (art. 3, paragrafo 1). Il Legislatore prende di mira il soggetto: se è “europeo”, anche se delocalizza il trattamento dei dati, deve esportare il modello di disciplina. Da un lato, tutto ciò rende omogenee le condizioni di partenza di tutti gli operatori economici che operano con l’estero e, dall’altro, rende beneficiari della disciplina persone fisiche anche che non “si trovano” in Europa;
2. nel caso in cui i soggetti interessati dal trattamento si trovino nell’Unione, sebbene il titolare o il responsabile del trattamento non siano stabiliti nell’Unione, quando le attività di trattamento riguardano: a) l’offerta di beni o la prestazione di servizi ai suddetti interessati nell’Unione, indipendentemente

15 Si può considerare ‘strutturato’ un fascicolo cartaceo che consenta una ricerca rapida e semplice di tutte le informazioni in esso contenute. Lo scopo di tale previsione, d’altronde, è anche quella di impedire l’elusione delle restrizioni previste dalla legge per il trattamento automatizzato di dati (cfr. *Manuale del diritto europeo in materia di protezione dei dati*, Publications Office of the European Union, 2018, p. 113).

16 Cfr. art. 2, paragrafo 2, lett. c), GDPR. Il “Considerando” 18 del GDPR precisa che «le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari o l’uso dei *social network* e attività *online* intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell’ambito di tali attività a carattere personale o domestico».

dall'obbligatorietà di un pagamento da parte dell'interessato oppure b) il monitoraggio del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione (art. 3, paragrafo 2). Questa ipotesi considera l'ubicazione del soggetto cui si riferiscono i dati personali: se si trova nell'Unione si applica il Regolamento¹⁷;

3. nell'evenienza in cui il trattamento sia effettuato da un titolare che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (art. 3, paragrafo 3).

Nel prevedere una disciplina così ampia, il legislatore europeo ha inteso evitare lacune di tutela che riguardano lo spazio europeo, introducendo alcune scelte di sostanziale *extra-territorialità* della propria efficacia per soddisfare le ragioni della parità di trattamento tra operatori economici e quelle della tutela del cittadino. La normativa, tuttavia, deve necessariamente confrontarsi con la dimensione 'ubiquitaria' dei trattamenti in rete e del fatto che non risulta ontologicamente possibile porre rimedio al fatto che gli strumenti di indagine/correttivi/autorizzativi non sono perseguibili ovunque.

A questo punto, è necessario comprendere cosa si intende per "*dato personale*", oggetto della protezione da parte della normativa¹⁸. Sintetizzando il dato normativo, rientra nell'ambito di tutela *qualsiasi informazione*, ossia qualunque elemento di conoscenza che possa riguardare la persona fisica (la sua vita professionale, privata, familiare o qualsiasi altro tipo di attività), che sia incentrata su una situazione di fatto (ad es. la presenza di una sostanza nel sangue di una persona), ma anche 'soggettiva', cioè riferirsi a opinioni o valutazioni (ad es. affidabilità di chi richiede un prestito a un istituto bancario).

L'informazione può essere resa disponibile, inoltre, in qualsiasi forma (alfabetica, numerica, grafica, fotografica o acustica), quale che sia il supporto materiale che la contiene (carta, *hard disk*, DVD, ecc.). Il

17 La norma si riferisce agli interessati che "si trovano" nell'Unione: si ritiene che "trovarsi" si riferisca a qualsiasi situazione (reale o virtuale) che colleghi la persona fisica al territorio europeo.

18 A tal proposito, l'art. 4, paragrafo 1, punto 1), GDPR, fa riferimento «a qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

fatto che l'informazione sia vera o falsa, poi, non rileva, anzi, l'inesattezza o la mendacità della stessa è idonea a produrre effetti pregiudizievoli ancora più severi rispetto a una vera o esatta.

È necessario anche che sia individuabile un collegamento tra informazione e persona fisica, nel senso che il dato tutelabile può riguardare direttamente l'interessato, quando l'elemento informativo è focalizzato su di esso (come nel caso dei dati identificativi, quali il nome, la data di nascita, ecc.), o indirettamente, quando invece si riferisca a oggetti che abbiano un legame con l'interessato (come nel caso di una targa di immatricolazione di un veicolo o di un numero telefonico).

Giova precisare che la protezione viene assicurata esclusivamente alle persone fisiche, che siano identificate o identificabili, con esclusione degli enti e delle persone giuridiche¹⁹. Rispetto al concetto di identificazione, si può affermare che si tratta del presupposto più importante, poiché, nel caso in cui venga meno, si dovrebbe parlare di "informazione anonima". Le informazioni "anonime" possono essere tali *ab origine* (la persona fisica, cioè, non è mai stata identificata o non è identificabile), oppure essere state successivamente "anonimizzate" (la persona fisica è resa anonima *ex post*, così da non consentirne più l'identificazione, con l'eliminazione integrale e definitiva di tutti gli elementi identificativi). Le "informazioni anonime", pertanto, rimangono fuori dal campo di applicazione delle norme in esame²⁰.

19 Anche le persone decedute sarebbero escluse dall'applicazione della tutela normativa. Ciò nonostante, il GDPR al "Considerando" 27 stabilisce che «gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute». Ciò ha consentito al legislatore nazionale di introdurre l'art. 2-terdecies al Codice della *privacy*, che stabilisce che i diritti azionabili dagli interessati (articoli da 15 a 22, GDPR), «[...] possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato [i.e. della persona deceduta], in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione».

20 Occorre, tuttavia, chiarire che la 'pseudonimizzazione', vale a dire il trattamento dei dati personali in modo tale che gli stessi non possano più 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, resta assoggettata alla legislazione in materia di protezione dei dati (cfr. *Manuale del diritto europeo in materia di protezione dei dati*, cit., p. 107). Il GDPR, infatti, riconosce diversi usi della pseudonimizzazione quale misura tecnica appropriata per migliorare la protezione dei dati ed è menzionata specificamente per la progettazione e la sicurezza del trattamento dei dati. È, inoltre, una garanzia adeguata che potrebbe essere utilizzata per il trattamento dei dati personali per finalità diverse da quelle per le quali sono stati inizialmente raccolti.

Più nello specifico, la definizione fa riferimento all'“identificativo”, ossia a un elemento presente nel dato personale che, in virtù dello stretto rapporto con l'interessato, permette il processo d'identificazione, che può essere “diretto”, quando avviene attraverso i cd dati identificativi immediati (nome, cognome, data di nascita, ecc.), o “indiretto”, quando si realizza, ad esempio, mediante un numero di telefono, la targa di immatricolazione un veicolo, un indirizzo IP (*Internet Protocol*), un numero di previdenza sociale, dei *file* informatici, dei *cookie*, degli strumenti di sorveglianza del traffico *web*, le immagini della videosorveglianza, ma anche dati biometrici, come le impronte digitali, le foto digitali o le scansioni dell'iride, in ogni caso con elementi che necessitano di essere combinati con altri (come una banca dati) per consentire la distinzione di una persona specifica dall'altra.

Sul punto il “Considerando” 26 del GDPR²¹ spiega che il parametro di riferimento consiste nel determinare la possibilità che mezzi identificativi ragionevoli siano a disposizione e siano gestiti dai potenziali utenti delle informazioni; ai fini della valutazione della sussistenza di un'esigenza di protezione, si deve considerare un insieme di fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici: una persona non è, dunque, considerata “identificabile” se la sua individuazione richiede tempi, sforzi o risorse irragionevoli.

4. La definizione di trattamento e i principi applicabili

Prima di illustrare nel dettaglio i principi applicabili al trattamento dei dati personali, si ritiene utile soffermarsi sulla nozione stessa di «trattamento», che deve essere identificata in «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio

21 “Considerando” 26: «[...] Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca».

di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»²². Si tratta di una nozione talmente ampia da abbracciare qualsiasi sorta di operazione eseguibile sui dati personali, «con o senza l'ausilio di processi automatizzati».

Ciò premesso, nel GDPR la disciplina dei principi della protezione dei dati si sviluppa su piani differenti. Ci sono disposizioni generali sui principi (art. 5) e altre disposizioni generali distinte per categorie di dati (artt. da 6 a 11). Nel dettaglio, i principi generali che devono essere rispettati in ogni fase dello sviluppo del trattamento sono:

1. «liceità, correttezza e trasparenza»;
2. «limitazione della finalità»;
3. «minimizzazione dei dati»;
4. «esattezza»;
5. «limitazione della conservazione»;
6. «integrità e riservatezza»;
7. «responsabilizzazione».

È lecito un trattamento che non violi norme generali e norme specifiche dell'ordinamento giuridico, pertanto è necessario o il *consenso dell'interessato*²³ per una o più specifiche finalità o un'altra base legittima prevista dalla legislazione, vale a dire le condizioni tassative e collocate sul medesimo livello di importanza rispetto al consenso, *ex art. 6 GDPR*.

Le cause di liceità, alternative al consenso, si configurano quando il trattamento deve essere strumentale *all'esecuzione di un contratto o di misure precontrattuali* adottate su richiesta dell'interessato o anche *all'adempimento di un obbligo legale al quale è soggetto il titolare del tratta-*

²² Cfr. art. 4, paragrafo 1, punto 2), GDPR.

²³ Per la definizione di consenso, cfr. art. 4, paragrafo 1, punto 11), GDPR: «Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». Il "Considerando" 32 precisa che lo stesso «[...] dovrebbe essere prestato mediante un atto positivo inequivocabile [...], ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. [...] Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste [...]».

mento²⁴; vi può essere anche l'ipotesi in cui il trattamento sia necessario alla *salvaguardia degli interessi vitali dell'interessato* o di un'altra persona fisica²⁵ oppure sia connesso *all'esecuzione di un compito di interesse pubblico o all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*²⁶; vi è, infine, l'ultimo caso in cui il trattamento sia dovuto ai fini del *perseguimento del legittimo interesse del titolare del trattamento* o di terzi²⁷, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, in particolare se quest'ultimo è un minore.

Per quanto concerne, infine, le autorità di polizia, l'art. 1, comma 2, D.Lgs. 18 maggio 2018, n. 51 prevede come espressa causa di liceità la necessità di svolgere i compiti istituzionali di tutela dell'ordine e della sicurezza pubblica, di prevenzione e repressione dei reati.

Particolari condizioni di liceità sono previste, poi, per le *"categorie particolari di dati personali"*²⁸ per i quali vige un divieto di trattamento,

24 Un esempio di rilievo è quello dei gestori delle strutture ricettive, i quali, ai sensi dell'art. 109, comma 3, Testo unico delle leggi di pubblica sicurezza (TULPS), sono tenuti a comunicare le generalità degli alloggiati alle Questure territorialmente competenti. Esempi analoghi sono anche rinvenibili nella normativa antiriciclaggio e in quella fiscale relativamente ai dati da far confluire nell'anagrafe tributaria.

25 Il "Considerando" 46, GDPR precisa che questa causa di liceità «dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica, [...] per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana [...]». Deve costituire, pertanto, l'*extrema ratio*.

26 Qui è l'interesse pubblico a prevalere sul divieto di trattamento. La fattispecie interessa essenzialmente l'attività istituzionale dei soggetti pubblici, funzionale allo svolgimento di compiti di interesse pubblico, pur potendosi applicare ai soggetti privati nell'esercizio di pubblici poteri. La base giuridica è costituita da una norma di legge o di regolamento o da atti amministrativi generali. L'art. 2-ter, comma 1-bis, Codice della *privacy*, così come modificato dal d.l. 8 ottobre 2021, n. 139, convertito con modificazioni dalla legge 3 dicembre 2021, n. 205, ha statuito che «[...] il trattamento dei dati personali da parte di un'amministrazione pubblica [...] è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti». Nel settore pubblico, dunque, assurge ad autonomo presupposto di liceità la (mera) necessità dell'adempimento del compito di pubblico interesse o dell'esercizio del pubblico potere.

27 All'individuazione dei casi concreti riconducibili alla fattispecie del legittimo interesse concorrere lo stesso GDPR, il quale espone nei "Considerando" un'ampia gamma di esempi. Sussiste, quindi, nei casi in cui «[...] l'interessato è un cliente o è alle dipendenze del titolare del trattamento», «[...] del titolare del trattamento interessato a trattare dati personali strettamente necessari a fini di prevenzione delle frodi [...]» (consid. 47), oppure nell'ipotesi di «[...] dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione [...]» (consid. 49).

28 Si fa riferimento a dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati

a meno che non si verifichino una serie tassativa di “eccezioni” (art. 9, GDPR), tra le quali si possono citare: l’interessato ha prestato il proprio consenso esplicito al trattamento; qualora i dati personali siano stati resi manifestamente pubblici dall’interessato; per il perseguimento di finalità politiche, filosofiche, religiose o sindacali da parte di una fondazione, associazione o altro organismo senza scopo di lucro; per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell’interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; per tutelare un interesse vitale dell’interessato o di un’altra persona fisica, qualora l’interessato si trovi nell’incapacità fisica o giuridica di prestare il proprio consenso; per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniquale volta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; per motivi di interesse pubblico rilevante sulla base del diritto dell’Unione o degli Stati membri; per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali²⁹; per motivi di interesse pubblico nel settore della sanità pubblica; per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Il principio di correttezza implica un concetto di rispetto di norme etiche, deontologiche non “codificate”, ovvero osservanza di accorgimenti per rendere equilibrate le singole posizioni, adeguando il trattamento alle esigenze reciproche, oltre lo stretto dato normativo. Le operazioni di trattamento non devono essere eseguite in segreto e gli interessati dovrebbero essere informati dei potenziali rischi. Inoltre, i responsabili del trattamento dei dati dovrebbero, per quanto possibile, agire in modo da conformarsi prontamente alla volontà dell’interessato, specialmente quando il suo consenso costituisce la base giuridica del trattamento dei dati.

Il concetto di trasparenza implica il dovere di tutelare la consapevolezza dell’interessato; può riferirsi alla tracciabilità del dato a favore

genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona (art. 9, comma 1, GDPR).

29 Questa eccezione si applica soltanto se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell’Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch’essa soggetta all’obbligo di segretezza conformemente al diritto dell’Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

dell'interessato, alle informazioni fornite alla persona prima dell'inizio del trattamento, alla facile accessibilità dei dati durante il trattamento, ma anche alle informazioni fornite agli interessati a seguito di una richiesta di accesso ai dati che li riguardano.

Le operazioni di trattamento devono essere illustrate agli interessati in modo facilmente comprensibile, affinché possano capire cosa accadrà ai loro dati. Ciò significa che la finalità specifica del trattamento dei dati personali deve essere conosciuta dall'interessato al momento della raccolta di detti dati personali. La trasparenza del trattamento richiede, infine, che sia utilizzato un linguaggio semplice e comprensibile. I soggetti coinvolti devono essere informati chiaramente sui rischi, sulle norme, sulle garanzie e sui diritti relativi al trattamento dei propri dati personali.

Il principio di limitazione della finalità si esprime nel senso che i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità [...]»³⁰, salvi gli ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche, che sono consentiti a seguito dell'adozione di garanzie adeguate, come l'anonimizzazione, la criptatura o la pseudonimizzazione dei dati e la limitazione dell'accesso.

Gli scopi, che si intendono perseguire mediante la 'raccolta' e il successivo trattamento dei dati devono essere, quindi, individuati con precisione, resi immediatamente evidenti, privi di ambiguità e non devono contrastare con la legge. Ogni finalità di trattamento, inoltre, deve avere la propria base giuridica specifica. Il principio evidenzia, dunque, che la finalità del trattamento ne condiziona la liceità pertanto, un nuovo scopo che sia emerso *medio tempore* e che non sia compatibile con le finalità iniziali deve avere la propria base giuridica specifica e non può fondarsi sul fatto che i dati fossero stati inizialmente acquisiti o trattati per un'altra finalità legittima³¹.

Il principio di minimizzazione dei dati impone che i dati personali siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»³². Esso implica una riduzione al minimo del numero dei dati, del tipo dei trattamenti, dei soggetti che a vario titolo possono avere contezza dei dati, del periodo di conser-

30 Articolo 5, paragrafo 1, lettera b), GDPR.

31 Così BERNARDI N., *Privacy. Protezione e trattamento dei dati*, IPSOA, Milano 2019, 81.

32 Articolo 5, paragrafo 1, lettera c), GDPR.

vazione. Determinante per una corretta valutazione del rispetto del principio di “minimizzazione” è l’esplicitazione iniziale della finalità. Si aggiunge, inoltre, che tale principio deve essere inteso in senso oggettivo, non potendosi attribuire rilevanza alla percezione soggettiva del titolare del trattamento.

Il principio di esattezza comporta che i dati personali debbano essere «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati³³». Il canone della esattezza del dato è di relativa facile applicazione per i dati oggettivi (che possono essere “veri” o “falsi”), mentre è di impossibile applicazione per i dati soggettivi (vedasi la profilazione). Per i dati soggettivi, la valutazione più congrua è quella della correttezza. Nel concetto di esattezza rientra anche quella di aggiornamento dei dati un tempo esatti e non più tali e di integrazione di dati un tempo completi di sopravvenuta lacunosità.

Il principio di limitazione della conservazione determina che i dati personali siano «conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati». Possono, comunque, essere «[...] conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici [...]»³⁴. L’articolo 17, paragrafo 1, lettera a), GDPR, precisa che, una volta venute meno le finalità per le quali i dati sono stati raccolti e trattati, gli stessi devono essere cancellati.

Il principio di integrità e riservatezza implica che i dati personali, infine, siano «trattati in maniera da garantire un’adeguata sicurezza [...], compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali³⁵». La sicurezza del trattamento si concretizza proprio in specifici obblighi gravanti sul trattamento del titolare, in modo da minimizzare i rischi di distruzione e perdita del dato (violazione di disponibilità), di modifica indebita (violazione di integrità), di divulgazione o accesso non autorizzati (violazione della riservatezza). Il legislatore europeo e, di conseguenza, anche quel-

33 Articolo 5, paragrafo 1, lettera d), GDPR.

34 Articolo 5, paragrafo 1, lettera e), GDPR.

35 Articolo 5, paragrafo 1, lettera f), GDPR.

lo nazionale hanno prefigurato per il titolare un modello di condotta flessibile, adattabile ai casi concreti, finalizzato al conseguimento dell'effettiva protezione dei dati personali, senza che siano indicate *ab origine* misure predefinite. Appare, pertanto, superato il modello delle "misure minime" di sicurezza, che erano elencate minuziosamente nella vecchia versione del Codice della *privacy* (artt. 33 e seg.) ed erano finalizzate ad assicurare un livello minimo di protezione.

L'art. 5 GDPR chiude l'elencazione dei principi con quello, fondamentale, di responsabilizzazione (*accountability*), concetto che esprime, in una parola, l'attribuzione al titolare del trattamento dell'obbligo giuridico di osservare il Regolamento e le altre fonti e dell'onere processuale della prova di averlo fatto. Si tratta di una delle novità più rilevanti introdotte dal GDPR e anche dal decreto legislativo 18 maggio 2018, n. 51 con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

È la disposizione più commentata dell'intero GDPR, i cui punti salienti sono di seguito sintetizzati:

- la responsabilizzazione richiede da parte dei titolari e dei responsabili del trattamento di adottare attivamente e in modo permanente misure finalizzate alla promozione e alla salvaguardia della protezione dei dati nelle attività di trattamento.
- I titolari e i responsabili del trattamento sono responsabili della conformità alla normativa in materia di protezione dei dati nell'ambito delle operazioni di trattamento e dei rispettivi obblighi.
- I titolari del trattamento devono essere in grado di dimostrare in qualsiasi momento agli interessati, al pubblico in generale e alle Autorità di controllo che essi operano in conformità delle disposizioni sulla protezione dei dati³⁶.

I titolari del trattamento possono facilitare il rispetto di questo requisito in diversi modi, tra cui:

- tenere un registro delle attività di trattamento e, su richiesta, metterlo a disposizione dell'Autorità di controllo (art. 30 GDPR);
- in determinate situazioni, designare il responsabile della protezione dei dati, che è coinvolto in tutte le questioni connesse alla protezione dei dati personali (artt. 37- 39 GDPR);

36 Cfr. *Manuale del diritto europeo in materia di protezione dei dati*, cit., p. 150.

- svolgere valutazioni d'impatto sulla protezione dei dati per i tipi di trattamento che presentano un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 GDPR);
- garantire la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita (art. 25 GDPR);
- prevedere modalità e procedure per l'esercizio dei diritti degli interessati (artt. 12 e 24 GDPR);
- aderire a codici di condotta approvati o a meccanismi di certificazione (artt. 40 e 42).

Si riporta un'importante precisazione a proposito del responsabile del trattamento e cioè che, pur non essendo il principio di responsabilizzazione specificamente rivolto a queste figure, esistono disposizioni connesse alla responsabilità, che contengono anche obblighi riguardanti questi ultimi, come tenere un registro delle attività di trattamento e designare il responsabile della protezione dei dati per le attività di trattamento che lo richiedono. I responsabili del trattamento devono, altresì, assicurare l'adozione di tutte le misure richieste per garantire la sicurezza dei dati. Il contratto, giuridicamente vincolante tra il titolare e il responsabile del trattamento, deve prevedere che quest'ultimo assista il titolare con riferimento al rispetto di alcuni obblighi, ad esempio nello svolgimento di una valutazione d'impatto sulla protezione dei dati o quando notifica al titolare del trattamento eventuali violazioni non appena ne viene a conoscenza.

5. I soggetti attivi del trattamento

Nel trattare il principio di responsabilizzazione è stato fatto cenno ai soggetti coinvolti nel trattamento dei dati personali. A questo punto diventa essenziale comprendere quali sono le varie figure e quali compiti e doveri ricadono su ciascuno di essi.

Nelle definizioni dell'art. 4 GDPR sono individuate le figure del titolare del trattamento, del responsabile del trattamento e del rappresentante, mentre agli articoli dal 37 al 39 è contemplato il responsabile della protezione dei dati.

Il titolare del trattamento, a norma dell'art. 4, paragrafo 1, punto 7), GDPR è «la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». La medesima disposizione chiarisce che, qualora le finalità e i mezzi del trattamento siano definiti

direttamente dal diritto europeo o degli Stati membri, il titolare può essere individuato direttamente dallo stesso atto normativo, a monte.

Il riferimento a una persona fisica quale titolare deve, tuttavia, limitarsi ai casi in cui il trattamento sia effettuato a titolo personale (*i.e.* libero professionista, artigiano, ecc.). Quando il trattamento avvenga nell'ambito di una persona giuridica o di un altro organismo, come una pubblica amministrazione, la qualifica di titolare deve essere riferita all'entità nel suo complesso (il Ministero, la Regione, la società, l'associazione, ecc.) e non alle persone fisiche che operano al suo interno, cui sono attribuiti poteri decisionali o rappresentativi: la formulazione della disciplina normativa esclude evidentemente la possibilità di titolarità individuali.

Costituisce un elemento di novità, invece, la disciplina della fattispecie dei "contitolari nel trattamento", che ricorre «allorché due o più titolari [...] determinano congiuntamente le finalità e i mezzi del trattamento³⁷». In tali casi i "contitolari" sono tenuti a stipulare un accordo interno per regolare «[...] le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal [...] regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati». L'accordo deve essere posto nella disponibilità dell'interessato, che, in ogni caso, può decidere di esercitare i propri diritti nei confronti di e contro ciascun titolare.

L'art. 24 GDPR definisce quali siano le responsabilità del titolare del trattamento, che si concretizzano essenzialmente nel mettere in atto misure tecniche e organizzative adeguate ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR, con l'obbligo ulteriore di procedere al riesame e all'aggiornamento delle misure qualora necessario. In estrema sintesi, il titolare è il capo che decide, ma è anche quello che sopporta le conseguenze dei trattamenti effettuati e ciò costituisce essenzialmente la massima espressione del cd "principio di responsabilizzazione". Egli deve scegliere e istruire i soggetti che sono autorizzati ad accedere ai dati personali, a mente degli artt. 29 e 32, paragrafo 4, GDPR; designa il "responsabile del trattamento" (art. 28 GDPR) e il "responsabile della protezione dei dati"

³⁷ Cfr. art. 26, paragrafo 1, GDPR.

(RPD), nei casi in cui sia previsto (art. 37 GDPR); qualora ci sia una violazione dei dati personali, infine, è tenuto a notificare tale evenienza al Garante per la protezione dei dati personali (articolo 33 GDPR) e a comunicarlo all'interessato (articolo 34 GDPR).

La protezione dei dati può essere realizzata già dalla fase di progettazione e sviluppo del processo di trattamento, mediante l'adozione di misure *standard* adeguate (*ccdd by design*), inoltre per impostazione predefinita (misure *by default*) devono essere adottate tecniche organizzative che impongano il trattamento dei soli dati necessari per ogni specifica finalità, con limitazioni previste in relazione alla quantità dei dati raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità (art. 25 GDPR).

Il ruolo attivo, delineato dalla normativa, determina che, nel caso in cui il titolare del trattamento sia un'Autorità pubblica, le condotte foriere di pregiudizio erariale siano frequentemente connotate da un atteggiamento di omissione o inerzia, poste in essere con dolo o colpa grave. Un'ipotesi specifica di danno erariale, imputabile ai pubblici dipendenti, può, infatti, delinearsi nei casi di pagamento di una somma di denaro a titolo di sanzione amministrativa pecuniaria inflitta dal Garante per la protezione dei dati personali nei riguardi di una pubblica amministrazione, nel cui ambito sia stato accertato un trattamento illecito di dati personali.

La configurabilità nelle predette evenienze della responsabilità personale dei pubblici dipendenti ha trovato conferma nella giurisprudenza della Corte dei conti³⁸, la quale ha messo in evidenza come «le conseguenze della violazione della disciplina in materia di protezione dei dati personali non si esauriscano nel provvedimento sanzionatorio irrogato dal Garante nei confronti dell'amministrazione pubblica, dovendo proseguire in sede di giudizio per danno erariale nei confronti della persona che con il proprio comportamento almeno di colpa grave abbia determinato la perdita patrimoniale correlata al pagamento della sanzione amministrativa³⁹».

38 Vds. Corte dei conti per la regione Calabria, sentenza 31 ottobre 2019, n. 429 e Corte dei conti per la regione Lazio, sentenza 28 maggio 2019, n. 246.

39 Così la circolare del Dipartimento della pubblica sicurezza, Segreteria del Dipartimento, prot. n. 68051 del 21 luglio 2023. Nella medesima circolare è stato raccomandato ai Dirigenti dei vari Uffici, centrali e periferici del predetto Dipartimento, di prestare particolare cura nella trattazione delle questioni che attengono alla specifica materia del trattamento dei dati personali, coinvolgendo anche la nuova figura del funzionario "referente per la protezione dei dati personali".

Il responsabile del trattamento è definito come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento» (art. 4, paragrafo 1, punto 8), GDPR). Anche rispetto alla scelta del responsabile, il titolare deve dimostrare di aver adottato le misure organizzative più appropriate, designando i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato⁴⁰.

La scelta di nominare un responsabile del trattamento si verifica quando il titolare decida di non gestire in prima persona una porzione o tutti i trattamenti di sua pertinenza; in questo caso, ha la possibilità di "esternalizzare" tale gestione, rivolgendosi a un soggetto che lo faccia per conto suo, vincolandolo obbligatoriamente con un "contratto di servizi". Il compito di trattare dati "per conto" implica un rapporto simile a quello della rappresentanza.

I contenuti dell'attività delegata al responsabile del trattamento, infatti, devono essere regolati «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 [*melius* "che definisca l'oggetto"] 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», (art. 28, paragrafo 3, DGPR). È stabilito, infine, che il contratto sia stipulato in forma scritta, anche in formato elettronico.

Come già precisato, il responsabile opera per conto del titolare, ma sulla base di "istruzioni" che riceve e attua; pertanto, è sempre il titolare che ha deciso le finalità e i mezzi del trattamento, a dover rispondere dell'attuazione delle misure tecniche e organizzative adeguate. Se un responsabile del trattamento, tuttavia, viola le vigenti disposizioni, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento vero e proprio e di tale illecito trattamento diviene *corresponsabile* (art. 28, paragrafo 10, GDPR). Al di fuori di questa specifica ipotesi, il responsabile del trattamento risponde *direttamente* per i danni causati dal mancato adempimento delle disposizioni normative specificamente dirette alla disciplina della sua figura o ha agito in modo difforme dalle istruzioni del titolare del trattamento.

⁴⁰ Cfr. art. 28, paragrafo 1, GDPR.

Dal complesso delle disposizioni vigenti, si evince che il responsabile svolge l'attività delegata dal titolare all'esterno dell'organizzazione di questi. La stipulazione di un contratto o altro atto giuridico che vincoli tali soggetti, regolando i reciproci rapporti giuridici, non si concilia, infatti, con l'esistenza tra gli stessi di un rapporto di lavoro dipendente. La figura del responsabile del trattamento incardinato nell'organizzazione del titolare, quindi, appare incompatibile con il nuovo quadro normativo. Ciò rappresenta un importante momento di discontinuità rispetto a quanto previsto dal vecchio Codice della *privacy*, il quale contemplava la possibilità di designare "responsabili interni" all'organizzazione del titolare (art. 29)⁴¹. Il titolare può, in ogni caso, affidare ai propri collaboratori e dipendenti compiti specifici in materia di protezione dei dati personali, analoghi a quelli assegnati dal Codice ai "responsabili interni", senza, tuttavia, che ciò determini l'acquisizione di una denominazione e di un ruolo specifico.

Nonostante l'apparente chiarezza dei concetti astratti, l'individuazione in concreto della responsabilità del trattamento è tutt'altro che pacifica e ha dato adito a numerose opinioni contrastanti⁴².

Per quanto concerne i soggetti autorizzati al trattamento, il Regolamento si limita a prevedere che chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento e 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 (art. 29 GDPR). I collaboratori e i dipendenti del titolare o del responsabile del trattamento possono, quindi, essere autorizzati a trattare i dati personali, a condizione che ricevano adeguate istruzio-

41 Questa disposizione è stata abrogata con il decreto legislativo di adeguamento, 10 agosto 2018, n. 101.

42 Si veda, ad esempio, la risposta del Garante per la protezione dei dati personali del 22 gennaio 2019 ai Consulenti del Lavoro, secondo la quale costoro devono essere considerati titolari quando sono persone fisiche (liberi professionisti) che trattano, in piena autonomia e indipendenza, i dati dei propri dipendenti oppure quelli dei propri clienti, mentre sono da configurare come responsabili esterni del trattamento quando trattano i dati dei dipendenti dei propri clienti (es: per l'elaborazione dei cedolini paga, la gestione dei trattamenti relativi all'assunzione e a quelli di fine rapporto, la gestione degli adempimenti previsti dalla disciplina previdenziale ed assistenziale, ecc.). In questi casi, è, infatti, il cliente ad essere titolare del trattamento dei dati dei propri dipendenti, che delega al consulente del lavoro lo svolgimento di tutti gli adempimenti previsti dalla normativa lavoristica e/o dal contratto di lavoro, impartendo specifiche direttive. Il consulente del lavoro dovrà, pertanto, farsi nominare dal cliente quale responsabile esterno del trattamento dei dati, con apposito contratto redatto per iscritto, in cui siano disciplinati dettagliatamente compiti e responsabilità incombenti su entrambi.

ni operative. Tali figure non vengono denominate ufficialmente dalle fonti normative, laddove prima del GDPR si parlava espressamente di “incaricato del trattamento”.

Il GDPR ha introdotto, viceversa, una nuova figura, di assoluta importanza, connotata dalla funzione di garanzia dell’osservanza delle disposizioni in materia di protezione dei dati personali, che è il responsabile della protezione dei dati. Questi svolge una funzione di informazione, consulenza, sorveglianza e di collegamento con il Garante e con gli interessati. Viene designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all’applicazione del GDPR e della normativa interna. Coopera con l’Autorità (e proprio per questo, il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 37, 38 e 39 del Regolamento).

Il GDPR prevede tre specifiche situazioni, tra loro alternative, in cui il titolare del trattamento e il responsabile designano sistematicamente (*melius*, obbligatoriamente) il responsabile della protezione dei dati⁴³. Tra queste situazioni, assume particolare rilievo quella in cui «il trattamento è effettuato da un’autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali». *Le autorità pubbliche e gli organismi pubblici, quindi, sono sempre tenuti a designare il RPD, indipendentemente dalla tipologia dei dati personali oggetto del trattamento.* Il soggetto investito può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi (se si tratta di una persona esterna)⁴⁴ e deve essere scelto in funzione

43 Art. 37, paragrafo 1, GDPR: «Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un’autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all’articolo 9 o di dati relativi a condanne penali e a reati di cui all’articolo 10».

44 In verità, l’art. 28, D.Lgs. 18 maggio 2018, n. 51 non contempla espressamente l’ipotesi di nomina tramite la stipulazione di un contratto di servizi, pertanto si ritiene che non sia ammissibile l’individuazione del RPD all’esterno dell’organizzazione del titolare del trattamento. In questo senso si è mosso il Dipartimento della pubblica sicurezza, che con il decreto

delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti precipui attribuiti a questa figura⁴⁵.

Il titolare o il responsabile del trattamento sono tenuti ad assicurarsi che il responsabile della protezione dei dati sia coinvolto adeguatamente e tempestivamente in tutte le questioni riguardanti la protezione dei dati personali e devono fornire le risorse necessarie per l'assolvimento dei compiti, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Relativamente ai compiti, gli artt. 39 GDPR, e 30, D.Lgs. 18 maggio 2018, n. 51, stabiliscono che questa figura debba almeno occuparsi di:

- a) *informare e fornire consulenza* al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

del Ministro dell'Interno, di concerto con il Ministro dell'Economia e delle Finanze, 6 febbraio 2020, ha definito le competenze dell'Ufficio VI – Sicurezza dati della Polizia di Stato, istituito presso la Segreteria del Dipartimento, che assicura le attività di raccolta di informazioni, analisi e verifica dei trattamenti dei dati effettuati, informazione, consulenza in favore del rispettivo responsabile, relativamente al Centro elettronico nazionale (CEN) della Polizia di Stato, ai sistemi informativi ed elaborativi, nonché alle reti di comunicazione della Polizia di Stato a livello centrale e periferico. Il responsabile dell'Ufficio viene considerato anche responsabile della protezione dei dati e svolge le relative funzioni di raccordo con il Garante. Il predetto ufficio provvede alle analisi dei rischi, all'elaborazione di direttive e atti di indirizzo.

Con circolare prot. n. 18635 del 9 marzo 2023, inoltre, è stata prevista l'istituzione del "referente della protezione dei dati personali", appartenente alla carriera dei funzionari della Polizia di Stato che espletano funzioni di polizia, avente il compito di fungere da 'punto di contatto' del responsabile della protezione dei dati - RPD e di coadiuvare i dirigenti delle articolazioni centrali e periferiche della Polizia di Stato. A favore di questa nuova figura sono stati organizzati allo stato due corsi di formazione.

- 45 Nel caso in cui il RPD sia un dipendente dell'Autorità pubblica o dell'organismo pubblico, è, in linea di massima, preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione. Nell'atto di designazione devono essere succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata. La specificazione dei criteri utilizzati, oltre a essere indice di trasparenza e di buona amministrazione, costituisce anche elemento di valutazione del rispetto del principio di "responsabilizzazione".

- b) *sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;*
- c) *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;*
- d) *cooperare con l'Autorità di controllo;*
- e) *fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*⁴⁶.

Il RPD non è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati, poiché spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento.

6. I principali adempimenti dei soggetti attivi del trattamento

A questo punto, dopo aver analizzato quali sono i soggetti attivi, può essere utile conoscere quali siano i principali adempimenti gravanti a carico degli stessi. A tal proposito, si deve fare innanzitutto riferimento all'obbligo, sancito dall'art. 30 GDPR, di tenuta di un registro delle attività di trattamento con lo scopo di monitorare e dimostrare che i trattamenti effettuati siano conformi alla disciplina normativa europea e nazionale; lo stesso costituisce, quindi, uno strumento fondamentale nell'attuazione del principio di responsabilità. Il GDPR prevede che tanto il titolare, quanto il responsabile del trattamento (ove tale figura sussista) debbano tenere un proprio registro.

Il censimento dei trattamenti rientra, a buon diritto, tra le attività prioritarie per la pianificazione e la gestione dell'attività di protezione dei dati personali: in sostanza, la conoscenza della propria struttura è

⁴⁶ A tale scopo, è imposto al titolare o responsabile del trattamento di pubblicare i dati di contatto del RPD, nonché di comunicare i medesimi al Garante. I dati di contatto devono contenere gli elementi necessari per poterlo raggiungere facilmente (ad es. recapito telefonico dedicato, indirizzo di posta elettronica personale, ecc.).

il tassello iniziale per enfatizzare azioni virtuose e rettificare attività a rischio o *contra legem*.

Il registro contiene le seguenti informazioni:

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il registro è tenuto in forma scritta, anche in formato elettronico, ed è messo a disposizione del Garante, quando sia da questi richiesto; occorre curare un aggiornamento periodico dei registri e che gli stessi siano coordinati con altri adempimenti documentali, quali le informative o altri atti che descrivono i trattamenti (dall'analisi dei rischi alla valutazione di impatto, alle istanze di consultazione preliminare). Sarebbe utile considerare il registro dei trattamenti come base dati iniziale, dalla quale attingere l'apparato informativo per gli altri adempimenti.

Tra questi obblighi bisogna comprendere quello inerente all'adozione di misure tecniche e organizzative adatte a garantire un livello di sicurezza adeguato al rischio, a mente dell'art. 32 GDPR. Naturalmente, adeguatezza al rischio significa adeguatezza a evitare o a ridurre (in termini socialmente accettabili) il rischio. Per la sicurezza del trattamento, pertanto, tutto parte dall'analisi del rischio, che va valutato nella sua sussistenza (c'è o meno un determinato rischio), nella sua frequenza (stima di quante volte il rischio in potenza diventa danno in atto), nella sua gravità (stima delle eventuali conseguenze del danno), nella determinazione delle misure (tecniche, organizzative, procedurali) e nel conteggio del costo economico per farvi fronte, nell'analisi comparative delle alternative.

Un ulteriore obbligo è descritto dall'art. 35 GDPR e consiste nella valutazione d'impatto sulla protezione dei dati, che deve intervenire quando un tipo di trattamento, allorché prevede, in particolare, l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche; il titolare del trattamento deve effettuare, pertanto, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Questo adempimento sostituisce l'obbligo di notificare alle Autorità di controllo il trattamento dei dati personali e si inserisce nel nuovo principio della responsabilizzazione del trattamento. Ai fini dell'adeguata elaborazione del sistema di sicurezza, pertanto, non sempre basta l'analisi dei rischi e la predisposizione di misure adeguate; in alcuni casi, caratterizzati dal livello elevato di rischio, bisogna documentare di avere valutato l'impatto sulla protezione dei dati, da cui dipende la protezione delle persone. Il significato della valutazione di impatto è quello di un *surplus* di ponderazione e di giustificazione a fronte di trattamenti ritenuti più pericolosi di altri⁴⁷.

Oltre alle ipotesi, meramente esemplificative, già previste dalla normativa, sulla base di quanto stabilito dall'art. 35, paragrafo 4, GDPR⁴⁸, il Garante ha adottato il provvedimento n. 467 dell'11 ottobre 2018, con il quale ha diffuso un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati. Si tratta di un elenco che non ha pretese di esaustività, adottato sulla base di quanto contenuto nelle «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento (UE) 2016/679», approvate il 4 aprile 2017 dal "Gruppo di lavoro articolo 29 per la protezione dei dati".

47 L'art. 35, paragrafo 3, GDPR richiede, in particolare, una valutazione nelle ipotesi di:

- a) trattamenti automatizzati, compresa la profilazione, di aspetti personali relativi a persone fisiche condotto in modo sistematico e globale;
- b) il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali, ai reati e alle connesse misure di sicurezza;
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (ad es. la videosorveglianza cittadina).

48 Art. 35, paragrafo 4, GDPR: «L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1 [...]».

La valutazione deve essere eseguita prima di procedere al trattamento; nei casi in cui il titolare non sia in grado di individuare misure idonee ad attenuare il rischio, residuando un “rischio elevato”, non è possibile avviare il trattamento ed è necessaria la consultazione preventiva del Garante, il quale, qualora ritenga che il trattamento non sia conforme alla normativa di riferimento fornisce un parere scritto.

Nello specifico, se il Garante ritiene che la valutazione sia stata condotta correttamente ma, ciò nonostante, permanga un rischio residuo, vieterà il trattamento. Se, viceversa, giunge alla conclusione che la valutazione non sia stata condotta correttamente o che le misure di minimizzazione siano insufficienti, può indicare dei rimedi per attenuare i rischi residui e ricondurli a un livello accettabile. È previsto, peraltro, un termine di otto settimane (sei per i trattamenti per finalità di polizia) prorogabile di ulteriori sei settimane (quattro nell'ipotesi disciplinate dal D.Lgs. 51/2018), trascorsi i quali e in assenza di una comunicazione, si intende reso un parere positivo, sebbene siano ammessi pareri tardivi negativi.

Il titolare del trattamento è sottoposto, infine, all'adempimento di particolari obblighi di notifica di una violazione dei dati personali all'Autorità di controllo (art. 33 GDPR) e di comunicazione all'interessato (art. 34 GDPR).

La violazione dei dati personali (*personal data breach*)⁴⁹ impone al titolare del trattamento, sempre nell'ottica dell'attuazione del principio di responsabilizzazione, un insieme di adempimenti, quali la notifica al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. In caso di notifica tardiva, la stessa deve essere corredata, inoltre, dai motivi del ritardo. Nella notifica deve essere descritta la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati, nonché le categorie e il numero approssimativo di registrazioni dei dati personali, deve essere comunicato il nome e i dati di contatto del responsabile della protezione dei dati, deve descrivere le probabili conseguenze della violazione dei dati personali

49 Definibile come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4, paragrafo 1, punto 12), GDPR).

e le misure adottate o di cui si propone l'adozione per porre rimedio o per attenuare i possibili effetti negativi⁵⁰. Il titolare del trattamento è obbligato a documentare tutte le violazioni, comprese le circostanze a esse relative, le conseguenze e i provvedimenti adottati per porre rimedio, al fine di consentire all'Autorità di controllo di verificare il rispetto delle disposizioni normative.

Il titolare del trattamento è tenuto a comunicare senza ingiustificato ritardo il *data breach* anche all'interessato, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Secondo il GDPR, la comunicazione non è richiesta se ricorrono determinate condizioni, come l'aver il titolare del trattamento messo in atto le misure tecniche e organizzative adeguate di protezione, oppure aver successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati o quando la comunicazione richiederebbe sforzi sproporzionati (art. 34, paragrafo 3, GDPR). Il Garante, in ogni caso, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato può chiedere al titolare di provvedere alla comunicazione (art. 34, paragrafo 4, GDPR).

7. I diritti dell'interessato

L'efficacia delle norme giuridiche in generale e dei diritti degli interessati in particolare dipende, in larga misura, dall'esistenza di meccanismi adeguati per la loro attuazione. Nell'era digitale, il trattamento dei dati si è diffuso capillarmente e diventa sempre più difficile da comprendere per gli individui. Al fine di ridurre gli squilibri di potere tra gli interessati e i titolari del trattamento, ai singoli sono stati attribuiti determinati diritti, affinché possano esercitare un maggiore controllo sul trattamento delle loro informazioni personali⁵¹.

Passando in rapida rassegna i diritti dell'interessato, è necessario specificare che il punto di partenza deve essere il diritto all'informazione che deve essere garantito dal titolare del trattamento, fatte salve alcune limitate eccezioni. Già nel Codice della *privacy* del 2003

50 Su questo aspetto il Comitato europeo per la protezione dei dati (EDPB – *European Data Protection Board*) ha adottato, il 14 dicembre 2021, le linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali.

51 Così *Manuale del diritto europeo in materia di protezione dei dati*, cit, p. 225.

l'informativa all'interessato rappresentava uno degli adempimenti principali in capo al titolare del trattamento. Essa è obbligatoria qualunque sia la condizione di liceità a fondamento del trattamento (consenso, esecuzione di un contratto, adempimento di un obbligo legale, ecc.). Prevede il GDPR all'art. 12 che l'informativa deve essere resa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori.

Le informazioni, che devono essere fornite prima dell'inizio del trattamento, sono indicate in modo tassativo dal GDPR, il quale, in tal modo, descrive una sorta di "modello di informativa". Si tratta di un "modello" di base che è, comunque, suscettibile di essere arricchito con ulteriori informazioni, in funzione delle caratteristiche concrete del trattamento.

Il GDPR discerne tra le informazioni da fornire a seconda che i dati siano raccolti presso l'interessato o meno, vale a dire siano ricavati presso un altro titolare⁵². Nel primo caso l'informativa deve contenere: *l'identità e i dati di contatto* del titolare del trattamento e del responsabile della protezione dei dati; *le finalità*, nonché *la base giuridica* del trattamento; *i legittimi interessi* perseguiti dal titolare del trattamento o da terzi (qualora la causa di liceità sia questa); *gli eventuali destinatari* o le eventuali categorie di destinatari dei dati personali; *l'eventuale intenzione di trasferire i dati personali* a un Paese terzo o a un'organizzazione internazionale; *il periodo di conservazione* dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; *l'esistenza del diritto di chiedere l'accesso, la rettifica o la cancellazione dei dati, la limitazione del trattamento o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati*; *l'esistenza del diritto di revoca* del consenso; *il diritto di proporre reclamo* a un'Autorità di controllo; *se la comunicazione di dati è un obbligo legale o contrattuale* oppure *un requisito necessario per la conclusione di un contratto*, nonché le possibili conseguenze della mancata comunicazione; *l'esistenza di un processo decisionale automatizzato*, compresa la profilazione (art. 13 GDPR).

Nel caso in cui le informazioni siano ottenute da un altro titolare, oltre ai suddetti elementi, va assicurata l'informativa anche sulle *categorie di atti* interessati e la *fonte* dei dati trattati (art. 14 GDPR).

⁵² Occorre precisare che la raccolta presso l'interessato non implica un contatto diretto tra titolare e interessato, essendo sufficiente che la fonte immediata di provenienza sia l'interessato e non un altro titolare.

Oltre al diritto di informazione, sono riconosciuti all'interessato altri diritti, che gli consentono di agire positivamente sul trattamento operato dal titolare. L'art. 12, paragrafo 3, GDPR, pone la regola generale, vigente per tutti i diritti azionati ad iniziativa dell'interessato, secondo la quale il titolare del trattamento deve fornire le informazioni richieste senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento dell'istanza; tale termine può essere prorogato di due mesi, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta l'istanza mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Il paragrafo 5 stabilisce anche che la soddisfazione dei diritti attivati su richiesta dell'interessato sia *gratuita*, salvo che le richieste siano manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo; in questo, caso, il titolare, tenuto, peraltro, a provare la manifesta infondatezza o eccessività, può o addebitare un contributo spese ragionevole, tenendo conto dei costi amministrativi sostenuti per gli adempimenti, o rifiutare di soddisfare la richiesta. È, in ogni caso, ammessa la possibilità di proporre reclamo a un'Autorità di controllo o un ricorso giurisdizionale all'autorità giudiziaria ordinaria.

Venendo a una rapida descrizione delle facoltà cui è ammesso l'interessato, si deve rappresentare che l'art. 15 GDPR prevede che l'interessato possa esercitare il diritto di accesso, al fine di conoscere se sia in corso un trattamento e, in caso affermativo, di avere accesso ai dati personali e a una determinata serie di informazioni «per essere consapevole del trattamento e verificarne la liceità» (“Considerando” 63). Esso costituisce una declinazione del diritto conoscitivo, che già deve essere assicurato dal titolare con l'informativa e, infatti, si concretizza nella richiesta dell'interessato di ottenere approssimativamente le medesime informazioni, che la normativa impone al titolare di fornire a monte del trattamento.

L'art. 16 GDPR riconosce il diritto di rettifica, che si concretizza nell'ottenimento, senza ingiustificato ritardo, dal titolare del trattamento della rettifica dei dati personali inesatti o dell'integrazione di quelli incompleti, anche fornendo una dichiarazione integrativa.

Il successivo art. 17 GDPR sancisce il diritto alla cancellazione, anche definito diritto all'oblio, che consente all'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo ri-

guardano senza ingiustificato ritardo, qualora non siano più necessari rispetto alle finalità per le quali sono stati raccolti e trattati. Un'altra ipotesi si verifica quando l'interessato revoca il consenso al trattamento e non sussiste altro fondamento giuridico per lo stesso o nel caso di un'opposizione al trattamento, non sussistendo alcun motivo legittimo prevalente. Infine, si può ottenere la cancellazione quando i dati personali sono stati trattati illecitamente o per adempiere a un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

La normativa europea prevede anche che possa essere esercitato il diritto di limitazione di trattamento (art. 18 GDPR), quando:

- a) venga contestata l'esattezza dei dati, per il periodo necessario al controllo degli stessi,
- b) il trattamento sia illecito, ma l'interessato non chieda la cancellazione dei dati, ma soltanto la limitazione,
- c) i dati personali siano necessari a favore dell'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, anche se il titolare del trattamento non abbia più interesse alla conservazione,
- d) l'interessato abbia esercitato il proprio diritto di opposizione, per il tempo strettamente necessario alla verifica dell'esistenza di un concomitante interesse legittimo del titolare del trattamento.

La funzionalità della limitazione deve essere prevista dal titolare già al momento della configurazione del trattamento (*by default ex art. 25 GDPR*), mediante l'adozione delle misure tecniche necessarie a evitare che il dato sia accessibile ad altri utenti o possa essere modificato o ulteriormente trattato, dopo l'esercizio del diritto. Il sistema dovrebbe, inoltre, indicare chiaramente che il trattamento dei dati personali è stato limitato.

Il diritto europeo (art. 20 GDPR) riconosce anche il diritto alla portabilità dei dati, che si concretizza nella facoltà di far interrompere il trattamento dei propri dati da parte di un titolare, chiedendo allo stesso di procedere al trasferimento diretto presso un altro titolare, se tecnicamente fattibile. Questo diritto può essere esercitato se il presupposto di liceità sia il consenso o l'esecuzione di un contratto e il trattamento sia effettuato con mezzi automatizzati⁵³.

⁵³ La legge 27 dicembre 2017, n. 205 (art. 1, comma 1021) ha prescritto al Garante per la protezione dei dati personali di adottare un provvedimento per disciplinare le modalità di veri-

L'art. 21 GDPR, infine, ammette l'esercizio del diritto di opposizione al trattamento, qualora la causa di liceità fosse l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o il perseguimento del legittimo interesse del titolare del trattamento o di terzi. Il titolare del trattamento, di conseguenza, deve astenersi dal trattare ulteriormente i dati personali, «salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

L'interessato può anche opporsi al trattamento per finalità di *marketing*, compresa l'eventuale profilazione, dovendo ottenere immediata e completa soddisfazione alla propria richiesta, mentre il trattamento a fini di ricerca scientifica o storica o a fini statistici può essere proseguito dal titolare, che dimostri che esso sia necessario per l'esecuzione di un compito di interesse pubblico.

8. Le autorità indipendenti di controllo

Oltre a garantire i diritti delle persone fisiche, è altrettanto importante istituire meccanismi che consentano agli interessati di contestare le violazioni dei loro diritti, ritenere responsabili i titolari del trattamento e chiedere un risarcimento. Il diritto a un ricorso effettivo, sancito dalla CEDU e dalla Carta dei diritti fondamentali dell'Unione europea, esige, poi, che siano messi a disposizione di ognuno anche mezzi di ricorso giurisdizionali.

La disciplina normativa europea ha previsto, a garanzia dell'applicazione dell'interno impianto legislativo, l'introduzione di Autorità

fica della presenza di adeguate infrastrutture per l'interoperabilità dei formati con cui i dati sono messi a disposizione dei soggetti interessati, anche ai fini della portabilità degli stessi. Il Garante, con provvedimento n. 121 del 22 febbraio 2018, si è occupato della verifica della presenza di adeguate infrastrutture per l'interoperabilità dei formati con cui i dati siano messi a disposizione degli interessati. Dal punto di vista tecnico, spiega il Garante, sebbene il Regolamento non configuri un obbligo in capo ai titolari del trattamento di introdurre o mantenere sistemi di trattamento tecnicamente compatibili, è opportuno favorire l'interoperabilità dei formati con cui i dati sono messi a disposizione dagli stessi. A tale scopo, il Garante potrà essere chiamato a vigilare affinché il formato dei dati sia idoneo a garantire che i dati medesimi siano riutilizzabili dall'interessato o da un diverso titolare con un minimo sforzo e potrà verificare che il titolare del trattamento non ponga in essere impedimenti - di natura giuridica, tecnica o finanziaria - volti a evitare o rallentare l'accesso, la trasmissione o il riutilizzo dei dati conferiti da parte dell'interessato o di un diverso titolare.

nazionali di controllo. L'esistenza di un quadro comune europeo impone, infatti, l'armonizzazione delle decisioni delle varie Autorità di controllo, sussistendo l'esigenza di operare unitariamente nei confronti dei titolari del trattamento e degli interessati. Questo significa creare una burocrazia comune e regole di collaborazione tra i soggetti che diventano centri periferici dell'esercizio di una funzione unitaria. Se, pertanto, sorgono o persistono differenze di vedute tra le Autorità di controllo, il garante capofila⁵⁴ e gli altri garanti dovranno coordinarsi tra di loro ed esternare una sola voce. È compito delle varie *Authority*, di conseguenza, cercare una soluzione per evitare discriminazioni di trattamento dei vari soggetti coinvolti dalla tutela dei dati personali.

Il GDPR prevede al Capo VI (artt. 51-59) le regole di istituzione e funzionamento delle Autorità nazionali, che hanno il compito di «controllare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione⁵⁵». Ogni Autorità deve agire in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri.

A livello centrale è istituito il Comitato europeo per la protezione dei dati (EDPB – *European Data Protection Board*), che è composto dai vertici delle Autorità di controllo nazionali e dal Garante europeo, o dai loro rappresentanti. La principale responsabilità del Comitato è garantire l'applicazione coerente del GDPR in tutta l'U.E., mediante la pubblicazione di linee guida, raccomandazioni e l'identificazione delle migliori pratiche relative all'interpretazione e all'applicazione del Regolamento. È tenuto anche a informare la Commissione europea in merito a questioni riguardanti la protezione dei dati personali, adottare pareri volti a garantire la coerenza dell'applicazione del GDPR da parte delle Autorità nazionali di vigilanza, in particolare in merito alle decisioni che hanno effetti transfrontalieri, fungere da organo di risoluzione nelle controversie tra Autorità nazionali che cooperano all'applicazione legislativa nel contesto di casi transfrontalieri, incoraggiare lo sviluppo di codici di condotta e l'istituzione di meccanismi di certificazione nel campo della protezione dei dati, promuovere la cooperazione e lo scambio efficace di informazioni e buone pratiche tra le autorità nazionali di vigilanza.

54 L'art. 56 GDPR definisce l'Autorità di controllo capofila come quella dello stabilimento principale o dello stabilimento unico del titolare o del responsabile del trattamento per i trattamenti transfrontalieri.

55 Cfr. art. 51 GDPR.

Per quanto riguarda il Garante per la protezione dei dati personali, le principali competenze si concretizzano nel controllare che i trattamenti di dati personali siano conformi al Regolamento, nonché a leggi e regolamenti nazionali e prescrivere, ove necessario, le misure da adottare per svolgere correttamente il trattamento; collaborare con le altre autorità di controllo e prestare assistenza reciproca; esaminare reclami proposti da un interessato o da un organismo, un'organizzazione o un'associazione e svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole; rivolgere ammonimenti al titolare o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento; imporre una limitazione provvisoria o definitiva del trattamento; ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento; segnalare, anche di propria iniziativa, al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali; formulare pareri su proposte di atti normativi e amministrativi; partecipare alla discussione su iniziative normative con audizioni presso il Parlamento; predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla *privacy* da trasmettere al Parlamento e al Governo; tenere registri interni delle violazioni più rilevanti e imporre sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale.

Relativamente ai ricorsi avverso le decisioni adottate dal Garante, l'art. 152, Codice della *privacy* prevede che le controversie siano attribuite all'autorità giudiziaria ordinaria, così come è devoluta alla medesima autorità giudiziaria il reclamo inizialmente proposto all'Autorità non trattato dalla stessa e i ricorsi contro i provvedimenti di irrogazione di un risarcimento dei danni.

CAPITOLO II

Il trattamento dei dati personali nell'attività di polizia

1. Il trattamento dei dati personali da parte della pubblica amministrazione. Presupposti di esercizio

Dopo aver esaminato la disciplina normativa di carattere generale, è necessario dedicare un sommario approfondimento al fenomeno, sem-

pre più frequente, in cui la pubblica amministrazione si trova, nell'ambito della propria attività, a progettare e svolgere interventi sui dati personali, che sono funzionali al perseguimento dei propri interessi istituzionali, dovendo, al contempo, tutelare coloro i cui dati sono trattati.

Già da questo primo inquadramento del fenomeno emerge nitidamente una tensione di fondo, vale a dire il contemperamento tra la tutela del soggetto cui i dati si riferiscono⁵⁶ e l'esigenza di perseguire uno specifico interesse di carattere pubblico, che è la missione istituzionale del titolare del trattamento: è proprio questa dualità a rappresentare il cuore del problema, che è implicita nel diritto alla protezione dei dati personali *tout court*, ma che affiora ancora più marcata quando uno dei due soggetti è chiamato a realizzare pubblici interessi, in particolare nel campo della *prevenzione, indagine, accertamento e perseguimento dei reati*.

Non è un caso che i trattamenti operati dalle amministrazioni siano sovente parte di un dibattito pubblico più intenso rispetto ai trattamenti realizzati dai soggetti privati, che spesso sono fondamentalmente invisibili al controllo di larga parte dell'opinione pubblica.

Il legislatore europeo, pertanto, ha previsto un regime di contrappesi per consentire il perseguimento di obiettivi pubblici preminenti, salvaguardando contestualmente alcuni diritti fondamentali individuali, contemplando, tuttavia, delle compressioni degli stessi, quando la loro limitazione sia proporzionata e strettamente necessaria.

Esemplificando, proprio al fine di comprendere la specifica *ratio* in questo costante bilanciamento, che talvolta si esprime in una preminenza dell'interesse pubblico rispetto alla posizione individuale del singolo cittadino, nel contesto della tutela della pubblica sicurezza è stato opportunamente affermato che «libertà e sicurezza non rappresentano valori contrastanti ma due facce della stessa medaglia, parimenti meritevoli di tutela per l'ordinamento costituito»⁵⁷. In una logica di beneficio globale a favore del cittadino, infatti, oltre alla specifica istanza di sicurezza, occorre salvaguardare anche le istanze di protezione dei dati nell'ottica della tutela di tutti i diritti individuali fondamentali ed essenziali.

⁵⁶ Tali possono essere, a titolo esemplificativo, i privati destinatari di provvedimenti e partecipanti a procedimenti amministrativi, ma anche i dipendenti di una pubblica amministrazione.

⁵⁷ MARANDOLA A., *Sicurezza e diritti fondamentali: aspetti processuali*, in *Processo penale e giustizia*, fasc. 11, 2019.

Proprio partendo da questo sillogismo, il GDPR contempla tra i presupposti di liceità del trattamento dei dati personali “l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri” di cui è investito il titolare del trattamento, entro i limiti in cui il trattamento di questi dati si configuri come necessario a tali fini; così facendo, il Regolamento – in quanto immediatamente efficace in tutti gli Stati membri dell’Unione europea – individua una condizione, un presupposto per il trattamento dei dati personali che risulta autosufficiente, nella misura in cui siano soddisfatte le prescrizioni poste dalla medesima fonte, quali il rispetto dei principi di cui all’art. 5 e delle altre disposizioni rilevanti poste dal Regolamento.

Il d.l. 8 ottobre 2021, n. 139, ha provveduto ad una risistemazione della disciplina dei trattamenti operati nello svolgimento di compiti di interesse pubblico o connessi all’esercizio di pubblici poteri; sono state introdotte, infatti, diverse modifiche. In primo luogo, la formulazione dell’art. 2-ter, comma 1, Codice della *privacy* è stata aggiornata, prevedendo che la base giuridica rilevante per i trattamenti relativi all’esecuzione di compiti a rilevanza pubblicistica possa essere fondata non solo su una norma di legge o di regolamento, ma *anche su atti amministrativi generali*. In secondo luogo, si introduce un nuovo comma 1-bis nel medesimo art. 2-ter, Codice della *privacy*, che stabilisce che il trattamento dei dati personali da parte delle pubbliche amministrazioni e soggetti ad esse parificati «è anche consentito se necessario per l’adempimento di un compito svolto nel pubblico interesse o per l’esercizio di pubblici poteri a essa attribuiti» nel rispetto dell’art. 6 GDPR. Si precisa, quindi, che, se la finalità del trattamento non è specificata nelle norme, i medesimi soggetti la individuano, dando adeguata pubblicità.

Per i *dati particolari* la disciplina è differente, poiché la regola generale è opposta, ossia quella del *divieto di trattamento*. Va, tuttavia, ricordato che a tale divieto il GDPR e il Codice della *privacy* pongono una serie articolata di eccezioni. Assumono rilievo, infatti, alcune basi giuridiche specifiche per i dati particolari, ossia il fatto che siano manifestamente pubblici e la sussistenza di motivi di interesse pubblico rilevante; il trattamento, in questa ipotesi, deve essere necessario per motivi di interesse pubblico, rilevante sulla base del diritto dell’Unione o degli Stati membri, deve essere proporzionato alla finalità perseguita, rispettare l’essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali dell’interessato.

In questo senso si è espresso anche il Garante per la protezione dei dati personali con nota del 27 novembre 2018 al Presidente del Consiglio dei Ministri, al Presidente della Conferenza delle regioni e delle province autonome e al Presidente dell'ANCI, in tema di trattamenti di categorie particolari di dati personali per motivi di interesse pubblico rilevante.

Nella citata nota il Garante ha chiarito anche che il D.Lgs. 10 agosto 2018, n. 101, innovando il Codice della *privacy*, aveva previsto che la “fonte regolamentare”, vale a dire i regolamenti dei singoli soggetti pubblici⁵⁸, fosse idonea a disciplinare il trattamento dei dati personali particolari solo «nei casi previsti dalla legge», laddove in precedenza l'ordinamento effettuava un generico rinvio anche ai regolamenti. È stato, tuttavia, precisato che «il richiamato inciso può ingenerare dubbi interpretativi in ordine alla necessità che la legge debba prevedere, nei singoli casi, quando un trattamento può essere disciplinato con fonte regolamentare. Tale interpretazione rischierebbe tuttavia di irrigidire eccessivamente la disciplina delle suddette categorie di dati precludendo, almeno nell'immediato, la possibilità di un opportuno aggiornamento dei regolamenti per il trattamento dei dati sensibili e giudiziari già adottati dai soggetti pubblici. Aggiornamento, questo, invece auspicabile anche in ragione dell'estensione dell'ambito applicativo di tale disciplina ai soggetti privati che trattino particolari categorie di dati, per motivi di interesse pubblico rilevante, nelle materie previste». Il Garante, pertanto, al fine di salvaguardare il vigente assetto di garanzie, aveva ritenuto che la citata locuzione dovesse essere interpretata come un rinvio a tutti quei casi in cui il soggetto chiamato a disciplinare le particolari categorie di dati fosse - in base a specifica disposizione legislativa - titolare di poteri regolamentari aventi carattere normativo (con esclusione, quindi, dei soggetti titolari di potestà regolamentare a rilevanza meramente interna).

Le citate recenti innovazioni normative del 2021, come già chiarito, hanno consentito alle amministrazioni di elaborare per proprio conto (mediante l'adozione di atti amministrativi generali) le disposi-

58 Ad esempio, il Ministro dell'Interno ha adottato il d.m. 24 maggio 2017, recante norme in materia di «Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196».

zioni con le quali specificare i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. In altre parole, con questa modifica, le amministrazioni competenti per il perseguimento di interessi pubblici rilevanti guadagnano un evidente (più ampio) spazio di manovra nel progettare, testare e realizzare modalità di trattamento anche quando sia necessario trattare dati personali particolari.

2. Il bilanciamento tra esigenze di trasparenza e di riservatezza. Il diritto di accesso ai documenti amministrativi

La pubblica amministrazione è legittimata al trattamento dei dati personali dei soggetti coinvolti a qualunque titolo nel suo agire, ma ciò comporta anche che la protezione dei dati condiziona in modo sistemico addirittura i presupposti e la cornice di esercizio del procedimento amministrativo, che deve essere completamente conformato al rispetto della normativa dedicata alla *privacy*.

Occorre, quindi, richiamare il processo evolutivo che ha riguardato l'azione amministrativa stessa, che, a partire dalla legge 7 agosto 1990, n. 241, ha subito una trasformazione radicale: se prima il segreto rappresentava la regola di un'amministrazione separata dai cittadini in una prospettiva "soggettiva", successivamente la prospettiva diventa "oggettivo-funzionale", volta, cioè all'attuazione dei principi costituzionali dell'imparzialità e del buon andamento, quindi l'azione amministrativa diventa funzionale al perseguimento dell'interesse pubblico e ha necessità di essere trasparente e aperta verso il cittadino, proprio al fine di dimostrare la sua capacità di assolvimento del compito individuato a monte dal legislatore⁵⁹. È da questo momento, pertanto, che viene riconosciuto l'esercizio del *diritto di accesso*, che, in ogni caso, deve essere inteso come una situazione strumentale alla tutela di una posizione giuridica soggettiva individuale e non al controllo generalizzato dell'operato delle pubbliche amministrazioni.

Tale circostanza ha conseguenze significative sul ruolo del cittadino nel rapportarsi all'amministrazione; le nuove frontiere del diritto amministrativo paiono dunque, per certi versi, ribilanciare l'asimmetria

⁵⁹ FRANCA S., *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Editoriale scientifica, Napoli, 2023, p. 33 ss.

tra pubblica amministrazione e privati sino quasi a prospettare una vera e propria inversione nei rapporti di forza, poiché il privato si trova a vantare una pretesa nei confronti dell'amministrazione che, a propria volta, è tenuta, salvo eccezioni, a dare corso all'istanza ostensiva.

La decisione dell'amministrazione in ordine al riconoscimento del diritto di accesso, tuttavia, non ha effetti unicamente sulla sfera giuridica soggettiva del richiedente, bensì anche su quella di eventuali soggetti terzi cui si riferiscono i dati contenuti nel documento di cui si chiede l'ostensione. In questa prospettiva, la visione rigida della pretesa del cittadino a fronte dell'obbligo dell'amministrazione deve essere necessariamente temperata, perché la pretesa ostensiva trova un limite non in un privilegio dell'amministrazione, bensì nell'interesse di un altro consociato, la cui sfera privata non può essere intaccata.

Ritornando a monte, pertanto, il diritto di accesso ai documenti amministrativi, come espressione e attuazione di un'azione amministrativa trasparente, volta alla realizzazione dell'interesse pubblico preminente, deve trovare limitazione tanto di fronte alle legittime ed eccezionali sacche di opacità dell'amministrazione⁶⁰, quanto di fronte alla sfera di riservatezza degli altri soggetti privati, a favore dei quali deve essere garantita l'anonimizzazione dei documenti o, addirittura, la preclusione dell'ostensione, se la predetta misura risulta insufficiente.

Questa configurazione dei rapporti tra diritto alla riservatezza e all'accesso agli atti amministrativi viene avvalorata dall'art. 86 GDPR, che chiarisce che «i dati personali contenuti in documenti ufficiali in

60 Cfr. art. 24, legge 7 agosto 1990, n. 24, che statuisce che il diritto di accesso è escluso per i documenti coperti da segreto di Stato e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge; nei procedimenti tributari; nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione; nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

A queste tipologie di documenti, per la Polizia di Stato vanno aggiunti quelli previsti dal d.m. 16 marzo 2022, che disciplina le categorie di documenti formati o comunque rientranti nella disponibilità degli uffici centrali e periferici del Ministero dell'Interno sottratti all'accesso, tra i quali si possono citare i documenti dalla cui divulgazione non autorizzata possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, nonché all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, i documenti relativi all'attività investigativa, i documenti istruttori e i relativi piani di difesa civile nelle parti in cui la relativa conoscenza può pregiudicare la sicurezza o la difesa nazionale, i documenti relativi ai procedimenti di concessione, acquisto e riacquisto della cittadinanza, la cui conoscenza può pregiudicare la sicurezza, la difesa nazionale o le relazioni internazionali, ecc.

possessione di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento».

A sua volta, il Codice della *privacy*, all'art. 59, delega la disciplina del diritto di accesso, intesa come definizione dei presupposti, delle modalità e dei limiti, e la relativa tutela giurisdizionale alla legge 7 agosto 1990, n. 241 e ai connessi regolamenti di attuazione, in questo modo confermando la predetta disciplina europea in materia e il generale impianto normativo che vede la pubblica amministrazione in un costante esercizio di equilibrio tra tutela della riservatezza e della trasparenza. Il medesimo rimando viene operato, per giunta, anche rispetto alla disciplina del cd accesso civico.

Il successivo art. 60, invece, stabilisce che «quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale». Nel caso, pertanto, delle categorie particolari di dati personali, il bilanciamento deve essere operato soltanto tra diritti e libertà fondamentali, laddove la mera esigenza della trasparenza amministrativa recede rispetto alla natura del dato di cui si chiederebbe l'ostensione, motivo per cui non è richiamata dalla disposizione *de qua* la disciplina dell'accesso civico, che, in questa ipotesi, è totalmente precluso⁶¹.

61 Il Garante per la protezione dei dati personali si è espresso sul punto con il cd provvedimento generale sui diritti di 'pari rango' del 9 luglio 2003, precisando che il destinatario della richiesta, nel valutare il rango del diritto di un terzo che può giustificare l'accesso o la comunicazione, deve utilizzare come parametro di raffronto non il diritto di azione e difesa che pure è costituzionalmente garantito (e che merita in generale protezione a prescindere dall'importanza del diritto sostanziale che si vuole difendere), quanto il diritto sottostante che il terzo intende far valere sulla base del materiale documentale che chiede di conoscere. Non è possibile, pertanto, secondo il Garante, aderire alla richiesta di accesso o di comunicazione da parte di terzi se i dati o il documento sono ritenuti utili dal richiedente per tutelare in giudizio un interesse legittimo o un diritto soggettivo che possono essere anche di rilievo, ma che restano comunque *sub-valenti* rispetto alla concorrente necessità di tutelare la riservatezza, la dignità e gli altri diritti e libertà fondamentali dell'interessato.

Il diritto alla protezione dei dati personali costituisce, pertanto, un vincolo di cui la pubblica amministrazione deve tenere conto nello svolgimento della propria azione quotidiana, tanto più in un contesto, come quello moderno, in cui il riutilizzo, senza costi aggiuntivi, dei dati precedentemente acquisiti è strumentale alla realizzazione di un modello di *open government*, inteso come modello amministrativo fondato su trasparenza, partecipazione e collaborazione. In questo senso si colloca la direttiva 2019/1024/UE relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, con una forte valorizzazione degli *open government data*.

Ulteriore motivo di potenziale crisi rispetto alla protezione dei dati personali, inoltre, potrebbe derivare dal moltiplicarsi delle ipotesi in cui l'amministrazione è tenuta a mettere a disposizione informazioni che la riguardano, che possono coincidere con dati personali rilevanti sul fronte dell'organizzazione e dell'azione amministrativa, al fine di garantire l'attuazione della disciplina di contrasto alla corruzione⁶².

Ben si comprende, in conclusione, come l'attività amministrativa è sempre più chiamata a strutturare percorsi di gestione delle modalità di esercizio dei propri poteri, in modo da contemperare diritti e interessi confliggenti in un contesto sociale in continua evoluzione, mediante l'attuazione degli obblighi di progettazione delle misure tecniche e organizzative *by design* e *by default*.

3. La protezione dei dati personali in ambito di polizia

Sono state analizzate nel primo capitolo le disposizioni normative generali in materia di trattamento dei dati personali, applicabili tanto ai soggetti pubblici, quanto ai soggetti privati, considerata la scelta del legislatore europeo e nazionale di applicare le medesime regole ad entrambi i contesti.

È stato, poi, posto un *focus*, nella prima parte di questo capitolo, sulla disciplina specifica applicabile alla pubblica amministrazione, cui soggiacciono inevitabilmente anche le Forze di polizia nello svolgimento delle proprie funzioni di carattere amministrativo, ed è

62 In questa direzione si muove, da ultimo, il D.Lgs. 25 maggio 2016, n. 97, di revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza.

emerso che, in ogni caso, l'attività di trattamento compiuta dall'amministrazione può essere connotata dalla presenza di tratti autoritativi; lo si vedrà, ad esempio, rispetto ai diritti degli interessati che trovano una significativa compressione a fronte di trattamenti in ambito pubblico e, più in generale, lo si registra rispetto al fatto che l'amministrazione titolare del trattamento possa agire indipendentemente dal consenso del soggetto interessato. Fatta eccezione, infatti, per alcuni casi di trattamenti strumentali ad attività non autoritativa – dove peraltro non è escluso che si possa ricondurre il trattamento nell'ambito di un compito di interesse pubblico – non pare predicabile una sostanziale equiparazione tra la situazione dell'amministrazione e del soggetto privato che tratta dati personali per il suo unico interesse. Al contrario, la sussistenza dell'interesse pubblico determina una diversa rilevanza dell'attività⁶³.

È stato, poi, sommariamente analizzato il diritto di accesso ai documenti amministrativi, che rientra nel più generico concetto di trasparenza dell'azione amministrativa e che risulta tuttora disciplinato dalla legge 7 agosto 1990, n. 241, con conseguente legittimazione all'esperimento di ricorsi giurisdizionali innanzi al giudice amministrativo, piuttosto che al Garante per la protezione dei dati personali o al giudice ordinario a mente dell'art. 152 Codice *privacy*⁶⁴. L'esercizio di questo diritto non va confuso, tuttavia, con l'accesso ai dati a favore dell'interessato, così come riconosciuto da ultimo nel GDPR, poiché muove dall'obiettivo opposto di trasparenza, di disvelamento dei contenuti in possesso della pubblica amministrazione, laddove il diritto di accesso ai dati viene esercitato con l'obiettivo di tutelare la protezione degli stessi, al fine di bloccare eventuali dispersioni indesiderate delle informazioni.

63 La pubblica amministrazione, d'altronde, si trova di fronte ad un'attività di bilanciamento fra numerose situazioni giuridiche soggettive: gli interessi pubblici primari, gli interessi privati coinvolti nell'esercizio delle funzioni, gli interessi ostensivi, il diritto alla protezione dei dati dei soggetti interessati, l'interesse a mantenere un buon andamento dell'azione amministrativa.

64 La differente giurisdizione potrebbe, in verità, produrre effetti anche sul riconoscimento di una preminenza della tutela dell'interesse pubblico rispetto a quello privato, considerato che tradizionalmente la prassi del Garante tende a considerare come recessive le esigenze di interesse pubblico rispetto alla protezione del singolo. Il sistema del giudice ordinario, invece, pare concepito nella prospettiva di confermare una sostanziale parificazione tra soggetti pubblici e privati, titolari del trattamento. Il giudice amministrativo, infine, riconosce una maggiore attenzione rispetto alla necessità di garantire una ponderazione equa e proporzionata tra protezione dei dati e interesse pubblico.

È necessario, a questo punto, analizzare la disciplina giuridica applicabile ai trattamenti dei dati personali effettuati per “finalità di giustizia penale” e per “finalità di polizia”.

3.1 Le limitazioni all'applicazione del GDPR

Una prima norma di rilievo è rappresentata dall'art. 23 GDPR, che prevede che l'applicazione di talune disposizioni del regolamento, relative ai diritti degli interessati e agli obblighi dei titolari del trattamento, possa essere limitata, sebbene tali limitazioni dovrebbero essere considerate eccezioni rispetto alla norma generale che consente l'esercizio dei diritti e l'imposizione degli obblighi contenuti nel GDPR, pertanto devono essere interpretate in modo restrittivo e applicate esclusivamente in circostanze specifiche e solo se sono soddisfatte determinate condizioni.

Le limitazioni all'attuazione della disciplina contenuta nel GDPR trovano giustificazione, in particolare, per salvaguardare:

- a) la sicurezza nazionale;
- b) la difesa;
- c) la sicurezza pubblica;
- d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
- e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
- f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
- g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
- h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri;
- i) la tutela dell'interessato o dei diritti e delle libertà altrui;
- j) l'esecuzione delle azioni civili.

L'art. 23 GDPR prescrive, in ogni caso, che debba essere garantito il rispetto dell'essenza dei diritti e delle libertà fondamentali, che

la misura sia necessaria e proporzionata, in una società democratica, per salvaguardare, tra l'altro, importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro e che venga assicurato il rispetto di alcune disposizioni di carattere generale, compreso il diritto degli interessati ad essere informati della limitazione, a meno che ciò possa compromettere la finalità stessa; anche in situazioni eccezionali, la protezione dei dati personali non può essere limitata nella sua interezza, ma deve essere mantenuta in tutte le misure di emergenza, di cui all'articolo 23 GDPR, contribuendo così al rispetto dei valori generali di democrazia e Stato di diritto, nonché dei diritti fondamentali sui quali si fonda l'Unione⁶⁵.

Le limitazioni, in definitiva, devono essere *proporzionali*, affinché non superino quanto strettamente necessario, e i soggetti titolari del trattamento rispondono, in ogni caso, delle decisioni intraprese, delle modalità di esercizio del trattamento nella piena applicazione del principio di responsabilizzazione, non essendo possibile giungere al punto di una sospensione generale di tutti i diritti⁶⁶. È stabilito, inoltre, il requisito dell'esistenza di una misura legislativa, che impone la vigenza di una norma unionale o nazionale, che legittimi il ricorso alla disciplina dell'art. 23 GDPR (a titolo temporaneo o permanente, a seconda dei presupposti di applicazione), non essendo sufficiente una valutazione d'iniziativa del titolare del trattamento della sussistenza dei requisiti fissati dal GDPR.

3.2 *Il trattamento a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. La direttiva 'LED'*

Oltre a questa disciplina derogatoria del regime comune, bisogna considerare che, qualora debba essere effettuato un trattamento a fini di prevenzione, indagine, accertamento e perseguimento di reati o

⁶⁵ Cfr. Linee guida 10/2020 sulle limitazioni a norma dell'articolo 23 del regolamento generale sulla protezione dei dati, adottate il 13 ottobre 2021, dall'*European data protection board* (EDPB - Comitato europeo per la protezione dei dati), p. 6.

⁶⁶ Tra i diritti comprimibili ci sono quello a informazioni trasparenti, il diritto di accesso, di rettifica, alla cancellazione, di limitazione di trattamento, l'obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, il diritto alla portabilità dei dati, di opposizione, il diritto di non essere sottoposti a un processo decisionale automatizzato relativo alle persone fisiche.

esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla pubblica sicurezza, la normativa di riferimento non è il GDPR, bensì la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016⁶⁷, così come attuata dal D.Lgs. 18 maggio 2018, n. 51 nell'ordinamento giuridico nazionale.

La direttiva sulla protezione dei dati, destinata alla polizia e alle autorità giudiziarie penali, tutela i dati personali relativi a diverse categorie di interessati coinvolti in procedimenti penali, quali testimoni, persone informate dei fatti, vittime, indiziati e complici⁶⁸. Le autorità di polizia e le autorità giudiziarie penali sono tenute a rispettare le disposizioni della direttiva quando trattano tali dati per finalità di applicazione della legge.

L'applicabilità della direttiva si estende sia al trattamento dei dati a livello nazionale e al trattamento in ambito transfrontaliero tra polizia e autorità giudiziarie degli Stati membri sia ai trasferimenti internazionali da parte delle autorità competenti verso Paesi terzi e organizzazioni internazionali. Non si applica al trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'U.E.

Nello specifico sistema tracciato per i trattamenti "di polizia" deve, tuttavia, essere considerato che durante il predetto trattamento il dato può cambiare la propria natura nel corso del proprio 'ciclo vitale', potendo essere acquisito in un procedimento penale e trattato dall'Autorità giudiziaria o dal Pubblico Ministero secondo le norme del codice di procedura penale e non più della direttiva 'LED' e del successivo decreto di attuazione.

Ciò premesso, occorre precisare che il principio generale è che il trattamento di dati genetici, dati personali concernenti reati, procedimenti e condanne penali e qualsiasi misura di sicurezza correlata, dati biometrici che identificano in modo univoco una persona, nonché eventuali dati personali sensibili, è consentito solo qualora esistano

67 Nota come direttiva 'LED' (*Law Enforcement Directive*) o anche "Direttiva di polizia".

68 Vds. art. 6, direttiva 'LED', che statuisce: «Gli Stati membri dispongono che il titolare del trattamento [...] operi una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali: a) le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato; b) le persone condannate per un reato; c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato, e d) altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b)».

garanzie adeguate alla prevenzione dei rischi che il trattamento di tali dati può comportare per gli interessi, i loro diritti e libertà fondamentali, segnatamente il rischio di discriminazione. Il trattamento di dati personali da parte delle autorità di polizia può avere, infatti, conseguenze rilevanti per gli interessati, per questo sono necessarie norme dettagliate sulla protezione dei dati in questo settore.

L'art. 1, paragrafo 2, chiarisce, infatti che «[...] gli Stati membri: a) tutelano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali; b) garantiscono che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione, qualora tale scambio sia richiesto dal diritto dell'Unione o da quello dello Stato membro, non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». È evidente, quindi, che in questo settore è richiesto alle autorità pubbliche, competenti nelle materie sottoposte alla disciplina *de qua*, un contemperamento tra i diritti e libertà personali delle persone fisiche e il perseguimento delle finalità istituzionali di prevenzione, indagine e repressione dei reati e di prevenzione di minacce alla pubblica sicurezza, che possono richiedere lo scambio di dati personali all'interno dell'Unione, di per sé non limitabile o escludibile per ragioni attinenti alla protezione dei dati personali.

La direttiva si basa, in larga misura, sui principi e sulle definizioni contenuti nel regolamento generale sulla protezione dei dati, tenendo conto della specificità dei settori della polizia e della giustizia penale. I principi applicabili al trattamento per finalità di polizia, infatti, sono sovrapponibili a quelli previsti dal GDPR, pertanto la raccolta di dati personali deve essere effettuata per quanto è strettamente necessario per la prevenzione di un pericolo concreto o per la repressione di un reato specifico. Ogni ulteriore raccolta di dati dovrebbe basarsi su una legislazione nazionale specifica. Il trattamento di dati sensibili, inoltre, dovrebbe essere limitato allo stretto necessario nel contesto di una particolare indagine.

Rispetto al trattamento dei dati a fini commerciali, che è disciplinato dal regolamento, il trattamento di dati connesso alla sicurezza, tuttavia, può richiedere un certo livello di flessibilità. Per esempio, garantire agli interessati lo stesso livello di protezione in termini di diritto di informazione, accesso o cancellazione dei propri dati personali potrebbe significare che qualsiasi operazione di controllo effettuata a fini di contrasto diventerebbe inefficace nel contesto dell'applicazione della legge. La direttiva non contiene, pertanto, il principio di trasparenza. In modo analogo, è necessario che anche i principi della mini-

mizzazione dei dati e della limitazione della finalità, che impongono di limitare i dati personali solo a quanto necessario rispetto alle finalità per le quali sono trattati e che siano trattati per finalità legittime e specifiche, vengano applicati in modo flessibile nei trattamenti di dati relativi alla sicurezza. Le informazioni raccolte e conservate dalle autorità competenti per un caso specifico possono rivelarsi, infatti, estremamente utili per la risoluzione di casi futuri⁶⁹.

Per quanto concerne i diritti esercitabili dagli interessati, anche nel campo del trattamento per finalità di polizia è riconosciuta una serie di diritti analoga a quella contemplata dal regolamento, cui tuttavia la direttiva 'LED' (e il decreto legislativo di attuazione) riserva una regolamentazione peculiare e differenziata, determinata dalle evidenti esigenze di segretezza correlate allo svolgimento dell'attività di polizia giudiziaria e di sicurezza, nonché di giustizia penale.

L'interessato ha diritto a ricevere *informazioni* dal titolare del trattamento, anche tramite un sito *internet* di riferimento, che devono includere 1) l'identità e i dati di contatto del titolare del trattamento, 2) i dati di contatto del responsabile della protezione dei dati, se previsto, 3) le finalità del trattamento previsto, 4) il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto della stessa e 5) il diritto di accesso, rettifica o cancellazione dei dati personali e di limitare il trattamento degli stessi. In aggiunta a questi obblighi generali di informazione, la direttiva stabilisce che, in casi specifici e per consentire l'esercizio dei loro diritti, i titolari del trattamento devono fornire agli interessati informazioni sulla base giuridica per il trattamento e sulla durata di conservazione dei dati. Se i dati personali devono essere trasmessi ad altri destinatari, anche in Paesi terzi o presso organizzazioni internazionali, gli interessati devono essere informati circa le categorie di tali destinatari. Infine, nei casi specifici, stabiliti dal legislatore nazionale, i titolari del trattamento devono fornire le ulteriori informazioni ritenute utili all'esercizio dei diritti, in particolare nel caso in cui i dati personali siano stati raccolti all'insaputa dell'interessato.

69 L'applicazione 'flessibile' dei vari principi ha comportato che è stato stabilito nel corso degli anni dalla normativa di settore e dalla giurisprudenza che quando i dati personali sono raccolti all'insaputa dell'interessato, quest'ultimo deve esserne informato non appena la divulgazione dei dati non arrechi più pregiudizio alle indagini.

È stato, poi, chiarito che, all'atto di conservare dati personali, deve essere operata una chiara distinzione tra i dati amministrativi e i dati di polizia, i dati personali di diverse categorie di interessati, quali sospettati, detenuti, vittime e testimoni e fra i dati basati sui fatti reali e quelli basati su sospetti o deduzioni.

Rispetto alle informazioni puntuali previste dal GDPR, l' informativa contemplata dalla direttiva si caratterizza per la sua generalità, nel senso che viene garantita a favore di una collettività imprecisata di soggetti, mediante il ricorso anche a pubblicazioni su siti *internet*.

Il diritto di informazione, inoltre, non è illimitato: l'art. 14, comma 1, D.Lgs. 18 maggio 2018, n. 51 prevede che per i dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale, il diritto *de quo* è esercitato conformemente a quanto previsto dalle disposizioni di legge o di regolamento che disciplinano tali atti e procedimenti, cioè nei limiti di quanto prescritto dal codice di procedura penale, nella parte in cui impone al pubblico ministero e alla polizia giudiziaria specifici obblighi di segreto relativamente agli atti di indagine.

La speciale normativa in analisi riconosce anche il *diritto di accesso*, che si sostanzia sia nella conferma dell'esistenza di un trattamento in corso, sia nella possibilità di ottenere la comunicazione di una serie dettagliata di dati e informazioni⁷⁰. Anche l'esercizio del diritto *de quo* può essere ritardato, limitato o totalmente escluso, nella misura e per il tempo in cui ciò costituisca uno strumento necessario e proporzionato, tenuto conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata, per la tutela del buon esito dell'attività di prevenzione, indagine, accertamento e perseguimento di reati o dell'esecuzione di sanzioni penali, nonché per l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza, per la tutela della sicurezza pubblica, della sicurezza nazionale e dei diritti e delle libertà altrui (art. 14, comma 2, D.Lgs. 51/18). Di questa decisione il richiedente deve essere reso partecipe senza ingiustificato ritardo e per iscritto, a meno che anche questa informazione possa compromettere la tutela dei suddetti beni primari.

⁷⁰ L'art. 11, D.Lgs. 18 maggio 2018, n. 51, oltre ai dati trattati, include: a) le finalità e il titolo giuridico del trattamento; b) le categorie di dati personali trattati; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati; d) il periodo di conservazione dei dati personali o, se non è possibile, i criteri per determinare tale periodo; e) il diritto di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano; f) il diritto di proporre reclamo al Garante, con i relativi dati di contatto; g) la comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine.

Sono esercitabili anche il *diritto di rettifica* dei dati personali inesatti e di integrazione di quelli incompleti (qualora sia attinente, pertinente e non eccedente rispetto alle finalità del trattamento), in applicazione del principio di esattezza, nonché il *diritto di cancellazione* e di *limitazione del trattamento*.

La cancellazione può essere chiesta quando il trattamento si configura come illegittimo, perché in contrasto con i principi generali o effettuato in assenza delle condizioni di liceità; è disposta, inoltre, quando ricorra per il titolare un vero e proprio obbligo legale (quindi ha una doppia natura di diritto e di obbligo).

Per quanto concerne la limitazione, l'art. 12, comma 3, D.Lgs. 51/18 chiarisce che «in luogo della cancellazione, il titolare del trattamento limita il trattamento quando l'esattezza dei dati, contestata dall'interessato, non può essere accertata o se i dati devono essere conservati a fini probatori»; questa operazione viene comunemente definita come "blocco". La limitazione cautelare, pertanto, può essere richiesta dall'interessato, ma può essere disposta anche d'ufficio dal titolare nell'ipotesi, appena tratteggiata, descritta dall'art. 12, comma 3.

L'interessato ha diritto di essere informato per iscritto dal titolare del trattamento del rifiuto di rettifica, di cancellazione o di limitazione del trattamento e dei relativi motivi, nonché del diritto di proporre reclamo dinanzi al Garante o di proporre ricorso giurisdizionale. Anche in queste ipotesi le informazioni possono essere ritardate, limitate o escluse.

In relazione agli adempimenti, la direttiva 'LED' prevede che le autorità competenti devono tenere un *registro* delle operazioni di trattamento che effettuano nei sistemi di trattamento automatizzato (art. 25). Le registrazioni delle consultazioni e delle comunicazioni devono consentire di stabilire la data e l'ora di tali operazioni, la motivazione e, nella misura del possibile, l'identificazione della persona che ha consultato il sistema o comunicato i dati personali, e i destinatari dei dati personali in questione. Le registrazioni devono essere usate ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali.

Quando un trattamento può presentare un rischio elevato per i diritti delle persone, a causa, per esempio, dell'uso di nuove tecnologie, i titolari del trattamento devono effettuare una *valutazione dell'impatto* sulla protezione dei dati, prima di procedere al trattamento, come previsto nel GDPR.

Il titolare, in attuazione del principio di responsabilizzazione, deve adottare tutte le misure volte a impedire l'accesso non autoriz-

zato ai dati personali trattati e garantire che le persone autorizzate abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione. In caso di violazione dei dati personali, i titolari devono notificare l'autorità di controllo entro tre giorni, descrivendo la natura della violazione, le probabili conseguenze, le categorie dei dati personali in questione e il numero approssimativo dei rispettivi interessati. La violazione dei dati personali, inoltre, deve essere comunicata all'interessato senza ingiustificato ritardo, quando è suscettibile di presentare un rischio elevato per i diritti e le libertà dello stesso.

Il trasferimento o la comunicazione a livello internazionale dovrebbero essere limitati alle autorità di polizia straniere ed essere basati su disposizioni giuridiche specifiche, possibilmente accordi internazionali, a meno che non siano necessari per prevenire un pericolo grave e imminente.

CAPITOLO III

Le pronunce del Garante per la protezione dei dati personali e dell'autorità giudiziaria in materia di attività di polizia

1. Lo studio della casistica in materia di polizia. L'utilizzo dei sistemi di videosorveglianza *'intelligente'* in ambito urbano

Dopo aver trattato tanto la disciplina di carattere generale, quanto quella specifica attinente all'attività di polizia in materia di protezione dei dati personali, si ritiene possa essere utile lo studio di alcuni casi, che riguardano la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, e, in particolare, l'analisi di talune situazioni in cui concretamente è stata coinvolta l'amministrazione di appartenenza di chi scrive, vale a dire la Polizia di Stato. Si tratta di una disamina di casi selezionati, valutato che le ricadute applicative della disciplina in materia di protezione dei dati personali sono numerosissime, soprattutto in un mondo sempre più digitalizzato e connesso.

Partendo da questo punto di osservazione, si ritiene possa essere particolarmente proficuo un approfondimento sui sistemi di videosorveglianza installati in ambito urbano, che riprendono aree pubbliche. Oggi, nelle nostre città, infatti, ci sono milioni di "occhi" che scrutano 24 ore su 24 quasi ogni angolo delle strade, rendendo estremamente difficile per chiunque nascondersi e tutelare la propria riservatezza:

che sia l'obiettivo di una videocamera di sorveglianza di una banca, di un museo o anche semplicemente del controllo del traffico stradale o addirittura del portone di un condominio, è impossibile pensare di poter percorrere una pubblica strada senza essere mai ripresi.

Relativamente agli impianti di videosorveglianza, è necessario premettere che il GDPR ha innovato la precedente disciplina, abolendo la notifica preventiva dei trattamenti all'Autorità di controllo, nota come *prior checking*, sostituendola con gli obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e di effettuazione di valutazioni di impatto, a causa della diffusione massiva degli impianti di videosorveglianza.

La pervasività di tali strumentazioni mette a disposizione degli investigatori centinaia di migliaia di ore di registrazioni e una quantità notevole di immagini, di differente qualità e risoluzione, da poter estrapolare nel caso in cui venga commesso un reato e sia necessario individuare l'autore. La qualità e la risoluzione delle immagini, peraltro, non incidono particolarmente sulle investigazioni, poiché, grazie a particolari *software* implementati anche con algoritmi di intelligenza artificiale, è possibile ricostruire il volto di una persona anche da un'immagine di bassa qualità⁷¹.

La *video content analysis* (anche detta analisi video intelligente) costituisce, infatti, un insieme di tecniche dell'intelligenza artificiale che consente ad un calcolatore di analizzare un flusso video, allo scopo di comprenderne il contenuto e di annotarlo automaticamente, senza l'intervento umano; i sistemi di analisi video possono richiamare l'attenzione dell'operatore quando avviene qualche evento specifico nella scena inquadrata dalla telecamera e permettono di ridurre i tempi della ricerca, offrendo la possibilità di trovare solo quelle sequenze video che soddisfano alcuni criteri specificati *a priori*.

Il Garante per la protezione dei dati personali, con il Provvedimento generale in tema di videosorveglianza 8 aprile 2010, ha considerato tali sistemi come eccedenti rispetto alla normale attività di videosorveglianza, in quanto in grado di determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento; il relativo utilizzo, pertanto, è stato giustificato

71 Sul punto cfr. BERNARDI N., *Privacy. Protezione e trattamento dei dati*, cit., p. 550: «[...] dalla fine degli anni Novanta, i modelli di intelligenza artificiale ispirati all'attività neurale hanno consentito di svolgere compiti come il riconoscimento di immagini o di volti, contribuendo allo sviluppo di una nuova tecnologia come la videosorveglianza cd 'intelligente', basata sul riconoscimento di immagini e movimenti».

solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso, sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza⁷².

Prima di installare una qualsiasi tecnologia biometrica, in conclusione, è necessario condurre un'attenta analisi preliminare, valutare l'impatto sulla dignità degli interessati e sulle implicazioni che tali sistemi comportano sui diritti fondamentali degli individui. I dati biometrici potranno essere oggetto di trattamento soltanto in presenza di una base giuridica e se il trattamento è adeguato, pertinente e non eccedente, rispetto alle finalità per le quali vengono utilizzati.

Per quanto concerne il trattamento tramite videosorveglianza effettuato per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, il citato Provvedimento generale dell'8 aprile 2010 ha stabilito che, sebbene anche per i soggetti pubblici sussista l'obbligo di fornire previamente l'informativa agli interessati (art. 13, Codice della *privacy*), la stessa può non essere resa quando i dati personali sono trattati per le ccdd finalità di polizia (tutela dell'ordine e della sicurezza pubblica e di polizia giudiziaria). In questi casi il trattamento deve, comunque, essere effettuato in base ad espressa disposizione di legge, che lo preveda specificamente.

Molto stimolante, per comprendere le ricadute pratiche della predetta disciplina normativa, è stato l'esame del provvedimento dell'11 gennaio 2024, che il Garante per la protezione dei dati personali ha adottato in merito a tre sistemi di intelligenza artificiale, denominati "*Marvel*"⁷³, "*Protector*"⁷⁴ e "*Precrisis*"⁷⁵, di cui si è dotato il Comune di Trento, finalizzati alla raccolta di informazioni in luoghi pubblici attraverso microfoni e

72 A scopo meramente esemplificativo, si può richiamare l'ipotesi di utilizzo di dati biometrici per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte, come processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore.

73 In questo progetto, i dati, immediatamente anonimizzati dopo la raccolta, dovevano essere analizzati al fine di rilevare in maniera automatizzata, mediante tecniche di intelligenza artificiale, eventi rilevanti ai fini della salvaguardia della pubblica sicurezza (es. assembramenti, aggressioni, scippi, risse, ecc.).

74 Il progetto prevedeva l'acquisizione di filmati da telecamere di videosorveglianza (senza segnale audio), ma anche la raccolta e l'analisi, mediante tecniche di intelligenza artificiale, di messaggi d'odio pubblicati sulla piattaforma "*Twitter*" (ora denominata "*X*") e commenti pubblicati sulla piattaforma "*YouTube*", al fine di rilevare eventuali emozioni negative (aggressività, rabbia o altre emozioni negative sul tema della religione), elaborando informazioni, al fine di identificare rischi e minacce per la sicurezza dei luoghi di culto.

75 In questo caso il Comune ha dichiarato che non è stato posto in essere alcun trattamento di dati personali, essendo il progetto ancora in fase di programmazione e analisi di contesto.

telecamere di videosorveglianza per rilevare potenziali situazioni di pericolo per la pubblica sicurezza.

Nella documentazione prodotta, il Comune ha dichiarato che le molteplici norme nazionali in materia di sicurezza urbana, volte al perseguimento del bene pubblico alla sicurezza, sono state ritenute un adeguato fondamento giuridico legittimante il trattamento⁷⁶.

È stato, inoltre, rappresentato che è stata garantita l'anonimizzazione dei volti delle persone e delle targhe dei veicoli (mediante sfocatura o alterazione), di modo che non fosse in concreto possibile riconoscere delle caratteristiche personali sufficienti per permettere di identificare univocamente i soggetti ritratti; inoltre, l'acquisizione dei video e degli audio era destinata al solo scopo di "addestrare" il *software* al riconoscimento di situazioni di pericolo. L'Ente territoriale, pertanto, ha dichiarato che la persuasione, cui si era addivenuti, era che le circostanze oggettive e gli accorgimenti tecnici fossero tali da escludere un sostanziale trattamento di dati riferibili a persone identificate o identificabili.

I microfoni, inoltre, erano stati tarati in modo da rilevare solo suoni molto forti, come un'esplosione o una sirena d'emergenza e, per la rara eventualità di registrazione delle voci di persone, era stata comunque prevista un'anonimizzazione alla fonte dei segmenti contenenti parlato, con alterazione delle caratteristiche della voce in modo da rendere l'identità del parlatore non più riconoscibile.

Il Garante, in verità, ha ritenuto che il Comune abbia posto in essere un vero e proprio trattamento di dati personali in particolare nella fase di raccolta delle informazioni ritenute d'interesse (filmati di videosorveglianza, audio proveniente dai microfoni, messaggi, commenti, profili ottenuti da reti sociali), perché l'acquisizione e la temporanea memorizzazione di dati personali, ancorché per una ridotta frazione temporale, costituisce un trattamento di dati personali, spesso anche appartenenti alle ccdd categorie particolari.

Ha concluso anche nel senso che le tecniche, impiegate successivamente alla raccolta dei dati, non potevano considerarsi idonee a realizzare un'effettiva anonimizzazione, poiché la sola sostituzione della voce

⁷⁶ Cfr. parere citato, p. 5: «la base giuridica per la normale attività di videosorveglianza posta in essere dal Comune, tramite il Corpo di polizia locale, è rinvenibile [...] [nell'] art. 6, comma 1, lettera e, [del Regolamento]), ai sensi in particolare di quanto previsto dal [d.l.] n. 11/2009, convertito in [legge] n. 38/2009, il quale attribuisce ai Comuni specifici compiti in materia di sicurezza urbana stabilendo, all'art. 6, comma 7, che "per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico"».

del soggetto parlante non è in alcun modo idonea ad anonimizzare i dati personali correlati a una conversazione, atteso che dal contenuto della stessa è possibile ricavare informazioni relative sia al soggetto parlante, sia a terzi e che tali informazioni possono rendere identificabile il parlante, i suoi interlocutori o i soggetti terzi a cui si fa riferimento nel discorso; allo stesso modo per le immagini, anche la tecnica di offuscamento dei visi non può ritenersi idonea ad assicurare l'effettiva anonimizzazione dei dati, atteso che gli interessati sono comunque potenzialmente identificabili tramite altre caratteristiche fisiche (corporatura, abbigliamento, caratteristiche fisiche particolari, ecc.) o informazioni detenute da terzi (notizie di stampa relative a fatti di cronaca ecc.) o ancora informazioni desumibili dalla localizzazione della telecamera.

Premesso, pertanto, che i progetti in parola costituivano trattamento a tutti gli effetti, il Garante, oltre ad un insieme di violazioni di regole procedurali e al mancato adempimento di svariati obblighi gravanti a carico del titolare del trattamento, fondamentalmente non ha riconosciuto la liceità e ha imposto il fermo totale dell'operatività degli stessi, essendo stato effettuato un trattamento in assenza di una previsione normativa di autorizzazione ed essendo stata potenzialmente lesa non soltanto la riservatezza dei cittadini, ma anche la libera manifestazione del pensiero, la partecipazione alla vita politica e sociale, la libertà di riunione e la libertà di manifestare la propria fede religiosa, poiché simili forme di sorveglianza negli spazi pubblici possono modificare il comportamento delle persone e condizionare finanche l'esercizio delle libertà democratiche.

Il principio imprescindibile, in definitiva ricavabile da questo provvedimento, è quello secondo il quale eventuali limitazioni ai diritti fondamentali, al rispetto della vita privata e alla protezione dei dati personali possono essere apportate soltanto se esse siano previste dalla legge e rispettino il contenuto essenziale dei diritti fondamentali, nonché il principio di proporzionalità, per cui possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a obiettivi di interesse generale riconosciuti dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Il d.l. 20 febbraio 2017, n. 14, inoltre, ha consentito ai Comuni l'installazione di sistemi di videosorveglianza ai soli fini di "prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria", previa stipula di un accordo per l'attuazione della sicurezza urbana con la Prefettura territorialmente competente; in queste ipotesi non è comunque contemplato l'utilizzo di microfoni per l'acquisizione del segnale audio.

1.1 Il Sistema automatico di riconoscimento immagini (S.A.R.I)

Venendo, nello specifico, all'esperienza della Polizia di Stato nel settore dell'utilizzo dell'intelligenza artificiale, la Polizia scientifica ha a propria disposizione dei *software* in grado di identificare, in poco tempo, l'autore di un reato da un *frame* sfocato di una telecamera di sicurezza: il portale *Sari* (Sistema automatico di riconoscimento immagini), presentato nel 2019, è capace di ricercare, grazie ad algoritmi di intelligenza artificiale, la foto di un soggetto ignoto all'interno della banca dati dei soggetti fotosegnalati "AFIS"⁷⁷ (la stessa in cui vengono salvate le impronte digitali), che contiene le immagini di circa 20 milioni di persone, realizzando un'attività che sarebbe impossibile svolgere manualmente.

In tempi brevissimi il *Sari* produce una lista di candidati, ordinata sulla base di un criterio di similarità e di una percentuale di '*matching*', con associazione di un punteggio che rappresenta la misura di somiglianza fornita; la lista deve essere, poi, revisionata a mano da un operatore specializzato per la ricerca di un possibile candidato su cui concentrare ulteriori investigazioni. Il sistema, inoltre, non esegue soltanto analisi di volti, ma, da un fotogramma di un soggetto ripreso di spalle o con il casco indossato, riesce ad effettuare una stima dell'altezza.

I risultati ottenuti sono certamente di tipo "investigativo" e non "forense" e servono ad evidenziare un sospettato e a farlo sottoporre ad altri accertamenti come un pedinamento o un confronto con testimoni, tuttavia sono in grado di orientare in modo significativo lo sviluppo delle attività di indagine.

L'introduzione di questo sistema ha indotto il Garante per la protezione dei dati personali ad attivare il procedimento di indagini, previsto dall'art. 37, D.Lgs. 51/2018, con una richiesta di informazioni al Ministero dell'Interno, in particolare sul sistema "*Sari Enterprise*"; il Ministero ha rappresentato che il sistema è destinato ad affiancare il sistema AFIS-SSA, per fornire all'operatore un supporto informatico in modo da agevolare l'attività di indagine. Il sistema AFIS-SSA, infatti, già consentiva una selezione tra le immagini presenti, caricate in occasione di fotosegnalamenti, mediante la selezione di connotati e contrassegni (ad es. colore degli occhi, tatuaggi, ecc.), inoltre tale

⁷⁷ Acronimo di "*Automated Fingerprint Identification System*", in italiano "Sistema Automatizzato di Identificazione delle Impronte".

applicativo risultava già incluso nel citato d.m. 24 maggio 2017 tra i trattamenti effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza.

"Sari Enterprise", pertanto, è stato presentato come un sistema che è in grado di effettuare le medesime elaborazioni di AFIS-SSA, con l'aggiunta dell'automatizzazione di alcune operazioni, che prima richiedevano l'inserimento manuale dei connotati fisici, di conseguenza non comporterebbe il trattamento di nuovi dati, ma una nuova modalità del trattamento dei medesimi dati biometrici.

Il Garante si è espresso con provvedimento del 26 luglio 2018, richiamando la disciplina posta dall'art. 7, D.Lgs. 51/2018, che consente il trattamento di categorie particolari di dati personali se specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento; nel caso di specie, l'inclusione di AFIS-SSA tra i trattamenti disciplinati dal d.m. 24 maggio 2017 sarebbe elemento necessario e sufficiente, oltre al fatto che il sistema in parola risponde pienamente alla finalità di consentire l'attività di identificazione, che è funzionale ai compiti di polizia. È stato valutato positivamente, in definitiva, che *"Sari Enterprise"* velocizza e semplifica ciò che era già gestito legittimamente dalla Polizia, per cui è stato giudicato *non critico sotto il profilo della protezione dei dati personali*.

Esito differente ha avuto la valutazione della seconda infrastruttura *Sari*, che è stata denominata *"real time"*: lo scopo, in questo caso, è il confronto, automatico e in tempo reale, dei volti inquadrati dalle telecamere con una lista contenente quelli delle persone da ricercare (*watch list*), la cui grandezza è di massimo 10.000 volti. Se il viso è presente nella lista, il sistema lancia un *alert* e lo segnala all'operatore addetto al controllo. Il sistema, progettato e sviluppato come soluzione mobile, prevede l'installazione di una serie di telecamere in un'area geografica predeterminata e delimitata, laddove sorga l'esigenza di disporre di una tecnologia di riconoscimento facciale per coadiuvare le Forze di polizia nella gestione dell'ordine e della sicurezza pubblica o in relazione a specifiche esigenze di polizia giudiziaria. Il *"Sari real time"* consente, inoltre, di registrare i flussi video delle telecamere, fungendo, in tal senso, quale attività di videosorveglianza.

Considerata la maggiore *"invasività"* del sistema, prima di rilasciare la propria autorizzazione, il Garante ha richiesto che fosse redatta una valutazione d'impatto sulla protezione dei dati personali. La valutazione è stata inviata al Garante che ha rilevato come l'identificazione di una persona in un luogo pubblico comporta il trattamento

biometrico di tutte le persone che circolano nello spazio pubblico monitorato; pertanto, si determinerebbe, con questa tecnologia, un'evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui.

È stato eccepito che il trattamento in parola rientrerebbe tra quelli disciplinati dalla direttiva 'LED' e decreto di attuazione interno e avrebbe ad oggetto dati rientranti tra le categorie particolari, in quanto relativi all'immagine degli individui, ma potenzialmente anche alle loro opinioni politiche o all'appartenenza a determinati sindacati, ecc., qualora il sistema sia utilizzato per monitorare manifestazioni in luogo pubblico, che hanno ricadute sulla gestione dell'ordine pubblico.

Per queste categorie di dati, l'art. 7 del D.Lgs. 51/2018 richiede una previsione del diritto dell'Unione europea o di legge o, nei casi previsti dalla legge, di regolamento. Nel proprio parere del 25 marzo 2021, il Garante, pur passando in rassegna le varie disposizioni normative citate dal Ministero nella propria valutazione, non ha trovato una base normativa adeguata, che consentisse esplicitamente l'utilizzo del sistema, pertanto ha espresso parere negativo alla messa in opera. Il "*Sari real time*" non è, quindi, mai entrato in uso. Come ulteriore prescrizione, il Garante ha chiesto anche di verificare che il sistema sia pienamente adeguato anche rispetto alle minoranze etniche⁷⁸.

Successivamente all'adozione del predetto parere, è entrato in vigore il d.l. 8 ottobre 2021, n. 139, così come convertito dalla legge 3 dicembre 2021, n. 205, che all'art. 9, comma 12 ha introdotto una deroga per i trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali alla regola generale prevista dal comma 9, secondo la quale « l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici [...] in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non

⁷⁸ Secondo alcuni studi, tra cui quelli condotti dal NIST (*National Institute of Standards and Technologies*), gli algoritmi che regolano il funzionamento dei sistemi di riconoscimento facciale avrebbero percentuali di precisione variabili: mentre nel caso di uomini di carnagione chiara si registrerebbe una precisione del 99%, quando si analizzano i volti di donne o di persone di colore, le percentuali scenderebbero, arrivando ad una precisione del 35% per le donne di pelle scura. La causa sarebbe da ricercare nei *dataset* utilizzati per alimentare le intelligenze artificiali, composte per l'80% da soggetti bianchi e per il 75% da uomini.

oltre il 31 dicembre 2025». Nell'ipotesi di trattamento "di polizia" il comma 12 stabilisce, tuttavia, che è possibile l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, essendo allo scopo sufficiente un parere preventivo favorevole del Garante⁷⁹.

Nonostante quest'apertura da parte del legislatore, allo stato, il sistema non è stato oggetto di rivalutazione, probabilmente in attesa dell'approvazione da parte del legislatore nazionale di un atto normativo di adattamento dell'ordinamento giuridico interno al regolamento 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, il quale all'art. 5, paragrafo 5 demanda a ciascuno Stato membro la decisione sulla possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di polizia nei limiti previsti, disciplinando tra l'altro condizioni e procedure per l'autorizzazione e per la notifica dell'uso di tali sistemi all'Autorità di protezione dei dati.

2. Il caso della divulgazione su *internet* di immagini e video inerenti ad un fermato, trattenuto nei locali di un Commissariato di pubblica sicurezza

Particolarmente degno di nota è il caso trattato dapprima con provvedimento del 26 novembre 2020 dal Garante per la protezione dei dati personali e successivamente definito con sentenza sfavorevole n. 8722/2023 del Tribunale civile di Roma, in sede di giudizio di opposizione, riguardante la divulgazione, tramite alcuni siti *internet*, delle immagini riprese all'interno di un Commissariato di P.S., relative a un episodio di violenta reazione autolesionistica da parte di un uomo in evidente stato di alterazione psico-fisica. Dal video risultava chiaramente identificabile il volto dell'uomo, mentre si procurava lesioni al

⁷⁹ Cfr. art. 9, comma 12, d.l. 8 ottobre 2021, n. 139: «i commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018».

capo, e si sentiva scanditamente che, tra i lamenti disperati, dichiarava di essere malato oncologico e di avere l'AIDS.

A seguito di tale divulgazione il Garante disponeva, nei confronti dei titolari del trattamento (riferibili ai siti *internet* suddetti), provvedimenti d'urgenza di limitazione provvisoria del trattamento *ex art.* 58, paragrafo 2, lett. f) del Regolamento, riferita all'ulteriore diffusione delle immagini relative al suddetto episodio con modalità che rendessero identificabile l'interessato e che risultassero altresì lesive della sua dignità; la divulgazione delle immagini, infatti, non poteva trovare giustificazione nel diritto di cronaca, pertanto è stata ritenuta anche in contrasto con gli artt. 8 e 10 delle "Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica", inerenti alla tutela della dignità delle persone e delle persone malate.

Le immagini ed il video in esame riguardavano un episodio accaduto in presenza di agenti di polizia, all'interno di un Commissariato; ciò ha indotto il Garante ad avviare un'istruttoria anche nei confronti del Ministero dell'Interno, cui sono stati chiesti chiarimenti circa l'avvenuta raccolta, registrazione e diffusione delle immagini e del video suddetti, alla luce della disciplina in materia di protezione dei dati personali, nonché sulle misure tecnico-organizzative adottate al fine di garantire il rispetto della disciplina suddetta, con particolare riferimento a quanto sancito dall'art. 14, d.p.r. 15 gennaio 2018, n. 15, rubricato "Diffusione dei dati e delle immagini personali".

Dal riscontro fornito dal Ministero, è risultato che l'interessato, trovandosi presso un ufficio del suddetto Commissariato (a seguito del suo arresto), verso le ore 03.15, mentre era sotto la custodia del personale di altro Commissariato, al culmine di una reazione emotiva, «iniziava a compiere atti di autolesionismo, dando violenti colpi di testa a una parete di cartongesso, che delimita quella stanza da un ambiente più grande, tanto da provocarne l'irreversibile deterioramento».

Il Ministero ha rappresentato anche che «per salvaguardare l'incolumità delle persone presenti ed evitare ulteriori danneggiamenti all'immobile, l'unità operativa "XX" decideva di ricorrere all'utilizzo dello spray al peperoncino, in dotazione al personale»; «tali operazioni formavano oggetto di documentazione audiovisiva. Si evidenzia al riguardo che le riprese sono state effettuate di propria iniziativa da uno degli operatori presenti sul posto, mediante l'attivazione di un dispositivo di comunicazione privato, tipo cellulare o *smartphone*, presuntivamente per offrire documentazione tanto degli atti di autolesionismo quanto del contestuale danneggiamento

dei beni dello Stato. Successivamente copia del filmato, dopo essere stata acquisita da *internet*, è stata opportunamente masterizzata su un cd ed è stata poi messa a disposizione dell'A.G. competente con separata comunicazione».

Nel riscontro suddetto è stato, altresì, fatto presente che le riprese in esame documentano "atti di polizia giudiziaria" ma che «le modalità con cui tali immagini sono state successivamente divulgate e diffuse su internet non sono attualmente note e formano, allo stato, oggetto di una autonoma e puntuale attività istruttoria, finalizzata a ricostruire i fatti e chiarire tali aspetti», rappresentando altresì che «le operazioni di raccolta e registrazione, nonché diffusione delle immagini personali in esame sono state realizzate in difformità alle disposizioni in materia, su iniziativa di operatori non autorizzati dalla gerarchia».

In un secondo momento, a seguito dell'avvio da parte del Garante del procedimento per l'irrogazione delle sanzioni, il Ministero ha chiarito che «gli approfondimenti finora eseguiti hanno comunque permesso di accertare che il video è stato realizzato su invito del capo equipaggio della pattuglia intervenuta - intento a gestire l'arrestato - da parte del secondo operatore. Quest'ultimo, ammettendo la sua superficialità, inviava il predetto filmato ad altro collega - in fase di individuazione - con l'intento di condividere le modalità operative adottate nel complesso intervento. L'operato dei poliziotti - che fin qui descritto può ritenersi direttamente discendente dalle mansioni correlate allo svolgimento del servizio - se ne è discostato invece per gli ulteriori sviluppi della vicenda, di seguito evidenziati. *In primis*, preme sottolineare che l'attività di registrazione del video è stata svolta di iniziativa da parte dei predetti operatori, utilizzando un dispositivo privato, senza tempestiva informazione e autorizzazione di un superiore gerarchico. Della predetta attività di registrazione è stata fatta menzione in un'integrazione del verbale di arresto, ma gli autori non hanno mai consegnato il filmato al personale del Commissariato competente per la redazione degli atti, il quale, per integrare l'informativa all'Autorità Giudiziaria, ha dovuto "scaricarlo" da *internet*. Oltre a ciò, l'agente che ha effettuato il video - che ha ammesso la sua superficialità - lo ha inviato ad altro collega, così originando la sequenza di atti divulgativi [tramite *chat whatsapp*]. [...] Pertanto, il trattamento dei dati personali per cui codesta Autorità ha avviato il procedimento sanzionatorio [...] è ascrivibile unicamente all'operato dei singoli soggetti che hanno materialmente contribuito alla diffusione di tali contenuti. Si tratta di comportamenti, non solo non ascrivibili direttamente all'Amministra-

zione, ma non evitabili, in quanto frutto dell'iniziativa sì di appartenenti alla Polizia di Stato, ma che nel far ciò hanno travalicato i compiti istituzionali - nel caso di specie di prevenzione e perseguimento dei reati - violando anche specifiche disposizioni regolamentari».

Il Garante ha rilevato che i dati in oggetto rientravano nelle 'categorie particolari', dichiarando il fermato il proprio stato di salute, e dovevano essere trattati a norma della direttiva 'LED' e del relativo decreto di attuazione, in quanto il trattamento è stato effettuato, in questo caso, a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, tuttavia, ha evidenziato come né il Commissariato in cui si sono svolti i fatti, né quello di appartenenza dell'equipaggio in trattazione avessero adottato alcuna misura idonea a garantire la dovuta sicurezza e riservatezza dei dati, né tantomeno a prevenirne la fuoriuscita e la diffusione via *internet*; di conseguenza, l'imputabilità del trattamento ai fini dell'adozione di misure correttive, sanzionatorie e/o risarcitorie era da ricondurre al Ministero.

È stato ritenuto sufficiente, quindi, che i fatti si siano svolti all'interno di uffici di polizia da parte di agenti nei confronti di una persona temporaneamente ristretta per stabilire un nesso di occasionalità necessaria in base alla quale la condotta è riferibile all'Amministrazione.

Sul piano delle misure tecniche e organizzative, il Ministero ha prodotto: 1) i documenti relativi al Documento programmatico sulla sicurezza del 2006, 2) la circolare prot. n. 4458 del 26 giugno 2018 del Capo della Polizia, illustrativa del nuovo quadro normativo nazionale in materia di protezione dei dati personali, 3) la circolare sull'aggiornamento professionale del personale della Polizia di Stato per l'anno 2019, che aveva stabilito che dovesse essere effettuata una giornata formativa di interesse generale sulla tematica dell'"anticorruzione e nuova disciplina in materia di protezione dei dati personali".

Il Garante ha dapprima ritenuto le misure non pienamente adeguate per la formazione di una piena ed effettiva conoscenza e consapevolezza da parte degli operatori di polizia dei rischi derivanti agli interessati dai trattamenti per finalità di polizia.

In secondo luogo, ha riscontrato che la divulgazione in questione risultava avvenuta in violazione della disciplina in materia di protezione dei dati personali di cui alla direttiva 'LED' ed al D.Lgs. n. 51/2018⁸⁰.

80 In particolare, è stata contestata la violazione dell'art. 14 del d.p.r. n. 15/2018, secondo cui «1. La diffusione di dati personali è consentita quando è necessaria per le finalità di polizia di cui all'articolo 3, fermo restando l'obbligo del segreto di cui all'articolo 329 del codice di pro-

Da questa conclusione è derivata anche la comminazione del pagamento di una sanzione amministrativa pecuniaria, che è stata fissata al minimo edittale di euro 50.000,00, grazie all'atteggiamento sempre collaborativo adottato dal Ministero dell'interno, aumentata, tuttavia, del 20% in relazione alla particolare natura dei dati in parola ed alla gravità della loro messa a disposizione di una platea indeterminata di soggetti.

Il Garante, inoltre, ha ingiunto alla pubblica amministrazione di trasmettere le direttive generali adottate in ambito nazionale sulla diffusione dei dati o delle immagini personali (art. 14, comma 3, d.p.r. 15 gennaio 2018, n. 15), promuovere adeguate ed ulteriori iniziative formative nei confronti del personale, individuare ulteriori misure tecnico-organizzative finalizzate a garantire il pieno rispetto dei principi e delle disposizioni previste dalla normativa vigente in materia di trattamento dei dati personali.

Avverso tale provvedimento il Ministero dell'Interno ha proposto opposizione al Tribunale civile di Roma *ex art. 152, Codice della privacy*, che ha definito la controversia con sentenza del 5 giugno 2023, citata.

Nel ricorso è stata contestata l'erronea attribuzione all'amministrazione non solo dell'originaria acquisizione delle immagini, ma anche della condivisione del video da parte dell'autore su *chat whatsapp* e della successiva diffusione su *internet*, considerato che tali attività sarebbero da ricondurre ai soli dipendenti del Commissariato, che avrebbero agito in assenza di un'autorizzazione gerarchica e sarebbero personalmente responsabili, in virtù dei principi applicabili alla responsabilità amministrativa del pubblico dipendente, che non comportano un'automatica estensione all'amministrazione di appartenenza delle condotte contestate.

È stato, inoltre, rappresentato che il dipendente è stato assoggettato a procedimento disciplinare e penale, per aver diffuso il video senza alcuna possibilità di controllo da parte dell'amministrazione, essendo stato autorizzato dal diretto superiore soltanto all'acquisizione per poter riferire all'autorità giudiziaria sui fatti ripresi.

cedura penale e fatti salvi i divieti previsti da altre disposizioni di legge o di regolamento; essa è comunque effettuata nel rispetto della dignità della persona. 2. La diffusione di immagini personali è consentita quando la persona interessata ha espresso il proprio consenso o è necessaria per la salvaguardia della vita o dell'incolumità fisica o è giustificata da necessità di giustizia o di polizia; essa è comunque effettuata con modalità tali da non recare pregiudizio alla dignità della persona. 3. Il Garante è informato delle direttive generali adottate in ambito nazionale sulla diffusione dei dati o delle immagini personali».

Il giudice ordinario, di contro, ha confermato la decisione del Garante per la protezione dei dati personali, imputando all'amministrazione una responsabilità diretta relativa alla fase di custodia e conservazione dei dati personali (immagine e dati sensibili dell'arrestato), pur originariamente acquisiti in maniera legittima e con la finalità di rappresentare l'accaduto alla competente autorità giudiziaria.

I dati in esame, infatti, una volta terminata la ripresa svolta per finalità istituzionali, dovevano essere trattati e conservati in sicurezza, mediante la predisposizione di misure tecnico-organizzative che avrebbero potuto consentirne una custodia sicura e impedirne l'impropria circolazione, come invece accaduto; era necessario, infatti, che il video fosse messo in sicurezza nell'immediatezza della registrazione, con salvataggio su apposito supporto informatico da custodire accuratamente e contestuale cancellazione dal dispositivo sul quale era stato effettuato, in modo da impedirne la circolazione.

È stato, inoltre, rilevato che la disciplina normativa in materia di protezione dei dati personali stabilisce che il titolare del trattamento sia la persona giuridica, non il legale rappresentante o l'amministratore, e introduce un regime derogatorio rispetto al comune principio dell'imputabilità personale della sanzione, configurando, di conseguenza, un'autonoma responsabilità della persona giuridica, che non deve essere intesa di tipo "oggettivo", ma come "colpa di organizzazione" per la mancata adozione delle cautele, organizzative e gestionali, necessarie a prevenire la commissione degli illeciti

Non è stata, inoltre, riconosciuta l'idoneità delle misure di formazione adottate precedentemente ai fatti, soprattutto in considerazione del carattere estremamente tecnico della materia e della molteplicità degli adempimenti richiesti dalla normativa vigente.

Di seguito a tali condanne, il Capo della Polizia – Direttore generale della pubblica sicurezza ha diramato la circolare prot. n. 90572 del 26 settembre 2023, con cui ha richiamato le linee di indirizzo concernenti l'utilizzo delle piattaforme digitali e dei *social media* da parte del personale della Polizia di Stato, già impartite con precedente circolare prot. n. 5428 del 24 ottobre 2019, nella quale era stato già precisato che «ogni operatore [...] non deve rivelare a terzi informazioni e dati, né pubblicare notizie, immagini ovvero audio relativi ad attività di servizio che, anche se apparentemente insignificanti, possono arrecare nocimento all'efficacia dei servizi di polizia e, in generale, alla funzionalità dell'Amministrazione ovvero alla *privacy* di terze persone».

È stata, pertanto, prescritta una rigorosa disciplina comportamentale nell'utilizzo delle piattaforme di messaggistica e dei *social media*, essendo stato ribadito il dovere di «interagire nel *web* tenendo un comportamento sempre improntato al massimo rispetto dei principi costituzionali, delle libertà fondamentali, della dignità della persona e di non discriminazione [...] in modo da evitare che il contenuto delle esternazioni individuali, di qualunque tipo, anche non verbali, possa essere equivocado o addirittura travisato o comunque strumentalizzato, con conseguente nocumento all'immagine e all'imparzialità della Polizia di Stato»⁸¹.

Di seguito, sono state ricordate tutte le conseguenze giuridiche derivanti da comportamenti non adeguati, in particolare che «la diffusione di fotografie o video che ritraggono persone (identificate o identificabili) coinvolte in interventi di polizia potrebbe dare luogo a un illecito trattamento di dati personali, con l'irrogazione da parte del Garante per la protezione dei dati personali di una sanzione amministrativa pecuniaria a carico del Dipartimento della pubblica sicurezza e la correlata responsabilità del personale dipendente per danno erariale. L'illecito trattamento di dati personali potrebbe, infine, essere oggetto di azione risarcitoria sul piano civile».

Come ultima prescrizione è stato precisato che «nei casi in cui sia necessario raccogliere la documentazione fotografica o audiovideo di specifiche attività di polizia (commissione di reati o turbamento dell'ordine pubblico) gli operatori possono utilizzare i dispositivi di ripresa privati (*smartphone*) quando siano indisponibili gli strumenti in dotazione a ciò destinati (*body-cam*, videocamere) o gli operatori adibiti allo specifico servizio (personale della polizia scientifica), con la precisazione che a tali riprese devono ritenersi applicabili le prescritte norme penali e disciplinari. In tali casi, le riprese fotografiche e audio-video effettuate per finalità di polizia dovranno essere tempestivamente trasferite sul supporto di memoria digitale messo a disposizione dall'ufficio incaricato di conservare la documentazione probatoria e cancellate dal dispositivo personale».

81 Cfr. TENORE V., *La libertà di pensiero tra riconoscimento costituzionale e limiti impliciti ed espliciti: i limiti normativi e giurisprudenziali per giornalisti, dipendenti pubblici e privati nei social-media*, in *Lavoro, diritti, Europa*, 2019, p. 5, che osserva che «è innegabile, [...], sul piano disciplinare, che la diffusione del messaggio ad un numero determinato o illimitato di persone rilevi solo per valutare la gravità della condotta in punto di proporzionalità punitiva o la più o meno vasta potenzialità lesiva dell'immagine aziendale (parimenti per una valutazione di proporzionalità punitiva), ma non certo per affermare la liceità *tout court* di un comportamento comunque offensivo o denigratorio».

A completamento di questa circolare, ne è stata diffusa anche un'altra, prot. n. 32489 del 28 dicembre 2023, relativa all'aggiornamento professionale per il personale della Polizia di Stato, che costituisce un vero e proprio obbligo per i dipendenti, a norma delle disposizioni del contratto collettivo di settore e dell'accordo nazionale quadro, sottoscritto con le organizzazioni sindacali maggiormente rappresentative. Con la citata circolare è stato stabilito che tutto il personale contrattualizzato approfondisse durante l'anno 2024 la tematica di interesse generale avente ad oggetto "Il trattamento e la tutela dei dati personali nell'attività di polizia – il corretto utilizzo personale dei *social*". In questo modo, si è cercato di garantire una più completa ed esaustiva formazione sulla materia, considerate le contestazioni del Garante e del Tribunale ordinario di Roma.

3. Il caso della pubblicazione sulle piattaforme istituzionali di alcuni video di violenze in occasione del comunicato stampa diramato per il fermo degli indiziati

Un ulteriore caso su cui si è espresso il Garante riguarda la pubblicazione sulle piattaforme istituzionali della Polizia di Stato di due video di violenze, subite da un uomo, poi deceduto, filmati originariamente dagli aggressori. I video sono stati pubblicati in occasione della comunicazione alla stampa del fermo degli otto indiziati di delitto; negli stessi viene ripresa l'aggressione e si sentono le voci dei presenti, in particolare quella disperata della vittima, che chiede aiuto e che risulta identificabile in relazione alle diverse fonti che hanno informato sulla vicenda, sebbene i volti siano stati oscurati. I filmati sono stati, poi, diffusi da diverse testate *on line* a carattere nazionale.

A seguito della divulgazione di tali video, il Garante ha avviato un'istruttoria nei confronti del Ministero dell'Interno, al quale ha inviato una richiesta di informazioni, rivolta anche al Commissariato interessato ed alla Questura di competenza, in ordine alle modalità e finalità della diffusione dei video in questione, agli atti con i quali è stata assunta la decisione di diffondere tali video, nonché alle misure tecnico-organizzative adottate al fine di garantire il rispetto della disciplina in materia di protezione dei dati personali.

Il Ministero ha riscontrato la richiesta del Garante, precisando che i video facevano riferimento a una grave vicenda che aveva riguardato una persona che viveva in uno stato di disagio sociale e di solitudine, che era stata oggetto di ripetuti atti di aggressione da parte

di giovani ragazzi che, per giunta, filmavano le loro scellerate azioni e le diffondevano attraverso l'utilizzo dei *social network*.

La decisione di pubblicare i video era stata presa dall'Ufficio comunicazione istituzionale (già Ufficio relazioni esterne e cerimoniale) della Segreteria del dipartimento, in occasione della comunicazione alla stampa della notizia dell'esecuzione del fermo di indiziato di delitto nei confronti di otto soggetti (di cui sei minori), ritenuti, a vario titolo, gravemente indiziati in concorso dei reati di minaccia, atti persecutori, tortura, danneggiamento, violazione di domicilio e sequestro di persona aggravato; è stato precisato, inoltre, che «la diffusione di tali video è stata preventivamente autorizzata dalle Autorità giudiziarie procedenti, che hanno ritenuto prevalenti, dopo attenta valutazione, le esigenze legate alla prevenzione e deterrenza di analoghi episodi delittuosi⁸²».

L'amministrazione, infatti, ha posto alla base della propria determinazione a procedere alla pubblicazione la necessità di far maturare nella collettività una piena consapevolezza di come quelle che potrebbero sembrare delle mere derive sociali possano sfociare in gesti atroci, pertanto è stata considerata la loro utilità al fine di evitare il ripetersi di reati analoghi. Nel caso di specie, d'altronde, i video delle aggressioni, girati dagli indiziati, erano già stati fatti circolare e si era valutata la possibilità che l'intera società civile potesse dimostrarsi non pienamente consapevole della gravità di certi comportamenti, ignorandoli, sottovalutandoli o, addirittura, giustificandoli in qualche modo. La diffusione dei video ha avuto, quindi, lo scopo di mostrare come tacere certi comportamenti possa rendere corresponsabili, soprattutto, se, come in questo caso, la vittima sia un soggetto debole, solo e indifeso.

Relativamente agli atti con i quali è stata assunta la decisione di divulgazione del materiale, la Questura procedente ha chiarito che l'autorizzazione alla pubblicazione è stata rilasciata al Dirigente della Squadra Mobile "verbalmente" dal Procuratore della Repubblica competente, previa visione ed adozione di ogni accorgimento utile a rendere non riconoscibili le persone in essi ritratte, ossia attraverso l'applicazione di filtri sui volti e sulle parti audio. Acquisito il nulla-osta dall'Autorità giudiziaria, il dirigente ha provveduto a darne comunicazione all'Ufficio stampa della Questura per il successivo inoltrare all'Ufficio relazioni esterne e cerimoniale del Dipartimento della pub-

82 Cfr. provvedimento *de quo*, p. 3.

blica sicurezza, che ha fornito il materiale, poi oggetto di divulgazione, applicando i filtri richiesti dall'Autorità giudiziaria.

È stato, inoltre, osservato che la diffusione dei video (con l'adozione degli opportuni accorgimenti) ha sortito effetti positivi sulla cittadinanza, avendo spinto alcuni soggetti non ripresi, eppure presenti agli episodi narrati, a riferire ulteriori circostanze e a fornire elementi utili per la ricostruzione dei fatti e per l'individuazione di altri rei rispetto ai quali hanno deciso di prendere le distanze. Quest'ultimo dato avrebbe confermato le esigenze di prevenzione e deterrenza che avevano motivato la divulgazione dei contenuti video.

Nonostante le osservazioni prodotte, il Garante ha rilevato che il Ministero, per mezzo della divulgazione suddetta, ha posto in essere un trattamento dei dati personali dell'interessato eccedente rispetto alle finalità del medesimo trattamento e non necessario per l'esecuzione di uno dei compiti disciplinati dal D.Lgs. n. 51/2018. È stato asserito, ancora, che tali violazioni renderebbero applicabile la sanzione amministrativa prevista dall'art. 42 del D.Lgs. n. 51/2018.

Il Ministero ha ulteriormente controdedotto nel senso che rientrerebbe nei compiti della Polizia di Stato la funzione di "prevenzione generale", che può essere perseguita anche attraverso la pubblicità data alla sanzione penale a favore della collettività e che il veicolo di tale informazione, in prima battuta, è di pertinenza degli organi di polizia giudiziaria e di giustizia penale (nel rispetto degli obblighi di segretezza che presidiano il processo). A tale scopo, è stato anche prodotta una nota della suddetta Procura che ha confermato ciò che aveva a suo tempo verbalmente autorizzato, vale a dire la divulgazione dei video, previa adozione degli accorgimenti tecnici (oscuramento o comunque apposizione di filtri sui volti e alterazione delle parti audio), necessari per non rendere riconoscibili i soggetti ripresi, conformemente a quanto previsto dalle disposizioni di legge in materia.

Per quanto concerne, infine, «il contenuto audio dei filmati - che, seppur "filtrato", ha dato la precisa percezione dello strazio patito dalla vittima - si [è ritenuto] che si sia dosato ragionevolmente e con equilibrio il sacrificio dei diritti personali della vittima, compresi dall'interesse pubblico preminente alla prevenzione e repressione dei reati, anche al fine di scuotere le coscienze con la straziante richiesta di aiuto, affinché il male non goda del comportamento indifferente degli altri⁸³».

83 Cfr. provvedimento *de quo*, p. 6.

Ciò premesso, il Garante, nella propria determina, ha stabilito che la divulgazione dei video era sicuramente riconducibile alle finalità di polizia, correlate con i compiti istituzionali svolti dalla Polizia di Stato, con particolare riferimento alla “prevenzione dei reati”, avvenuta nell’esercizio dell’attività di polizia di sicurezza e non giudiziaria. Ha, quindi, ritenuto che fosse non rilevante l’autorizzazione della Procura della Repubblica ai fini della protezione dei dati personali, quanto, piuttosto, soltanto allo scopo di escludere che la divulgazione di tali immagini potesse avvenire in violazione di legge o incidere negativamente sui procedimenti penali in corso; ha considerato non rilevante anche la circostanza che dalla divulgazione sia scaturita la volontà di alcuni testimoni dei fatti di collaborare con la polizia giudiziaria, essendo stata espressamente posta a giustificazione del trattamento soltanto l’esigenza di prevenzione e deterrenza di altri, ipotetici reati.

Il Garante, inoltre, ha eccepito che nel primo video si sente ‘scanditamente’ la voce della vittima, mentre prova a difendersi e chiede soccorso e non risulta essere stato applicato alcun filtro su quelle parti dell’audio, nonostante la richiesta della Procura e quanto dichiarato dal Ministero; nel secondo video, anche se non si sentono ‘scanditamente’ le voci degli aggressori e della vittima, da quello che si può vedere (persone che brandiscono randelli) e sentendo le urla strazianti della vittima, associate a dei rumori forti, si percepisce chiaramente la crudeltà di quanto sta accadendo.

L’*Authority* ha rilevato anche che sulla stampa erano stati divulgati oltre i dati identificativi della vittima (nome, cognome, immagine del volto in primo piano, dove viveva, ecc.), anche la notizia che fosse affetto da disturbi psichici; inoltre, era stata resa pubblica la circostanza che le sevizie subite dall’uomo avevano causato uno stato di degrado psico-fisico dello stesso, che ne aveva causato il decesso.

Il trattamento in questione è stato, pertanto, considerato relativo a dati particolari, pertanto sottoposto al regime dell’art. 14, d.p.r. 15 gennaio 2018, n. 15⁸⁴, di conseguenza è stato ritenuto “non necessario” per la finalità di prevenzione dei reati ed avvenuta in pregiudizio della dignità dell’interessato, la cui tutela deve essere garantita anche dopo la morte⁸⁵.

84 Vds. nota n. 80 a p. 177.

85 A mente dell’art. 2-terdecies, Codice della *privacy*, i diritti possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell’interessato o per ragioni familiari meritevoli di protezione, ma la divulgazione massiva, con mezzi di comunicazione raggiungibili da

La natura dei dati in parola (condizioni di salute e la particolare crudezza dei fatti documentati) e il fatto che il Ministero abbia pubblicato, in un secondo momento, anche un altro video, nonostante avesse proceduto a cancellare quelli divulgati inizialmente dopo il primo intervento del Garante, ha indotto l'Autorità di controllo all'adozione di una condanna al pagamento di euro 75.000,00, a titolo di sanzione amministrativa pecuniaria, in una misura, pertanto, superiore al minimo edittale.

4. Il caso del trattamento illecito di dati personali di un dipendente civile di una Questura

Si ritiene possa essere, infine, interessante analizzare il provvedimento dell'11 novembre 2021 del Garante, con il quale questi si è espresso in ordine a un reclamo presentato da un dipendente civile, in servizio presso una Questura da diversi anni, poiché la condotta, oggetto di valutazione, rientra nell'ambito di applicazione generico del regolamento, manifestando un carattere puramente ed esclusivamente amministrativo, a dimostrazione del fatto che le Forze di polizia sono soggette anche alla disciplina generale del GDPR.

Con il reclamo il dipendente ha lamentato che l'Ufficio di appartenenza procedesse, in modo del tutto arbitrario, ad effettuare sorveglianze e controlli a suo carico, sostanziosi tale illegale attività nelle intercettazioni delle comunicazioni personali, in voce e dati, in pedinamenti e nei controlli dei colloqui intrattenuti con terzi soggetti. Di tutto questo sarebbe stato formato un fascicolo personale aperto a nome del dipendente.

Nell'esposto è stato affermato, inoltre, che la Questura aveva risposto ad una richiesta di accesso agli atti in modo negativo, dichiarando formalmente che "nulla risulta agli atti d'Ufficio". Non soddisfatto dal riscontro ricevuto, il reclamante ribadiva le sue richieste alla Questura e presentava, altresì, ricorso alla Commissione per l'accesso ai documenti amministrativi, che lo respingeva per tardività e anche per l'attestata inesistenza - da parte del datore di lavoro - dei documenti oggetto dell'istanza di accesso.

una platea di soggetti indefinita e potenzialmente illimitata, ha reso impossibile qualsiasi controllo e obiezione, con la conseguenza che i diritti del defunto diventano, in questo caso, degni di protezione.

In particolare, il reclamante ha anche lamentato che nella nota difensiva trasmessa alla Commissione per l'accesso ai documenti amministrativi, il Questore, dopo aver rappresentato che gli atti, oggetto della richiesta di accesso, non risultavano esistenti, ha fornito informazioni personali riferite al dipendente, ritenute per giunta di natura 'particolare', testualmente dichiarando che «giova precisare che il nominato in oggetto già da qualche anno è stato autore di due bizzarre missive indirizzate al Presidente della Provincia di XX, per le quali non è stato, all'epoca, interessato il medico competente di questo ufficio [...] in data 31 dicembre u.s. si presentava, presso questi Uffici, il titolare della Agenzia XX, con sede in XX rappresentando di aver ricevuto una raccomandata da parte del sig. XX relativa all'accesso ai dati personali, in esercizio dei diritti di cui agli artt.15 e seguenti del Regolamento UE 2016/679, presumibilmente trattati da quella agenzia [...] Si rappresenta, pertanto, come il dipendente, pur svolgendo gli incarichi d'ufficio affidatigli con ordinaria diligenza e mantenendo un contegno serio e riservato, in occasione di interlocuzioni con lo scrivente, relativamente alle istanze sopracitate, è apparso essere sempre reticente e pretestuoso, al punto da far insorgere nell'interlocutore dubbi sulla fondatezza delle sue richieste. Si fa riserva, comunque, di interessare eventualmente al riguardo il medico competente ai sensi del D.Lgs. 81/2008».

Il dipendente civile ha concluso, quindi, nel senso che il trattamento dei suoi dati personali, effettuato con la trasmissione della predetta nota, sia avvenuto, per i dati ritenuti eccedenti, in violazione degli artt. 5, 6, 7 e 9 del Regolamento.

A seguito della presentazione del reclamo ed essendo state ritenute inconferenti le motivazioni addotte dal Questore in merito alla divulgazione di ulteriori informazioni rispetto alla mera insussistenza della documentazione richiesta⁸⁶ alla Commissione per l'accesso ai documenti amministrativi, il Garante ha dato avvio al procedimento di accertamento ed ha analizzato se l'ostensione alla Commissione del contenuto degli scambi epistolari intervenuti tra il reclamante e il titolare di un'agenzia

⁸⁶ Nelle motivazioni presentate al Garante il Questore ha affermato: «Nel fornire la memoria difensiva alla predetta Commissione e, comunque, nell'ottica di una corretta gestione dei dati e di collaborazione con la medesima Commissione nonché allo scopo di tutelare l'interesse del dipendente, lo scrivente, al fine unicamente di assicurare una più ampia valutazione dei fatti, rappresentava quanto disponibile al fascicolo del dipendente, senza per questo voler illegittimamente divulgare dati attinenti la sfera personale del sig. XX».

investigativa e la palesata riserva di valutare l'opportunità di interessare il medico competente circa la condotta del dipendente potessero essere considerati lesivi dei principi e dei presupposti di trattamento, fissati dal GDPR, concretandosi un'attività meramente amministrativa, sebbene posta in essere da un Ufficio di polizia.

Innanzitutto, entrambe le informazioni fornite sono state configurate come dati personali, anche, pertanto, la valutazione dell'interessamento del medico competente, poiché fondata sull'asserire che il soggetto fosse autore di due bizzarre missive, che avrebbero giustificato un accertamento sullo stato di salute psicofisico.

In secondo luogo, è stato rilevato come il trattamento (vale a dire la comunicazione alla Commissione) non è stato effettuato con il consenso dell'interessato e non risulta neppure legittimato dalle altre ipotesi di liceità previste dall'art. 6 GDPR, anzi la stessa è risultata eccedente, apparendo rilevante ed esaustivo, per la decisione che la Commissione era chiamata ad adottare, unicamente la circostanza dell'inesistenza dei documenti di cui il reclamante chiedeva l'ostensione oppure gli eventuali motivi che avessero ostato all'accesso, qualora realmente esistenti.

Le comunicazioni, essendo attinenti solo alla persona dell'interessato, sono state giudicate come non rientranti in quel margine di libertà di elaborare la propria tesi che va riconosciuto a chi è parte di un procedimento amministrativo giustiziale, quale quello davanti alla Commissione per l'accesso; inoltre, i dati del reclamante, obiettivamente screditanti, non sono stati giudicati funzionali "allo scopo di tutelare l'interesse del dipendente", come sostenuto dal Questore.

Il Garante, pertanto, ha dichiarato l'illiceità del trattamento effettuato dalla Questura, poiché in violazione dei principi posti dall'art. 5 GDPR e in assenza di una delle condizioni legittimanti di cui all'art. 6 GDPR e, a mente dell'art. 58, paragrafo 2, lett. b), GDPR, ha rivolto un ammonimento al titolare del trattamento, decidendo, tuttavia, di non infliggere una sanzione amministrativa pecuniaria, in considerazione del fatto che il trattamento ha visto come destinataria la sola Commissione per l'accesso e che il titolare non ha tratto alcun vantaggio economico dalla comunicazione.

Considerazioni conclusive

Nello sviluppo di quest'elaborato, si è cercato di fornire un quadro d'insieme della normativa vigente nel diritto unionale e nazionale in

materia di protezione dei dati personali, ponendo un occhio di riguardo alle attività di trattamento che vengono svolte dalle Forze di polizia ed è stato evidenziato che l'obiettivo di fondo, che il legislatore ha inteso perseguire, è stato quello di operare un dialogo tra prospettive diverse, che sarebbero naturalmente in antitesi. È stato messo in luce che, per raggiungere tale obiettivo, il sistema delle norme si muove nella consapevolezza che l'adempimento del dovere di ciascuno porti al miglior equilibrio delle posizioni e questo può essere fatto solo qualora le parti si pongano nel reciproco ascolto delle proprie esigenze.

Realizzare un trattamento "proporzionato" (rispetto alla finalità) è il primo passo per deflazionare il conflitto, riportandolo piuttosto in un contesto nel quale il vantaggio ottenuto in sicurezza supera la sensazione di intrusione dovuta al trattamento dei dati personali, specie da parte delle Forze di polizia o dalle autorità in genere. Il principio di proporzionalità, quindi, richiede di indirizzare la protezione dei dati personali non solo come adempimento giuridico, da realizzare più per obbligo che per convinzione, ma come componente fondamentale nello svolgimento delle attività istituzionali.

Partendo da questa prospettiva, diventa consequenziale chiedersi se sia veramente corretto affermare, come sempre più spesso accade, che per garantire il diritto alla sicurezza, che è un diritto fondamentale, occorra necessariamente limitare la *privacy*, che è anch'essa un diritto fondamentale. L'argomento diventa di cruciale importanza, soprattutto in considerazione delle sfide che l'evoluzione tecnologica pone all'uomo moderno e, di conseguenza, al legislatore.

Si fa riferimento, in particolare, all'intelligenza artificiale e alle forme pervasive di controllo - tramite la raccolta, l'analisi ed il confronto di immagini, di voci, di dati biometrici, di dati di natura disparata, aggregati grazie ad enormi potenzialità di calcolo - che consentono la potenziale conoscibilità dei comportamenti umani e, persino, delle emozioni.

È stato sottolineato che il legislatore europeo si è cimentato con questo nuovo e sconosciuto contesto soltanto qualche mese fa con il regolamento 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, laddove il normatore interno sta ancora oggi affrontando questo difficile e complesso tema, nell'ottica dell'adozione di un atto normativo interno di adattamento.

A tale scopo, è opinione di chi scrive che il principio che dovrebbe guidare l'analisi debba essere sempre la proporzionalità del trattamento, che, se ben applicato, dovrebbe condurre alla possibilità di utilizzare anche questa tecnologia, al fine di ampliare gli strumenti a

disposizione delle forze dell'ordine per la tutela della pubblica sicurezza e le connesse libertà e diritti inviolabili, senza, però, portare ad una compressione della protezione dei dati personali e dei diritti patrimoniali inviolabili, in essa coinvolti, assicurando un vantaggio sociale e limitando entro chiari, ben definiti, trasparenti e controllati limiti il potenziale senso di intrusione nella sfera privata.

Si è ben consapevoli, tuttavia, che si tratta di una sfida difficile, anche perché il diritto alla *privacy*, ancora oggi, viene diffusamente considerato recessivo davanti al diritto alla sicurezza, al punto che spesso si avverte quasi la sensazione che siano gli stessi soggetti interessati ad essere disposti a barattare il diritto alla protezione dei dati personali con quello di sicurezza, tuttavia, è necessario non perdere di vista e dilapidare il patrimonio di modernità e di reale libertà che la tutela della riservatezza ha garantito all'uomo moderno, inteso, così, come individuo degno di protezione in tutte le sue espressioni e non soltanto rispetto alla tutela dell'incolumità fisica o della proprietà privata.

Bibliografia

- ARENA G., *La tutela della riservatezza nella società dell'informazione*, in AA.VV., *Scritti in onore di Pietro Virga*, I, Milano, 1994.
- BARETTONI ARLERI A., *Trasparenza amministrativa e tutela della privacy*, in (a cura di) AMOROSINO S., *Le trasformazioni del diritto amministrativo. Scritti degli allievi per gli ottanta anni di Massimo Severo Giannini*, Milano, 1995.
- BERNARDI N., *Privacy. Protezione e trattamento dei dati*, IPSOA, Milano 2019.
- BRUNO G., *Diritto alla privacy: la storia e l'evoluzione*, in *Diritto.it*, 2023.
- CARPINO M., *Il trattamento dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento dei reati*, Giappichelli, Torino, 2024.
- FRANCA S., *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Editoriale scientifica, Napoli, 2023.
- *Manuale del diritto europeo in materia di protezione dei dati*, Publications Office of the European Union, 2018.
- MARANDOLA A., *Sicurezza e diritti fondamentali: aspetti processuali*, in *Processo penale e giustizia*, fasc. 11, 2019.
- PATAVINI P. – TRONCONE F., *L'oscuramento dei dati personali nei provvedimenti della Corte costituzionale*, Servizio studi Corte costituzionale, 2020.
- PONTI B., *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, Angeli, Milano, 2023.
- RODOTÀ S., *La privacy tra individuo e collettività*, in *Politica del diritto*, 1975.
- TENORE V., *La libertà di pensiero tra riconoscimento costituzionale e limiti impliciti ed espliciti: i limiti normativi e giurisprudenziali per giornalisti, dipendenti pubblici e privati nei socialmedia*, in *Lavoro, diritti, Europa*, 2019.
- WARREN S. D. – BRANDEIS L. D., *The Right to Privacy*, in *Harvard Law Review*, IV, 1890.

Parte IV
Documenti, Normativa e Giurisprudenza di interesse

“Aspetti finanziari e contabili delle gestioni straordinarie degli enti sciolti per infiltrazioni e condizionamenti di tipo mafioso”.

di Nunzio Mario Tritto*

Abstract

Il fenomeno dello scioglimento degli enti locali per infiltrazioni e condizionamenti della criminalità organizzata rappresenta una delle più significative misure preventive stabilite dall'ordinamento per la tutela della legalità democratica a livello territoriale. Il presente contributo si occupa dei profili economico-finanziari che caratterizzano le gestioni straordinarie degli enti sciolti per infiltrazioni mafiose, esaminando tanto le cause strutturali del “dissesto amministrativo” (e spesso anche contabile) quanto le strategie di risanamento necessarie per il ripristino della legalità ed il ritorno *in bonis* degli enti interessati. Al fine di rendere più utile il lavoro, vengono altresì riportate le più significative esperienze internazionali relative a fattispecie analoghe a quelle del contrasto della corruzione negli enti locali e del ripristino della normalità economico-finanziaria nella gestione contabile dei medesimi.

The so-called dissolution of local authorities due to infiltration and conditioning by organized crime is one of the most significant preventive measures provided for by the law for the protection of democratic legality at the territorial level. This paper deals with the economic and financial profiles that characterize the extraordinary management of entities dissolved due to mafia infiltration, examining both the structural causes of the administrative and often also financial failure and the recovery strategies necessary for the resto-

* Magistrato della Corte dei conti.

ration of legality and the return to performing status of the entities concerned. In order to make the work more useful, the most significant international experiences relating to cases similar to those of the fight against corruption in local authorities and the restoration of economic and financial normality in the accounting management of the same are also reported.

1. Considerazioni preliminari

Il fenomeno dello scioglimento degli enti locali per infiltrazioni e condizionamenti della criminalità organizzata rappresenta una delle più significative misure preventive previste dall'ordinamento per la tutela della legalità democratica a livello territoriale¹. L'istituto, disciplinato dall'art. 143² del decreto legislativo 18 agosto 2000, n. 267 (re-

1 Per le novità derivanti dall'introduzione dei cd sistemi *accrual* anche in relazione agli enti soggetti ad infiltrazioni della criminalità organizzata, si veda: TRITTO N. M., *La nuova contabilità accrual per le amministrazioni pubbliche - Quadro concettuale e ITAS*, Roma, 2025.

2 Secondo la vigente formulazione dell'art. 143: "1. Fuori dai casi previsti dall'articolo 141, i consigli comunali e provinciali sono sciolti quando, anche a seguito di accertamenti effettuati a norma dell'articolo 59, comma 7, emergono concreti, univoci e rilevanti elementi su collegamenti diretti o indiretti con la criminalità organizzata di tipo mafioso o similare degli amministratori di cui all'articolo 77, comma 2, ovvero su forme di condizionamento degli stessi, tali da determinare un'alterazione del procedimento di formazione della volontà degli organi elettivi ed amministrativi e da compromettere il buon andamento o l'imparzialità delle amministrazioni comunali e provinciali, nonché il regolare funzionamento dei servizi ad esse affidati, ovvero che risultino tali da arrecare grave e perdurante pregiudizio per lo stato della sicurezza pubblica.

2. Al fine di verificare la sussistenza degli elementi di cui al comma 1 anche con riferimento al segretario comunale o provinciale, al direttore generale, ai dirigenti ed ai dipendenti dell'ente locale, il prefetto competente per territorio dispone ogni opportuno accertamento, di norma promuovendo l'accesso presso l'ente interessato. In tal caso, il prefetto nomina una commissione d'indagine, composta da tre funzionari della pubblica amministrazione, attraverso la quale esercita i poteri di accesso e di accertamento di cui è titolare per delega del Ministro dell'interno ai sensi dell'articolo 2, comma 2-quater, del decreto-legge 29 ottobre 1991, n. 345, convertito, con modificazioni, dalla legge 30 dicembre 1991, n. 410. Entro tre mesi dalla data di accesso, rinnovabili una volta per un ulteriore periodo massimo di tre mesi, la commissione termina gli accertamenti e rassegna al prefetto le proprie conclusioni.

3. Entro il termine di quarantacinque giorni dal deposito delle conclusioni della commissione d'indagine, ovvero quando abbia comunque diversamente acquisito gli elementi di cui al comma 1 ovvero in ordine alla sussistenza di forme di condizionamento degli organi amministrativi ed elettivi, il prefetto, sentito il comitato provinciale per l'ordine e la sicurezza pubblica integrato con la partecipazione del procuratore della Repubblica competente per territorio, invia al Ministro dell'interno una relazione nella quale si dà conto della eventuale sussistenza degli elementi di cui al comma 1 anche con riferimento al segretario comunale o provinciale, al direttore generale, ai dirigenti e ai dipendenti dell'ente locale. Nella relazione sono, altresì, indicati gli appalti, i contratti e i servizi interessati dai fenomeni di compromissione o interferenza con la criminalità organizzata o comunque connotati da condizionamenti o da una condotta antigiuridica. Nei casi in cui per i fatti oggetto de-

cante il Testo unico degli enti locali, T.U.E.L.), costituisce una *extrema ratio* finalizzata a ripristinare il corretto funzionamento delle istituzioni

gli accertamenti di cui al presente articolo o per eventi connessi sia pendente procedimento penale, il prefetto può richiedere preventivamente informazioni al procuratore della Repubblica competente, il quale, in deroga all'articolo 329 del codice di procedura penale, comunica tutte le informazioni che non ritiene debbano rimanere segrete per le esigenze del procedimento.

4. Lo scioglimento di cui al comma 1 è disposto con decreto del Presidente della Repubblica, su proposta del Ministro dell'interno, previa deliberazione del Consiglio dei ministri entro tre mesi dalla trasmissione della relazione di cui al comma 3, ed è immediatamente trasmesso alle Camere. Nella proposta di scioglimento sono indicati in modo analitico le anomalie riscontrate ed i provvedimenti necessari per rimuovere tempestivamente gli effetti più gravi e pregiudizievoli per l'interesse pubblico; la proposta indica, altresì, gli amministratori ritenuti responsabili delle condotte che hanno dato causa allo scioglimento. Lo scioglimento del consiglio comunale o provinciale comporta la cessazione dalla carica di consigliere, di sindaco, di presidente della provincia, di componente delle rispettive giunte e di ogni altro incarico comunque connesso alle cariche ricoperte, anche se diversamente disposto dalle leggi vigenti in materia di ordinamento e funzionamento degli organi predetti.

5. Anche nei casi in cui non sia disposto lo scioglimento, qualora la relazione prefettizia rilevi la sussistenza degli elementi di cui al comma 1 con riferimento al segretario comunale o provinciale, al direttore generale, ai dirigenti o ai dipendenti a qualunque titolo dell'ente locale, con decreto del Ministro dell'interno, su proposta del prefetto, è adottato ogni provvedimento utile a far cessare immediatamente il pregiudizio in atto e ricondurre alla normalità la vita amministrativa dell'ente, ivi inclusa la sospensione dall'impiego del dipendente, ovvero la sua destinazione ad altro ufficio o altra mansione con obbligo di avvio del procedimento disciplinare da parte dell'autorità competente.

6. A decorrere dalla data di pubblicazione del decreto di scioglimento sono risolti di diritto gli incarichi di cui all'articolo 110, nonché gli incarichi di revisore dei conti e i rapporti di consulenza e di collaborazione coordinata e continuativa che non siano stati rinnovati dalla commissione straordinaria di cui all'articolo 144 entro quarantacinque giorni dal suo insediamento.

7. Nel caso in cui non sussistano i presupposti per lo scioglimento o l'adozione di altri provvedimenti di cui al comma 5, il Ministro dell'interno, entro tre mesi dalla trasmissione della relazione di cui al comma 3, emana comunque un decreto di conclusione del procedimento in cui dà conto degli esiti dell'attività di accertamento. Le modalità di pubblicazione dei provvedimenti emessi in caso di insussistenza dei presupposti per la proposta di scioglimento sono disciplinate dal Ministro dell'interno con proprio decreto.

7-bis. Nell'ipotesi di cui al comma 7, qualora dalla relazione del prefetto emergano, riguardo ad uno o più settori amministrativi, situazioni sintomatiche di condotte illecite gravi e reiterate, tali da determinare un'alterazione delle procedure e da compromettere il buon andamento e l'imparzialità delle amministrazioni comunali o provinciali, nonché il regolare funzionamento dei servizi ad esse affidati, il prefetto, sulla base delle risultanze dell'accesso, al fine di far cessare le situazioni riscontrate e di ricondurre alla normalità l'attività amministrativa dell'ente, individua, fatti salvi i profili di rilevanza penale, i prioritari interventi di risanamento indicando gli atti da assumere, con la fissazione di un termine per l'adozione degli stessi, e fornisce ogni utile supporto tecnico-amministrativo a mezzo dei propri uffici. Decorso inutilmente il termine fissato, il prefetto assegna all'ente un ulteriore termine, non superiore a 20 giorni, per la loro adozione, scaduto il quale si sostituisce, mediante commissario ad acta, all'amministrazione inadempiente. Ai relativi oneri gli enti locali provvedono con le risorse disponibili a legislazione vigente sui propri bilanci.

8. Se dalla relazione prefettizia emergono concreti, univoci e rilevanti elementi su collegamenti tra singoli amministratori e la criminalità organizzata di tipo mafioso, il Ministro dell'interno trasmette la relazione di cui al comma 3 all'autorità giudiziaria competente per territorio, ai fini

ni locali qualora queste ultime risultino compromesse da fenomeni di infiltrazione mafiosa.

In effetti, *“la natura giuridica dello scioglimento di cui si parla è singolare e complessa, in quanto non si configura come un semplice provvedimento sanzionatorio volto a punire singoli comportamenti illegittimi o irregolari, ma si qualifica come una misura di prevenzione di carattere straordinario, atta a rispondere ad una situazione in cui gli organi elettivi risultano essere condizionati, influenzati o infiltrati da organizzazioni criminali di stampo mafioso, compromettendo così la regolarità dell’attività amministrativa nonché il regolare funzionamento dei servizi pubblici affidati al comune o alla*

dell’applicazione delle misure di prevenzione previste nei confronti dei soggetti di cui all’articolo 1 della legge 31 maggio 1965, n. 575.

9. Il decreto di scioglimento è pubblicato nella Gazzetta Ufficiale. Al decreto sono allegate la proposta del Ministro dell’interno e la relazione del prefetto, salvo che il Consiglio dei ministri disponga di mantenere la riservatezza su parti della proposta o della relazione nei casi in cui lo ritenga strettamente necessario.

10. Il decreto di scioglimento conserva i suoi effetti per un periodo da dodici mesi a diciotto mesi prorogabili fino ad un massimo di ventiquattro mesi in casi eccezionali, dandone comunicazione alle Commissioni parlamentari competenti, al fine di assicurare il regolare funzionamento dei servizi affidati alle amministrazioni, nel rispetto dei principi di imparzialità e di buon andamento dell’azione amministrativa. Le elezioni degli organi sciolti ai sensi del presente articolo si svolgono in occasione del turno annuale ordinario di cui all’articolo 1 della legge 7 giugno 1991, n. 182, e successive modificazioni. Nel caso in cui la scadenza della durata dello scioglimento cada nel secondo semestre dell’anno, le elezioni si svolgono in un turno straordinario da tenersi in una domenica compresa tra il 15 ottobre e il 15 dicembre. La data delle elezioni è fissata ai sensi dell’articolo 3 della citata legge n. 182 del 1991, e successive modificazioni. L’eventuale provvedimento di proroga della durata dello scioglimento è adottato non oltre il cinquantesimo giorno antecedente alla data di scadenza della durata dello scioglimento stesso, osservando le procedure e le modalità stabilite nel comma 4.

11. Fatta salva ogni altra misura interdittiva ed accessoria eventualmente prevista, gli amministratori responsabili delle condotte che hanno dato causa allo scioglimento di cui al presente articolo non possono essere candidati alle elezioni per la Camera dei deputati, per il Senato della Repubblica e per il Parlamento europeo nonché alle elezioni regionali, provinciali, comunali e circoscrizionali, in relazione ai due turni elettorali successivi allo scioglimento stesso, qualora la loro incandidabilità sia dichiarata con provvedimento definitivo. Ai fini della dichiarazione d’incandidabilità il Ministro dell’interno invia senza ritardo la proposta di scioglimento di cui al comma 4 al tribunale competente per territorio, che valuta la sussistenza degli elementi di cui al comma 1 con riferimento agli amministratori indicati nella proposta stessa. Si applicano, in quanto compatibili, le procedure di cui al libro IV, titolo II, capo VI, del codice di procedura civile.

12. Quando ricorrono motivi di urgente necessità, il prefetto, in attesa del decreto di scioglimento, sospende gli organi dalla carica ricoperta, nonché da ogni altro incarico ad essa connesso, assicurando la provvisoria amministrazione dell’ente mediante invio di commissari. La sospensione non può eccedere la durata di sessanta giorni e il termine del decreto di cui al comma 10 decorre dalla data del provvedimento di sospensione.

13. Si fa luogo comunque allo scioglimento degli organi, a norma del presente articolo, quando sussistono le condizioni indicate nel comma 1, ancorché ricorrano le situazioni previste dall’articolo 141”.

*provincia. Si tratta di un intervento che, pur incidendo in modo significativo sull'autonomia locale, si giustifica in ragione della necessità di tutelare un interesse pubblico superiore, quello della sicurezza democratica e della legalità sul territorio, prevenendo quindi fenomeni di ingerenza mafiosa che potrebbero minare alla base le fondamenta dell'ordinamento costituzionale e amministrativo. Tale interpretazione è stata ribadita anche dalla Corte costituzionale, che ha riconosciuto allo scioglimento un carattere eminentemente preventivo, piuttosto che punitivo, giustificando così la sua natura e i limiti alle forme ordinarie di tutela e partecipazione"*³.

Gli ultimi dati disponibili in materia di gestioni commissariali⁴ evidenziano come alle sempre presenti problematiche di legalità si accompagnino sistematicamente criticità di carattere finanziario e/o contabile che richiedono interventi strutturali di risanamento. Tale correlazione non è meramente casuale, ma riflette la natura sistemica del condizionamento posto in essere dalla criminalità organizzata, che si manifesta attraverso la compromissione dell'intero apparato amministrativo, con particolare riguardo alla gestione delle risorse pubbliche⁵.

Il presente contributo intende analizzare in modo approfondito i profili economico-finanziari che caratterizzano le gestioni straordinarie degli enti sciolti per infiltrazioni mafiose, esaminando tanto le cause strutturali del "dissesto amministrativo" (e spesso anche contabile) quanto le strategie di risanamento necessarie per il ripristino della legalità ed il ritorno *in bonis* degli enti interessati. Al fine di rendere più utile il lavoro, verranno altresì riportate le più significative esperienze internazionali relative a fattispecie analoghe a quelle del contrasto alla corruzione negli enti locali e del ripristino della normalità economico-finanziaria nella gestione contabile dei medesimi.

3 In tal senso: TRITTO N. M., *Manuale di diritto prefettizio*, Roma, 2025, p. 255 ss.

4 Secondo la relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3), nel 2024 sono state attivate n. 28 procedure che hanno interessato altrettanti enti locali per una popolazione complessiva di oltre 451.000 abitanti; dal punto di vista territoriale, 10 enti risultano ubicati in Calabria, 9 in Campania, 4 in Sicilia, 3 in Puglia e 2 nel Lazio. La distribuzione demografica degli enti interessati evidenzia come il fenomeno non sia limitato ai piccoli comuni: si va infatti dai 685 abitanti di Mojo Alcantara (ME) ai 65.944 abitanti di Castellammare di Stabia (NA), con una media di circa 16.100 abitanti per ente commissariato.

5 Per un sintetico esame dei legami tra mafia ed economia: AA.VV., *Le mafie nell'economia legale: scambi, collusioni, azioni di contrasto*, Bologna, 2019.

2. Il quadro normativo di riferimento

Come si è accennato, l'art. 143 del T.U.E.L. (relativo allo "Scioglimento dei consigli comunali e provinciali conseguente a fenomeni di infiltrazione e di condizionamento di tipo mafioso o similare. Responsabilità dei dirigenti e dipendenti") si inserisce in un più ampio sistema di prevenzione amministrativa che trova le sue radici storiche nella legislazione antimafia degli anni Novanta del Novecento⁶. La norma, modificata nel tempo per adeguarsi all'evoluzione dei fenomeni criminali, prevede lo scioglimento degli organi elettivi qualora sussistano "elementi su collegamenti diretti o indiretti con la criminalità organizzata di tipo mafioso o similare degli amministratori ... ovvero su forme di condizionamento degli stessi".

Dal punto di vista finanziario, la misura del commissariamento si configura come un intervento di risanamento amministrativo integrato, che deve necessariamente coniugare il ripristino della legalità con la ricostituzione di equilibri economico-finanziari sostenibili. Tale duplice finalità emerge chiaramente dalla disciplina dell'art. 145⁷ del

6 Per un esame storico del fenomeno si rimanda a: TRITTO N. M., *Storia contemporanea e della Pubblica Amministrazione italiana - Approfondimenti*, Roma, 2022.

7 "1. Quando in relazione alle situazioni indicate nel comma 1 dell'articolo 143 sussiste la necessità di assicurare il regolare funzionamento dei servizi degli enti nei cui confronti è stato disposto lo scioglimento, il prefetto, su richiesta della commissione straordinaria di cui al comma 1 dell'articolo 144, può disporre, anche in deroga alle norme vigenti, l'assegnazione in via temporanea, in posizione di comando o distacco, di personale amministrativo e tecnico di amministrazioni ed enti pubblici, previa intesa con gli stessi, ove occorra anche in posizione di sovraordinazione. Al personale assegnato spetta un compenso mensile lordo proporzionato alle prestazioni da rendere, stabilito dal prefetto in misura non superiore al 50% del compenso spettante a ciascuno dei componenti della commissione straordinaria, nonché, ove dovuto, il trattamento economico di missione stabilito dalla legge per i dipendenti dello Stato in relazione alla qualifica funzionale posseduta nell'amministrazione di appartenenza. Tali competenze sono a carico dello Stato e sono corrisposte dalla prefettura, sulla base di idonea documentazione giustificativa, sugli accreditamenti emessi, in deroga alle vigenti disposizioni di legge, dal Ministero dell'interno. La prefettura, in caso di ritardo nell'emissione degli accreditamenti è autorizzata a prelevare le somme occorrenti sui fondi in genere della contabilità speciale. Per il personale non dipendente dalle amministrazioni centrali o periferiche dello Stato, la prefettura provvede al rimborso al datore di lavoro dello stipendio lordo, per la parte proporzionalmente corrispondente alla durata delle prestazioni rese. Agli oneri derivanti dalla presente disposizione si provvede con una quota parte del 10% delle somme di denaro confiscate ai sensi della legge 31 maggio 1965, n. 575, e successive modificazioni, nonché del ricavato delle vendite disposte a norma dell'articolo 4, commi 4 e 6, del decreto-legge 14 giugno 1989, n. 230, convertito, con modificazioni, dalla legge 4 agosto 1989, n. 282, relative ai beni mobili o immobili ed ai beni costituiti in azienda confiscati ai sensi della medesima legge n. 575 del 1965. Alla scadenza del periodo di assegnazione, la commissione straordinaria potrà rilasciare, sulla base della valutazione dell'attività prestata dal personale assegnato, apposita certificazione di lodevole servizio che costituisce titolo valutabile ai fini della progressione di carriera e nei concorsi interni e pubblici nelle amministrazioni dello Stato, delle regioni e degli enti locali.

T.U.E.L., che attribuisce alle commissioni straordinarie il compito di predisporre, entro sessanta giorni dall'insediamento, un piano di priorità degli interventi per fronteggiare gravi disservizi ed avviare la sollecita realizzazione delle opere pubbliche indifferibili.

La giurisprudenza amministrativa ha progressivamente consolidato il principio secondo cui lo scioglimento per infiltrazioni mafiose costituisce una misura preventiva e non sanzionatoria, finalizzata alla tutela della collettività piuttosto che alla punizione degli amministratori coinvolti. Tale orientamento, confermato dal Consiglio di Stato con la sentenza n. 4026 del 17 giugno 2019, sottolinea come *“ogni amministratore eletto con l'influenza della mafia, deve, allora, comportare una risposta dello Stato tanto straordinaria quanto lo è la sottrazione del potere di governo a chi formalmente lo ha conquistato con le elezioni ma che, nella*

2. Per far fronte a situazioni di gravi disservizi e per avviare la sollecita realizzazione di opere pubbliche indifferibili, la commissione straordinaria di cui al comma 1 dell'articolo 144, entro il termine di sessanta giorni dall'insediamento, adotta un piano di priorità degli interventi, anche con riferimento a progetti già approvati e non eseguiti. Gli atti relativi devono essere nuovamente approvati dalla commissione straordinaria. La relativa deliberazione, esecutiva a norma di legge, è inviata entro dieci giorni al prefetto il quale, sentito il comitato provinciale della pubblica amministrazione opportunamente integrato con i rappresentanti di uffici tecnici delle amministrazioni statali, regionali o locali, trasmette gli atti all'amministrazione regionale territorialmente competente per il tramite del commissario del Governo, o alla Cassa depositi e prestiti, che provvedono alla dichiarazione di priorità di accesso ai contributi e finanziamenti a carico degli stanziamenti comunque destinati agli investimenti degli enti locali. Le disposizioni del presente comma si applicano ai predetti enti anche in deroga alla disciplina sugli enti locali dissestati, limitatamente agli importi totalmente ammortizzabili con contributi statali o regionali ad essi effettivamente assegnati.

3. Le disposizioni di cui ai commi 1 e 2 si applicano, a far tempo dalla data di insediamento degli organi e fino alla scadenza del mandato elettivo, anche alle amministrazioni comunali e provinciali, i cui organi siano rinnovati al termine del periodo di scioglimento disposto ai sensi del comma 1 dell'articolo 143.

4. Nei casi in cui lo scioglimento è disposto anche con riferimento a situazioni di infiltrazione o di condizionamento di tipo mafioso, connesse all'aggiudicazione di appalti di opere o di lavori pubblici o di pubbliche forniture, ovvero l'affidamento in concessione di servizi pubblici locali, la commissione straordinaria di cui al comma 1 dell'articolo 144 procede alle necessarie verifiche con i poteri del collegio degli ispettori di cui all'articolo 14 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203. A conclusione degli accertamenti, la commissione straordinaria adotta tutti i provvedimenti ritenuti necessari e può disporre d'autorità la revoca delle deliberazioni già adottate, in qualunque momento e fase della procedura contrattuale, o la rescissione del contratto già concluso.

5. Ferme restando le forme di partecipazione popolare previste dagli statuti in attuazione dell'articolo 8, comma 3, la commissione straordinaria di cui al comma 1 dell'articolo 144, allo scopo di acquisire ogni utile elemento di conoscenza e valutazione in ordine a rilevanti questioni di interesse generale si avvale, anche mediante forme di consultazione diretta, dell'apporto di rappresentanti delle forze politiche in ambito locale, dell'Anci, dell'Upi, delle organizzazioni di volontariato e di altri organismi locali particolarmente interessati alle questioni da trattare”.

sostanza, piega il risultato elettorale in danno, diretto o indiretto, della collettività degli onesti a vantaggio delle cosche dominanti”.

Un elemento di particolare rilevanza è l'evoluzione del requisito della prova del condizionamento: la giustizia amministrativa ha infatti precisato che è sufficiente un *“atteggiamento di debolezza, omissione di vigilanza e controllo, incapacità di gestione della “macchina” amministrativa da parte degli organi politici che sia stato idoneo a beneficiare soggetti riconducibili ad ambienti “controindicati”*”⁸.

La sostenibilità democratica dell'istituto dello scioglimento per infiltrazioni mafiose rappresenta una questione di crescente rilevanza nel dibattito giuridico e politico. La sospensione dell'auto-governo democratico locale, pur giustificata dall'eccezionalità delle circostanze, pone infatti interrogativi sulla proporzionalità della misura e sulla sua compatibilità con i principi costituzionali della democrazia rappresentativa⁹.

Il bilanciamento tra esigenze di legalità e principi democratici richiede un approccio particolarmente attento alla proporzionalità degli interventi. La giurisprudenza costituzionale ha riconosciuto la legittimità dell'istituto sulla base del carattere straordinario delle situazioni di infiltrazione mafiosa, ma ha anche sottolineato la necessità di limitare la durata e l'intensità dell'intervento sostitutivo¹⁰.

Il rafforzamento delle garanzie procedurali rappresenta un'esigenza sempre più avvertita per assicurare la piena compatibilità dell'istituto con i principi dello stato di diritto. E a tal proposito, ad esempio, potrebbero ipotizzarsi vari interventi innovativi - quali l'introduzione dell'obbligo di comunicazione alle Camere dell'avvio delle procedure di accesso presso gli enti disposte dai prefetti, la pubblicazione delle relazioni prefettizie anche nei casi di archiviazione dei relativi procedimenti, il potenziamento delle tutele giurisdizionali sia in fase preventiva che successiva, un maggior ruolo attribuito anche

8 Cons. Stato, Sez. III, 28 maggio 2013, sentenza n. 2895; T.A.R. Roma, sez. I, 02/03/2021, sentenza n. 2537.

9 Si veda, tra i tanti: ROLLI R., *Principio di democrazia e scioglimento dei consigli comunali per infiltrazioni mafiose: la partecipazione alla luce del pensiero di Mario Nigro*, Nomos, n. 6/2024.

10 Secondo la sentenza n. 103 del 19 marzo 1993 della Corte costituzionale si tratta di *“una misura di carattere straordinario, dunque, rigorosamente ancorata alle finalità enunciate nel titolo della legge 22 luglio 1991, n. 221, di conversione del d.l. 31 maggio 1991, n. 164 che la qualifica come “misura urgente ... conseguente ai fenomeni di infiltrazione e di condizionamento di tipo mafioso”. Tale qualificazione, collegando la misura ad una emergenza straordinaria, attribuisce a quell'emergenza il valore di limite e di misura del potere, esercitabile perciò solo nei luoghi e fino a quando si manifesti tale straordinario fenomeno eversivo”*.

alla Corte dei conti (come si vedrà meglio *infra*) - che andrebbero tutti nella direzione di rendere più efficace, efficiente e trasparente l'istituto, anche nell'ambito di una maggiore compatibilità del medesimo con la normativa euro-unitaria ed internazionale.

3. Le cause strutturali del dissesto finanziario negli enti infiltrati dalla criminalità organizzata

Passando all'esame concreto delle fattispecie, può *in primis* rilevarsi come l'analisi delle relazioni prefettizie e dei rapporti prodotti dalle commissioni straordinarie riveli una correlazione sistemica tra la presenza di condizionamenti da parte della criminalità organizzata ed il deterioramento delle condizioni finanziarie degli enti locali interessati¹¹. Tale correlazione non rappresenta un mero corollario del fenomeno, ma ne costituisce spesso uno degli strumenti funzionali attraverso cui le organizzazioni criminali riescono a condizionare le scelte amministrative¹².

Come osservato dall'unanime dottrina¹³, il controllo delle risorse pubbliche costituisce uno degli obiettivi primari delle strategie di infiltrazione mafiosa negli enti locali. La compromissione dei meccanismi di gestione finanziaria consente infatti alle organizzazioni criminali di conseguire molteplici vantaggi: l'accesso privilegiato agli appalti pubblici, la possibilità di orientare le scelte di investimento in funzione dei propri interessi economici, la creazione di canali di riciclaggio del denaro illecito attraverso il circuito degli affidamenti pubblici, ecc..

L'esame delle situazioni concrete evidenzia che le irregolarità più gravi e diffuse riguardano la gestione delle entrate tributarie¹⁴, settore

11 Secondo quanto emerge della già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

12 Per un esame delle questioni dal punto di vista penale si rimanda a: TRITTO N. M., *Manuale superiore di diritto penale*, Roma, 2022.

13 Sono troppo numerosi i riferimenti a riguardo, pertanto si rimanda per una sintesi a: CHAMPEYRACHE C., *Destructive entrepreneurship: The cost of the mafia for the legal economy*, *Journal of Economic*, n. 1/2018, pp. 157-172.

14 Secondo quanto emerge della già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3) nel Comune di Monteforte Irpino (AV), ad

nel quale si registrano sistematiche anomalie che vanno ben oltre le comuni inefficienze amministrative.

Un elemento ricorrente nelle relazioni commissariali è la presenza di atteggiamenti di favore verso gli evasori, finalizzati all'ottenimento di consenso elettorale. Tale fenomeno assume particolare gravità quando coinvolge soggetti riconducibili alla criminalità organizzata, configurandosi come una vera e propria forma di scambio politico-mafioso mediato dalla gestione delle risorse tributarie¹⁵.

Le disfunzioni nei sistemi di accertamento tributario si manifestano attraverso diverse modalità operative che rivelano un disegno sistematico di compromissione della funzione impositiva. La mancata informatizzazione dei processi di accertamento, la carenza di controlli incrociati, l'assenza di piani strutturati di lotta all'evasione costituiscono altrettanti indicatori di una gestione orientata a favorire l'elusione fiscale piuttosto che a garantire l'equità contributiva¹⁶.

Parallelamente alle disfunzioni nel sistema delle entrate, si registrano sistematiche irregolarità nella gestione della spesa pubblica locale¹⁷, che si manifestano attraverso modalità operative che evidenziano l'alterazione dei normali meccanismi di controllo e programmazione finanziaria.

Una delle anomalie più ricorrenti riguarda l'utilizzo improprio di fondi vincolati per il finanziamento di spese correnti, in violazione dei principi della contabilità armonizzata e delle disposizioni del T.U.E.L. in materia di equilibri di bilancio¹⁸. Tale pratica, oltre a determinare squilibri strutturali nei conti dell'ente, configura spesso ipotesi

esempio, è stata riscontrata una gestione contraria ai principi contabili e un eccessivo ricorso ad entrate vincolate per coprire le spese correnti, oltre alla tardività nei pagamenti, con conseguente aggravio di interessi e sanzioni a carico dell'ente.

15 Per una disamina del funzionamento dei sistemi tributari locali si rimanda a: TRITTO N. M., *Manuale superiore di diritto tributario*, Roma, 2024.

16 Nel Comune di Caivano (NA) è stata rilevata una bassissima percentuale di riscossione dei tributi e la presenza di debiti fuori bilancio da riconoscere per un importo pari a circa 447.000 euro: tale situazione ha richiesto l'implementazione di un sistema integrato di accertamento e riscossione (cfr. relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno, doc. LXXXVIII n. 3).

17 Per un esame approfondito dei sistemi di gestione della spesa pubblica locale si rimanda a: TRITTO N. M., *Contabilità pubblica, scienza delle finanze e diritto finanziario*, Roma, 2023, p. 381 ss.

18 Anche in tal caso si rimanda a: TRITTO N. M., *Contabilità pubblica, scienza delle finanze e diritto finanziario*, Roma, 2023, p. 477 ss.

di responsabilità amministrativa¹⁹ e, nei casi più gravi, penale²⁰ degli amministratori coinvolti.

La proliferazione di debiti fuori bilancio rappresenta un altro indicatore significativo della compromissione dei meccanismi di controllo della spesa²¹. La formazione di passività non regolarmente contabilizzate può derivare da diverse cause: l'affidamento di servizi o forniture senza la necessaria copertura finanziaria, l'autorizzazione di spese in carenza dei presupposti procedurali previsti dalla normativa, la mancata tempestiva ricognizione delle obbligazioni assunte dall'ente e così via.

L'infiltrazione mafiosa negli enti locali determina la sistematica compromissione dei sistemi di controllo interno²², sia attraverso la collusione diretta del personale preposto sia mediante l'alterazione delle procedure di verifica e monitoraggio.

La mancanza di un efficiente controllo di gestione emerge come elemento costante nelle situazioni di "dissesto amministrativo" connesso ad infiltrazioni della criminalità organizzata; l'assenza di adeguati sistemi di monitoraggio delle *performance* finanziarie facilita infatti la perpetrazione di irregolarità ed impedisce la tempestiva individuazione di situazioni di anomalie contabili e non solo.

I rapporti con gli organi di revisione economico-finanziaria risultano del resto spesso alterati in contesti caratterizzati da infiltrazione mafiosa: la nomina di revisori compiacenti, l'omessa trasmissione di documenti e di informazioni rilevanti, la mancata adozione dei rilievi formulati dagli organi di controllo costituiscono altrettante manifestazioni della compromissione del sistema dei controlli interni.

4. Gli strumenti normativi di sostegno finanziario (e non solo)

Il legislatore ha progressivamente sviluppato un articolato sistema di sostegno finanziario specificamente dedicato agli enti sottopo-

19 Per i profili di responsabilità amministrativa: TRITTO N. M., *Manuale superiore di diritto amministrativo*, Roma, 2024, p. 651 ss.

20 Per i profili di responsabilità penale: TRITTO N. M., *Manuale superiore di diritto penale*, Roma, 2024, p. 177 ss.

21 Si veda a riguardo: GIULIETTI W., *Disciplina contabile e obbligazioni pecuniarie della pubblica amministrazione: i debiti fuori bilancio*, in *Diritto dell'economia*, n. 2/2016, pp. 347-379.

22 Per un esame completo della disciplina dei controlli interni (regionali e non solo), si rimanda a: TRITTO N. M., *Il sistema dei controlli interni regionali: criticità e prospettive di riforma*, in *Federalismi*, n. 11/2022, pp. 199-217.

sti a commissariamento per infiltrazioni della criminalità organizzata, nella consapevolezza che il successo delle operazioni di risanamento dipende anche dalla disponibilità di adeguate risorse economiche.

Le disposizioni introdotte dalla legge di bilancio del 2018 (nello specifico, l'art. 1, commi 277 e 278 della legge 27 dicembre 2017, n. 205²³) hanno istituito presso il Ministero dell'Interno un fondo con dotazione iniziale di cinque milioni di euro annui, specificatamente destinato a favorire iniziative di investimento da parte delle commissioni straordinarie. La disciplina del fondo in esame prevede un meccanismo di incremento automatico delle risorse disponibili attraverso l'attribuzione delle economie rivenienti dal fondo ordinario per il finanziamento dei bilanci degli enti locali. Tale meccanismo ha consentito di elevare significativamente la dotazione del fondo: a partire dal 2019, infatti, oltre ai cinque milioni di euro ordinari, vengono assegnate economie per circa diciotto milioni di euro annui, raggiungendo un ammontare complessivo di oltre ventitré milioni per ciascun anno.

Il decreto del Ministro dell'Interno del 18 maggio 2018, adottato di concerto con il Ministro dell'economia e delle finanze, poi, ha definito i criteri e le modalità del riparto delle risorse del fondo, attribuendo priorità agli enti con popolazione fino a 15.000 abitanti. Tale scelta riflette la considerazione che i comuni di minori dimensioni, pur essendo spesso quelli più esposti ai fenomeni di infiltrazione mafiosa, dispongono generalmente di risorse finanziarie più limitate per affrontare i necessari interventi di risanamento. La distribuzione delle risorse avviene sulla base di piani di intervento predisposti dalle commissioni straordinarie, che devono indicare le opere ed i progetti da

23 "277. Al fine di consentire la realizzazione e la manutenzione di opere pubbliche negli enti locali che si trovano nella condizione di scioglimento ai sensi dell'articolo 143 del testo unico di cui al decreto legislativo 18 agosto 2000, n. 267, nello stato di previsione del Ministero dell'interno è istituito un fondo con una dotazione iniziale di 5 milioni di euro annui a decorrere dall'anno 2018. Con decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, sono definiti i criteri e le modalità di riparto del fondo, attribuendo priorità agli enti con popolazione residente fino a 15.000 abitanti. Ai relativi oneri si provvede mediante corrispondente utilizzo delle risorse del Fondo ordinario per il finanziamento dei bilanci degli enti locali iscritto nello stato di previsione del Ministero dell'interno, stanziato ai sensi dell'articolo 1-bis del decreto-legge 25 novembre 1996, n. 599, convertito, con modificazioni, dalla legge 24 gennaio 1997, n. 5.

278. La dotazione del fondo di cui al comma 277 è annualmente incrementata con le risorse non utilizzate in ciascun anno, rivenienti dal medesimo Fondo ordinario per il finanziamento dei bilanci degli enti locali ai sensi dell'articolo 1-bis del decreto-legge 25 novembre 1996, n. 599, convertito, con modificazioni, dalla legge 24 gennaio 1997, n. 5, le quali sono versate all'entrata del bilancio dello Stato per essere riassegnate al fondo di cui al comma 277. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio".

realizzare in coerenza con le priorità individuate ai sensi dell'art. 145, comma 2 del T.U.E.L.²⁴. Tale previsione assicura che l'utilizzo delle risorse sia funzionale agli obiettivi di risanamento e non costituisca un mero sostegno finanziario indifferenziato.

Accanto al sostegno finanziario cd diretto, l'ordinamento prevede specifici strumenti per il potenziamento delle risorse umane a disposizione delle commissioni straordinarie, nella consapevolezza che il successo delle operazioni di risanamento dipende anche dalla disponibilità di personale qualificato ed affidabile.

L'art. 145 del T.U.E.L. prevede infatti la possibilità di assegnare alle commissioni straordinarie, in posizione di sovra-ordinazione, personale amministrativo e/o tecnico con comprovata esperienza e professionalità²⁵. Tale strumento si è rivelato particolarmente utile per sopperire alla carenza di organico che caratterizza molti enti commissariati e per garantire la presenza di figure professionali adeguate nei settori più esposti a rischi di condizionamento mafioso, anche a fronte del fatto che spesso i componenti delle commissioni medesime sono privi di specifiche competenze in ambito economico, finanziario e contabile. Il personale assegnato in posizione di sovra-ordinazione viene impiegato prioritariamente nei settori più critici quali l'urbanistica, l'edilizia, i lavori pubblici, i settori economico-finanziari e la polizia municipale, in quanto aree particolarmente complesse e altresì permeabili ai condizionamenti criminali. La scelta delle figure da assegnare avviene previa approfondita istruttoria curata dalle Prefetture-U.T.G. territorialmente competenti con il contributo delle Forze di polizia, al precipuo fine di verificare i requisiti di idoneità morale e professionale

24 *"Per far fronte a situazioni di gravi disservizi e per avviare la sollecita realizzazione di opere pubbliche indifferibili, la commissione straordinaria di cui al comma 1 dell'articolo 144, entro il termine di sessanta giorni dall'insediamento, adotta un piano di priorità degli interventi, anche con riferimento a progetti già approvati e non eseguiti. Gli atti relativi devono essere nuovamente approvati dalla commissione straordinaria. La relativa deliberazione, esecutiva a norma di legge, è inviata entro dieci giorni al prefetto il quale, sentito il comitato provinciale della pubblica amministrazione opportunamente integrato con i rappresentanti di uffici tecnici delle amministrazioni statali, regionali o locali, trasmette gli atti all'amministrazione regionale territorialmente competente per il tramite del commissario del Governo, o alla Cassa depositi e prestiti, che provvedono alla dichiarazione di priorità di accesso ai contributi e finanziamenti a carico degli stanziamenti comunque destinati agli investimenti degli enti locali. Le disposizioni del presente comma si applicano ai predetti enti anche in deroga alla disciplina sugli enti locali disestati, limitatamente agli importi totalmente ammortizzabili con contributi statali o regionali ad essi effettivamente assegnati".*

25 Sui trasferimenti di personale nella P.A., anche se datato, si veda: CANAUZ M., *La pubblica amministrazione in Italia tra organizzazione e gestione del personale*, in *Economia Aziendale*, n. 4/2008, pp. 27-109.

dei soggetti individuati. Il sostegno in termini di risorse umane comporta oneri a carico dello Stato, che provvede al rimborso perequativo ai datori di lavoro diversi dalle amministrazioni pubbliche centrali o periferiche; tale meccanismo di finanziamento assicura che il potenziamento degli organici non gravi sui bilanci degli enti commissariati, spesso già caratterizzati da situazioni di grave squilibrio finanziario.

5. Le strategie di risanamento finanziario

L'analisi delle strategie ipotizzabili (ed anche effettivamente poste in essere) per risanare le finanze degli enti sciolti per infiltrazioni e condizionamenti della criminalità organizzata evidenzia la necessità di un approccio sistematico articolato su più direttrici di intervento, necessariamente coordinate ed integrate tra loro.

Il contrasto all'evasione tributaria rappresenta una priorità assoluta: secondo gli ultimi dati disponibili²⁶, il 100% delle gestioni commissariali ha dovuto porre in essere specifiche iniziative in tal senso. Gli interventi adottati si sono altresì caratterizzati per l'utilizzo di tecnologie informatiche avanzate e per l'implementazione dei sistemi di controllo incrociato²⁷, che consentono di individuare situazioni di irregolarità precedentemente non emerse. Specifici *software* consentono infatti di effettuare controlli incrociati tra diverse banche dati (anagrafe tributaria, catasto, registri camerali, ecc.) per facilitare l'individuazione del cd sommerso fiscale²⁸.

Il recupero dei crediti pregressi costituisce un altro pilastro delle strategie di incremento delle entrate. È infatti necessario procedere sistematicamente alla ricognizione delle posizioni debitorie arretrate e all'emissione degli atti di accertamento e delle relative notifiche di pagamento. Dove necessario e possibile, va considerata la possibilità dell'incremento delle aliquote tributarie fino ai limiti massimi consentiti dalla legge, con particolare riferimento all'IMU e alla TARI. Tale

26 Di cui alla già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

27 In materia: CROVATO F., *Ias e controlli fiscali*, Milano, 2011, pp. 449-456; e più aggiornato: TRITTO N. M., *Manuale superiore di diritto tributario*, Roma, 2024.

28 Per un'analisi della fattispecie: CHIARINI B. – MARZANO E., *Evasione fiscale e sommerso economico in Italia: fatti stilizzati, differenze tra periodi e puzzles*, in *Moneta e Credito*, n. 239/2007.

intervento, pur comportando un aggravio del carico fiscale per i cittadini, si rende spesso indispensabile per assicurare la sostenibilità finanziaria dell'ente interessato da fenomeni di infiltrazione criminale nel medio-lungo periodo.

Anche l'affidamento dei servizi di riscossione a società esterne specializzate rappresenta una strategia sempre più diffusa. Tale scelta consentirebbe di superare le inefficienze dell'apparato interno, spesso compromesso da situazioni di collusione o comunque di inadeguatezza professionale, affidando le attività di recupero crediti a soggetti (teoricamente) dotati di competenze tecniche specifiche e di strumenti operativi più efficaci²⁹.

Sul versante delle uscite, va rilevato come gran parte degli enti commissariati abbia adottato iniziative volte ad una tendenziale razionalizzazione della spesa³⁰, dimostrando l'approccio sistematico delle commissioni rispetto all'obiettivo del risanamento finanziario. In effetti, la riorganizzazione del settore economico-finanziario costituisce spesso il primo intervento adottato, nella consapevolezza che l'efficacia di ogni strategia di risanamento dipenda dalla disponibilità di strutture amministrative adeguate ed allo stesso tempo affidabili. Gli interventi di riorganizzazione, comunque, riguardano di solito differenti aspetti della macchina burocratica degli enti locali: la ridefinizione delle competenze e delle responsabilità, l'implementazione di nuove procedure di controllo, l'aggiornamento dei sistemi informatici di gestione, la formazione del personale e così via.

Il rispetto dei tempi di pagamento previsti dalla normativa sui debiti commerciali costituisce un obiettivo prioritario, sia per evitare l'aggravio di interessi e sanzioni sia per ripristinare la credibilità dell'ente nei rapporti con i fornitori³¹.

29 In tal senso: CHIPARO G. M., *La riscossione comunale: fonti e modelli, atti della riscossione, termini e notificazioni, misure cautelari ed esecuzione forzata*, Milano, 2024.

30 Si veda la precedente nota n. 25.

31 La verifica del rispetto degli obblighi normativi in tema di fondo garanzia debiti commerciali e di tempestività dei pagamenti, introdotti dall'art. 1, commi 859 e ss. della legge 30 dicembre 2018, n. 145 (cd legge di bilancio 2019), riveste un ruolo centrale nell'ambito dei controlli sugli enti locali, anche in ragione della circostanza che la riduzione dei tempi di pagamento delle Pubbliche Amministrazioni si pone tra le riforme abilitanti del Piano nazionale di ripresa e resilienza che l'Italia si è impegnata a realizzare (Riforma n. 1.11 - Riduzione dei tempi di pagamento delle pubbliche amministrazioni e delle autorità sanitarie). A riguardo, si rappresenta che il comma 2 dell'art. 4-bis del decreto-legge 24 febbraio 2023, n. 13, convertito, con modificazioni, dalla legge 21 aprile 2023, n. 41 prevede: «*Le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decre-*

La definizione agevolata delle posizioni debitorie dell'ente nei confronti dell'erario e di altri soggetti creditori rappresenta uno strumento importante per ridurre l'esposizione finanziaria complessiva e per "liberare" risorse da destinare ad interventi prioritari.

Nei casi di più grave compromissione degli equilibri di bilancio, è possibile il ricorso agli strumenti previsti dagli artt. 243 e seguenti

to legislativo 30 marzo 2001, n. 165, nell'ambito dei sistemi di valutazione della performance previsti dai rispettivi ordinamenti, provvedono ad assegnare, integrando i rispettivi contratti individuali, ai dirigenti responsabili dei pagamenti delle fatture commerciali nonché ai dirigenti apicali delle rispettive strutture specifici obiettivi annuali relativi al rispetto dei tempi di pagamento previsti dalle vigenti disposizioni e valutati, ai fini del riconoscimento della retribuzione di risultato, in misura non inferiore al 30 per cento. Ai fini dell'individuazione degli obiettivi annuali, si fa riferimento all'indicatore di ritardo annuale di cui all'articolo 1, commi 859, lettera b), e 861, della legge 30 dicembre 2018, n. 145. La verifica del raggiungimento degli obiettivi relativi al rispetto dei tempi di pagamento è effettuata dal competente organo di controllo di regolarità amministrativa e contabile sulla base degli indicatori elaborati mediante la piattaforma elettronica per la gestione telematica del rilascio delle certificazioni di cui all'articolo 7, comma 1, del decreto-legge 8 aprile 2013, n. 35, convertito, con modificazioni, dalla legge 6 giugno 2013, n. 64». Con riferimento al fondo di garanzia debiti commerciali, esso ha la funzione di «sopperire alla incapacità dell'ente di coordinare l'assunzione di obbligazioni (legittimamente iscritte in bilancio) con la effettiva disponibilità della liquidità necessaria al loro pagamento alle scadenze di legge» (cfr. Corte costituzionale, sentenza n. 78/2020). L'articolo 1, comma 859 della citata legge n. 145/2018 prevede infatti che «a partire dall'anno 2021, le amministrazioni pubbliche, diverse dalle amministrazioni dello Stato e dagli enti del Servizio sanitario nazionale, di cui all'articolo 1, comma 2, della legge 31 dicembre 2009, n. 196, applicano: a) le misure di cui alla lettera a) dei commi 862 ..., se il debito commerciale residuo, di cui all'articolo 33 del decreto legislativo 14 marzo 2013, n. 33, rilevato alla fine dell'esercizio precedente non si sia ridotto almeno del 10 per cento rispetto a quello del secondo esercizio precedente. In ogni caso le medesime misure non si applicano se il debito commerciale residuo scaduto, di cui al citato articolo 33 del decreto legislativo n. 33 del 2013, rilevato alla fine dell'esercizio precedente, non è superiore al 5 per cento del totale delle fatture ricevute nel medesimo esercizio; b) le misure di cui ai commi 862 ... se rispettano la condizione di cui alla lettera a), ma presentano un indicatore di ritardo annuale dei pagamenti, calcolato sulle fatture ricevute e scadute nell'anno precedente, non rispettoso dei termini di pagamento delle transazioni commerciali, come fissati dall'articolo 4 del decreto legislativo 9 ottobre 2022, n. 231». Le misure di cui al comma 862 consistono nello stanziamento in parte corrente di «un accantonamento denominato Fondo di garanzia debiti commerciali, sul quale non è possibile disporre impegni e pagamenti, che a fine esercizio confluisce nella quota accantonata del risultato di amministrazione, per un importo pari: a) al 5 per cento degli stanziamenti riguardanti nell'esercizio in corso la spesa per acquisto di beni e servizi, in caso di mancata riduzione del 10 per cento del debito commerciale residuo oppure per ritardi superiori a sessanta giorni, registrati nell'esercizio precedente; b) al 3 per cento degli stanziamenti riguardanti nell'esercizio in corso la spesa per acquisto di beni e servizi, per ritardi compresi tra trentuno e sessanta giorni, registrati nell'esercizio precedente; c) al 2 per cento degli stanziamenti riguardanti nell'esercizio in corso la spesa per acquisto di beni e servizi, per ritardi compresi tra undici e trenta giorni, registrati nell'esercizio precedente; d) all'1 per cento degli stanziamenti riguardanti nell'esercizio in corso la spesa per acquisto di beni e servizi, per ritardi compresi tra uno e dieci giorni, registrati nell'esercizio precedente».

del T.U.E.L.³², con particolare riferimento ai piani di riequilibrio finanziario pluriennale disciplinati dall'art. 243-bis³³.

32 Per un esame completo della disciplina dei piani di riequilibrio finanziari pluriennali, si rimanda a: TRITTO N. M., *Il piano di riequilibrio finanziario pluriennale e le modifiche (d)all'amministrazione dell'ente locale*, in *Federalismi*, n. 13/2021, pp. 258-273.

33 "1. I comuni e le province per i quali, anche in considerazione delle pronunce delle competenti sezioni regionali della Corte dei conti sui bilanci degli enti, sussistano squilibri strutturali del bilancio in grado di provocare il dissesto finanziario, nel caso in cui le misure di cui agli articoli 193 e 194 non siano sufficienti a superare le condizioni di squilibrio rilevate, possono ricorrere, con deliberazione consiliare alla procedura di riequilibrio finanziario pluriennale prevista dal presente articolo. La predetta procedura non può essere iniziata qualora sia decorso il termine assegnato dal Prefetto, con lettera notificata ai singoli consiglieri, per la deliberazione del dissesto, di cui all'articolo 6, comma 2, del decreto legislativo 6 settembre 2011, n. 149.

2. La deliberazione di ricorso alla procedura di riequilibrio finanziario pluriennale è trasmessa, entro 5 giorni dalla data di esecutività, alla competente sezione regionale della Corte dei conti e al Ministero dell'interno.

3. Il ricorso alla procedura di cui al presente articolo sospende temporaneamente la possibilità per la Corte dei conti di assegnare, ai sensi dell'articolo 6, comma 2, del decreto legislativo 6 settembre 2011, n. 149, il termine per l'adozione delle misure correttive di cui al comma 6, lettera a), del presente articolo.

4. Le procedure esecutive intraprese nei confronti dell'ente sono sospese dalla data di deliberazione di ricorso alla procedura di riequilibrio finanziario pluriennale fino alla data di approvazione o di diniego di approvazione del piano di riequilibrio pluriennale di cui all'articolo 243-quater, commi 1 e 3.

5. Il consiglio dell'ente locale, entro il termine perentorio di novanta giorni dalla data di esecutività della delibera di cui al comma 1, delibera un piano di riequilibrio finanziario pluriennale di durata compresa tra quattro e venti anni, compreso quello in corso, corredato del parere dell'organo di revisione economico-finanziario. Qualora, in caso di inizio mandato, la delibera di cui al presente comma risulti già presentata dalla precedente amministrazione, ordinaria o commissariale, e non risulti ancora intervenuta la delibera della Corte dei conti di approvazione o di diniego di cui all'articolo 243-quater, comma 3, l'amministrazione in carica ha facoltà di rimodulare il piano di riequilibrio, presentando la relativa delibera nei sessanta giorni successivi alla sottoscrizione della relazione di cui all'articolo 4-bis, comma 2, del decreto legislativo 6 settembre 2011, n. 149.

5-bis. La durata massima del piano di riequilibrio finanziario pluriennale, di cui al primo periodo del comma 5, è determinata sulla base del rapporto tra le passività da ripianare nel medesimo e l'ammontare degli impegni di cui al titolo I della spesa del rendiconto dell'anno precedente a quello di deliberazione del ricorso alla procedura di riequilibrio o dell'ultimo rendiconto approvato, secondo la seguente tabella:

Rapporto passività/impegni di cui al titolo	Durata massima del PRFP
Fino al 20 per cento	4 anni
Superiore al 20 per cento e fino al 60 per cento	10 anni
Superiore al 60 per cento e fino al 100 per cento per i comuni fino a 60.000 abitanti	15 anni
Oltre il 60% per comuni con popolaz.sup.a 60.000 ab.e oltre il 100% per tutti gli altri	20 anni

6. Il piano di riequilibrio finanziario pluriennale deve tenere conto di tutte le misure necessarie a superare le condizioni di squilibrio rilevate e deve, comunque, contenere:

a) le eventuali misure correttive adottate dall'ente locale ai sensi dell'articolo 1, comma 168, della legge 23 dicembre 2005, n. 266, in considerazione dei comportamenti difforni dalla sana gestione finanziaria e del mancato rispetto degli obiettivi posti con il patto di stabilità interno accertati dalla competente sezione regionale della Corte dei conti;

b) la puntuale ricognizione, con relativa quantificazione, dei fattori di squilibrio rilevati, dell'eventuale disavanzo di amministrazione risultante dall'ultimo rendiconto approvato e di eventuali debiti fuori bilancio;

c) l'individuazione, con relative quantificazione e previsione dell'anno di effettivo realizzo, di tutte le misure necessarie per ripristinare l'equilibrio strutturale del bilancio, per l'integrale ripiano del disavanzo di amministrazione accertato e per il finanziamento dei debiti fuori bilancio entro il periodo massimo di dieci anni, a partire da quello in corso alla data di accettazione del piano;

d) l'indicazione, per ciascuno degli anni del piano di riequilibrio, della percentuale di ripiano del disavanzo di amministrazione da assicurare e degli importi previsti o da prevedere nei bilanci annuali e pluriennali per il finanziamento dei debiti fuori bilancio.

7. Ai fini della predisposizione del piano, l'ente è tenuto ad effettuare una ricognizione di tutti i debiti fuori bilancio riconoscibili ai sensi dell'articolo 194. Per il finanziamento dei debiti fuori bilancio l'ente può provvedere anche mediante un piano di rateizzazione, della durata massima pari agli anni del piano di riequilibrio, compreso quello in corso, convenuto con i creditori.

7-bis. Al fine di pianificare la rateizzazione dei pagamenti di cui al comma 7, l'ente locale interessato può richiedere all'agente della riscossione una dilazione dei carichi affidati dalle agenzie fiscali e relativi alle annualità ricomprese nel piano di riequilibrio pluriennale dell'ente. Le rateizzazioni possono avere una durata temporale massima di dieci anni con pagamenti rateali mensili. Alle rateizzazioni concesse si applica la disciplina di cui all'articolo 19, commi 1-quater, 3 e 3-bis, del decreto del Presidente della Repubblica 29 settembre 1973, n. 602. Sono dovuti gli interessi di dilazione di cui all'articolo 21 del citato decreto del Presidente della Repubblica n. 602 del 1973.

7-ter. Le disposizioni del comma 7-bis si applicano anche ai carichi affidati dagli enti gestori di forme di previdenza e assistenza obbligatoria.

7-quater. Le modalità di applicazione delle disposizioni dei commi 7-bis e 7-ter sono definite con decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero del lavoro e delle politiche sociali, da adottare entro trenta giorni dalla data di entrata in vigore della presente disposizione.

7-quinquies. L'ente locale è tenuto a rilasciare apposita delegazione di pagamento ai sensi dell'articolo 206 quale garanzia del pagamento delle rate relative ai carichi delle agenzie fiscali e degli enti gestori di forme di previdenza e assistenza obbligatoria di cui ai commi 7-bis e 7-ter.

8. Al fine di assicurare il prefissato graduale riequilibrio finanziario, per tutto il periodo di durata del piano, l'ente:

a) può deliberare le aliquote o tariffe dei tributi locali nella misura massima consentita, anche in deroga ad eventuali limitazioni disposte dalla legislazione vigente;

b) è soggetto ai controlli centrali in materia di copertura di costo di alcuni servizi, di cui all'articolo 243, comma 2, ed è tenuto ad assicurare la copertura dei costi della gestione dei servizi a domanda individuale prevista dalla lettera a) del medesimo articolo 243, comma 2;

c) è tenuto ad assicurare, con i proventi della relativa tariffa, la copertura integrale dei costi della gestione del servizio di smaltimento dei rifiuti solidi urbani e del servizio acquedotto;

d) è soggetto al controllo sulle dotazioni organiche e sulle assunzioni di personale previsto dall'articolo 243, comma 1;

e) è tenuto ad effettuare una revisione straordinaria di tutti i residui attivi e passivi conservati in bilancio, stralciando i residui attivi inesigibili o di dubbia esigibilità da inserire nel conto del patrimonio fino al compimento dei termini di prescrizione, nonché una sistematica attività di accertamento delle posizioni debitorie aperte con il sistema creditizio e dei procedimenti di realizzazione delle opere pubbliche ad esse sottostanti ed una verifica della consistenza ed integrale ripristino dei fondi delle entrate con vincolo di destinazione;

f) è tenuto ad effettuare una rigorosa revisione della spesa con indicazione di precisi obiettivi di riduzione della stessa, nonché una verifica e relativa valutazione dei costi di tutti i servizi erogati dall'ente e della situazione di tutti gli organismi e delle società partecipati e dei relativi costi e oneri comunque a carico del bilancio dell'ente;

g) può procedere all'assunzione di mutui per la copertura di debiti fuori bilancio riferiti a spese di investimento in deroga ai limiti di cui all'articolo 204, comma 1, previsti dalla legislazione vigente, nonché accedere al Fondo di rotazione per assicurare la stabilità finanziaria degli enti locali di cui all'articolo 243-ter, a condizione che si sia avvalso della facoltà di deliberare le aliquote o tariffe nella misura massima prevista dalla lettera a), che abbia previsto l'impegno ad alienare i beni patrimoniali disponibili non indispensabili per i fini istituzionali dell'ente e che abbia provveduto alla rideterminazione della dotazione organica ai sensi dell'articolo 259, comma 6, fermo restando che la stessa non può essere variata in aumento per la durata del piano di riequilibrio.

9. In caso di accesso al Fondo di rotazione di cui all'articolo 243-ter, l'Ente deve adottare entro il termine dell'esercizio finanziario le seguenti misure di riequilibrio della parte corrente del bilancio: a) a decorrere dall'esercizio finanziario successivo, riduzione delle spese di personale, da realizzare in particolare attraverso l'eliminazione dai fondi per il finanziamento della retribuzione accessoria del personale dirigente e di quello del comparto, delle risorse di cui agli articoli 15, comma 5, e 26, comma 3, dei Contratti collettivi nazionali di lavoro del 1° aprile 1999 (comparto) e del 23 dicembre 1999 (dirigenza), per la quota non connessa all'effettivo incremento delle dotazioni organiche;

b) entro il termine di un quinquennio, riduzione almeno del 10 per cento delle spese per acquisti di beni e prestazioni di servizi di cui al macro-aggregato 03 della spesa corrente, finanziate attraverso risorse proprie. Ai fini del computo della percentuale di riduzione, dalla base di calcolo sono esclusi gli stanziamenti destinati:

1) alla copertura dei costi di gestione del servizio di smaltimento dei rifiuti solidi urbani;

2) alla copertura dei costi di gestione del servizio di acquedotto;

3) al servizio di trasporto pubblico locale;

4) al servizio di illuminazione pubblica;

5) al finanziamento delle spese relative all'accoglienza, su disposizione della competente autorità giudiziaria, di minori in strutture protette in regime di convitto e semiconvitto;

c) entro il termine di un quinquennio, riduzione almeno del 25 per cento delle spese per trasferimenti di cui al macro-aggregato 04 della spesa corrente, finanziate attraverso risorse proprie. Ai fini del computo della percentuale di riduzione, dalla base di calcolo sono escluse le somme relative a trasferimenti destinati ad altri livelli istituzionali, a enti, agenzie o fondazioni lirico-sinfoniche;

c-bis) ferma restando l'obbligatorietà delle riduzioni indicate nelle lettere b) e c), l'ente locale ha facoltà di procedere a compensazioni, in valore assoluto e mantenendo la piena equivalenza delle somme, tra importi di spesa corrente, ad eccezione della spesa per il personale e ferme restando le esclusioni di cui alle medesime lettere b) e c) del presente comma. Tali compensazioni sono puntualmente evidenziate nel piano di riequilibrio approvato;

d) blocco dell'indebitamento, fatto salvo quanto previsto dal primo periodo del comma 8, lettera g), per i soli mutui connessi alla copertura di debiti fuori bilancio pregressi.

9-bis. In deroga al comma 8, lettera g), e al comma 9, lettera d), del presente articolo e all'articolo 243-ter, i comuni che fanno ricorso alla procedura di riequilibrio finanziario pluriennale prevista dal presente articolo possono contrarre mutui, oltre i limiti di cui al comma 1 dell'articolo 204, necessari alla copertura di spese di investimento relative a progetti e interventi che garantiscano l'ottenimento di risparmi di gestione funzionali al raggiungimento degli obiettivi fissati nel piano di riequilibrio finanziario pluriennale, per un importo non superiore alle quote di capitale dei mutui e dei prestiti obbligazionari precedentemente contratti ed emessi, rimborsate nell'esercizio precedente".

Secondo gli ultimi dati disponibili³⁴, nel 2024 su un totale di n. 28 enti sciolti per infiltrazioni e condizionamenti della criminalità organizzata, n. 2 hanno adottato piani di riequilibrio finanziario pluriennale³⁵.

6. La gestione degli enti in dissesto finanziario

Una categoria particolare di enti commissariati è rappresentata da quelli che hanno già dichiarato il dissesto finanziario³⁶ prima dello scioglimento per infiltrazioni e condizionamenti della criminalità organizzata.

Anche in questo caso, secondo gli ultimi dati disponibili³⁷, nel 2024 su un totale di n. 28 enti sciolti per infiltrazioni e condizionamenti della criminalità organizzata, n. 2 già si trovavano in stato di dissesto finanziario³⁸.

Negli enti in dissesto, com'è noto, la commissione straordinaria deve operare in coordinamento con l'organo straordinario di liquidazione, che mantiene le competenze relative alla gestione del passivo ed alla liquidazione delle attività dell'ente³⁹. Tale coordinamento richiede un'attenta delimitazione delle rispettive competenze e una stretta collaborazione per assicurare la coerenza degli interventi adottati. Negli enti in dissesto finanziario, infatti, particolare importanza assume la valorizzazione del patrimonio di riferimento, che può contribuire significativamente al miglioramento della situazione finanziaria degli enti stessi; si rende pertanto necessario procedere sistematicamente alla ricognizione dei beni di proprietà dell'ente ed alla valutazione delle possibilità di dismissione e/o di diversa utilizzazione economica dei relativi cespiti.

34 Di cui alla già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

35 Si tratta dei comuni di Scilla (RC) e di Monteforte Irpino (AV).

36 Disciplinato dai capi II-V del titolo VIII della parte seconda del T.U.E.L. (artt. 244 e seguenti).

37 Di cui alla già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

38 Si tratta dei comuni di Randazzo (CT) e di Calvi Risorta (CE).

39 Sull'argomento, tra i tanti, si rimanda a: GUERRERA A. – GNOFFO S., *L'organo straordinario di liquidazione e gli organi di governo del comune consustanziali alla sana gestione: un caso di studio*, in *Azienda Pubblica*, n. 4/2022, pp. 417-445.

Un altro strumento importante per il miglioramento della situazione patrimoniale di tali enti è rappresentato dalla dismissione delle partecipazioni societarie, particolarmente rilevanti in alcuni casi (specie negli enti di maggiori dimensioni).

7. I profili di controllo e trasparenza nella gestione finanziaria

Un aspetto fondamentale dell'attività delle commissioni straordinarie negli enti locali sciolti per infiltrazioni e condizionamenti della criminalità organizzata⁴⁰ riguarda la (già accennata) riorganizzazione dei sistemi di controllo interno ed il ripristino di adeguati *standard* di trasparenza amministrativa, elementi essenziali per prevenire la riproposizione di fenomeni di infiltrazione mafiosa.

L'aggiornamento dei regolamenti di contabilità costituisce spesso uno dei primi interventi da porre in essere, nella consapevolezza che la presenza di una disciplina interna obsoleta e/o inadeguata facilita in misura rilevante la perpetrazione di irregolarità finanziarie (e non solo). L'implementazione di sistemi informatici per la gestione finanziaria rappresenta del resto un elemento chiave della strategia di modernizzazione da adottare negli enti sciolti per infiltrazioni e condizionamenti della criminalità organizzata: la digitalizzazione dei processi contabili consente infatti di aumentare significativamente il livello di controllo e di tracciabilità delle operazioni finanziarie, in tal modo creando uno "scudo" utile ad impedire l'emergere recidivante di condotte illecite.

È necessario poi porre particolare attenzione ad ulteriori interventi, tra i quali, ad esempio, il rafforzamento dei sistemi di controllo attraverso la nomina di nuovi revisori dei conti, la costituzione di uffici per i procedimenti disciplinari, l'adozione di regolamenti specifici per il controllo di gestione e così via. Anche la riorganizzazione del controllo economico-finanziario appare una misura utile, che riflette la necessità di ripristinare l'effettività dei controlli interni, spesso compromessi dalle situazioni di infiltrazione mafiosa. Un altro settore che va particolarmente curato, in quanto in esso si concentrano tradizionalmente le maggiori criticità, è quello dei contratti pubblici, che richiedono pertanto attenti interventi in ogni fase dei

⁴⁰ In materia, si veda: TRITTO N. M., *Alcune riflessioni in tema di lotta alla criminalità organizzata*, in *Rivista Giurisprudenza Penale*, n. 11/2023.

vari procedimenti di riferimento. La digitalizzazione delle procedure amministrative rappresenta uno strumento importante per aumentare il livello di trasparenza e di controllo nella gestione delle risorse pubbliche e costituisce un ulteriore elemento da privilegiare nell'ottica del risanamento degli enti sciolti per infiltrazioni e condizionamenti della criminalità organizzata. Il risanamento dell'ente, infatti, può avvenire anche attraverso la digitalizzazione delle procedure e la pubblicazione degli atti nel portale amministrazione trasparente; l'implementazione degli obblighi di trasparenza previsti dal D.Lgs. n. 33/2013 e ss.mm.ii. assume particolare rilevanza negli enti sciolti per infiltrazioni mafiose, costituendo un importante strumento di prevenzione della corruzione⁴¹.

8. Esperienze internazionali di contrasto alla corruzione sistemica negli enti locali

L'esperienza italiana nel contrasto alle infiltrazioni della criminalità organizzata negli enti locali trova interessanti elementi di confronto con analoghe esperienze internazionali di lotta alla corruzione sistemica a livello locale.

Nella realtà statunitense, ad esempio, diversi Stati hanno sviluppato legislazioni specifiche per affrontare situazioni di grave dissesto amministrativo-finanziario degli enti territoriali.

Il *Municipalities Financial Recovery Act*⁴² dello Stato della Pennsylvania, ad esempio, prevede un sistema di intervento statale articolato su più livelli, che va dal semplice monitoraggio finanziario fino alla nomina di amministratori straordinari con poteri sostitutivi. Il sistema presenta interessanti analogie con il modello italiano, pur operando in un contesto istituzionale profondamente diverso. Particolare interesse riveste l'implementazione dei cd *early warning systems* che consentono di individuare precocemente situazioni di criticità finanziaria negli enti locali. Tali sistemi si basano su indicatori quantitativi (rapporti di bilancio, andamento delle entrate tributarie, livello di indebitamento) e qualitativi (qualità dei sistemi di controllo interno, trasparenza amministrativa,

41 DELSIGNORE M. – RAMAJOLI M., *La prevenzione della corruzione e l'illusione di un'amministrazione senza macchia*, in *Rivista trimestrale di diritto pubblico*, n. 1/2019, pp. 61-77.

42 *Act of 1987*, P.L. 246, No. 47.

efficienza gestionale) che permettono di attivare tempestivamente interventi preventivi⁴³.

In altri Stati americani, come quello di New York, poi, sono presenti specifiche istituzioni (i cd *Fiscal Oversight Boards*) con competenze di supervisione finanziaria sugli enti locali che presentino situazioni di criticità. Tali organismi, composti da esperti nominati dal governo statale, esercitano funzioni di monitoraggio e controllo analoghe a quelle svolte in Italia dalle commissioni straordinarie, pur operando in un quadro di maggiore collaborazione con gli organi elettivi locali⁴⁴.

Nel Regno Unito, l'*Audit Commission* ha sviluppato nel corso degli anni un articolato sistema di controllo della gestione finanziaria degli enti locali, che include specifici protocolli per la gestione di situazioni di crisi finanziaria. Il sistema delle cd *best value inspections* prevede verifiche sistematiche della qualità dei servizi e dell'efficienza gestionale degli enti locali, con particolare attenzione agli aspetti di economicità e trasparenza. Le ispezioni possono essere attivate su base programmata o a seguito di segnalazioni specifiche, e possono condurre all'adozione di misure correttive vincolanti. In caso di gravi deficienze gestionali, il *Secretary of State* può esercitare specifici poteri che autorizzano interventi sostitutivi anche molto incisivi, fino alla nomina di commissari straordinari. Il sistema britannico presenta interessanti elementi di confronto con quello italiano, con particolare riferimento all'articolazione dei livelli di intervento e all'attenzione per gli aspetti di *performance management*⁴⁵.

In Francia, le *Chambres régionales des comptes* esercitano un controllo sistematico sulla gestione finanziaria degli enti locali, con com-

43 In effetti, "in conjunction with assessing a municipality's current fiscal stability under subsections (a) and (b) and section 201, the department shall develop an early warning system utilizing necessary fiscal and socioeconomic variables to identify municipal financial emergencies before they reach crisis proportions and to notify an affected municipality appropriately. The department shall be responsible for testing the validity and reliability of these variables and shall continuously monitor them to assure their effectiveness. In developing an early warning system, the department may employ or contract with municipal fiscal consultants as deemed necessary to execute the provisions of this subsection. Notice shall be published in the Pennsylvania Bulletin that the early warning system has been developed and the system may not become operational until the publication of the notice" (section 121, lett. f del *Municipalities Financial Recovery Act*).

44 Per un esame approfondito del funzionamento di tali istituzioni si rimanda al recente: LÓPEZ-SANTANA M., *Financial oversight boards in the US Federal System: Insights from the Puerto Rican debt crisis*, in *The Journal of Federalism*, n. 2/2023, pp. 201-226.

45 Per un esame approfondito del sistema britannico si rimanda a: TRITTO N. M., *Le crisi finanziarie degli enti locali tra discipline ad hoc e disposizioni generali: un'analisi comparatistica*, in *Rivista della Corte dei conti*, n. 5/2023, pp. 45-53.

petenze specifiche in materia di prevenzione e contrasto del dissesto finanziario⁴⁶. Il sistema francese prevede una specifica *procédure d'alerte* che consente alle *Chambres* di attivare procedimenti di verifica straordinaria quando sussistano elementi indicatori di gravi irregolarità gestionali e tale procedura può anche condurre all'adozione di misure correttive vincolanti⁴⁷. Il confronto con il sistema francese evidenzia alcune interessanti convergenze nell'approccio al contrasto del "dissesto amministrativo-finanziario" degli enti locali, particolarmente per quanto riguarda l'attenzione agli aspetti preventivi e l'integrazione tra controlli di legalità e controlli di gestione.

In Germania, il sistema dei cd *Kommunalaufsicht* (controlli comunali) prevede forme articolate di supervisione statale sugli enti locali, con particolare attenzione agli aspetti di sostenibilità finanziaria e di legalità amministrativa. Il sistema tedesco prevede l'adozione di cd *Haushaltssicherungskonzepte* (piani di risanamento finanziario) quando sussistano situazioni di squilibrio di bilancio, con meccanismi di controllo e monitoraggio che presentano interessanti analogie con i piani di riequilibrio previsti dall'ordinamento italiano. L'esperienza tedesca si caratterizza per una particolare attenzione agli aspetti preventivi del controllo finanziario, con l'implementazione di sistemi di monitoraggio continuo che consentono di individuare precocemente situazioni di criticità e di attivare tempestivamente gli interventi correttivi necessari⁴⁸.

9. L'efficacia degli interventi di risanamento: indicatori e risultati

Tornando all'ordinamento italiano, va rilevato come la valutazione dell'efficacia economico-finanziaria degli interventi di risanamento posti in essere nell'ambito degli enti sciolti per infiltrazioni e condizionamenti della criminalità organizzata richieda l'adozione di specifici indicatori di *performance* che consentano di misurare oggettivamente i risultati conseguiti.

46 BENOIT O., *Les Chambres régionales des comptes face aux élus locaux*, in *Revue française de science politique*, n. 4/2003, pp. 535-558.

47 Per l'esame di casi specifici si rimanda a: *Chambre régionale des comptes Grand Est, Rapport d'activité 2022*, p. 23, reperibile in: https://www.ccomptes.fr/system/files/2023-05/2023.04.24_Rapport_activite_2022_CRC_GE_web.pdf.

48 Per un esame approfondito del sistema tedesco si rimanda a: KUHLMANN S. – PROELLER I. – SCHIMANKE D. – ZIEKOW J., *Public Administration in Germany*, Birmingham, 2022.

Il tasso di riscossione delle entrate tributarie costituisce uno degli indicatori più significativi dell'efficacia delle politiche di risanamento adottate; l'analisi dei dati disponibili evidenzia incrementi significativi della capacità di riscossione nella quasi totalità degli enti commissariati, con particolare riferimento all'IMU e alla TARI⁴⁹.

Il tempo medio di pagamento dei debiti commerciali rappresenta un altro indicatore importante della capacità gestionale dell'ente; la riduzione di tale indicatore, oltre a comportare risparmi diretti in termini di interessi e sanzioni, contribuisce al miglioramento della reputazione creditizia dell'ente e facilita i rapporti con i fornitori⁵⁰.

Il raggiungimento e mantenimento dell'equilibrio di bilancio costituisce l'obiettivo finale di ogni seria e duratura strategia di risanamento finanziario: l'analisi dei dati disponibili evidenzia che la quasi totalità degli enti commissariati appare in grado di conseguire l'equilibrio di bilancio entro il periodo di durata della gestione commissariale, sebbene spesso attraverso misure di contenimento della spesa e di incremento delle entrate particolarmente rigorose⁵¹.

Accanto agli indicatori prettamente contabili, la valutazione dell'efficacia degli interventi di risanamento finanziario deve considerare anche indicatori di qualità della gestione che riflettano il miglioramento dei processi amministrativi e del livello di servizio offerto alla cittadinanza.

Il grado di digitalizzazione dei processi amministrativi costituisce un indicatore importante della modernizzazione dell'apparato burocratico degli enti locali (e non solo)⁵²; l'implementazione di sistemi informatici avanzati, oltre a migliorare l'efficienza gestionale, contribuisce significativamente all'aumento della trasparenza e alla riduzione dei margini di discrezionalità, la cui eccessiva dilatazione, *a contrario*, determina l'insorgere di pericolosi pertugi dai qua-

49 Ciò secondo i dati di cui alla già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

50 A tale riguardo si rimanda alla precedente nota n. 30.

51 Ciò secondo i dati di cui alla già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

52 In materia, si veda: ORTIZ-RODRÍGUEZ F. – TIWARI S. – SICILIA M. – NIKIFOROVA A., *Electronic Governance with Emerging Technologies*, Londra, 2022, pp. 144 e 160.

li spesso la criminalità organizzata riesce a infiltrarsi nell'apparato amministrativo dell'ente locale.

Il miglioramento della qualità dei servizi pubblici rappresenta pertanto uno degli obiettivi primari da perseguire, riservando particolare attenzione al ripristino di *standard* adeguati nell'erogazione dei servizi essenziali alla cittadinanza (si pensi ai settori socio-assistenziali, scolastici e socio-culturali, ambiti nei quali possono realizzarsi significativi interventi anche per sostenere le fasce più deboli della popolazione).

Per quanto riguarda l'incremento delle entrate, come si è già evidenziato in precedenza, tutte le commissioni hanno avviato iniziative di contrasto all'evasione tributaria, conseguendo risultati in termini di recupero crediti e di incremento della base imponibile. L'utilizzo di tecnologie informatiche avanzate può migliorare notevolmente l'efficacia dei controlli fiscali e consentire altresì di individuare situazioni di evasione precedentemente non emerse.

10. Le criticità emergenti e le prospettive di sviluppo

Nonostante i risultati generalmente positivi conseguiti dalle commissioni straordinarie, l'analisi delle gestioni commissariali degli enti locali sciolti per infiltrazioni e condizionamenti della criminalità organizzata evidenzia alcune criticità strutturali che richiedono specifiche misure di intervento per essere superate.

La carenza di personale qualificato rappresenta una delle principali criticità di cui si è detto, particolarmente grave negli enti di minori dimensioni; tale carenza riflette sia l'oggettiva difficoltà di reperire figure professionali adeguate in contesti territoriali spesso caratterizzati da limitata attrattività economica sia la necessità di sostituire personale coinvolto in situazioni di collusione o comunque di inadeguatezza professionale.

Un'altra criticità ricorrente è rappresentata dalla resistenza al cambiamento manifestata da parte del personale e, in alcuni casi, della stessa cittadinanza. L'analisi delle relazioni commissariali evidenzia come circa il 18% dei dipendenti degli enti commissariati abbia mostrato atteggiamenti di diffidenza o scarsa collaborazione nei confronti delle commissioni⁵³.

⁵³ Ciò secondo i dati di cui alla già citata relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo ma-

La sostenibilità finanziaria nel lungo periodo rappresenta poi una sfida particolarmente complessa per gli enti che presentino gravi squilibri strutturali. Sebbene le commissioni straordinarie riescano generalmente a ripristinare l'equilibrio di bilancio nel breve periodo, la sostenibilità di tale equilibrio dipende poi dalla capacità degli organi elettivi successivamente insediatisi di mantenere *standard* gestionali accettabili.

L'esperienza maturata suggerisce alcune prospettive di evoluzione normativa che potrebbero contribuire a migliorare ulteriormente l'efficacia degli interventi di risanamento.

Un primo ambito di possibile sviluppo riguarda il rafforzamento degli strumenti preventivi di individuazione e contrasto delle situazioni di infiltrazione mafiosa negli enti locali. L'implementazione di sistemi di monitoraggio continuo, analoghi agli *early warning systems* dell'esperienza statunitense (e non solo), potrebbe consentire di intervenire precocemente sulle situazioni di criticità, riducendo la necessità di ricorrere alla misura drastica dello scioglimento.

Un secondo ambito di sviluppo concerne l'integrazione con gli strumenti di programmazione europea, particolarmente rilevante nell'attuale fase di implementazione del Piano Nazionale di Ripresa e Resilienza. L'esperienza ha evidenziato come le risorse di cui al P.N.R.R. possano costituire un'importante leva per il risanamento degli enti commissariati, ma anche la necessità di specifici protocolli per assicurare il corretto utilizzo di tali risorse⁵⁴.

Un terzo ambito di sviluppo riguarda il potenziamento della cooperazione interistituzionale tra i diversi soggetti coinvolti nelle operazioni di risanamento.

Dal punto di vista della ricerca e dello sviluppo, l'analisi delle gestioni commissariali apre interessanti prospettive di approfondimento che potrebbero contribuire al miglioramento dell'efficacia degli interventi futuri.

Un primo ambito di ricerca concerne lo sviluppo di modelli predittivi che consentano di individuare precocemente gli enti locali a maggior rischio di infiltrazione mafiosa, sulla base di indicatori finanziari, amministrativi e territoriali. L'applicazione di tecniche di

fioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno (doc. LXXXVIII n. 3).

⁵⁴ Per un'analisi del P.N.R.R. nel contesto giuridico-economico italiano, si veda: TRITTO N. M., *Contabilità pubblica, scienza delle finanze e diritto finanziario*, Roma, 2023, p. 28 ss.

intelligenza artificiale (quali quelle del cd *machine learning* e dei cd *data analytics*) ai dati amministrativi potrebbe consentire di sviluppare strumenti di allerta precoce particolarmente efficaci⁵⁵.

Un secondo ambito di ricerca riguarda l'analisi dell'efficacia nel lungo periodo degli interventi di risanamento, attraverso studi che seguano l'evoluzione degli enti commissariati nei periodi successivi alla conclusione della gestione straordinaria; tale tipo di analisi potrebbe fornire importanti indicazioni per il miglioramento delle strategie di intervento e per l'identificazione dei fattori critici di successo.

Un terzo ambito di ricerca concerne l'analisi comparata dei modelli internazionali di contrasto alla corruzione sistemica negli enti locali, al fine di identificare *best practices* trasferibili nel contesto italiano; il confronto con le esperienze di altri ordinamenti potrebbe suggerire interessanti spunti per l'evoluzione del sistema italiano di prevenzione e contrasto delle infiltrazioni della criminalità organizzata negli enti locali (e non solo)⁵⁶.

11. Considerazioni conclusive

L'analisi delle gestioni straordinarie degli enti sciolti per infiltrazioni mafiose conferma la natura sistemica del rapporto tra condizionamento mafioso e dissesto finanziario negli enti locali. I dati esaminati evidenziano come il deterioramento delle condizioni economico-finanziarie non costituisca un mero sintomo collaterale dell'infiltrazione criminale, ma rappresenti spesso uno degli strumenti attraverso cui tale infiltrazione si realizza e si perpetua.

L'esperienza dimostra l'efficacia di un approccio integrato che coniughi interventi di ripristino della legalità con strategie articolate di risanamento finanziario: i risultati conseguiti in termini di incremento delle entrate tributarie e di razionalizzazione della spesa

55 "I sistemi di intelligenza artificiale ... "racchiudono" differenti realtà, genericamente individuate con il termine di I.A. (si pensi, ad esempio, al cd *machine learning*, al cd *deep learning*, alla cd *predictive analytics*, al cd *data mining*, alla cd *blockchain*, alla *robotica*, ecc.). Per intelligenza artificiale, dunque, possono sinteticamente intendersi tutti quei sistemi e/o procedimenti e/o software che "simulano" l'intelligenza umana, al fine sostanzialmente di porre in essere un dato compito (con risparmio di tempo e maggiore precisione rispetto a quanto potrebbe fare un essere umano)": cfr. TRITTO N. M., *Il danno erariale da intelligenza artificiale*, in *Federalismi*, n. 7/2024, pp. 281-299.

56 Si veda a riguardo: TRITTO N. M., *Le crisi finanziarie degli enti locali tra discipline ad hoc e disposizioni generali: un'analisi comparatistica*, in *Rivista della Corte dei conti*, n. 5/2023, pp. 45-53.

confermano infatti la validità del modello di intervento sviluppato dall'ordinamento italiano.

La dimensione finanziaria delle gestioni straordinarie emerge come elemento centrale per la valutazione dell'efficacia dell'istituto dello scioglimento degli enti per infiltrazioni della criminalità organizzata. Il successo degli interventi di risanamento dipende infatti dalla capacità di ricostruire equilibri economico-finanziari sostenibili, senza i quali risulta impossibile assicurare il regolare funzionamento dei servizi pubblici essenziali e mantenere la fiducia della cittadinanza nelle istituzioni democratiche.

L'analisi ha evidenziato altresì l'importanza strategica degli strumenti di sostegno predisposti dal legislatore, particolarmente il fondo per gli investimenti degli enti sciolti per infiltrazioni mafiose e la possibilità di assegnare personale in posizione di sovra-ordinazione; tali strumenti si configurano quali elementi essenziali per il successo delle operazioni di risanamento *tout court*, consentendo alle apposite commissioni di disporre delle risorse finanziarie ed umane necessarie per gli interventi più urgenti e strutturali.

Nonostante i risultati positivi evidenziati dall'analisi, permangono sfide significative per il futuro del sistema di contrasto alle infiltrazioni mafiose negli enti locali. La carenza di personale qualificato, la resistenza al cambiamento in alcuni contesti territoriali, la necessità di assicurare la sostenibilità finanziaria nel lungo periodo rappresentano altrettante criticità che richiedono specifiche strategie di intervento.

Dal punto di vista pratico, l'esperienza italiana fornisce evidenze empiriche sui meccanismi attraverso cui la corruzione sistemica influenza la gestione finanziaria degli enti locali e sulle strategie più efficaci per contrastarla. L'esperienza italiana presenta altresì elementi di particolare rilevanza per il dibattito internazionale sul contrasto alla corruzione negli enti locali, offrendo un modello di intervento che integra strumenti di prevenzione amministrativa con misure di risanamento finanziario. Il confronto con esperienze analoghe in altri ordinamenti evidenzia infatti alcune specificità del modello italiano, ma anche interessanti convergenze nell'approccio al contrasto del "dissesto amministrativo-finanziario".

Sulla base dell'analisi condotta, appaiono sicuramente necessari interventi tendenti al potenziamento degli strumenti preventivi (con l'implementazione di sistemi di monitoraggio continuo che consentano di individuare precocemente situazioni di criticità), al rafforzamento della formazione (con lo sviluppo di programmi di formazione speciali-

stica per il personale delle commissioni straordinarie e per i funzionari degli enti a rischio), all'integrazione con la programmazione europea (con la definizione di protocolli specifici per l'utilizzo delle risorse europee negli enti commissariati), allo sviluppo della cooperazione interistituzionale (con il rafforzamento della collaborazione tra i diversi soggetti istituzionali coinvolti nelle operazioni di risanamento), all'implementazione di sistemi di valutazione (con lo sviluppo di indicatori standardizzati per la valutazione dell'efficacia degli interventi di risanamento).

La sfida per il futuro consiste nel far evolvere il sistema verso forme di intervento sempre più efficaci e tempestive, che consentano di prevenire la degenerazione delle situazioni di criticità e che assicurino la sostenibilità nel lungo periodo dei risultati conseguiti.

Un ambito di particolare interesse per il futuro è rappresentato dall'applicazione di tecnologie di intelligenza artificiale per l'individuazione precoce di situazioni a rischio di infiltrazione mafiosa. L'utilizzo di algoritmi predittivi basati sull'analisi dei bilanci comunali potrebbe consentire di sviluppare sistemi di allerta precoce particolarmente efficaci⁵⁷ ed in tale contesto potrebbe ipotizzarsi un maggiore coinvolgimento delle Sezioni regionali di controllo della Corte dei conti. Le anomalie nelle serie storiche delle entrate tributarie, i *pattern* irregolari nella gestione della spesa pubblica, le correlazioni statistiche tra indicatori finanziari e presenza di criminalità organizzata sul territorio rappresentano altrettante variabili che potrebbero essere integrate in modelli predittivi sofisticati; i sistemi di controllo automatizzati non dovrebbero sostituire ma integrare i tradizionali strumenti di vigilanza, fornendo agli organi di controllo elementi di valutazione aggiuntivi e supportando l'allocazione ottimale delle risorse ispettive e di indagine sulla base del rischio effettivo.

La sostenibilità nel lungo periodo dei risultati conseguiti dalle commissioni straordinarie rappresenta una delle sfide più complesse per il successo dell'istituto dello scioglimento degli enti locali; l'esperienza dimostra come il semplice ripristino dell'equilibrio finanziario durante la gestione commissariale non garantisca automaticamente il mantenimento di tale equilibrio successivamente al ripristino degli organi elettivi; i fattori di rischio recidivante di situazioni di infiltrazione mafiosa inclu-

⁵⁷ A riguardo si evidenzia come la Banca d'Italia, attraverso l'Unità di Informazione Finanziaria (UIF), abbia recentemente pubblicato uno studio che utilizza tecniche di *machine learning* per analizzare i dati finanziari e identificare *pattern* statistici associati al rischio di infiltrazione criminale: cfr. *Un modello di machine learning per l'identificazione di aziende collegate alla criminalità organizzata in Italia*, in *Quaderni dell'antiriciclaggio*, n. 22/2024.

dono infatti la persistenza delle condizioni ambientali che hanno favorito l'infiltrazione originaria, la mancanza di un ricambio effettivo della classe dirigente locale, la debolezza del tessuto economico e sociale, la presenza ancora attiva di organizzazioni criminali sul territorio⁵⁸.

Le strategie di consolidamento degli effetti positivi ottenuti nei contesti degli enti infiltrati dalla criminalità organizzata richiedono pertanto un approccio sistemico che vada oltre il semplice ripristino dell'equilibrio finanziario: la formazione del personale, il rafforzamento delle competenze tecnico-specialistiche, l'implementazione di sistemi di controllo permanenti, la promozione della partecipazione civica rappresentano altrettanti elementi essenziali per assicurare la sostenibilità dei risultati ottenuti.

L'innovazione tecnologica⁵⁹, come si è già visto, rappresenta uno strumento fondamentale per il miglioramento della trasparenza e dell'efficienza nella gestione degli enti locali. L'esperienza evidenzia l'importanza strategica della digitalizzazione dei procedimenti amministrativi per prevenire la riproposizione di fenomeni di corruzione ed infiltrazione mafiosa. L'implementazione di piattaforme digitali per l'erogazione dei servizi ai cittadini contribuisce significativamente alla riduzione dei margini di discrezionalità e all'aumento della tracciabilità delle operazioni. L'adozione di sistemi di *business intelligence* per l'analisi dei dati amministrativi e finanziari consente di individuare anomalie ed irregolarità in tempi significativamente più rapidi rispetto ai metodi tradizionali; tali sistemi, basati sull'analisi automatizzata di grandi volumi di dati, potrebbero essere estesi anche agli enti non commissariati come strumento di prevenzione.

Del resto, la dimensione europea del contrasto alle infiltrazioni mafiose negli enti locali assume crescente importanza, sia per l'utilizzo di fondi europei sia per lo scambio di *best practices* con altri Stati membri

58 Il caso del Comune di Caivano (NA) è particolarmente emblematico: nonostante l'impegno della commissione straordinaria, la presenza ancora attiva di organizzazioni malavittose ha ostacolato l'attività di risanamento, come attestano "*i numerosi episodi criminali verificatisi nel corso della gestione commissariale*". Tale situazione ha reso necessaria la proroga della gestione commissariale di ulteriori sei mesi (relazione sull'attività svolta dalle commissioni per la gestione straordinaria degli enti sciolti per infiltrazione e condizionamenti di tipo mafioso, trasmessa alla Presidenza della Camera dei deputati in data 16 luglio 2025 dal Ministero dell'Interno, doc. LXXXVIII n. 3).

59 In materia, si veda: TRITTO N. M., *La Pubblica Amministrazione italiana e la nuova frontiera tecnologica: intelligenza artificiale ed efficienza gestionale dei sistemi pubblici nazionali*, in *LexItalia*, n. 4/2024.

dell'Unione europea. Lo scambio di esperienze con altri ordinamenti che affrontano problemi analoghi di corruzione sistemica negli enti locali potrebbe infatti fornire spunti utili per il miglioramento del sistema italiano. La partecipazione a *network* europei dedicati al contrasto della corruzione e l'implementazione di progetti di cooperazione transnazionale rappresenterebbero pertanto direzioni di sviluppo promettenti⁶⁰.

La sfida per il futuro del sistema di contrasto alle infiltrazioni mafiose negli enti locali consiste nel far evolvere l'istituto dello scioglimento degli enti adeguandolo alle nuove forme assunte dalla criminalità organizzata ed alle trasformazioni del contesto sociale ed economico di riferimento⁶¹.

Il valore simbolico dell'istituto, che rappresenta infatti la risposta democratica dello Stato alle derive invasive della criminalità organizzata, trascende la relativa dimensione tecnico-giuridica per assumere il significato più profondo di affermazione dei valori costituzionali di legalità e di giustizia sociale. In tale prospettiva, in effetti, ogni singola gestione commissariale, con i suoi successi e le sue criticità, contribuisce alla costruzione di un patrimonio di esperienza e competenza che rappresenta una risorsa strategica per l'intero sistema democratico del Paese, caratterizzato sempre dall'affermazione della legalità in un'ottica di proporzionalità degli interventi.

60 Per le più recenti iniziative in materia di lotta alla corruzione transnazionale si rimanda a: TRITTO N. M., *Novità e proposte in tema di repressione della corruzione transnazionale*, in *Rivista Penale*, n. 10/2023, pp. 885-895.

61 In sintesi è necessario un potenziamento del sistema di monitoraggio (con l'implementazione di indicatori standardizzati per la valutazione dell'efficacia degli interventi e per l'individuazione precoce di situazioni a rischio di ricaduta), il rafforzamento della formazione specialistica (con lo sviluppo di programmi formativi specifici per i commissari straordinari e per il personale di supporto, con particolare attenzione agli aspetti finanziari e gestionali), il miglioramento della comunicazione istituzionale (con il potenziamento degli strumenti di comunicazione con la cittadinanza per favorire la comprensione del valore delle operazioni di risanamento e la partecipazione civica), lo sviluppo di sistemi predittivi (con investimenti nella ricerca e sviluppo di sistemi basati su intelligenza artificiale per l'individuazione precoce di situazioni a rischio di infiltrazione mafiosa), l'integrazione con la programmazione europea (con la definizione di protocolli specifici per l'utilizzo delle risorse europee negli enti commissariati e sviluppo di progetti di cooperazione transnazionale), il rafforzamento del sostegno *post*-commissariale (con l'implementazione di programmi di accompagnamento e monitoraggio degli enti nei primi anni successivi alla conclusione della gestione straordinaria), la valutazione di possibili modifiche legislative per rafforzare le garanzie procedimentali e migliorare l'efficacia preventiva dell'istituto, lo sviluppo di un approccio sistemico che integri l'istituto dello scioglimento con altri strumenti di prevenzione e contrasto della criminalità organizzata e la cooperazione con altri Stati per il contrasto della corruzione sistemica negli enti locali.

