RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0259 • articolo sottoposto a peer review • pubblicato in anteprima il 13 gen. 2026

Benedetto Ponti

Trattamento dei dati personali e standard di legalità: elementi di preminenza delle esigenze di circolazione?

Muovendo dai caratteri del meta-principio della finalità del trattamento e dalla clausola di necessarietà, il saggio mostra come il GDPR costruisca uno standard di legalità "funzionale", anche con riferimento ai trattamenti finalizzati all'esecuzione di un compito di interesse pubblico. In ragione del margine di manovra aperto, in materia, dallo stesso GDPR, l'ordinamento italiano è stato invece caratterizzato inizialmente da una disciplina ispirata ad uno *strict legality standard* (che richiedeva una predeterminazione legislativa analitica di dati, operazioni e finalità), per poi allinearsi alla legalità funzionale, in ragione delle modifiche al Codice della privacy introdotte nel 2021. I due standard analizzati comportano un diverso bilanciamento tra esigenze di tutela dei dati personali ed esigenze della loro circolazione. Il saggio si chiude con l'illustrazione di due esempi, uno di rilievo nazionale (le Basi di dati di interesse nazionale nel contesto del PDND) e uno europeo (il Regolamento EHDS), al fine di evidenziare come – più di recente – si vanno affermando strategie normative che, tramite un uso "strategico" delle basi di liceità e del meta-principio di finalità del trattamento, mirano ad incentivare la circolazione e l'uso secondario dei dati personali, segnando una tendenza alla progressiva erosione della centralità del consenso, ed un diverso bilanciamento rispetto alle esigenze di tutela.

GDPR – Circolazione dei dati – Legalità funzionale – Finalità del trattamento – EHDS

Personal data processing and legality standards: evidence of the growing primacy of data free movement?

Starting from the features of the meta-principle of purpose limitation and the necessity clause, the essay shows how the GDPR constructs a functional standard of legality, including with regard to data processing carried out for the performance of a task in the public interest. Given the margin of discretion left by the GDPR in this domain, the Italian legal system was initially characterised by a framework inspired by a strict legality standard (requiring detailed legislative predetermination of data, operations, and purposes), before subsequently aligning with functional legality as a result of the amendments to the Privacy Code introduced in 2021. The two standards analysed entail a different balance between the need to protect personal data and the need to ensure their circulation. The essay concludes by illustrating two examples – one at the national level (the national-interest databases in the context of the PDND) and one at the European level (the EHDS Regulation) – in order to show how, more recently, regulatory strategies have emerged that, through a "strategic" use of lawful bases for data processing and of the meta-principle of purpose limitation, aim to encourage the circulation and secondary use of personal data. These developments signal a trend toward the progressive erosion of the centrality of consent and a shift in the balance between data protection and data-sharing needs.

GDPR – Data free movement – Instrumental legality – Processing purpose – EHDS

L'Autore è professore associato di Diritto amministrativo nell'Università degli studi di Perugia

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato* a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Il GDPR: non solo garanzia di protezione, ma anche della circolazione dei dati personali

Come noto, il regolamento generale sulla protezione dei dati personali, entrato in vigore nel 2018, costituisce da allora un punto di riferimento, un *benchmark*, per la tutela dei dati personali[1]. Tuttavia, come spesso la dottrina si è incaricata di ricordare, la *tutela* dei dati personali non costituisce l'oggetto *esclusivo* di quella normativa: infatti, come il primo articolo del regolamento chiarisce (a più riprese), accanto ed in concorrenza con questo obiettivo, il regolamento intende anche assicurare la *libera circolazione* dei dati personali[2]. Le ragioni di questa (apparente) anfibologia sono altrettanto note: definire un quadro di regole, istituti, attori e procedure atte a bilanciare l'esigenza di assicurare tutela ai dati personali (e, per essi, alla libertà, all'autodeterminazione e alla dignità delle persone fisiche), da una parte, e di non ostacolare *oltremisura* lo sviluppo e l'esercizio di tutte quelle attività di carattere economico, politico e sociale che si basano sul trattamento dei dati personali. Il GDPR, detto altrimenti, prende atto del paradigma digitale e di rete, che abilita soluzioni particolarmente economiche, efficaci, potenti (per la produzione di beni, servizi e altre utilità, anche nell'ambito del settore pubblico) e che presuppongono il trattamento dei dati personali: tali soluzioni non devono essere *impedite*, ma piuttosto promosse, in quanto irregimentate/contenute all'interno di un quadro di regole volto ad assicurare un "elevato livello di tutela dei dati personali".

In termini generali, la tutela dei dati riposa innanzitutto nelle *modalità di trattamento*, che devono risultare sempre rispettose dei principi enucleati all'art. 5 del GDPR. I principi, a loro volta, sono plasmati attorno al *meta-principio* che caratterizza l'impianto complessivo di tutela dei dati personali, secondo il modello europeo, così come "precipitato" nel GDPR, principio per il quale il *trattamento* dei dati personali è sempre connesso ad una specifica *finalità*, che ne giustifica la raccolta o la formazione (*ab origine*) e che accompagna tutto il successivo ciclo di trattamento, affinché questo resti *lecito*[3]. E così: la *finalità* costituisce il principale referente rispetto al quale si valuta il rispetto del principio per cui ogni trattamento deve essere *corretto* e *trasparente*; ancora: i trattamenti successivi sono leciti solo se la *finalità* di tali trattamenti è *compatibile* con quella originaria; la *finalità* costituisce il parametro cui si rapporta l'identificazione di quali dati personali sia lecito raccogliere e trattare (principio di *minimizzazione*), ed il tempo per il quale tali dati possono essere conservati (principio di *limitazione della conservazione*). Di più, e preliminarmente (con specifico riferimento, per altro, al principio di *liceità del trattamento*), solo

1. Buttarelli 2016.
2. *Ex multis*: Colapietro 2018; Hoofnagle–Van Der Sloot–Borgesius 2019; Zorzi Galgano 2019-b; Comandè–Schneider 2021; Midiri 2025.
3. Bendiek–Römer 2019.

alcune tipologie di finalità forniscono una base di liceità al trattamento dei dati personali. Si tratta delle finalità che integrano le basi di liceità del trattamento, così come individuate nell'art. 6, eventualmente integrate all'art. 9 da ulteriori requisiti, con riferimento al trattamento dei dati personali cd. "particolari". In assenza (quantomeno) di una di queste basi di liceità, il trattamento è *ipso iure* illecito. Pertanto, si può dire che gli istituti posti a tutela dei dati personali si possono riconoscere – essenzialmente – nell'esistenza di alcune condizioni prescritte dalla legge (dal GDPR) che abilitano il trattamento (e che pertanto, se assenti o carenti, lo impediscono rendendolo *illecito*): tali condizioni attengono ai *presupposti* del trattamento (le basi di liceità) e alle *modalità* del trattamento (i principi sul trattamento), che risultano tutti connessi al meta-principio della finalità del trattamento.

Il rispetto di tali regole costituisce il *meccanismo di protezione dei dati* (per gli interessati), e al tempo stesso (per ciò stesso) un vincolo, *per chi intenda farne uso* (il titolare del trattamento), e pertanto la vigenza di ciascuno di essi (basi e principi) costituisce anche un "ostacolo" alla libera circolazione dei dati.

Ma il GDPR, come detto, non si preoccupa solo di assicurare *tutela* ai dati personali; è inteso anche a favorirne la circolazione. Il primo, fondamentale fattore che opera in questo senso va riconosciuto nella stessa natura della fonte del regolamento europeo. Tale fonte, nella misura in cui è suscettibile di applicarsi direttamente in modo uniforme sul territorio di tutti gli ordinamenti che compongono l'Unione europea (condizione per il vero non sempre realizzata nelle disposizioni del regolamento, come proprio il caso dei trattamenti giustificati dall'esercizio di un compito di interesse pubblico sta a testimoniare), rimuove gli ostacoli (alla circolazione tra gli Stati membri) connessi alla disomogeneità delle tutele assicurate in precedenza (cioè, in vigenza della direttiva 95/46/CE), nei diversi ordinamenti nazionali[4].

Oltre a questo essenziale contributo, nel regolamento si può però identificare un altro fattore che opera nel senso di *favorire* la circolazione. Tale fattore è rappresentato dalla centralità assunta dalla clausola di *necessarietà* come presupposto di liceità del trattamento[5]. Fatta salva la base di liceità che poggia sul consenso dell'interessato (art. 6, lett. a), tutte le basi di liceità disposte dal GDPR poggiano sulla *clausola di necessarietà*. Infatti, è lecito il trattamento che risulti *necessario*, di volta in volta: per l'esecuzione di un contratto di cui l'interessato è parte (lett.b); per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (lett. c); per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (lett. d); per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (lett. e); per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (lett. f). La clausola di necessarietà risulta quindi *pervasiva*, anche tenuto conto del fatto che – come la dottrina si è incaricata di chiarire, a fronte di alcune inerzie interpretative – il GDPR non instaura alcuna gerarchia di valore o di preferenza tra le diverse basi di liceità[6]. Questo significa che il dato personale, *a prescindere dal consenso dell'interessato*, è autorizzato a circolare (base di liceità) ogniqualvolta il suo trattamento risulti *necessario* ad uno dei fini di cui all'art. 6. La *necessarietà*, dunque, abilita e favorisce la circolazione.

Si noti che, con riferimento alla clausola di necessarietà, il meta-principio della finalità del trattamento opera in modo duplice. Per un verso, coopera nel senso di *incentivare* la circolazione, dal momento che – come detto – la clausola di necessarietà acquista senso con riferimento a questa o quella specifica finalità del trattamento. D'altra parte, tuttavia, gli *usi secondari* dei dati personali (e, quindi, la loro stessa circolazione) sono leciti solo nella misura in cui le finalità per i quali sono effettuati tali *ulteriori trattamenti* risultano non incompatibili con quelle che ne avevano giustificato (in origine) la raccolta. Dunque, la finalità del trattamento opera anche come *limite* alla circolazione.

È all'interno di queste coordinate generali che si propone di leggere la disciplina relativa al trattamento dei dati personali funzionale all'esercizio di funzioni pubbliche.

4. Lin 2024; Chirică 2017; Lynskey 2015.
5. Lindsay 2017; Brouwer 2011; Elgesem 1999.
6. Zorzi Galgano 2019-a; Voigt–Von dem Bussche 2017.

2. Protezione e circolazione dei dati nei trattamenti funzionali all'esercizio delle funzioni pubbliche: quale base di liceità?

Tra le basi di liceità predisposte (e quindi, autorizzate) dal GDPR, quella di cui alla lett. e) dell'art. 6 richiama esplicitamente "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", e costituisce pertanto la fattispecie elettiva dalla quale occorre partire per inquadrare il discorso relativo al regime del trattamento dei dati nel caso dell'esercizio di una funzione pubblica. Vale la pena, tuttavia, di verificare se ed in che misura anche le altre basi di liceità potrebbero concorrere a tale fine[7]. Il consenso pare da escludersi, quantomeno tutte le volte in cui il perseguimento di interessi pubblici finisce per radicare in capo al titolare del trattamento una posizione tanto di *potere* quanto di *dovere* tale da risultare incompatibile con i caratteri che devono connotare il consenso (che deve consistere in una "manifestazione di volontà libera", oltre che specifica, informata e inequivocabile dell'interessato). Diversamente, quando l'esercizio di compiti di interesse pubblico si traduce in atti basati che presuppongono il consenso (il contratto, l'accordo), potrebbe risultare plausibile che il trattamento dei dati personali possa appoggiarsi anche su questa base; e tuttavia, anche in questo caso occorre verificare con maggiore attenzione la fattispecie in questione, dal momento che l'esistenza di un atto (finale) perfezionato sulla base di un *accordo* tra l'amministrazione e la parte interessata potrebbe giungere a suggello di uno schema decisionale niente affatto paritario, né del tutto libero. Si pensi, per fare un solo esempio, all'accordo di cui all'art. 11 della legge 241/1990, che costituisce sempre una modalità alternativa di conclusione del procedimento rispetto all'adozione di un provvedimento unilaterale, nel quale l'amministrazione potrebbe, invece, scegliere di spendere il suo potere asimmetrico e unilaterale. Pertanto, affinché la base di liceità fondata sul consenso possa supportare l'esercizio di una funzione amministrativa, occorre non solo che questa si perfezioni in un atto fondato sull'incontro tra la volontà delle parti (a valle), ma anche che (a monte) non sia configurabile – in capo all'amministrazione – una situazione di potere. Tutte le volte, cioè, in cui l'amministrazione agisca (e debba agire) con strumenti di diritto privato, quali il contratto. Ma, in questi casi, la liceità del trattamento dei dati è già prevista (e delimitata) dalla diversa base di liceità di cui all'art. 6, co. 1, lett. b).

La base di liceità di cui alla lett. c) (trattamento necessario per "adempiere un obbligo legale al quale è soggetto il titolare del trattamento") costituisce invece un presupposto applicabile all'esercizio di compiti assegnati ad amministrazioni pubbliche per il perseguimento di interessi pubblici, come confermato dalla giurisprudenza della Corte di giustizia. Tuttavia, si tratta di una fattispecie in cui l'amministrazione si trova astretta in una condizione di vincolo (l'adempimento di un obbligo legale) tale da renderla quasi indistinguibile (sotto il profilo del regime applicabile) da un soggetto di diritto comune (che fosse astretto a consimile vincolo, come accade più di frequente); inoltre, tale base di liceità presuppone un forte grado di predeterminazione del trattamento (quali dati, quali operazioni, per quali finalità) con la conseguenza che il relativo regime è quasi integralmente assorbito nella fattispecie legislativa che disciplina l'obbligo. Insomma, si tratterebbe di *attività vincolata*, ciò che pare escludere l'assegnazione di un potere discrezionale applicabile (anche) alle modalità di trattamento dei dati personali.

Analogo sarebbe il ragionamento con riferimento alla base di liceità di cui all'art. 6, co. 1, lett. d). La "salvaguardia degli interessi vitali dell'interessato" o di altra persona fisica, infatti, è base giuridica idonea ad attivare qualsiasi intervento così giustificato, da chiunque posto in essere, e quindi anche, ma non solo, nell'esercizio di compiti di interesse pubblico. Né il fatto che vi siano articolazioni del pubblico potere esplicitamente e stabilmente dedicate a fronteggiare situazioni di urgenza ed emergenza appare altrimenti dirimente. Infatti, secondo la giurisprudenza, la base di cui alla lett. d) va interpretata in modo *restrittivo*, facendo riferimento a casi come incidenti gravi, emergenze mediche o disastri naturali in cui occorre trattare dati per proteggere la vita

7. Sul punto, vedi *amplius*: Franca 2023; Ponti 2023-a; Niger 2022; Francario 2022; Carullo 2020.

o l'incolumità e non vi è tempo o modo di raccogliere il consenso *o fare affidamento su altra base*[8].

Infine, è lo stesso GDPR ad escludere che la base di liceità connessa al perseguimento del legittimo interesse del titolare del trattamento (art. 6, co. 1, lett. f) sia applicabile ai trattamenti di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Una statuizione preziosa, perché esplicita e corrobora (in negativo) il presupposto di liceità di cui alla lett. e). Infatti, tale esclusione contribuisce a chiarire che il titolare che effettua trattamenti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, non persegue interessi che gli sono propri, ma interessi *altrui* (interessi pubblici, generali, della collettività) e che sono affidati alla sua cura, in una condizione ontologicamente *servente* rispetto ad essi.

Anche alla luce di questa sintetica disamina, appare quindi utile concentrarsi sulla base di cui alla lett. e), che si conferma come la base di liceità più rilevante, quanto all'esercizio di poteri e compiti funzionali al perseguimento di interessi pubblici.

3. *Necessary clause* e trattamento dei dati personali per l'esercizio dei compiti di interesse pubblico

Secondo lo *standard legale* fissato nel GDPR, ogni qualvolta Il trattamento di un dato personale (comune[9]) risulta necessario "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", quel trattamento è in potenza lecito, fatto salvo il rispetto dei principi di cui all'art. 5. Lo schema legale in questione, dunque, non predetermina gli elementi essenziali del trattamento (quali dati, sottoposti a quale operazione, per quale finalità), né impone che la legge debba farlo. Ciò che rileva, ai fini della liceità del trattamento, è che esso (a prescindere da come sia poi strutturato) risulti *necessario* per l'esecuzione del compito di interesse pubblico. La clausola di necessarietà, applicata in questo modo, costruisce un modello di *legalità* (in relazione al trattamento dei dati personali) che potremmo definire *funzionale*: la liceità del trattamento dipende non dal rispetto di una regola predeterminata che lo disciplina, ma dalla attitudine del trattamento ad assicurare l'esecuzione del compito di interesse pubblico[10]. Entro queste coordinate, la base giuridica rileva (come necessaria) nella misura in cui indica (e deve indicare) quale sia il compito di interesse pubblico, quale sia cioè la finalità, l'interesse alla cui cura il soggetto (tendenzialmente, ma non necessariamente) pubblico è (così) preposto, e solo in questa misura. Ciò ha due ordini di conseguenze principali. Per un verso, la f*inalità del trattamento* (di cui al meta-principio del GDPR) finisce per coincidere con la *finalità dei compiti di interesse pubblico*, e in questo contesto gioca il medesimo (duplice) ruolo che abbiamo tratteggiato in linea generale. Per un verso, la finalità di interesse pubblico *attiva* la circolazione dei dati (il dato può circolare, se la circolazione è necessaria al perseguimenti dell'interesse pubblico); per altro verso, la stessa finalità di interesse pubblico opera come *limite* a questa circolazione, dal momento che, perché il trattamento (secondario) risulti lecito, occorrerà verificare se la finalità in vista della quale tale trattamento viene posto in essere (perché necessario) risulta "non incompatibile" con la finalità che aveva giustificato la raccolta/formazione originaria del dato personale in questione. In secondo luogo, le modalità di trattamento risultano potenzialmente rimesse (anche in modo integrale) alla autonoma determinazione del soggetto "investito" dei compiti di interesse pubblico, il quale è tenuto a *rendere conto* delle scelte compiute in merito (in

8. Cfr. CGUE C252/21 *Meta Platforms Inc. vs Bundeskartellamt*.
9. Lo schema legale per quanto concerne il trattamento dei dati "particolari" (i.e., i "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati 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") è ancora modellato sulla clausola di necessarietà, ma è reso più esigente da ulteriori elementi: il trattamento deve essere necessario per dare soddisfazioni a ragioni di interesse pubblico rilevante, così qualificate dal diritto dell'Unione o degli Stati membri; diritto che deve risultare proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, co. 2, lett. g).
10. Ponti 2023-a.

accordo con il principio di responsabilizzazione, art. 5, co. 2), scelte che però gli pertengono.

Quali sono, tuttavia, i caratteri che qualificano un trattamento come *necessario*, ai fini dell'esecuzione di un compito di interesse pubblico? L'analisi della giurisprudenza della Corte di giustizia ha consentito di verificare che la *necessarietà* consiste in un rapporto di strumentalità del mezzo impiegato (il trattamento dei dati) rispetto al fine (l'esecuzione del compito di interesse pubblico ovvero l'integrazione della finalità del trattamento), e che detta strumentalità risulta realizzata nella misura in cui il trattamento risulta *efficace* (cioè, idoneo a consentire l'esecuzione del compito di interesse pubblico)[11]. Ora, i trattamenti possono risultare più o meno invasivi della sfera giuridica dell'interessato (in ragione di fattori diversi, quali: la quantità e qualità dei dati personali oggetto di trattamento, la tipologia di operazioni effettuate, i rischi cui sono di conseguenza esposti gli interessati). Sotto questo profilo, la stessa giurisprudenza ha chiarito che, tenuto conto del principio di *minimizzazione*, un trattamento *meno invasivo* risulta necessario, in luogo di un altro, *più invasivo*, solo se e nella misura in cui risulti *altrettanto efficace* nel perseguire l'interesse pubblico. Questa notazione ci consente di identificare quale sia il bilanciamento tra esigenze di tutela e esigenze di circolazione realizzato mediante la codificazione della clausola di necessarietà applicata ai trattamenti strumentali all'esercizio di funzioni pubbliche. Tale clausola, infatti, sconta di per sé effetti di compressione o sacrificio delle esigenze di tutela, e che coincidono con gli effetti determinati da tutti i trattamenti dei dati personali che risultano *strumentali* al perseguimento di una finalità pubblica, dato un certo livello di efficacia della soluzione impiegata. Pertanto, a conferma della natura funzionale dello standard di legalità connesso alla clausola di necessarietà, è l'*efficacia del trattamento* applicato ai dati personali la misura che lega in termini di proporzionalità l'equilibrio (adattabile, non predeterminato) che si realizza tra esigenze di tutela ed esigenze di circolazione[12].

4. Margini di manovra e *strict legality standard*

Lo standard di *legalità funzionale* posto dal GDPR non è però l'unico che può regolare il trattamento dei dati personali per l'esercizio di funzioni pubbliche. Infatti, la disciplina eurounitaria, *in parte qua* apre uno spazio agli Stati membri per introdurre (o mantenere) una disciplina interna utile ad adattare il quadro normativo del GDPR. Origini e ragioni di questa clausola di adattamento sono state indagate altrove; basti qui chiarire che essa si giustifica anche perché consente agli ordinamenti di potersi "distaccare" dallo standard della *legalità funzionale*, anche per tenere conto delle tradizioni e delle caratteristiche del diritto amministrativo interno. Come noto, è (stato) questo il caso anche dell'ordinamento nazionale italiano che, per il periodo compreso tra l'entrata in vigore della disciplina interna di adeguamento al GDPR (agosto 2018) e le modifiche al Codice della privacy introdotte a seguito del c.d. decreto "capienze" (ottobre 2021), ha sperimentato un diverso standard legale, per come definito dalle disposizioni (per come allora formulate) agli art. 2-*ter* e seguenti. Tale disciplina, anche in virtù della interpretazione che ne aveva fatto il Garante della privacy, imponeva (invece) che il trattamento dei dati personali (operato per il perseguimento di interessi pubblici) fosse predeterminato da una norma di legge (o di regolamento, ma di carattere meramente esecutivo) quanto a: la tipologia di dati da trattare, il tipo di operazioni da effettuarsi, la finalità da perseguire. Dunque, una *strict legality rule*, nella quale si realizza un (ben diverso bilanciamento) tra esigenze di circolazione ed esigenze di tutela. Le seconde

11. Ponti, 2023-a.

12. Fa eccezione (sempre nella giurisprudenza della Corte di giustizia) l'ipotesi dello specifico trattamento che consista nella *pubblicazione* dei dati personali. Infatti, la diffusione al pubblico dei dati personali rappresenta una tipologia di trattamento idonea a determinare un pregiudizio così grave e intenso da modificare i temini del giudizio di proporzionalità, che trasmuta in giudizio di *stretta indispensabilità*. Secondo questa regola di bilanciamento, non solo tale trattamento deve essere previsto esplicitamente dal legislatore, ma esso risulta comunque incompatibile con il GDPR qualora sia astrattamente disponibile e concretamente sperimentabile una diversa soluzione, basata su un diverso (e meno invasivo) trattamento dei dati personali, *anche se meno efficace*: cfr. Ponti 2023-a; CGUE C-184/20, *Vyriausioji tarnybinės etikos komisija*.

appaiono più pienamente assecondate, nella misura in cui è il legislatore a dover autorizzare in modo esplicito, rigido e analitico le specifiche modalità di trattamento dei dati personali; le prime, invece, risultano maggiormente sacrificate, dal momento che – in assenza di una specifica previsione legislativa – il trattamento dei dati (che pure risulti funzionale al perseguimento dell'interesse pubblico) risulta interdetto. Un regime di *legalità funzionale* "temperata", tuttavia, era applicato al caso della *circolazione* dei dati *tra diverse amministrazioni*: in questo caso, la mancata previsione dello scambio dei dati – che pure risultasse necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali – era possibile, sebbene comunque soggetto ad un onere di notificazione al Garante[13].

A seguito delle modifiche introdotte nell'autunno del 2021, il quadro nazionale italiano è stato profondamente modificato, ed appare oggi sostanzialmente allineato allo standard della *legalità funzionale*, così come disposto nel GDPR. Infatti, non solo alle amministrazioni è stato assicurato il potere di disciplinare i trattamenti con propri atti organizzativi (anche in assenza di una autorizzazione legislativa[14]), ma ad esse è *comunque* accordata la possibilità di effettuare i trattamenti dei dati personali (compresa la circolazione dei dati all'interno del settore pubblico) che risultino *necessari* per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri loro attribuiti[15]. Rimane ferma, però, l'eccezione relativa al trattamento che consiste nella pubblicazione dei dati personali (anche quando funzionale all'assolvimento di compiti di interesse pubblico), che richiede una apposita norma legislativa che lo preveda, secondo l'interpretazione offerta dal Garante[16].

5. Strategie legislative per la circolazione dei dati

Come detto, il meta-principio della finalità del trattamento opera (anche) come limite alla circolazione dei dati personali, dal momento che il (conseguente) principio di *limitazione della finalità* impone che i trattamenti secondari siano effettuati per finalità *non incompatibili* con quelle che hanno giustificato la raccolta/formazione originaria del dato personale in questione. Rispetto a questo *elemento strutturale*, che costituisce una matrice identificativa del modello europeo di tutela dei dati, i legislatori hanno utilizzato in *modo strategico* la leva normativa, per ovviare all'intrinseco effetto di limitazione alla circolazione che ne deriva.

Un paio di esempi possono essere sufficienti, al fine di rappresentare come le esigenze di circolazione e di condivisione dell'informazione, all'interno del settore pubblico (e tra settori pubblici di differenti Stati membri dell'Unione europea, come si dirà tra poco), stanno portando a "forzare" le logiche del GDPR.

Un primo esempio è tratto dal contesto nazionale italiano e fa riferimento a quelle banche dati in cui sono raccolte e organizzate categorie omogenee di informazioni allo scopo precipuo di rendere

13. A seguito della notificazione, la comunicazione dei dati da una amministrazione all'altra poteva avere inizio solo decorsi quarantacinque giorni, senza che il Garante fosse intervenuto prescrivendo delle misure *a garanzia degli interessati*.
14. Cfr. l'art. 2-*ter*, co. 1 del Codice privacy attualmente vigente, per effetto delle modifiche introdotte dal d.l. 139/2021, convertito in legge 205/2021.
15. Cfr. l'art. 2-*ter*, co. 1-*bis* del Codice privacy. Appaiono quindi non del tutto condivisibili le preoccupazioni espresse in dottrina, laddove si prospetta *l'incompatibilità* del quadro normativo nazionale (come risultante dalle modifiche introdotte nel 2021) rispetto a quello europeo (cfr. Carullo 2024). Infatti, il citato comma 1-*bis* dell'art. 2-*ter* del Codice privacy non fa che riprodurre (in termini quasi letterali) lo standard legale di cui all'art. 6, co. 1, lett. e) del GDPR; pertanto, le obiezioni richiamate andrebbero semmai indirizzate al regolamento, e dovrebbero concernere lo *standard di legalità funzionale* da esso introdotto, nella misura in cui non appare del tutto in linea con le esigenze imposte dalla vigenza – sul piano interno – del principio di legalità, in quanto applicato al trattamento dei dati personali. Sul punto – oltre al contributo di Francario, in questo numero della Rivista (Francario 2025) – cfr. anche Franca 2023.
16. Cfr., *ex multis*, il provvedimento dell'11 aprile 2024, doc. web n. 10019523 e il Provvedimento del 24 gennaio 2024, doc. web n. 9987578.

tali informazioni disponibili al sistema pubblico nel suo complesso, e a ciascuna delle sue componenti, al fine di alimentare l'esercizio delle rispettive funzioni amministrative; quelle *basi di dati di interesse nazionale*, disciplinate agli artt. 60 e ss. del Codice dell'amministrazione digitale. Il legislatore utilizza in modo strategico il meta-principio di finalità, poiché assegna in modo esplicito alla banca dati *il compito di raccogliere, conservare determinate informazioni per renderle disponili alle altre amministrazioni*. Così facendo, l'intervento legislativo (che costituisce e/o qualifica la base di dati di interesse nazionale) "spezza" la catena di valutazioni circa la *compatibilità* tra le finalità originaria della raccolta e le finalità dei successivi trattamenti secondari. La raccolta, la conservazione e l'allineamento delle informazioni, compresi i dati personali, che vanno a costituire la specifica *base di dati*, sono trattamenti che *ab initio* hanno *la finalità* di rendere le informazioni utili e disponibili alla circolazione, così che la successiva valutazione di compatibilità (rispetto al trattamento posto in essere dall'amministrazione che fruisce del servizio di "erogazione dei dati") avrà *sempre* esito positivo, *by design*. In questo modo, il principio di limitazione della finalità è utilizzato per devitalizzarne la componente *di tutela* e per esaltarne la componente *di circolazione*. Non deve sfuggire la circostanza per cui questo meccanismo può operare anche in virtù del *margine di manovra* aperto alle legislazioni nazionali dall'art. 6, commi 2 e 3 del GDPR; in particolare, è il comma 3 che consente ai legislatori (degli Stati membri e dell'Unione) di introdurre "disposizioni specifiche per adeguare l'applicazione delle norme del regolamento", anche per quanto riguarda "le limitazioni della finalità".

Non è quindi casuale che, nel momento in cui – anche per effetto della spinta impressa dal PNRR – si è proceduto a edificare e mettere in opera una infrastruttura tecnica capace *effettivamente* di far circolare le informazioni all'interno del sistema pubblico (la Piattaforma digitale nazionale dei dati – PDND), le prime banche dati designate per essere integrate nel sistema sono state proprio le Basi di dati di interesse nazionale[17]: il presupposto normativo volto a favorire la circolazione dei dati (anche personali) all'interno del sistema pubblico ha così trovato riscontro in una soluzione volta a consentire *effettivamente* (sul piano tecnico ed organizzativo) la circolazione dei dati[18].

Un secondo esempio è rappresentato dalla strategia perseguita a livello europeo, volta a porre rimedio agli ostacoli alla circolazione dei dati sanitari, ostacoli determinati dalla frammentazione dei regimi giuridici nazionali, anche in ragione delle clausole di apertura a discipline nazionali contenute nell'art. 9 del GDPR (e che si aggiungono a quelle di cui all'art. 6, commi 2 e 3 di cui si è già detto)[19]. Il recentissimo *Regolamento sullo spazio europeo dei dati sanitari*-EHDS[20], infatti, utilizza la leva di una normativa *ad hoc* (di livello unionale) al fine di fornire le basi giuridiche utili ad assicurare che i dati sanitari possano circolare all'interno dell'Unione, così da promuovere una serie di finalità, identificate all'art. 53 del regolamento[21]. Il Regolamento EHDS (come descritto in modo

17. Come previsto dall'art. 50-*ter*, comma 2 del Codice dell'amministrazione digitale, così come integrato dal d.l. 77/2021, "In fase di prima applicazione, la Piattaforma [digitale nazionale dei dati, ndr] assicura prioritariamente l'interoperabilità con le basi dati di interesse nazionale".

18. Ponti 2023-b.

19. Quinn–Ellyne–Yao 2024.

20. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

21. Le finalità che il regolamento promuove possono essere sintetizzate come segue: cura del pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro; definizione delle politiche nel settore sanitario o dell'assistenza; statistiche relative al settore sanitario o dell'assistenza; istruzione o insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce

analitico nel considerando 52) fa un uso *strategico* delle basi giuridiche così come identificate nel GDPR. Per un verso, utilizza la base di cui all'art. 6, par. 1, lett. c), completa dei requisiti aggiuntivi di cui all'art. 9, par. 2, lett. i) e j), per rendere obbligatoria la comunicazione/messa a disposizione dei dati sanitari (che rientrano nelle categorie di dati identificati all'art. 51) da parte dei soggetti qualificati come "Titolari dei dati sanitari" (art. 60). Utilizza, poi, la base di cui all'art. 6, par. 1, lett. e), completa dei requisiti aggiuntivi di cui all'art. 9, par. 2, lett. da g) a j), per assegnare ai costituendi/designandi "Organismi responsabili dell'accesso ai dati sanitari" (artt. 55, 57-59) *i compiti di interesse pubblico*, che consistono nella gestione dell'accesso ai dati resi disponibili dai titolari dei dati sanitari. In particolare, tra i molti compiti assegnati, spiccano quelli di decisione sulle domande di accesso ai dati sanitari (presentate dagli "Utenti dei dati sanitari") e la conseguente autorizzazione all'accesso a tali dati presso i rispettivi titolari (art. 57, par. 1, lett. a); nonché la pubblicazione e l'aggiornamento di una serie di informazioni utili a consentire la circolazione dei dati sanitari e a dare conto dei risultati conseguiti dagli utenti (art. 57, par. 1, lett. j)[22]. Sulla base di questa infrastruttura di *governance*, gli "Utenti dei dati sanitari", purché dotati di una base giuridica prevista dall'articolo 6, par. 1, lett. e), o f), possono presentare richieste di accesso e di autorizzazione all'uso secondario e – qualora autorizzati – utilizzare i dati sanitari che già assicurano il rispetto delle condizioni di cui all'art. 9, par. 2. A tale fine, il regolamento impedisce agli Stati membri di introdurre condizioni ulteriori (compreso il consenso dell'interessato) per l'uso secondario, se non a limitati fini e solo per alcune tipologie di dati personali[23].

Anche qui, l'uso strategico della leva normativa è utile a *svincolare* il dato sanitario (personale) dalla (specifica) finalità connessa alle ragioni della sua originaria raccolta e trattamento, e renderlo disponibile agli *utenti secondari* già caratterizzato da finalità ulteriori e diverse, così che il trattamento *ulteriore* di questi dati sarà (sempre) *lecito*, nella misura in cui (al netto del rispetto delle prescrizioni del regolamento EHDS) tali trattamenti risultino compatibili con le finalità esplicitamente selezionate e qualificate[24] dal regolamento stesso.

Il meccanismo di incentivazione dell'uso secondario dei dati sanitari abilitato dall'EHDS è

alla sanità pubblica o alla valutazione delle tecnologie sanitarie; miglioramento ed ottimizzazione della prestazione di assistenza sanitaria.

22. Gli organismi responsabili dell'accesso ai dati sanitari devono pubblicare, tra le altre cose: un catalogo nazionale contenente informazioni dettagliate sulla fonte e sulla natura dei dati sanitari elettronici e sulle condizioni per la loro messa a disposizione; le domande di accesso ai dati sanitari; tutte le autorizzazioni ai dati rilasciate o le richieste di dati sanitari approvate come pure le decisioni di diniego, unitamente alla relativa motivazione; i risultati o gli esiti dell'uso secondario comunicati dagli utenti dei dati sanitari.
23. Se il considerando 52, a questo fine, suggerisce che "Stati membri non dovrebbero più poter mantenere o introdurre, a norma dell'articolo 9, paragrafo 4, del regolamento (UE) 2016/679, ulteriori condizioni, comprese limitazioni e disposizioni specifiche che richiedono il consenso delle persone fisiche, per quanto riguarda il trattamento per l'uso secondario dei dati sanitari elettronici personali a norma del presente regolamento, ad eccezione dell'introduzione di misure più rigorose e garanzie supplementari a livello nazionale intese a tutelare la sensibilità e il valore di taluni dati come previsto dal presente regolamento", l'articolato dispone (di conseguenza) che agli Stati membri è consentito introdurre misure più rigorose e garanzie supplementari a livello nazionale solo se intese a tutelare la sensibilità e il valore dei dati, e solo relativamente a dati ricompresi entro alcune categorie di dati sanitari, ossia: i dati genetici, epigenomici e genomici umani; altri dati molecolari umani; i dati provenienti dalle applicazioni per il benessere; nonché dati sanitari provenienti da biobanche e banche dati associate (cfr. art. 51, par. 4).
24. L'art. 53 identifica tali finalità in modo particolarmente ampio, non solo con riferimento alla numerosità delle casistiche previste (lett. da a) a f) dell'art. 53, par. 1), ma anche con riferimento alle modalità con le quali ciascuna di queste finalità è stata formulata. Ciò che, anche a parere dei primi commentatori della disciplina appare una forzatura del modello di tutela di cui al GDPR, in ragione della enorme discrezionalità che appare rimessa in capo agli Organismi responsabili dell'accesso ai dati sanitari nell'autorizzare l'uso secondario dei dati sanitari elettronici: cfr. Quinn–Ellyne–Yao 2024.

di recentissima introduzione, ed occorre ancora capire se ed in che misura sarà efficace: in termini simili a quelli già visti nel primo esempio, tale *effettività* passa non solo per la abilitazione di un quadro normativo idoneo a consentire la circolazione dei dati[25], ma anche dalla realizzazione di una coerente infrastruttura tecnica. Infatti, l'EHDS intende costruire uno spazio per la circolazione dei dati sanitari *elettronici*, ed una parte significativa del regolamento è dedicata a realizzare anche i presupposti *tecnologici* necessari a tale fine, ossia ad assicurare che i dati raccolti (in sede di uso primario) siano codificati in modo tale, poi, da risultare *interoperabili*. Uno sforzo di armonizzazione e coordinamento tecnico non meno impegnativo rispetto a quello di carattere legale[26].

Entrambi gli esempi analizzati indicano una più recente prevalenza delle esigenze di circolazione, che si realizzano mediante una modificazione del modo in cui tali esigenze si combinano con quelle di tutela dei dati personali. Tale prevalenza opera, in particolare, lungo due direttrici. Per un verso, attraverso la perdita di centralità del consenso, come base di legittimazione del trattamento dei dati personali, a favore delle altre basi di liceità previste dal GDPR, fondate invece sulla clausola di necessarietà e – per conseguenza – sulla versione *funzionale* dello *standard di legalità*. Per altro verso, per un uso strategico della *leva normativa primaria* (a livello nazionale o europeo), mediante la quale il meta-principio della finalità del trattamento (che non viene rinnegato, né abbandonato) è (piuttosto) impiegato al fine di esaltare le sue ricadute in termini di *abilitazione della circolazione dei dati*, e per attenuare fin dove possibile le (opposte) ricadute in termini di tutela dell'interessato. Non appaia paradossale osservare come, in questo movimento, la fonte legislativa primaria finisca per essere utilizzata a ridimensionare le esigenze più garantiste del principio di legalità.

Riferimenti bibliografici

R. Becker, D. Chokoshvili, E.S. Dove (2024), *Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?*, in "International Data Privacy Law", vol. 14, 2024, n. 3

A. Bendiek, M. Römer (2019), *Externalizing Europe: the global effects of European data protection*, in "Digital Policy, Regulation and Governance", vol. 21, 2019, n. 1

E.R. Brouwer (2011), *Legality and data protection law: The forgotten purpose of purpose limitation*, in L.F.M. Besselink, F. Pennings, S. Prechal (eds.),"The eclipse of the legality principle in the European Union", Kluwer Law International, 2011

G. Buttarelli (2016), *The EU GDPR as a clarion call for a new global digital gold standard*, in "International Data Privacy Law", vol. 6, 2016, n. 2

G. Carullo (2024), *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in "CERIDAP", 2024, n. 3

G. Carullo (2020), *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, in "Rivista italiana di diritto pubblico comunitario", 2020, 1-2

S. Chirică (2017), *The main novelties and implications of the new general data protection regulation*, in "Perspectives of business law journal", vol. 6, 2017

25. Sulla incompletezza di tale quadro giuridico, con rifermento a talune fasi del trattamento e a talune categorie di utenti dei dati sanitari, cfr. Becker–Chokoshvili–Dove 2024.

26. Cfr. il Capo II (Uso primario), Sezione 3 (Infrastruttura transfrontaliera per l'uso primario dei dati sanitari elettronici personali), nonché l'intero Capo III (Sistemi di cartelle cliniche elettroniche e applicazioni per il benessere) del Regolamento EHDS.

G.D. Colapietro (2018), *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in "federalismi.it", 2018, n. 22

G. Comandè, G. Schneider (2021), *Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities*, in "Computer Law & Security Review", vol. 41, 2021

D. Elgesem (1999), *The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data*, in "Ethics and Information Technology", vol. 1, 1999, n. 4

S. Franca (2023), *I dati personali nell'amministrazione pubblica: attività di trattamento e tutela del privato*, Università degli Studi di Trento, 2023

F. Francario (2025), *Il trattamento dei dati personali per finalità d'interesse pubblico*, in "Rivista italiana di informatica e diritto", 2025, n. 2

F. Francario (2022), *Protezione dati personali e Pubblica Amministrazione*, in "GiustiziaInsieme", 1° settembre 2021 e in C. Pisani, G. Proia, A. Topo (a cura di) "Privacy e Lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro", vol. II, Giuffrè, 2022

C.J. Hoofnagle, B. Van Der Sloot, F.Z. Borgesius (2019), *The European Union general data protection regulation: what it is and what it means*, in "Information & Communications Technology Law", vol. 28, 2019, n. 1

Y. Lin (2024), *More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance*, in "Columbia Journal of Transnational Law", vol. 62, 2024, n. 1

D. Lindsay (2017), *The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data*, in D.J.B. Svantesson, D. Kloza (eds.), "Trans-Atlantic Data Privacy Relations as a Challenge for Democracy", European Integration and Democracy Series. Intersentia, 2017

O. Lynskey (2015), *The foundations of EU data protection law*, Oxford University Press, 2015

F. Midiri (2025), *Il ruolo delle autorità indipendenti nella regolazione del trattamento dei dati*, in "Rivista italiana di informatica e diritto", 2025, n. 2

S. Niger (2022), *La protezione dei dati personali nella pubblica amministrazione. L'esperienza italiana*, in "European review of digital administration & law", vol. 3, 2022, n. 2

S. Orlando (2024), *Sulla necessità di un controllo di liceità sostanziale per tutte le basi del trattamento dei dati personali*, in "Persona e mercato", 2024, n. 3

B. Ponti (2023-a), *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

B. Ponti (2023-b), *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in "Istituzioni del federalismo: rivista di studi giuridici e politici", 2023, n. 3

P. Quinn, E. Ellyne, C. Yao (2024), *Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?*,in "Computer Law & Security Review", vol. 54, 2024

P. Voigt, A. Von dem Bussche (2017), *The EU general data protection regulation (GDPR). A practical guide*, 1st edition, Springer, 2017

N. Zorzi Galgano (2019-a), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019

N. Zorzi Galgano (2019-b), *Le due anime del GDPR e la tutela del diritto alla privacy*, in "Persona e mercato dei dati. Riflessioni sul GDPR", Cedam, 2019