Benedetto Ponti

Attività amministrativa e trattamento dei dati personali

Gli standard di legalità tra tutela e funzionalità

FrancoAngeli

Collana di Diritto

SAGGI E RICERCHE

Benedetto Ponti

Attività amministrativa e trattamento dei dati personali

Gli standard di legalità tra tutela e funzionalità

FrancoAngeli

Collana di Diritto

SAGGI E RICERCHE

ISBN 9788835128380
ISBNe 9788835153962

Copyright © 2023 by FrancoAngeli s.r.l., Milano, Italy. ISBN 9788835153962

a M., con ardore

 ISBN 9788835153962

 ISBN 9788835153962

Indice

Introduzione

Come ampiamente noto, e dibattuto da tempo, i dati personali costituiscono una materia prima indispensabile e consustanziale all'esercizio delle funzioni pubbliche. Non è certamente casuale che, quantomeno nel contesto europeo, quando sono emerse delle distinte, inedite minacce alla libertà e alla dignità dei consociati, determinate dallo sviluppo e dalla disponibilità delle tecnologie informatiche di conservazione ed elaborazione delle informazioni, le preoccupazioni si sono appuntate principalmente sul settore pubblico, e sul *potere* pubblico in particolare[1], anche sulla base della consapevolezza delle tragedie maturate nel corso del XX secolo. La raccolta dei dati personali da parte delle pubbliche amministrazioni (e di tutto l'insieme ulteriore, più o meno vasto, di soggetti che a vario titolo esercitano compiti di interesse pubblico) avviene in modo sistematico (dalla culla alla tomba, *e oltre*), in connessione con l'esercizio di una estrema varietà di compiti. A questo dato, si aggiunge la naturale attitudine *concentrativa* del potere pubblico, ossia la ontologica tendenza delle organizzazioni governate secondo criteri politici (*in primis*, gli Stati) ad operare in vista di obiettivi identificati e coordinati in modo unitario (indirizzo politico). A questo elemento, si aggiunga il monopolio dell'uso legittimo della forza, per avere un quadro (non completo, ma) sufficiente ad evidenziare le ragioni per le quali, fin dagli albori, l'attore da tenere sotto controllo, con riferimento alle potenzialità connesse al trattamento dei dati personali – perché ritenuto *oggettivamente* più pericoloso – fosse il potere pubblico.

Sarebbe certamente interessante indagare in modo (più) approfondito come questa iniziale (e ben giustificata) preoccupazione sia (almeno in parte)

[1] Cfr. Rodotà S. (1973), *Elaboratori elettronici e controllo sociale*, Bologna. Braibant G. (1971), "La protection des droits individuels au regard du développement de l'informatique", *Revue internationale de droit comparé*, 23-4, 793-817; Touffait A. (1973), "Libertés publiques et Informatique", in *Exposé Académie Science morale et politique*, G.P. II; Vitalis, A. (1981), *Informatique, pouvoir et libertés*, Paris; Scholtz R., Pitschas R. (1984), *Informationelle Selbstbestimmung und staatliche Informationsverantwortung*, Berlin.

alla base anche di alcuni successivi sviluppi, che hanno visto invece il progressivo affermarsi di *poteri privati*, che sono andati costituendosi proprio a partire dallo sfruttamento delle tecnologie dell'informazione e della comunicazione, al punto da rivaleggiare (nell'evo contemporaneo) proprio con i poteri pubblici, per dimensioni, capacità di influenza, erogazione di servizi, etc[2]. Sarebbe, cioè, interessante indagare come il diverso approccio alla capacità di *concentrazione* nella raccolta e nell'uso dei dati personali adottato nei confronti dei poteri pubblici, rispetto a quelli privati, abbia determinato condizioni (più) favorevoli (o, per converso, abbia frapposto minori ostacoli) per lo sviluppo di questi secondi (anche per effetto delle vere e proprie faglie regolatorie che caratterizzano le relazioni transatlantiche, su questi temi in particolare[3]). Nel corso di questa trattazione, non mancherà modo di ritornare su questo argomento, sebbene ai soli fini della nostra indagine.

Tuttavia, oggetto del presente lavoro sono i profili di liceità dell'uso dei dati personali *ai fini dell'esercizio delle funzioni pubbliche*, così come appaiono delinearsi nel contesto giuridico dell'Unione Europea e nel nostro ordinamento nazionale per effetto, in particolare, dell'adozione del regolamento generale per la protezione dei dati personali (di qui in poi: GDPR). Per ragioni connesse (non solo, ma anche) al dato positivo, l'indagine non può non tenere conto anche dei profili di liceità dell'uso dei dati personali sulla base di presupposti diversi; e questo per (almeno) due ordini di motivi, di assoluto rilievo. In primo luogo, perché il regime disegnato dal GDPR è costruito in modo compatto e trasversale, così che i medesimi istituti trovano applicazione nei diversi, variegati contesti in cui il trattamento dei dati personali può venire in rilievo[4]. In secondo luogo, perché proprio il profilo *funzionale* (le finalità per le quali i dati personali sono trattati) rappresenta uno

[2] Sul punto, *ex multis*, si vedano i saggi raccolti nel n.3/2021 del numero monografico della rivista *Diritto Pubblico* dedicato ai *Poteri Privati*, nonché Moore M. e Tambini D. (2018), (eds.), *Digital dominance: The power of Google, Amazon, Facebook and Apple*. New York; Pollicino O. (2023), *Potere digitale*, in Ruotolo M. e Cartabia M. (eds), *Potere e Costituzione – Enciclopedia del diritto-I tematici*, Milano, V.

[3] Nicola F. G. e Pollicino O. (2020), "The balkanization of data privacy regulation", in *West Virginia Law Review*, 123(1), 61-116. Schwartz P. M. e Karl-Nikolaus P. (2018), "Transatlantic Data Privacy Law", Georgetown Law Journal, 115-180; temi di un confronto tuttavia non più solo "transatlantico": Rotenberg M. (2020), "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection", in *European Law Journal*, 1 ss.

[4] Le tensioni determinate dall'approccio regolatorio applicato con il GDPR rispetto alla dicotomia pubblico/privato sono sottolineate da Zopf, F. (2022), "Two worlds colliding the gdpr in between public and private law", in *European Data Protection Law Review* (EDPL), 8(2), 210-220. A proposito della "*application of data protection rules to public and private actors*" fa riferimento alla "*elimitation of the public/private divide*", cfr. Lynskey O. (2015), *The foundations of EU data protection law*, Oxford.

dei (se non, il) principi(o) cardine attorno al quale è costruita la tutela dei dati personali. Anche così, però, la disciplina del trattamento dei dati personali in connessione con l'esercizio di funzioni pubbliche presenta degli elementi di specificità, che meritano di essere indagati in modo dedicato, dal momento che – per le ragioni che sono oggetto di questo studio – essa abilita un *framework* operativo affatto peculiare, i cui tratti si vogliono qui indagare ed alcuni dei suoi effetti esplicitare.

Il punto di partenza da cui muove questa indagine è – in via di prima approssimazione – il seguente. Per un verso, 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 GDPR, in altri termini, definisce un regime legale relativo all'uso dei dati personali che risulta immediatamente efficace e pienamente operativo, ogni qualvolta venga in rilievo "l'esecuzione di un compito di interesse pubblico" o "l'esercizio di pubblici poteri". Il che per altro rende chiara la rilevanza centrale, sistematica, e permanente che tale regolazione ricopre nell'economia diuturna dell'agire delle amministrazioni pubbliche. La disciplina a tutela dei dati personali (con i suoi principi, sistematicamente esposti, connessi tra loro e sviluppati in corrispondenti diritti degli interessati) costituisce un formante stabile dell'attività amministrativa[5].

Allo stesso tempo, tuttavia, lo stesso GDPR apre uno spazio (per il vero, molto ampio) all'intervento degli Stati membri, per adeguare l'applicazione delle norme del regolamento con riguardo al trattamento che sia funzionale all'esercizio di compiti di interesse pubblico o di pubblici poteri. In questo modo, il GDPR ammette (ma, si badi bene, non richiede, né impone) la conservazione o l'introduzione di un regime legale *ulteriore* rispetto a quello definito dal GDPR stesso, regime la cui definizione è rimessa all'iniziativa e

[5] La centralità acquisita dalla disciplina del trattamento dei dati personali nel regime di diritto amministrativo è testimoniata, ad esempio, dall'attenzione riservata al tema più di recente dall'Associazione italiana dei professori di diritto amministrativo (AIPDA), che nell'aprile del 2022 ha dedicato un incontro specifico a queste tematiche (Convegno "Trattamento dei dati personali e documenti amministrativi: le frontiere della discrezionalità", svoltosi presso la Sapienza di Roma il 29 aprile del 2022).

alle determinazioni degli Stati membri. Il regolamento, dunque, prospetta un *framework* regolatorio caratterizzato da un duplice standard legale (*dual legality standard*), nel quale due livelli normativi possono concorrere (ed effettivamente concorrono) alla disciplina del medesimo oggetto.

L'ipotesi del *dual legality standard* rappresenta, nell'economia di questo lavoro, lo strumento utile per analizzare ed interpretare l'interazione tra i due livelli di disciplina. Mettere a tema la concorrenza dei due livelli di disciplina, in questo specifico settore, non è solo necessario per ricostruire il quadro normativo positivo e vigente, in un dato momento. Ciò consente anche di apprezzare come il margine di manovra rimesso agli Stati membri, per come effettivamente utilizzato, incida in termini significativi sui margini di manovra disponibili *alle amministrazioni*, ai fini della sperimentazione e della messa in opera di servizi, applicativi e procedure che richiedono l'impiego di dati personali. Sotto questo profilo, analizzando il *dual legality standard* potremo meglio apprezzare le diverse modalità in cui può atteggiarsi il *principio di legalità*, con riguardo all'uso dei dati personali in vista dell'esecuzione di compiti di interesse pubblico. Come si avrà modo di argomentare, a seconda della strategia assunta dallo Stato membro in ordine al *se* e *come* occupare gli spazi di disciplina concessi dal regolamento, tale principio tende ad assumere differenti declinazioni. Di modo che, quantomeno con riferimento a questa materia (ovverosia, quello che potremmo definire *il regime giuridico relativo all'uso dei dati personali ai fini dell'esercizio/esecuzione di un compito di interesse pubblico*), si potrà constatare che il regime di legalità appare mutevole: alle componenti più classicamente *prescrittive* del principio, se ne affiancano altre di carattere più propriamente *descrittivo*, nella misura in cui parte del relativo regime risulta effettivamente *disponibile* ai legislatori nazionali, ed astretto semmai a vincoli giuridici *interni* (principi costituzionali, principi generali dell'ordinamento). Una matassa non agevole da sbrogliare, nella quale convivono e si confrontano esigenze di primario rilievo, di carattere soggettivo (la tutela della dignità e della libertà della persona, l'autodeterminazione informativa, la tutela dei dati personali) e collettivo (la funzionalità, l'efficacia e l'efficienza dei servizi pubblici, la trasparenza dei poteri pubblici, la loro *accountability*, e – più in generale – il principio democratico), come pure elementi organizzativi e di contesto, quali le infrastrutture di raccolta e condivisione dell'informazione ovvero l'assetto del mercato.

L'immanenza sistematica dei principi posti a tutela dei dati personali deve, peraltro, renderci avvertiti che la sua rilevanza va ben oltre la considerazione degli aspetti solamente procedimentali dell'agire amministrativo. Infatti, nella misura in cui il trattamento dei dati personali si deve accordare a

criteri e parametri delineati dallo *standard legale*, esso condiziona la predisposizione dei mezzi (in particolare, di quelli conoscitivi) che conformano l'agire amministrativo in modo sistemico, e che dispiegano effetti che corrono paralleli al procedimento amministrativo e – piuttosto – ne costruiscono i presupposti e la cornice di esercizio. Si pensi a come le questioni connesse al regime di tutela dei dati personali incidono sulla interconnessione tra i sistemi informativi, sull'interoperabilità delle banche dati, sull'architettura informativa delle funzioni, per come concretamente organizzate ed esercitate. Pertanto, il formante della tutela dei dati personali predetermina i percorsi dell'attività amministrativa, e costituisce un elemento oramai centrale della relativa disciplina, sotto molteplici profili.

Questo lavoro intende indagare ed evidenziare come – entro il margine di manovra abilitato dal *framework* disegnato dal GDPR – il *dual legality standard* consente al legislatore dello Stato membro di articolare un regime legale capace di bilanciare (anche in termini impliciti) i diversi interessi in gioco, in modo anche molto differenziato. L'esame dei diversi standard legali effettivamente declinati sul piano del diritto positivo si serve anche dello scrutinio approfondito di alcuni casi di studio, attraverso il quale è possibile evidenziare gli effetti prodotti, tanto in termini di tutela dei dati, quanto in termini di riserva di iniziativa riconosciuta alle amministrazioni e di promozione dell'innovazione amministrativa.

In conclusione, sulla scorta degli elementi emersi nel corso dell'analisi, il lavoro suggerisce alcune coordinate dommatiche entro cui reinquadrare le opzioni ordinatrici abilitate dal *dual legality standard*, coordinate che appaiono utili a tratteggiare i caratteri e le dinamiche della legalità, per come questa si atteggia nella disciplina del trattamento dei dati personali ai fini dell'esercizio delle funzioni amministrative. A partire da questo inquadramento teorico è anche possibile trarre una serie di indicazioni, che potranno essere applicate per uso consapevole e strategico degli spazi di adattamento resi disponibili dal regolamento.

 ISBN 9788835153962

1. Dalla General Data Protection Regulation *alle legislazioni nazionali: principi, vincoli e spazi di manovra*

1. Il quadro dell'UE sulla protezione dei dati

Il regolamento generale sulla protezione dei dati dell'UE ha l'obiettivo di garantire un livello coerente ed elevato di protezione per gli individui /le persone con riguardo ai propri dati personali, ed insieme di assicurare la libera circolazione di tali dati nell'ambito dell'Unione[1]. Di conseguenza, ha un ampio campo di applicazione, che copre sia il settore privato che quello pubblico. I dati personali sono definiti in modo molto ampio come *qualsiasi* informazione relativa a una persona fisica identificata o identificabile. Il termine *elaborazione* deve essere interpretato in senso lato (in accordo alla definizione contenuta all'art. 4(2)) e copre qualsiasi insieme di operazioni che viene eseguito su dati personali, inclusa la loro raccolta, organizzazione, conservazione, adattamento, recupero, cancellazione o distruzione. Il regolamento si riferisce alla persona i cui dati vengono elaborati come *interessato*; il termine *titolare del trattamento* si riferisce l'organismo responsabile del trattamento dei dati personali. Il titolare determina le finalità e i mezzi del

[1] La logica del regolamento appare infatti quella di "coniugare il massimo grado di libertà per i titolari del trattamento – accentuando la fase di controllo preventivo e puntando tutto sulla responsabilizzazione – con il massimo grado di tutela per gli interessati" Califano L. (2017), *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in Califano L., Colapietro C. (eds.), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Napoli, 23. "sembra chiaro infatti con il regolamento l'intento di portare a maggior compimento una normativa sulla privacy che, più che occuparsi di riservatezza, tenda a regolare *in primis* la libera circolazione dei dati (e dunque la loro protezione), di pari passo con la libera circolazione dei diritti, delle merci e delle persone all'interno dell'Unione, così Durst L. (2019), *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in Rocco P. (eds.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 59.

trattamento e può essere una persona fisica o persona giuridica, nonché un'autorità pubblica o una sua articolazione. Il GDPR consente il trattamento dei dati personali solo quando ciò è conforme ai principi di protezione dei dati di cui all'articolo 5, tra cui la *liceità correttezza e trasparenza* del trattamento; la *limitazione della finalità* del trattamento e la *minimizzazione dei dati*. Il principio di trattamento lecito, trasparente e corretto richiede che la raccolta e l'ulteriore trattamento dei dati personali si basino su un fondamento giuridico e che i soggetti interessati siano informati circa l'uso che viene fatto dei loro dati. Inoltre, il principio della limitazione della finalità del trattamento richiede che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e non ulteriormente trattati in modo incompatibile con tali finalità. Il principio della "minimizzazione dei dati" prescrive che i dati personali siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati. I principi fondamentali di protezione dei dati nell'art. 5 GDPR sono formulati in modo molto generale, tuttavia, e molte altre disposizioni del regolamento contengono misure di implementazione che rendono più concretamente applicabili questi principi, nella pratica. In particolare, l'art. 6 GDPR definisce quali siano i *presupposti legali* per il trattamento dei dati personali. Con specifico riferimento al settore pubblico, il regolamento autorizza il trattamento dei dati personali per l'esercizio di compiti di interesse pubblico *senza il consenso dell'interessato* quando il trattamento si basi sul diritto nazionale (oltre che su quello dell'UE). Tali atti normativi sono sottoposti a un test di proporzionalità (art. 6, par. 3) al fine di garantire che il trattamento non risulti eccedente rispetto a quanto *necessario* per il raggiungimento della finalità che lo legittimano. Le finalità per le quali i dati personali vengono elaborati forniscono quindi un importante punto di riferimento quando si applica il test di proporzionalità al fondamento giuridico su cui si basa l'operazione. Fornisce infatti una un'indicazione circa la portata effettivamente necessaria del trattamento dei dati, comprese le categorie di dati personali che devono essere trattati. Così facendo, rende possibile l'applicazione del test di proporzionalità e l'esame della liceità, correttezza e trasparenza del trattamento dei dati. Per verificare l'impatto di questi principi, prenderemo in esame due serie di requisiti che sono particolarmente importanti nell'ambito dei poteri di controllo utilizzati nell'ambito del settore pubblico. Innanzitutto, esaminiamo il principio di limitazione delle finalità e le sue implicazioni: come detto, questo principio è di importanza centrale per l'applicazione di altre misure a salvaguardia dei dati e, quindi, è un fattore chiave per l'effettiva protezione dei dati personali in generale. In secondo luogo, esaminiamo i diritti di trasparenza dei beneficiari/destinatari di strumenti di decisione, diritti che costituiscono uno stru-

mento indispensabile per garantire ai cittadini il controllo dei propri dati. Vedremo, infine, alcuni margini di manovra che il GDPR concede nell'applicazione dei principi di limitazione delle finalità e dei diritti di trasparenza dei singoli.

2. Il principio di limitazione delle finalità

Il "principio di limitazione delle finalità" (art. 5(1)(b) GDPR) richiede che i dati personali siano raccolti per finalità determinate, esplicite e legittime e non ulteriormente trattati con modalità che siano incompatibili con questi scopi. Secondo i pareri espressi nel corso del tempo dal WP29, prima, e dall'EDPB – in seguito all'entrata in vigore del GDPR – il *principio di limitazione delle finalità*[2] si basa sulla nozione che le finalità del trattamento dei dati devono essere esplicite e specifiche. Per finalità "esplicite" si intende che le finalità del trattamento dei dati personali siano chiaramente indicate, spiegate o comunque espresse in forma intelligibile. Il criterio di finalità "specifica" richiede che le finalità siano sufficientemente definite per consentire l'indicazione e l'attuazione di eventuali garanzie di protezione dei dati necessarie e per delimitare l'ambito delle operazioni di trattamento. Il titolare del trattamento deve valutare attentamente per quali finalità verranno utilizzati i dati personali e non deve raccogliere dati personali che non siano necessari, adeguati o pertinenti per le finalità cui è destinato (e legittimato) il trattamento.

Pertanto, uno scopo vago o espresso in termini eccessivamente generici risulta non adeguato con riferimento al criterio di specificità. Ora, il grado di specificazione richiede una valutazione caso per caso, un esame in cui vengono prese in considerazione tutte le circostanze rilevanti. Il WP29, ad esempio, ha fornito esempi pratici di formulazioni di finalità che considera troppo generiche: "scopi di marketing", "scopi informatici" e "ricerca futura". Tutti questi scopi condividono la caratteristica di poter essere facilmente ulteriormente specificati, fornendo maggiori dettagli: quale tipo di marketing, quale area dell'IT e quale tipo di ricerca? Questi esempi mostrano che una formulazione dello scopo non soddisferà il requisito della specificazione dello scopo se il suo campo di applicazione può essere facilmente ristretto fornendo ulteriori dettagli riguardo al campo particolare o al contesto in cui sarà applicato il trattamento. Le linee guida generali fornite dall'organo consultivo del WP29 possono essere trasposte anche con riferimento all'esercizio di compiti di interesse pubblico, quali ad esempio le misure prevenzione

[2] Cfr. Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203).

delle frodi in ambito previdenziale, oppure di prevenzione della corruzione – esempi su cui poi torneremo, più concretamente, quando analizzeremo gli impatti del *dual legality standard* nell'ordinamento nazionale. In primo luogo, il diritto nazionale di cui trattasi deve soddisfare il requisito della "finalità esplicita", stabilendo un collegamento tra il trattamento dei dati personali e le finalità perseguite. Verificando la normativa rilevante, i cittadini devono poter riconoscere che i propri dati personali sono raccolti ed esaminati ai fini di prevenzione e indagine sulle frodi. In secondo luogo, lo scopo della normativa nazionale deve soddisfare i requisiti della "finalità specifica". Alla luce degli esempi discussi sopra, si tratta di comprendere quanto specifiche debbano essere le formulazioni che individuano le finalità del trattamento, quando tali trattamenti siano strumentali all'esercizio o all'esecuzione di compiti di interesse pubblico. Questa formulazione dello scopo può essere – ad esempio – ulteriormente specificata determinando il campo della sicurezza sociale in cui si intenda operare, o quale meccanismo di contrasto alla corruzione si intende supportare, mendiate il trattamento dei dati. L'esempio dei trattamenti nel settore della sicurezza sociale è interessante, considerato che di recente è stato oggetto di numerosi casi di uso scorretto, sproporzionato quando non illecito dei dati personali degli assistiti, e dei cittadini in generale[3]. La gamma dei rischi sociali coperti è ampia, che va dalla disoccupazione e malattia (temporanee) al mantenimento dei figli, alla vecchiaia e all'assistenza sociale. Ciascuno di questi settori han caratteristiche distintive, e questo si riflette nelle condizioni che abilitano l'accesso alle prestazioni, condizioni che variano a seconda dei diversi regimi di sicurezza sociale. È importante riconoscere questa divergenza nelle condizioni di beneficio perché porta alla conclusione che le amministrazioni devono raccogliere e analizzare diversi insiemi e categorie di dati personali al fine di rilevare le non conformità rispetto ai diversi regimi previdenziali. Ad esempio:

[3] Cfr. *ex multis*, Gantchev V. (2019), "Data protection in the age of welfare conditionality: Respect for basic rights or a race to the bottom?" *European Journal of Social Security*, 21(1), 3–22. https://doi.org/10.1177/1388262719838109; Choroszewicz M., Mäihäniemi B. (2020), "Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries", *Global Perspectives*; 1(1): 12910. doi: https://doi.org/10.1525/gp.2020.12910; Wieringa M. (2023), "Hey SyRI, tell me about algorithmic accountability: Lessons from a landmark case", in *Data & Policy*, 5, E2; Hadwick D. e Lan S. (2021), "Lessons to Be Learned from the Dutch Childcare Allowance Scandal: a Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany", in *World Tax J.*, 609 ss.; Del Gatto, S. (2020), "Potere algoritmico, digital welfare state e garanzie per gli amministrati. I nodi ancora da sciogliere", in *Rivista italiana di diritto pubblico comunitario*, 6, 829-855; Costantini F., Franco G. (2019), "Decisione automatizzata, dati personali e pubblica amministrazione in Europa: verso un 'Social credit system'?", in *Istituzioni del Federalismo*, 3, 715-738.

l'amministrazione assistenziale potrebbe avere motivi legittimi per conoscere il consumo di acqua ed elettricità (o di altri beni di consumo) di un beneficiario nell'ambito di un regime basato sui bisogni (assistenza sociale), tuttavia questa informazione sarebbe completamente irrilevante in un regime di assicurazione contro la disoccupazione. Queste notazioni rimandano alla funzione essenziale del principio di limitazione della finalità, che il WP29 ha indicato come "pietra angolare della protezione dei dati". Alcune delle garanzie centrali nella normativa sulla protezione dei dati possono essere applicate efficacemente solo quando le finalità del trattamento dei dati sono specificate con sufficiente precisione. Quando si applica il test di proporzionalità rispetto ad una finalità formulato in modo molto ampio/generico – come ad esempio nel caso "indagine sulle frodi nella sicurezza sociale" – la gamma di dati che possono essere considerati pertinenti per la raccolta e l'ulteriore elaborazione è molto più ampia rispetto a definizioni di finalità più ristrette e specifiche per settore come potrebbe essere la "prevenzione delle frodi nell'assicurazione contro la disoccupazione". Adottando una legislazione che definisce le finalità in modo così generale, si ottiene l'effetto di massimizzare l'estensione dei poteri di controllo, e contemporaneamente si incide sui diritti alla protezione dei dati degli interessati, limitandoli. Tuttavia, come avremo modo di vedere, nel prossimo capitolo, analizzando il ruolo della base giuridica nell'ambito dello schema di legittimazione del trattamento dei dati personali formulato (dal GPDR) nei termini della *necessary clause*, non sempre sarà necessario che la finalità del trattamento sia esplicitamente riportata nel testo della base giuridica che assegna il compito (o il potere) all'amministrazione pubblica. Ciò comporta, come vedremo, che la finalità del trattamento potrebbe rimane implicita fino al momento di una sua concreta individuazione/perimetrazione, che potrebbe avvenire in una fase successiva alla identificazione del compito di interesse pubblico, e secondo modalità ulteriori, fermo restando il criterio di strumentalità necessaria del trattamento rispetto all'esercizio/esecuzione di tale compito

3. I diritti di trasparenza dei destinatari dei trattamenti

Come già accennato, la funzione del principio di limitazione delle finalità non è solo quella di fissare i limiti dell'ambito del trattamento, ma è anche quella di facilitare l'esercizio di alcuni diritti dell'interessato sanciti dal GDPR. Un fondamentale sistema di diritti riconosciuti all'interessato attiene alla trasparenza del trattamento dei dati, che è uno dei principi centrali del GDPR, enunciato all'art. 5, par. 1. I requisiti concreti per salvaguardare la trasparenza del trattamento dei dati possono essere reperiti nella sezione 2

del GDPR ("Informazioni e accesso ai dati personali"). Gli artt. 13 e 14 del GDPR specificano gli obblighi di informazione per i titolari del trattamento quando trattano i dati personali. La principale differenza tra le due disposizioni risiede nel loro ambito di applicazione. L'art. 13 si applica alla situazione in cui i dati personali sono raccolti *presso l'interessato*, mentre l'art. 14 riguarda i casi in cui i dati trattati non sono stati ottenuti presso l'interessato. L'art. 15 GDPR, a sua volta, stabilisce il corrispondente diritto di accesso, che garantisce l'accesso degli interessati alle informazioni relative al trattamento dei dati personali che lo riguardano. La gamma di informazioni coperte dai diritti di trasparenza degli interessati ai sensi del GDPR è ampio. I destinatari di trattamenti hanno il diritto di conoscere l'identità del responsabile del trattamento dei loro dati personali e le finalità del trattamento dei dati, nonché le categorie di dati personali oggetto di tale trattamento. Inoltre, l'amministrazione deve fornire ulteriori informazioni nei casi in cui si avvalga di un processo decisionale automatizzato (compresa la *profilazione*), ai sensi dell'art. 22: gli interessati hanno il diritto di essere portati a conoscenza dell'uso di queste tecniche e inoltre ricevere informazioni significative sulla logica coinvolta, nonché sul significato e le conseguenze previste di tale trattamento. Tuttavia, in letteratura è aperto il dibattito se tale previsione comporti la chiara affermazione di un "diritto alla spiegazione del processo decisionale automatizzato"[4]. In primo luogo, perché l'articolo 22 GDPR si applica solo nel caso in cui la decisione si basa esclusivamente su un processo integralmente automatizzato. Nel caso in cui – invece – al processo di automazione si aggiunga/si affianchi un (qualche) intervento umano, il diritto alla "spiegazione" sembra non trovare applicazione. Ed inoltre, anche nel caso in cui si tratti di una decisione automatizzata effettivamente soggetta al "diritto di spiegazione", essa è limitata ad ottenere informazioni significative solo limitatamente alla funzionalità *ex ante* del sistema, e non anche (invece) a una spiegazione *ex post* della logica utilizzata da un algoritmo per raggiungere una specifica decisione. In ogni caso, è (in gran parte) da questo nucleo di regolazione che il giudice amministrativo italiano ha derivato la (recente) formulazione giurisprudenziale di quei principi di cd. *legalità algoritmica* che reggono l'applicazione di strumenti di elaborazione automatizzata all'esercizio di funzioni pubbliche[5].

[4] Cfr. Wachter S., Mittelstadt B., Floridi L. (2017), "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", in *International Data Privacy Law*, 7/2, 76–99; Malgieri G., Comandé G. (2017), "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", in *International Data Privacy Law*, 7/4, 262.

[5] Cfr., *ex multis*, Carloni E. (2020), "I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo", in *Diritto amministrativo*, n. 2, 273-304;

4. Il cd. "margine di manovra"

Il GDPR è un testo che pone una disciplina dichiaratamente "generale", la cui adozione ha per altro richiesto il raggiungimento di soluzioni di compromesso tra esigenze contrastanti. Alcuni degli emendamenti proposti al testo iniziale sono stati chiaramente portati avanti con l'obiettivo di limitare o condizionare il campo di applicazione delle salvaguardie inizialmente proposte, anche con riferimento ai casi in cui i poteri pubblici si trovano a trattare dati personali nel perseguimento di una missione di interesse pubblico. A tale scopo, è tornata utile la risalente formula del cd. "margine di manovra". Questa formula è un portato del considerando (9) della Direttiva sulla protezione dei dati personali ("Gli Stati membri disporranno di un margine di manovra di cui potranno valersi, nell'applicazione della direttiva potranno quindi precisare nella loro legislazione nazionale le condizioni generali di liceità dei trattamenti […] nei limiti di tale margine di manovra e conformemente al diritto comunitario, potranno verificarsi divergenze nell'applicazione della direttiva e che queste potranno ripercuotersi sulla circolazione dei dati sia all'interno dello Stato membro che nelle Comunità"). Le implicazioni

Simoncini A (2019), "Profili costituzionali dell'amministrazione algoritmica", in *Riv. Trim. Diritto Pubbl.*, 2019, 4, 1145; Paolantonio N. (2021), "Il potere discrezionale della pubblica automazione. Sconcerto e stilemi (sul controllo giudiziario delle "decisioni algoritmiche")", in *Diritto Amministrativo*, 4, 813; Avanzini G. (2019), *Decisioni amministrative ed algoritmi informatici. Predominazione, analisi predittiva e nuove forme di intellegibilità*, Napoli; Ferrara R. (2019), "Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale", in *Diritto Amministrativo*, 4, 774; Civitarese Matteucci S. (2019), "«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità", in *Diritto pubblico*, 1, 5-42; Cavallo Perin R. e Alberti I. (2020), *Atti e procedimenti digitali*, in Cavallo Perin R., e Galetta D.U. (eds.), *Diritto dell'Amministrazione pubblica digitale*, Torino,119-158; Galetta D.-U. (2020), "Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia", in *Rivista italiana di diritto pubblico comunitario*, 3/4, 501; Macchia M. (2022), "Pubblica amministrazione e tecniche algoritmiche", in *DPCE Online*, 1, 51; Carullo G. (2021), "Decisione amministrativa e intelligenza artificiale", in *Diritto dell'Informazione e dell'Informatica*, 3, 431; Simoncini M. (2021), "Lo Stato digitale. L'agire provvedimentale dell'amministrazione e le sfide dell'innovazione tecnologica", in *Riv. Trim. Dir. Pubbl.*, 2, 529; Masucci A. (2020) "L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri", in *Diritto Pubblico,* 3, 943-979; Marchianò G. (2020), "La legalità algoritmica nella giurisprudenza amministrativa", in *Il diritto dell'economia*, 3, 229-258; Strinati C. (2020), "Algoritmi e decisioni amministrative", in *Foro Amm.*, 7, 1591 , fasc. 7; Azzena L. M. (2021), "L'algoritmo nella formazione della decisione amministrativa: l'esperienza italiana", in *Revista brasileira de estudos políticos*, 123, 503; nonché, sia consentito rinviare ai saggi raccolti in Ponti B. (eds.) (2022), *Gli algoritmi pubblici tra legalità e partecipazione*, Sezione monografica in *Rivista italiana di informatica e diritto*, 4, 2.

pratiche di questo "margine di manovra" ai sensi della direttiva erano inizialmente poco chiare. Nel 2003, la Corte di giustizia ha adottato la sentenza *Lindqvist*, in cui la Corte ha affrontato l'equilibrio tra la piena armonizzazione della protezione dei dati nell'UE e il "margine di manovra" per gli Stati membri in termini astratti: "È vero che la direttiva 95/46 concede agli Stati membri un margine di manovra in determinate aree e li autorizza a mantenere o introdurre regole particolari per situazioni specifiche come un gran numero delle sue disposizioni dimostrano. Tuttavia, tali possibilità dovevano essere utilizzate secondo le modalità previste dalla direttiva 95/46 e conformemente al suo obiettivo di mantenere un equilibrio tra la libera circolazione dei dati personali e tutela della vita privata"[6].

Inizialmente, il margine di manovra non era previsto nel testo del GDPR, che ruotava intorno al concetto di *piena armonizzazione*. Tuttavia, le successive modifiche hanno portato ad una riproposizione di quella stessa logica, in molti diversi settori[7], comprese le regole di individuazione dei titoli di legittimazione del trattamento dei dati personali connesso all'esercizio di funzioni pubbliche. Il considerando 10 del regolamento GDPR, infatti, che formula l'obiettivo di "assicurare una livello di protezione coerente ed elevato" che "dovrebbe essere equivalente in tutti gli Stati membri", è stato modificato per includere la formula del margine di manovra. Secondo la formulazione del considerando 10:

> Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati

[6] Cfr. Corte di Giustizia UE, causa C-101/01, *Bodil Lindqvist*, punto n. 84.

[7] "The GDPR allows diverging solutions in many of its aspects. In doing so, it creates further inconsistencies between the legal solutions at the level of Member States, thereby contributing to legal uncertainty for those affected by its rules. More than 69 opening clauses (…) open up space for different legal solutions, interpretations, and, eventually, application in practice. Opening clauses also affect the legal nature and level of harmonization of the GDPR, which is very often described by legal scholars as a directive wearing the suit of a regulation" così Miscenic E. e Hoffmann A.-L. (2020), "The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)", in *EU and comparative law issues and challenges series (ECLIC)*, 44-61, che richiamano l'ampio dibattito sviluppatosi nella dottrina tedesca circa l'effettivo grado di intensità dell'effetto di armonizzazione che il GDPR sarebbe in grado di conseguire (vedi, ivi, nota n. 39). "Die Datenschutz-Grundverordnung etabliert kein einheitliches Datenschutzrecht in der Europäischen Union, sondern eine Ko-Regulierung des Datenschutzes durch Union und Mitgliedstaaten (*Il regolamento generale sulla protezione dei dati non stabilisce una legge uniforme sulla protezione dei dati nell'Unione europea, ma una coregolamentazione della protezione dei dati da parte dell'Unione e degli Stati membri.*)", così Roßnagel A. (2017), "Gesetzgebung im Rahmen der Datenschutz-Grundverordnung", in *Datenschutz Datensich*, 41, 277.

membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE, gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

Tali indicazioni si sono poi concretizzate nell'art. 6 del regolamento, che disciplina le basi giuridiche necessarie per il trattamento dei dati personali: il terzo comma di tale articolo è stato modificato per consentire l'adozione (o il mantenimento) di leggi nazionali che "adattino l'applicazione delle regole" del GDPR. L'elenco delle regole che possono essere adattate è lungo e tocca quasi ogni aspetto del quadro dell'UE sulla protezione dei dati ("le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX.").

Nel contesto dell'articolo 6, la capacità di limitare l'applicabilità del principio di finalità è gravida di conseguenze. Questo correttivo può essere utilizzato dalle legislazioni nazionali in diverse direzioni, creando esattamente quel "margine di manovra" di cui si è detto. Ciò che non riguarda solo la portata dei poteri delle amministrazioni abilitate dalle legislazioni nazionali, ma ha anche un impatto sull'applicazione del principio di proporzionalità e sull'esercizio dei diritti alla trasparenza da parte degli interessati. In merito a quest'ultimo punto, l'art. 23 del GDPR crea un'altra limitazione notevole: quando agiscono nel perseguimento di un interesse pubblico rilevante, le legislazioni degli Stati membri possono limitare i diritti di trasparenza dell'interessato. L'articolo 23, paragrafo 1, del GDPR fornisce un elenco di aree in cui tali misure restrittive possono essere adottate. Gli emendamenti approvati in corso di elaborazione del GDPR hanno ampliato l'ambito di applicazione potenziale di questo "margine di manovra"; e così – ad esempio – "questioni fiscali" è stato cambiato in "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". Le ragioni che spiegano la riproposizione della formula del "margine di manovra" possono essere molteplici[8]. Un'opzione possibile è che il margine di manovra per gli Stati membri sia stata una risposta alle preoccupazioni per cui – con l'introduzione del GDPR – si sarebbe registrato un impatto negativo sull'elevato livello di protezione dei dati già esistente in alcuni paesi membri. Consentendo alla legislazione nazionale di specificare le regole del GDPR, questi paesi avrebbero potuto continuare a perseguire gli elevati standard già assicurati dalla legislazione nazionale. Tuttavia, il rischio è che il riconoscimento di un margine di manovra possa tradursi in un'arma a doppio taglio. Limitando l'effetto di piena armonizzazione/uniformazione del livello di protezione, il margine di manovra – che consente a determinati Stati membri di offrire uno standard di protezione più elevato – può consentire di converso l'affermazione di standard di protezione più ridotti in altri paesi (o anche in diversi contesti operativi, nel medesimo paese)[9]. Ciò che conferma, in definitiva, che con riferimento all'esercizio dei poteri pubblici, la normativa sulla protezione dei dati personali dettata dal GDPR si presta ad una applicazione capace di adattarsi ad esigenze, finalità e approcci anche molto diversificati.

[8] Cfr. de Hert P., Papakonstantinou V. (2016), "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", in *Computer Law & Security Review*, 32/2, 179-194 ("Nevertheless, an important intervention seems to have occurred during the trilogue stage: a new Article (provisionally numbered 2a) has been inserted, warranting a significant level of autonomy to Member States (…) it is understandable that Member States may wish to maintain a level of autonomy while setting the conditions for the legal grounds of "legal obligations" or "public interest", according to which personal data processing may occur regardless of individual consent within their jurisdictions", 186). Più in generale si è osservato come "The GDPR's tortuous passage over four years had been accompanied by *aggressive lobbying by corporate interests* and *by a sometimes intransigent EU Council*. Dogged by hostility and stalling tactics, the initiative often ran into trouble. At times throughout its gestation, there was a real risk that the process might collapse" (Davies S. (2016), "The Data Protection Regulation: A Triumph of Pragmatism over Principle", in *Eur. Data. Prot. L. Rev.* 290, corsivo aggiunto).

[9] "Peraltro, su vari temi, specie quelli legati all'azione dei pubblici poteri, il Regolamento ammette o richiede discipline integrative da parte degli Stati membri (v. ad esempio l'art. 6, par. 2) e dunque prefigura un quadro che potrebbe conservare un buon grado di eterogeneità", così Fonderico G. (2018), "La regolazione amministrativa del trattamento dei dati personali", in *Giorn. Dir. Amm.*., 4, 418.

5. Il GDPR come disciplina uniforme e gli spazi accordati alla differenziazione nazionale

La scelta di adottare una disciplina uniforme a livello eurounitario in materia di tutela dei dati personali (e di garanzia della loro circolazione), mediante l'opzione per l'adozione di un regolamento, in luogo della precedente direttiva, si è giustificata anche in ragione della necessità – avvertita su più fronti – di ridurre i margini di differenziazione che la direttiva lasciava aperti agli Stati membri, dal momento che la (conseguente) frammentazione del quadro normativo è stata considerata un ostacolo tanto con riferimento alla tutela effettiva dei diritti e delle libertà dei cittadini, quanto con la promozione delle condizioni per lo sviluppo del mercato unico. Tale obiettivo, tuttavia, non è stato conseguito in modo uniforme con riferimento a tutti gli aspetti normati dal GDPR, essendovene alcuni in cui è lo stesso regolamento a riconoscere spazi anche significativi di differenziazione alla legislazione nazionale (e così in qualche modo "tradendo" l'intento originario e la stessa natura della fonte utilizzata). L'ambito dei trattamenti operati nell'assolvimento dei compiti di pubblico interesse è tra quelli maggiormente interessati da questa dinamica (in parte contraddittoria), segno che si è trattato di uno degli ambiti in cui più complesso è stato il raggiungimento di un accordo[10].

Vengono in rilievo, in particolare, le seguenti disposizioni:

- L'art. 6, par. 2:

Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

- L'art. 6, par. 3:

La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

[10] Cfr. Davies S. (2016), "The Data Protection Regulation: A Triumph of Pragmatism over Principle", cit., 294: "The Regulation was originally intended to obviate the need for implementing legislation at the national level, and would thus create a harmonized framework. This aim has failed substantially. Because of the associated controversy and a lack of commitment from the EU Council, the GDPR became a creature of consensus: part Directive and part Regulation. Its recitals provide vast scope for wiggle-room by Member States".

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. *Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento*, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

Come si vede, si tratta previsioni che riguardano esclusivamente alcuni titoli di legittimazione specifici, ovvero "il trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (lett. c)) e "il trattamento necessario 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)).

Rispetto a questa clausola di apertura a legislazioni di adattamento degli Stati membri, va fatta una prima notazione: il fatto che il regolamento consenta (ma non imponga) agli Stati membri di introdurre disposizioni più specifiche al fine di determinare con maggiore precisione requisiti specifici per il trattamento, con espresso riferimento ai trattamenti di cui alle lett. c) ed e), costituisce indicazione del fatto che il regolamento può essere applicato *anche a legislazione* (degli Stati membri) *vigente*. Ciò significa che il regolamento non osta a che lo Stato membro scelga di introdurre disposizioni più specifiche, ad esempio – per quanto qui ci occupa – indicando direttamente nella legge le finalità rispetto alle quali autorizzare il trattamento dei dati personali, con riguardo a specifici compiti di interesse pubblico; ma nemmeno lo impone. Se il legislatore dello Stato membro non interviene, è lecito (ai sensi del regolamento) utilizzare come base giuridica quella già esistente, e formulare sulla base di essa una valutazione di necessità quanto al trattamento dei dati personali, valutazione idonea a sorreggere il requisito di finalità. Resta fermo, tuttavia, che vi sono casi in cui l'intervento legislativo (anche statale) può risultare necessario, in particolare qualora sia considerato necessario mettere in opera un meccanismo che richieda il trattamento di dati personali la cui finalità iniziale risulti non compatibile con quella ulteriore. In tale caso, infatti, il trattamento è lecito solo se appositamente autorizzato

dal diritto dell'unione o dello Stato membro (art. 6, par. 4). Altri casi in cui l'intervento del legislatore appare indispensabile anche con riferimento alla esplicitazione della finalità (ed anche alla tipologia) del trattamento possono dipendere dalla serietà/gravità della compressione prodotta dal trattamento stesso nella sfera giuridica dell'interessato, a cominciare proprio dalla tutela del diritto alla protezione dei dati personali (su cui vedi più ampiamente i capp. 2 e 3, *infra*).

Una più generale, ed essenziale osservazione di cui occorre tenere conto è la seguente: il fatto che alcune disposizioni del GDPR facoltizzino il legislatore degli Stati membri a normare un determinato aspetto hanno un preciso scopo/effetto, che è quello di *aprire* al legislatore statale spazi di intervento in materia che altrimenti – in assenza di tali clausole "facoltizzanti" – gli sarebbero preclusi, dal momento che – in termini di rapporti tra le fonti – il regolamento europeo non solo è direttamente applicabile, ma prevale (determinandone la disapplicazione) sulle fonti nazionali incompatibili con esso[11]. In questo senso, tali clausole valgono a definire il rapporto tra legislatore europeo del GDPR e i legislatori nazionali. Laddove questi spazi non sono aperti, la legislazione nazionale (anche quella di rango primario) può intervenire solo in esecuzione, e non ad integrazione del GDPR.

Il fatto che questi spazi siano stati aperti, con riferimento ai requisiti di legittimazione al trattamento di cui alle lett. c) ed e), sta a significare che, con riferimento a questi titoli di legittimazione soltanto, ed in particolare – per quanto qui ci interessa – con riferimento al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, i legislatori nazionali possono intervenire per integrare i requisiti di legittimazione, rispetto ad una serie molto ampia di elementi (basti verificare l'elenco degli oggetti su cui i legislatori possono intervenire, per come individuati nelle due disposizioni qui sopra richiamate). Il che ha, quantomeno, due ordini di conseguenze:

1) in primo luogo, il legislatore nazionale può legittimamente intervenire per completare il quadro generale di legittimazione al trattamento dei dati personali, ossia per definire le regole atte a legittimare l'uso/il trattamento

[11] "General and direct applicability of EU regulations can, therefore, result in the exclusion of possibility to apply Member States' national law that is in direct collision with the EU regulation. Provided that the provisions of the regulation are clearly formulated, this secondary law instrument can offer a strong harmonization effect", così Miscenic E. e Hoffmann A.-L. (2020), "The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)", cit., 47; sulle implicazioni della efficacia diretta e della generale applicabilità della fonte *regolamento*, cfr. anche Craig P. e de Burca G. (2015), *EU Law: Text, Cases, and Materials*, Oxford, 106 e ss; Lorenzmeier S. (2017), *Europarecht - schnell erfasst*, Berlin, Heidelberg, 147.

dei dati personali necessario all'assolvimento dei compiti di interesse pubblico. In altre parole, con riferimento a tale titolo di legittimazione, la competenza legislativa è effettivamente distribuita tra legislatore eurounitario (il GDPR) e legislazioni nazionali, in quanto queste ultime sono legittimate a normare tutti gli oggetti indicati all'art. 6, parr. 2 e 3, per esigenze di *adeguamento* della disciplina posta dal GDPR;

2) in secondo luogo, così facendo il regolamento apre notevoli spazi di manovra al legislatore, al fine di attrarre alla sede legislativa la definizione di una serie consistente di elementi relativi non solo alla disciplina (generale) del trattamento, ma anche quanto alla predisposizione e realizzazione dei singoli strumenti da porre a supporto dell'esercizio di compiti di interesse pubblico.

Per un verso, tutto ciò cospira ad un rafforzamento del principio di legalità, nella misura in cui il margine di manovra sia utilizzato per arricchire i presupposti e le condizioni di liceità dell'esercizio di funzioni pubbliche che comportino il trattamento di dati personali. Per altro verso, tale assetto pare richiamare una più risalente caratteristica della disciplina delle comunità europee, in termini di *deference* nei confronti del ruolo dei legislatori nazionali, quando venga in gioco la disciplina dell'organizzazione e dell'azione dei poteri pubblici amministrativi. Una sorta di riserva *di fatto* in materia di legislazione "amministrativa", che pare trovare una rinnovata applicazione anche con riferimento alla disciplina a tutela dei dati personali.

È sulla base di questa *deference*, e degli spazi di adattamento così aperti, che si concretizza la possibilità di ricostruire il vigente quadro di disciplina dei trattamenti dei dati personali per l'esercizio dei compiti di (e dei poteri) di interesse pubblico alla stregua della categoria interpretativa che definiamo con la nozione di *dual legality standard*.

2. Il trattamento finalizzato all'esercizio di compiti di interesse pubblico e la clausola di necessarietà: quale standard legale?

1. Il trattamento dei dati personali per compiti di interesse pubblico nel regime della direttiva. La clausola di necessità come vincolo al legislatore statale e come parametro di interpretazione

Prima di arrivare all'analisi del regime giuridico abilitato dal GDPR (e soggetto al facoltativo completamento/ arricchimento ad opera dei legislatori locali), è certamente utile, anzi indispensabile, inquadrare rapidamente il regime giuridico relativo al medesimo oggetto (*i.e.* il regime giuridico relativo all'uso dei dati personali ai fini dell'esercizio/esecuzione di un compito di interesse pubblico), in vigenza della Direttiva 95/46/CE. Come noto, sotto il profilo del modello regolatorio, con specifico riguardo ai principi ed agli istituti di tutela dei dati personali, la disciplina del GDPR è ampiamente tributaria del quadro normativo disegnato nella direttiva, sì che – ad esempio – i presupposti di legittimazione del trattamento disposti dal regolamento all'art. 6 risultano ampiamente coincidenti con quelli contenuti nel corrispondente art. 7 della direttiva. Tuttavia, ai fini del nostro discorso, il punto di distanza tra la direttiva ed il GDPR – ovvero la tipologia di fonte impiegata – comporta un ordine di effetti rilevantissimo. Infatti, la direttiva, per divenire applicabile[1], necessita degli atti normativi interni di recepimento. Di conseguenza, nel regime della direttiva è comunque necessario un atto legislativo

[1] "Quanto alla *diretta applicabilità*, occorre distinguere tra i due profili individuati a proposito dei regolamenti. Con riferimento al primo e cioè alla non necessità di misure di adattamento, è giocoforza affermare che la direttiva "non" gode della diretta applicabilità. Il meccanismo descritto nel comma 3 dell'art. 288 Tfue infatti richiede che la direttiva riceva attuazione da parte degli Stati membri attraverso apposite misure. A differenza di quanto avviene a proposito dei regolamenti, gli Stati membri sono tenuti ad adattare, cioè a modificare, l'ordinamento interno in modo da assicurare che il risultato voluto dalla direttiva sia raggiunto. In mancanza, la direttiva non è in grado, da sola, di ottenere il risultato voluto", così Daniele L. (2015), *Atti dell'Unione europea*, in Enciclopedia del diritto - Annali VIII, par. 8-10.

dello stato membro che traduca in normativa *interna, applicabile* le disposizioni contenute nella direttiva. Dunque, sebbene l'art. 7, comma 1, lett. e) della direttiva 95/46/CE detti il presupposto di liceità fondato sull'assolvimento dei compiti di interesse pubblico con le *stesse espressioni* che compaiono oggi nell'art. 6, comma 1, lett. e) del GDPR, l'impatto determinato dalla sistematica delle fonti è molto diverso. Nel caso della direttiva, il presupposto di liceità connesso alla clausola di *necessarietà*, per divenire efficace, deve passare per la disciplina nazionale di recepimento. La quale legislazione (nazionale), ovviamente, è soggetta ai vincoli imposti dalla direttiva. Ciò comporta – in questo caso – che il principio per cui l'esecuzione di compiti di interesse pubblico costituisce un presupposto di legittimità si traduce in un vincolo per il legislatore nazionale, che non potrà (ad esempio) escludere tale presupposto da quelli che devono essere previsti nella normativa di recepimento. Ancora, tale disposizione (della direttiva) opererà anche come canone e parametro di interpretazione della disciplina nazionale di recepimento, così producendo i propri effetti anche nei confronti degli interpreti del diritto (interno)[2]. E tuttavia, entro questi vincoli, il compito di definire lo *standard legale* cui è soggetto l'esercizio di funzioni di interesse pubblico che comporti l'uso di dati personali finisce per essere rimesso al legislatore nazionale, perché l'applicazione del presupposto di liceità *deve passare* per la declinazione (quanto a forma e modi, fermi restando gli obiettivi) da parte del legislatore interno. Gli effetti di questo riparto normativo (quello

[2] Con specifico riferimento al vincolo prodotto dalla direttiva sull'interpretazione delle disposizioni che la recepiscono, quanto ai presupposti di liceità, e in particolare di quelli connessi al trattamento per finalità di interesse pubblico, si veda quanto stabilito dalla Corte di giustizia nella causa C-524/06 ("occorre ricordare che la direttiva 95/46 mira, come risulta in particolare dal suo ottavo 'considerando', a rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. Il decimo 'considerando' aggiunge che il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità.

La Corte ha così statuito che l'armonizzazione delle suddette legislazioni nazionali non si limita ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa (v. sentenza 6 novembre 2003, causa C-101/01, Lindqvist, Racc. pag. I-12971, punto 96). Pertanto, considerato l'obiettivo di garantire un livello di tutela equivalente in tutti gli Stati membri, la nozione di necessità come risultante dall'art. 7, lett. e), della direttiva 95/46, che mira a delimitare con precisione una delle ipotesi in cui il trattamento di dati personali è lecito, non può avere un contenuto variabile in funzione degli Stati membri. Si tratta quindi di una nozione autonoma del diritto comunitario che deve essere interpretata in maniera tale da rispondere pienamente alla finalità di tale direttiva come definita dal suo art. 1, n. 1.", par. 50-52); sulla direttiva 95/46 come paradigma interpretativo, capace di produrre effetti anche al di là del suo ambito di applicazione territoriale, cfr. Zhang K. (2019), "Incomplete Data Protection Law", in *German Law Journal*, 15(6), 1071-1104.

abilitato dalla direttiva) sono di grande momento: la *necessità* di una legislazione nazionale, chiamata a tradurre, adattare e precisare il regime disegnato nella direttiva, comporta il fatto che è il legislatore nazionale a ricoprire il ruolo di *dominus* dello standard legale mediante il quale tradurre/declinare il trattamento dei dati personali a fini di esercizio di compiti di interesse pubblico. Non solo perché, nell'esercizio di questo ruolo normativo, il legislatore nazionale dispone di spazi di manovra significativi, ma soprattutto perché ciò comporta che *il parametro legale* che conforma (prima ancora, legittima) l'uso dei dati personali per l'esercizio di compiti di interesse pubblico è quello (e solo quello) definito nella legislazione nazionale. Pertanto, sotto il regime della direttiva, i legislatori nazionali hanno avuto l'agio per definire tale parametro legale, dal momento che dall'adozione della legislazione interna sarebbero dipese sia *la definizione dei requisiti di legittimazione*, sia la loro *concreta attivazione*. Insomma, sotto il regime della direttiva, lo standard legale è unico, perché definito su di un singolo piano normativo, che è quello del legislatore nazionale. In questo modo, la questione dello *standard di legalità* applicabile è *assorbita* dai parametri dell'ordinamento nazionale, è attratta inevitabilmente all'interno di questi parametri. In altre parole, con riferimento al presupposto di legittimità connesso all'esercizio di compiti di interesse pubblico, nel vigore del regime direttiva, è il legislatore interno che deve *non solo disciplinare quali sono le modalità con le quali sono definiti ed assegnati i compiti di interesse pubblico*, *ma anche declinare quali sono i presupposti e le condizioni di trattamento dei dati personali, in tali circostanze*. Pertanto, tale regime finisce per essere naturalmente attratto entro i confini del principio di legalità così come definito ed operante nell'ordinamento dello stato membro che recepisce la direttiva. È al legislatore nazionale che spetta definire fonti, requisiti, caratteri sulla base dei quali deve operare l'assegnazione dei compiti. Inoltre, tale disciplina di recepimento – formulata mediante atti legislativi interni – è destinata ad essere interpretata e sistematizzata sulla base degli istituti caratteristici dell'ordinamento in questione (principi costituzionali rilevanti, norme costituzionali, principi generali del diritto, principi di diritto amministrativo caratteristici dell'ordinamento in questione, etc.). Lo *standard legale* applicato è, e non può che essere, quello definito dal legislatore interno, e questo non può che essere coerente, non può che riflettere lo *standard legale* applicabile all'esercizio delle funzioni e dei poteri pubblici, così come definiti dall'ordinamento domestico.

È evidente che, anche in questo schema, l'influsso dell'ordinamento dell'Unione resta rilevante, sia con riferimento alla materia *de qua*, sia con riferimento all'impatto complessivo esercitato dall'ordinamento dell'Unione

sulla (ri)configurazione del principio di legalità anche nei singoli ordinamenti nazionali[3]. E tuttavia, lo *schermo* frapposto dalla *necessaria* intermediazione da parte della legislazione (interna) di recepimento contribuisce a tenere distinti i due contesti ordinamentali, così che gli istituti di tutela dei dati personali (ivi compresi i presupposti di legittimazione del trattamento) sono destinati ad essere intermediati dalla legislazione domestica, ciò che impedisce in termini strutturali che il quadro giuridico disegnato con la direttiva si configuri come di per sé sufficiente a regolamentare l'uso dei dati personali (ivi compreso quello a fini di esercizio dei compiti di interesse pubblico).

Come noto, proprio gli spazi di adattamento che sono ontologicamente connessi al meccanismo di armonizzazione della disciplina direttiva/recepimento, nonché il concreto (ampio) utilizzo che ne hanno fatto gli Stati membri, hanno condotto a quella frammentazione del quadro normativo europeo che ha finito per portare al cambio di strategia, tradottosi nell'adozione del GDPR.

Con specifico riferimento al titolo di legittimazione qui in rilievo (l'assolvimento di compiti di interesse pubblico), vale la pena notare che il margine di differenziazione/adattamento trovava una specifica e differenziale giustificazione, connessa proprio all'opportunità di riconoscere agli Stati

[3] L'impatto prodotto dalla partecipazione dell'ordinamento nazionale a quello comunitario (prima) e dell'Unione (dopo) sulla configurazione del *principio di legalità*, così come riconosciuto ed applicato nell'ordinamento nazionale (ed anche sulla sua crisi) è oggetto di studi ampi e stratificati nel tempo. Senza alcuna pretesa di completezza, ma solo a titolo indicativo, si vedano: Merusi F. (2007), "Il principio di legalità nel diritto amministrativo che cambia", in *Diritto pubblico*, 2, 427-444; Cassese S. (2017), "Verso un diritto europeo italiano", in *Riv. trim. dir. pubbl.*, 303; Cassese S. (2009), *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino; Picozza E. (1997), *Attività amministrativa e diritto comunitario*, in *Enc. giur.*, Roma, Agg. III, 23; Della Cananea G. (2011), *Diritto amministrativo europeo. Principi e istituti*, Milano; Pajno A. (2017), "*Diritto europeo e trasformazioni del diritto amministrativo*. *Alcune provvisorie osservazioni*, in *Rivista italiana di diritto pubblico comunitario*, 27/2, 467-478; Massera A., *I principi generali dell'azione amministrativa tra ordinamento nazionale e ordinamento comunitario*, in *Diritto Amministrativo*, 4, 707; Angiolini V. (1999), *Legalità dell'amministrazione interna e comunitaria*, in (eds) Pinelli C., *Amministrazione e legalità. Fonti normative e ordinamenti. Atti del Convegno, Macerata, 21 e 22 maggio 1999*, Milano; Portinaro P.P., *Il principio di legalità*, in Enciclopedia delle scienze sociali, Roma, 1996, 216 ss.; Chiti M. P. e Natalini A. (eds.) (2012), *Lo spazio amministrativo europeo: le pubbliche amministrazioni dopo il Trattato di Lisbona*, Bologna; Bassi N. (2001), *Principio di legalità e poteri amministrativi impliciti*, Milano, in spec. 220 ss.; Mattarella B. G. (2006), "Il Rapporto autorità-libertà e il diritto amministrativo europeo", in *Riv. Trim. Dir. Pubbl.*, 909- 928; Iannotta L. (2001), *Principio di legalità e amministrazione di risultato*, in *Scritti in onore di Elio Casetta*, vol. II, Napoli, 2001; Perongini S. (2004), *Principio di legalità e risultato amministrativo*, in Immordino M. e Police A. (eds.) *Principio di legalità e amministrazione di risultati*, Atti Convegno di Palermo 27-28 febbraio 2003, Torino, 39-50.

membri lo spazio nel quale tradurre la disciplina all'interno dei principi, degli istituti e delle discipline che sono propri dell'agire pubblico e che hanno (tradizionalmente) un tasso elevato di specificità nazionale connessa (in particolare, ma non solo) al carattere fortemente *nazionale* dei regimi di diritto amministrativo. Anche qui, è noto che il processo di integrazione europea (una integrazione guidata dal diritto) abbia contribuito a "ravvicinare" regimi di diritto amministrativo un tempo molto diversificati e distanti tra loro. Ma questo processo di progressivo ravvicinamento non ha condotto ad un assetto uniforme. I regimi nazionali di diritto amministrativo mantengono le loro peculiarità, margini significativi di differenziazione (connessi a tradizioni costituzionali che sono sì *comuni*, ma non anche *identiche*), ivi comprese le modalità con le quali si declina principio di legalità nei diversi contesti giuridici.

Va poi notato che in ogni caso il superamento del regime della direttiva (a ben tredici anni dalla sua adozione) ha lasciato in eredità delle legislazioni nazionali già fortemente caratterizzate, dal momento che la stessa direttiva aveva imposto loro di definire un quadro legale che desse attuazione (anche) al presupposto di liceità del trattamento connesso all'esercizio di funzioni pubbliche. In altri termini, il GDPR non opera su un terreno più o meno "vergine" (come era stato il caso della direttiva), ma si innesta su quadri regolatori già conformati (sebbene, come detto, in termini anche molto differenziati) dai medesimi principi e da analoghi istituti.

2. Il trattamento dei dati personali per compiti di interesse pubblico nel regime del regolamento

2.1. Efficacia diretta e liceità del trattamento: l'art. 6, par. 1, lett. e) come disposizione immediatamente applicabile

Come si può constatare da un agile confronto tra il testo della direttiva (art. 7, lett. e): "Gli Stati membri dispongono che *il trattamento* di dati personali *può essere effettuato* soltanto *quando* … e) *è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati*"; e quello del GDPR (art. 6, par. 1, lett. e): "*Il trattamento è lecito solo se e nella misura in cui* ricorre almeno una delle seguenti condizioni … e) il trattamento *è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*"), anche con riferimento al titolo di liceità/legittimazione all'utilizzo di dati personali per l'esecuzione di compiti

di interesse pubblico, il regolamento ha ripreso e riproposto in termini essenzialmente analoghi la medesima fattispecie, utilizzando quasi esattamente le medesime parole. L'idea di fondo è che l'esistenza di un nesso di strumentalità (necessaria) che intercorra tra l'effettuazione di un determinato trattamento e l'esecuzione di un compito di interesse pubblico integra, *di per sé*, la preliminare condizione di liceità del trattamento in questione (fatto salvo il rispetto degli ulteriori principi *sul trattamento*). Tuttavia, la (quasi) identità testuale, mediata dalla diversa fonte normativa in cui è iscritta, è destinata a produrre effetti notevolmente differenziati. Per la verità, alcuni di questi effetti sono già anticipati anche nel testo, dal momento che nella direttiva il legislatore esplicita, con la formula di apertura dell'articolo 7 ("Gli Stati membri dispongono che…"), la necessaria intermediazione da parte del legislatore nazionale, nel tradurre e recepire i requisiti di legittimità in disposizioni di diritto interno. Si tratterebbe, per la verità, di una *dictio* ridondante, proprio in ragione della circostanza per cui è la fonte in sé ad imporre l'intermediazione del legislatore nazionale. Come sottolineato nel paragrafo precedente, questa circostanza ha comportato l'attrazione del modello di tutela dei dati personali nell'orbita della signoria del legislatore interno, con specifico riferimento alla declinazione del titolo di legittimazione dei poteri pubblici e al connesso *standard legale*. In questo modo, nel modello della direttiva, spettava interamente al legislatore nazionale declinare tale titolo di legittimazione nell'ambito del *principio di legalità* così come inteso dall'ordinamento interno. Anzi, l'*intermediazione necessaria* del legislatore interno comportava, di fatto, la necessità di un intervento legislativo nazionale (o subnazionale, a seconda dei criteri di riparto del sistema ordinamentale dello specifico stato membro), con la conseguenza che – se *anche per ipotesi* il legislatore interno avesse optato per *pedissequa riproposizione del medesimo testo della direttiva*, ciò avrebbe comunque comportato l'integrazione di tale testo nel parametro legale interno, ed in ogni caso si sarebbe trattato di una opzione *disponibile*. In concreto, in tal modo, la clausola di necessarietà – tradotta (e, al limite, arricchita/completata) dal legislatore interno – si sarebbe comunque articolata in un testo legislativo destinato ad essere integrato sistematicamente all'interno dei meccanismi dommatici ed interpretativi propri di quello stesso ordinamento (interno). A conferma, si noti che il legislatore nazionale italiano, prima dell'avvento del GDPR, nel recepire la direttiva 46/95/CE ha nel corso del tempo *variamente* modulato il regime giuridico del trattamento dei dati effettuato per l'esercizio di funzioni pubbliche[4]: lo standard legale applicato è quindi parzialmente *mutato* nel tempo,

[4] In effetti, nell'immediato recepimento della direttiva, avvenuto con la l. 31 dicembre 1996, n. 675, lo standard basato sul presupposto del trattamento necessario appare variamente

ma è rimasto nella piena disponibilità del legislatore interno, e (*pro tempore*, di volta in volta) quello così formulato è stato l'unico standard legale applicabile all'esercizio delle funzioni pubbliche.

Con la trasposizione del medesimo requisito di liceità nel testo del GDPR (un regolamento UE ai sensi dell'art. 288 del Tfue), questa dinamica muta profondamente. Infatti, il regolamento – per sua stessa natura – è fonte ad efficacia diretta ed immediata. Ha effetti non nei confronti degli Stati membri (vincolati quanto al risultato, ma competenti a scegliere i mezzi per ottenerlo, entro i margini più o meno ampi, in dipendenza del dettaglio e della precisione con cui la direttiva è formulata), ma direttamente anche nei confronti di tutti i soggetti giuridici interni (allo Stato membro). Pertanto, nel caso che qui interessa, il requisito di necessità del trattamento non ha bisogno di essere tradotto in disposizioni legislative interne, ma è direttamente efficace. Al netto di quanto si dirà a seguire, a proposito del margine di adattamento accordato agli Stati membri, dunque, la clausola di *necessarietà* risulta direttamente ed immediatamente efficace. Ciò determina un diverso rapporto tra l'operatività di questa clausola ed il principio di legalità. Infatti, non è (più) in virtù delle revisioni legislative dell'ordinamento interno (in sede di recepimento della direttiva) che il trattamento necessario per l'esecuzione di compiti di interesse pubblico è autorizzato come lecito, ma lo è (*lecito*) per

articolato: con riferimento ai dati personali di versi da quelli sensibili, il requisito è così declinato: *"*il trattamento di dati personali da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti" (art. 27, comma 1, mentre al comma 2 è disposta la disciplina differenziale per il trattamento che consista nella comunicazione o diffusione), una formulazione che lascia ampio spazio di dispiegamento dello standard legale fondato sul principio di legalità, anche in considerazione del fatto che l'attribuzione del *potere* di trattare i dati personali giustificata dalla strumentalità del trattamento all'esercizio delle funzioni istituzionali è comunque operata *dal legislatore*; il parametro della necessarietà fa capolino con riferimento alla specifica disciplina del trattamento che consiste nella comunicazione o diffusione del dati (sempre da parte dei soggetti pubblici), trattamento che è giustificato solo se previsto da una espressa norma di legge o di regolamento, oppure se "comunque" necessario per lo svolgimento delle funzioni istituzionali (ma in questo caso va notificato al Garante, che può disporne il divieto: cfr. art. 27, comma 2). Con l'adozione del "Codice in materia di protezione dei dati personali", ad opera del d.lgs. 30 giugno 2003, m 196 (di qui in avanti "Codice"), tale disciplina viene in parte integrata, precisando la portata del presupposto di legittimazione del trattamento dei dati personali comuni operata da sotti pubblici ("Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente") ciò che comporta la declinazione della clausola di *necessarietà* con riferimento al trattamento dei dati effettuato per fini istituzionali all'interno di una stessa amministrazione.

effetto diretto della disposizione del regolamento[5]. Ciò comporta una *riconfigurazione* delle modalità in cui il principio di legalità opera, con riferimento all'esercizio delle funzioni e dei compiti di interesse pubblico che comportano *necessariamente* l'utilizzo di dati personali. Per verificare i termini di questa riconfigurazione, occorre prima chiarire in che termini il principio di legalità è chiamato in causa.

2.2. Presupposti del trattamento dei dati e principio di legalità: clausola di necessarietà e modalità di trattamento

Come noto, la tutela dei dati personali costituisce un diritto fondamentale della persona umana, sia in virtù dell'interpretazione evolutiva di altri diritti fondamentali (privacy, dignità personale, libertà personale, etc.), sia in ragione dell'esplicito, specifico riconoscimento di tale diritto nell'ambito della carta dei diritti fondamentali dell'Unione europea (art. 8)[6]. L'insieme dei dati personali di ciascuno, dunque, ricade all'interno di un'area di protezione che afferisce direttamente alla tutela di tali informazioni e indirettamente (per suo tramite) alla tutela di molteplici diritti della personalità[7]. Non è necessario, ai nostri fini, addentrarci nella risalente diatriba relativa al carattere autonomo (o meno) della tutela assicurata ai dati personali, ovvero se questa si

[5] "Alle pubbliche amministrazioni, dunque, il conferimento sulla base del diritto dell'Unione o dello Stato membro del compito di perseguire un interesse pubblico, che di per sé indica pure la finalità generale del trattamento, attribuisce anche la possibilità di effettuare i trattamenti di dati necessari per l'esecuzione di tale compito, ovviamente nel rispetto delle disposizioni del GDPR, ma senza bisogno che ogni trattamento sia preventivamente e ulteriormente individuato come adempimento di un obbligo legale", così Bombardelli M. (2022), *Dati personali (Tutela)*, in Mattarella B.G. e Ramajoli M., *Funzioni amministrative* - Enciclopedia del diritto - I tematici, Milano, III, 360.

[6] In dottrina la tutela dei dati viene ricondotta ad un «unico valore costituzionale rappresentato dalla protezione della persona nella sua integrità fisica e morale, nella sua proiezione spaziale e nel modo di relazionarsi con altri soggetti, così da garantire il libero e completo svolgimento della sua personalità» (così Scagliarini S. (2013), *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013, 108); cfr. Rodotà S. (2009), *Data Protection as a Fundamental Right*, in Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds), *Reinventing Data Protection?*, Springer.

[7] Cfr. Bygrave, L. (2014), *Data Privacy Law—An International Perspective*, Oxford; Id. (2002), *Data Protection Law—Approaching Its Rationale, Logic and Limits*, The Hague; Tavani, H. (2008). *Informational Privacy: Concepts, Theories, and Controversies*, in Himma K. e Tavani H. (eds.), *The Handbook of Information and Computer Ethics*, Indianapolis, 131-164; Rodotà S. (2004), "Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy", in *Europa e diritto privato*, 1-10; Id (1991), ""Privacy" e costruzione della sfera privata. Ipotesi e prospettive", in *Politica del diritto*, 4, 521-546; G. Buttarelli G. (1997), *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Milano;

giustifichi (ed acquisti rilievo) solo nella misura in cui risulti strumentale alla tutela di un diritto/di un bene ulteriore, ovvero se i dati personali siano tutelati *in quanto tali* a prescindere dalle ricadute ulteriori conseguibili. Oppure, secondo una differente prospettiva, se il consenso all'uso dei dati da parte dell'interessato costituisca l'esercizio di un più complessivo diritto all'autodeterminazione informativa, quale dimensione di estrinsecazione della dignità e della libertà personale, o piuttosto l'elemento di un negozio diretto volto ad abilitare la partecipazione dell'interessato alle dinamiche di sfruttamento commerciale connesse al trattamento dei dati[8]. Qui interessa invece sottolineare come, in ogni caso, il dato personale si manifesta (ed è assunto dall'ordinamento) come proiezione della soggettività personale, un elemento costitutivo della sfera soggettiva e come tale oggetto, per un verso, di protezione rispetto ad intrusioni/appropriazioni/usi non autorizzati e dall'altro suscettibile di disposizione da parte dell'interessato. Entro queste coordinate, l'uso – *rectius*, il *trattamento* – dei dati personali (altrui) si configura in via di principio come una compressione o comunque una limitazione della sfera soggettiva personale, e – in accordo con l'architettura di tale diritto per come consacrata nella carta dei diritti fondamentali dell'UE – per poter essere *lecita* necessita o del consenso dell'interessato, o – altrimenti – di un fondamento legittimo *previsto dal diritto.* I presupposti di liceità di cui all'art. 6 (e di cui all'art. 9 e 10, per quanto riguarda i dati particolari e giudiziari) fanno applicazione di questo schema, secondo moduli differenziati. Accanto al presupposto del consenso, in tutti gli altri casi lo schema di liceità del trattamento si articola a partire dalla clausola di *necessarietà*: sempre, cioè, il trattamento è lecito solo nella misura in cui si configura come *necessario* per la realizzazione dell'attività in vista della quale tale trattamento viene effettuato (*finalità del trattamento*), tale attività potendo consistere, a seconda del titolo

[8] Cfr., ad esempio, Lynskey O. (2015), *The foundations of EU data protection law*, cit. 231 ss., dove si argomenta che la prospettiva dei *property rights* costituirebbe un quadro concettuale utile a rafforzare la dimensione dell'autodeterminazione personale; ma v. anche, *ex multis*, Thouvenin, F. (2021), "Informational Self-Determination: A Convincing Rationale for Data Protection Law?", in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 4/246-257; Yu X., Zhao Y. (2019), "Dualism in data protection: Balancing the right to personal data and the data property right", in *Computer Law & Security Review*, 35/5; Sattler, A. (2018), *From Personality to Property?*, in Bakhoum, M., Conde Gallego, B., Mackenrodt, MO., Surblytė-Namavičienė, G. (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law, vol 28. Berlin, Heidelberg. Sulla tutela dei dati personali come *diritto fondamentale*, cfr. González Fuster G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, New York; Richards N. M. (2015), "Why Data Privacy Law Is (Mostly) Constitutional/ The Contemporary First Amendment: Freedom of Speech, Press, and Assembly Symposium", in *William & Mary Law Review*, 56, 1501-1532.

di legittimazione in questione, nell'esecuzione di un contratto, nell'adempimento di un obbligo legale, nella salvaguardia di interessi vitali, nell'esecuzione di un compito di interesse pubblico, nel perseguimento del legittimo interesse del titolare del trattamento (che costituiscono le categorie di finalità del trattamento suscettibili di legittimare il trattamento di dati personali). Analogo è lo schema relativo alla liceità del trattamento dei dati particolari, sebbene le condizioni legittimanti risultino appesantite/rafforzate. In particolare, anche nell'ambito dell'art. 9, domina – accanto al presupposto del consenso – la clausola di *necessarietà* del trattamento.

Ora, è bene notare che la clausola di *necessarietà* designa un requisito esterno rispetto ai contenuti, ai caratteri, alle specifiche caratteristiche del trattamento (così autorizzato/legittimato). In virtù di tale clausola, dato un trattamento – *quale che esso sia* – esso risulterà lecito se risulti necessario per il perseguimento di una finalità che rientri nel novero di almeno una delle categorie-presupposto indicate all'art. 6 (par. 1, lett. b)-f)), ovvero all'art. 9 (par. 2, lett. b), c), f)-j). In altri termini, la clausola di *necessarietà* non dice nulla (e non impone nulla) a proposito del *trattamento*. I vincoli relativi alle *modalità* con cui deve essere effettuato il trattamento – infatti – si trovano altrove: nelle disposizioni che recano i principi sul trattamento (l'art. 5, in particolare[9]), o – ad esempio – laddove si pongono limiti e condizioni a quella specifica *modalità* di trattamento identificato nel *trattamento automatizzato* (art. 22), ovvero in tutte le altre disposizioni (a cominciare da stessi art. 6, 9 e 10) che contemplano la clausola di necessarietà, ma dispongono anche ulteriori casi, condizioni, modalità. In altre parole, il GDPR reca una quantità varia e diversificata di *vincoli modali* inerenti al trattamento dei dati personali, e tuttavia tali vincoli – che risultano caratteristici del regime di tutela – non compaiono, non sono contemplati, non integrano i presupposti di *liceità* delineati all'art. 6 (e all'art. 9). Si tratta di un elemento rilevante. Secondo questa impostazione, laddove il presupposto di liceità poggia sulla clausola di necessarietà, tale presupposto non attiene *alle modalità* con le quali il trattamento è effettuato: a questi fini, le modalità di trattamento sono indifferenti. Ciò che rileva è, invece, se il trattamento sia o meno *necessario*,

[9] Rilevano, in particolare, il par. 1, lett. a) ("I dati personali sono: (…) trattati *in modo* lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»"); il par. 1, lett. e) ("I dati personali sono: (…) 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 (…)") il par. 1, lett. f) ("I dati personali sono (…) trattati *in maniera* da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»"), corsivi aggiunti.

in vista della realizzazione di questa o quella tra le categorie di finalità contemplate nell'art. 6 e nell'art. 9. Pertanto, la clausola di *necessarietà* opera nel senso di abilitare (rendere lecito, in via di principio) il trattamento dei dati personali *a prescindere dalle specifiche modalità con le quali esso è effettuato*.

Il trattamento, dunque, rileva solo in relazione alla connessione strumentale con la finalità. La declinazione dei presupposti di liceità fissa un *valore soglia* di questa connessione: deve trattarsi di un trattamento *necessario* (e non solamente *utile*, oppure *non incompatibile*). Ma quale trattamento sia effettuato (a questi fini), non rileva.

2.3. Principio di legalità e clausola di necessarietà: lo schema del GDPR

Il trattamento dei dati personali consiste nell'effettuazione di una o più delle operazioni (anche in combinazione tra loro) indicate in via esemplificativa all'art. 4, n. 2): ciascuna di queste operazioni si configura come una intromissione, limitazione o comunque alterazione della sfera soggettiva dei soggetti interessati dal trattamento[10]. Schematicamente, qualora un'intromissione/compressione/limitazione sia operata da un soggetto pubblico, per il

[10] "La l. n. 675 invece, *tutela i dati personali indipendentemente* dalla loro comunicazione e diffusione, *dalla possibilità stessa della lesione del valore sociale dell'individuo*. Oggetto della norma è qualsiasi attività che riguardi i dati personali;(…) La legge ritiene, infatti, che qualsiasi attività che abbia per oggetto dati personali, anche se non comunicati e diffusi, *può conferire a chi la effettua un potere che occorre disciplinare*; che occorra salvaguardare non tanto il prestigio sociale della persona, quanto piuttosto la sua libertà rispetto al potere informatico", così Giannantonio E. (1999), *Dati personali (tutela dei)*, in *Enciclopedia del diritto*, agg. III, par. 1 (corsivi aggiunti). Con specifico riferimento alla pretesa di tutela dei dati trattati a fini di interesse pubblico, cfr. Carullo G. (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*, 1, 131 ss.: "Si può perciò affermare che, nella prospettiva dell'interessato, ed ai fini che qui interessano, il bene della vita tutelato dal Regolamento siano i dati personali e la relativa capacità dispositiva sugli stessi. In altri termini, il Regolamento riconosce l'esistenza di un interesse a un bene della vita consistente nel poter decidere, salvo specifiche eccezioni, se e come i propri dati personali possano essere trattati da terzi, e per quali fini. Ciò significa che nei casi in cui un'autorità pubblica tratti dati personali sulla base della condizione di liceità di cui all'art. 6, lett. e), l'interessato è titolare di una serie di diritti e prerogative atte a consentirgli di esercitare la propria capacità dispositiva in ordine ai propri dati personali (…) Se ne deve concludere che, per quanto sin qui detto, nei casi di trattamento ai sensi dell'art. 6, par. 1, lett. e), la posizione giuridica soggettiva nascente tra l'interessato ed il titolare a seguito del trattamento di dati personali risulti autonoma rispetto alle attività amministrative che si basino su detti dati", *ivi* 149.

perseguimento dei compiti di interesse pubblico[11], secondo il canone tradizionale imposto dal principio di legalità essa risulta (*risulterebbe*) lecita nella misura in cui la legge/l'ordinamento *la preveda* e *la autorizzi*. In particolare, il principio di tipicità (quale corollario del principio di legalità), impone che l'atto autoritativo/imperativo possa legittimamente incidere (comprimendola/limitandola) sulla sfera giuridica dei destinatari dell'azione amministrativa solo se l'ordinamento ha conferito un potere idoneo a produrre tale effetto (in *forme* tipiche e secondo *modalità* tipiche di esercizio) all'amministrazione che agisce. Se consideriamo ciascun trattamento come una compressione/limitazione della sfera giuridica degli interessati, e lo inquadriamo nella matrice del principio di legalità, ci accorgiamo immediatamente che lo schema disegnato della clausola di *necessarietà* non si accorda con questa matrice. Infatti, mentre il principio di legalità impone che il potere sia conferito secondo modalità tipiche (quale potere viene conferito? quale limitazione della sfera giuridica è autorizzata? secondo quali forme?) nel caso del trattamento dei dati personali, ciò che rileva (per rendere lecito il trattamento) non attiene alla sua forma, al tipo di limitazione/compressione subito dall'interessato, ma ad un aspetto ulteriore e diverso: l'attitudine del trattamento in questione (quali che ne siano le forme, le qualità, le modalità) a consentire il conseguimento di una determinata finalità, secondo un nesso di strumentalità declinato nei termini della *necessarietà*.

Le conseguenze sono di grande momento. Il titolo di legittimazione disegnato dall'art. 6, par. 1, lett. e) è disposto in modo specifico per i trattamenti di dati personali finalizzati all'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui siano investiti i titolari del trattamento. Entro queste coordinate, pertanto, *il trattamento dei dati personali compiuto da soggetti investiti di poteri pubblici o dell'esecuzione di compiti di interesse pubblico non appare attratto entro lo schema tipico del principio di legalità*. Non risponde cioè allo schema per il quale la disciplina normativa attribuisce un potere tipico, per forme, effetti e modalità di esercizio. Piuttosto, risponde ad uno schema differente, uno schema nel quale il tipo di potere esercitato (quella quota di *potere*, quale intromissione/compressione/limita-

[11] In modo tutto sommato coerente con questa impostazione, da parte di alcuno si è inquadrata la situazione giuridica vantata dall'interessato nel rapporto con il titolare che tratta i dati personali in base al presupposto di cui all'art. 6(1)(e) GDPR, alla stregua dell'interesse legittimo: cfr. Carullo G. (2020), "Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato", cit.: "Si può perciò ritenere che, quantomeno in tutti i casi in cui il potere di trattare dati personali coattivamente non sia interamente predeterminato dal legislatore, la posizione giuridica soggettiva rinvenibile in capo all'interessato sia qualificabile, nella prospettiva del nostro ordinamento, quale interesse legittimo",141.

zione della sfera giuridica altrui che si manifesta nel *trattamento di dati personali*, senza il consenso dell'interessato) è reso lecito dalla norma in virtù *non di un'esplicita attribuzione*, ma in ragione della operatività della *clausola di necessarietà*. Il soggetto investito dell'esecuzione di un compito di interesse pubblico o dell'esercizio di un potere pubblico, *per ciò solo* è *anche investito del potere* di (è autorizzato ad) eseguire quei trattamenti di dati personali che risultino strumentali – *sub specie* della *necessarietà* – a tali fini[12]. Quali siano questi trattamenti, che forma e che modalità assumano, sono elementi che non assumono rilievo, ai fini della configurazione del presupposto di liceità della loro effettuazione.

2.4. Clausola di necessarietà e poteri impliciti

Lo schema descritto è quindi diverso da quello tipico del principio di legalità, nella sua configurazione classica, e tutt'ora dominante. Piuttosto, il modo con il quale la clausola della *necessarietà* assegna il potere ricalca abbastanza fedelmente lo *schema finalistico* proprio di un *potere implicito*. Con questa espressione, si fa riferimento a quella categoria di fattispecie nelle quali l'attribuzione del potere non avviene in modo esplicito da parte della norma (il potere non è *nominato* dalla fattispecie), ma viene invece desunto dall'interprete (*implicito*) in quanto la relativa disponibilità in capo all'agente si giustifica *perché necessaria* per il conseguimento degli scopi, degli obiettivi, delle finalità traguardate dalla stessa norma. Come noto, la nozione di potere implicito, di derivazione nord americana e che ha conosciuto notevole fortuna – ad esempio – nel sistema di riconoscimento di poteri e competenze in capo alle istituzioni della Comunità (economica) europea, prima, e dell'Unione, in seguito, è oggetto di ampio dibattito – in dottrina e in giurisprudenza – proprio perché – nella sua formalizzazione più asciutta (*l'amministrazione dispone di tutti i poteri che risultano necessari per il conseguimento delle finalità affidatele dall'ordinamento*) – essa risulta incompatibile

[12] Circa le origini dello schema insito nella *clausola di necessarietà*, da reperirsi nella *Necessary and Proper Clause*, della Costituzione statunitense, come mediata dalle clausole sui poteri impliciti delle istituzioni della comunità europea, cfr. Calvano R. (2006), *I poteri impliciti comunitari. L'art. 308 TCE come base giuridica per l'espansione dell'azione comunitaria*, in Mangiameli S. (eds.), *L'ordinamento europeo. L'esercizio delle competenze*, Milano, 100 ss.; nonché Skunbiszewski K. (1989), *Implied powers of International Organizations*, in *International Law at a time of Perplexity, Essays in Honour of S. Rosenne*, Dordrecht-Boston-Londra.

con i requisiti minimi imposti dal principio di legalità[13]. Tale principio, infatti, si contraddistingue proprio perché esige che il potere sia esplicitamente identificato dalla legge per essere assegnato in esercizio all'amministrazione (principio di attribuzione, *nominatività*) e sia dalla legge almeno in parte (ma in termini sostanziali) delimitato quanto alle forme, alle condizioni ed ai modi del suo esercizio (principio di *tipicità*). La clausola della *necessarietà* contraddice certamente il principio di attribuzione, nella misura in cui *per definizione* non identifica *ex ante* il potere da esercitarsi, rimettendone la determinazione ad una decisione *ex post*, o comunque contingente, strettamente correlata alle specifiche caratteristiche ed esigenze del caso concreto, in relazione alla finalità attribuita. Meno acuto può risultare il profilo di contrasto connesso al rispetto del principio di tipicità, quantomeno per quanto concerne le *forme* e le *procedure* di esercizio del potere, in dipendenza di un regime residuale ed immanente che regoli le modalità di esercizio del potere, come nel caso di una disciplina generale sul procedimento (sebbene anche questa considerazione vada diversamente calibrata con riferimento all'esercizio di poteri *normativi* – come distinti da quelli *provvedimentali* – il cui esercizio appare meno presidiato in termini di garanzie procedimentali). Nell'ordinamento nazionale, come noto, il problema dei *poteri impliciti* si è posto con particolare evidenza con riferimento a quelle figure organizzative specifiche e peculiari che rispondono allo schema soggettivo della *autorità amministrative indipendenti*, e sotto il correlato profilo funzionale, al modello della funzione di *regolazione* (e di regolazione dei mercati, in particolare). Come noto, proprio con riferimento alla opportunità di riconoscere a questi soggetti – tecnicamente qualificati – lo spazio di manovra utile e necessario per adattare gli strumenti di regolazione di ambienti e mercati complessi ed in continua evoluzione, si è affermata l'esigenza di assegnare funzioni formulate per obiettivi di ampia portata (il mantenimento delle corrette

[13] Sui poteri impliciti in relazione ai requisiti e alle esigenze del principio di legalità, si veda Bassi N. (2001), *Principio di legalità e poteri amministrativi impliciti*, cit.; Morbidelli G. (2007), "Il principio di legalità e i c.d. poteri impliciti", in *Diritto amministrativo,* 4, 723 ss.; Spuntarelli S. (2023), *Poteri impliciti*, in Ruotolo M. e Cartabia M. (eds), *Potere e Costituzione* – Enciclopedia del diritto-I tematici, Milano, V; Manfredi G. (2021), *Legalità procedurale*, in *Diritto amministrativo*, 4,749 ss; Gemmi A. (2021), "Il principio di legalità tra "authorities" e "golden power": quale spazio per i poteri impliciti", in *Rivista Italiana di Diritto Pubblico Comunitario*, 2, 365-397; Giardina A. (1975), *The rule of law and implied powers in the European communities*, in *The Italian Yearbook of International Law*, 99-111, nonché, Pantalone P. (2020), "Regolazione indipendente e anomalie sostenibili al cospetto delle matrici della legalità", in *P.A. Persona e Amministrazione*, I, 446 ss.; Ramajoli M. (2018), "Consolidamento e metabolizzazione del modello delle Autorità di regolazione nell'età delle incertezze", in *Rivista della regolazione dei mercati*, 2, 17 ss.; Pantalone P. (2018), *Autorità indipendenti e matrici di legalità*, Napoli.

condizioni concorrenziali di mercato, la tutela dei consumatori, la trasparenza del mercato azionario, la tutela di risparmiatori ed investitori, etc.), corredate dalla attribuzione di poteri generici (spesso coincidenti con la finalità da perseguire), solo parzialmente dettagliati, a volte innominati[14]. È in tale contesto, in particolare, che pur a fronte dei dubbi e delle riserve sollevati in dottrina, sono stati perimetrati i criteri di ammissibilità dell'esercizio da parte di questi soggetti di ipotesi concrete di *poteri impliciti*. Per un verso, il legittimo esercizio di questa tipologia di poteri (a fronte di un corredo legislativo carente sotto il profilo dei requisiti di nominatività e tipicità) è stato condizionato ad un recupero sul *fronte procedimentale* (in termini di legittimazione) di quanto strutturalmente mancante sul piano soggettivo (dal momento che l'indipendenza comporta un disconnessione delle autorità dal circuito dell'indirizzo politico e della responsabilità politica e politico-amministrativa), sebbene più di recente il giudice amministrativo abbia formulato delle riserve esplicite in ordine alla capacità della legalità procedimentale di sopperire in modo pieno al deficit di legittimazione *democratica* delle autorità[15]. Per altro verso, si è variamente argomentato che i poteri impliciti sono

[14] Sul punto, la letteratura è davvero amplissima: senza alcune pretesa di esaustività, ma solo in termini esemplificativi, si rinvia a: Predieri A. (1997), *L'erompere delle autorità amministrative indipendenti*, Firenze, 1997. Cerulli Irelli V. (1993), *Premesse problematiche allo studio delle 'amministrazioni indipendenti'*, in *Mercati e amministrazioni indipendenti*, Bassi F. e Merusi F., Milano, 3 ss.; Amato G. (1997), *Autorità semi-indipendenti ed autorità di garanzia*, in *Riv. trim. dir. pubbl.*, 1997, 645 ss.; Franchini C. (1988), "Le autorità amministrative indipendenti" in *Rivista trimestrale di diritto pubblico*, 3, 539 ss., Casavola F. P. (1997), *Quale 'statuto' per le Autorità indipendenti*, in Amato G. (eds.), *Regolazione e garanzia del pluralismo*, Milano, 18 ss.; Cassese S. (1996), "Poteri indipendenti, Stati, relazioni ultrastatali", in *Foro it.*, V, 7 ss.; Merusi F. (2000), *Democrazia e autorità indipendenti. Un romanzo 'quasi' giallo*, Bologna; Clarich M. (2001), *Un approccio 'madinsoniano'*, in Grassini F. A. (eds.), *L'indipendenza delle autorità*, il Mulino, 92 ss.; Merloni F. (1997), "Fortuna e limiti delle cosiddette autorità amministrative indipendenti", in *Pol. Dir.*, 639 ss.; Nissolai S. (1996), *I poteri garanti della Costituzione e le autorità indipendenti*, Pisa; Passaro M. (1996), *Le amministrazioni indipendenti*, Torino; Perez R. (1996), "Autorità indipendenti e tutela dei diritti", in *Riv. trim. dir. pubbl.*, 115 ss.; Pericu G. (1996), "Brevi riflessioni sul ruolo istituzionale delle autorità amministrative indipendenti", in *Diritto amministrativo*, 1 ss; D'Alberti M. (1995), *Autorità indipendenti (dir. amm.)*, in *Enc. giur.*, IV, Roma; Longobardi N. (1991), *Le 'amministrazioni indipendenti': profili introduttivi*, in *Scritti per Mario Nigro*, II, 73 ss.; Manetti M. (1994), *Poteri neutrali e Costituzione*, Milano; Massera A. (1988), *'Autonomia' e 'indipendenza' nell'amministrazione dello Stato*, in *Studi in onore di M. S. Giannini*, III, Milano, 449 ss.; Piga F. (1987), "Modernizzazione dello Stato: le istituzioni della funzione di controllo", in *Foro amm.*, I, 809 ss.,

[15] Cfr. Consiglio di Stato, VI. 14 dicembre 2020, n. 7972 (*Telecom e Vivendi vs. Consob*) ("E' bene precisare che la descritta funzione di "compensazione" non comporta un pieno recupero del fondamento democratico della legalità, in ragione della non omogeneità tra predeterminazione legislativa sostanziale delle regole e partecipazione procedimentale, ma assicura un maggiore livello di garanzie per il privato", par. 3.1.1.), con nota di Gemmi A. (2021), *op. cit.*

ammissibili solo se il loro esercizio (e, prima ancora, la loro spettanza) risulta strumentale all'esercizio di un altro potere (esplicitamente conferito)[16]. Dunque, entro questa lettura, è la connessione di strumentalità con altro potere (esplicito, cioè positivamente attribuito) a rendere legittimo il ricorso all'esercizio di poteri *desunti*, e quindi impliciti. Secondo questa lettura, diversamente, qualora la giustificazione del potere implicito fosse da reperirsi esclusivamente nella connessione strumentale (sebbene sotto il profilo della *necessarietà*) al perseguimento di finalità, scopi, obiettivi – pure delineati e assegnati dalla legge: nei termini della declinazione della cd. *legalità-indirizzo* – essa risulterebbe inammissibile, perché dischiuderebbe le porte all'arbitrarietà di un potere in grado di giustificare sé stesso, in ragione delle esigenze dettate dallo *stato delle cose.* Pur consapevoli delle diverse sfaccettature in cui la questione dei poteri impliciti si è posta tradizionalmente nel nostro ordinamento – anche in considerazione della circostanza per cui il dibattito più recente è in parte condizionato dalle peculiarità proprie del modello organizzativo e funzionale delle autorità (indipendenti) di regolazione, e dai connessi, specifici (nonché, problematici) profili di *legittimazione* – è qui sufficiente sottolineare come – ai sensi dell'interpretazione prevalente dei profili di compatibili con principio di legalità – acquista rilievo la circostanza che il potere implicito sia giustificato *dalla connessione strumentale all'esercizio di altro potere* (esplicitamente attribuito) o solo in ragione della strumentalità (necessaria) al conseguimento degli obiettivi assegnati all'amministrazione. Tale distinzione, infatti, pare trovare una qualche significativa corrispondenza nella descrizione delle attività in ragione delle quali è formulato il requisito di legittimazione di cui all'art. 6, par. 1, lett. e) del GDPR. Nell'identificare le attività "pubbliche" che ricadono nell'ambito di questa fattispecie, in effetti, il regolamento fa distinto riferimento, da una parte, all'esecuzione di un *compito di interesse pubblico*, e dall'altra, (all'esecuzione di un *compito connesso*) *all'esercizio di pubblici poteri*, di cui sia investito il titolare del trattamento. Ciò che sembra distinguere tra loro le due sub-fattispecie sembra essere proprio la circostanza che il compito di interesse pubblico sia corredato, o meno, anche dall'attribuzione di un *pubblico potere*[17]. Per entrambe queste fattispecie, vale la connessione di strumentalità necessaria quale requisito di legittimazione del trattamento di dati personali.

[16] Per la ricostruzione dottrinale dei modelli di giustificazione delle diverse ipotesi di potere implicito, si v. Bassi N. (2001), *Principio di legalità e poteri amministrativi impliciti*, cit. e Morbidelli G. (2007), "Il principio di legalità e i c.d. poteri impliciti", cit.

[17] Riprende questa distinzione, e ne trae significative indicazioni, ad esempio, Carullo G. (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*, cit., *passim*.

Nella misura in cui qualsiasi trattamento dei dati personali si configura – quale effettivamente risulta essere – come una interferenza nella sfera soggettiva degli interessati, esso può pertanto risultare legittimo – se agito per il perseguimento di interessi pubblici, in accordo ai criteri del principio di legalità-indirizzo – solo se inquadrato come manifestazione dell'esercizio di un *potere*[18], e come tale soggetto ai criteri di legittimazione derivanti dal principio di legalità (garanzia). Tale potere (quello speso nel trattamento dei dati personali ai fini dell'esercizio di compiti di interesse pubblico) si declina *però* secondo lo schema del *potere implicito*, dal momento che esso non risulta attribuito esplicitamente dalla norma, ma assegnato in modo *innominato*: sono leciti tutti i trattamenti che risultino *necessari* all'esecuzione di un compito di interesse pubblico ovvero connessi all'esercizio di pubblici poteri.

Pertanto, ciò che si può osservare – per il tramite dell'inquadramento della clausola di necessarietà entro le coordinate del potere implicito – è che la configurazione dei requisiti di liceità per il trattamento dei dati personali a fini di esercizio di compiti di interesse pubblico non risulta del tutto allineata ai criteri di ammissibilità dei poteri impliciti alla luce del principio di legalità, per come declinati dalla giurisprudenza amministrativa nazionale. Si configura, in sintesi, un disallineamento tra i criteri di legittimazione del trattamento dei dati personali ai fini dell'esercizio dei compiti di interesse pubblico, così come identificati nel GDPR, e i criteri di legittimazione di tali trattamenti, letti alla luce del principio di legalità. È (anche) in ragione di questo disallineamento che si articola la lettura, proposta in questo lavoro, in termini di duplice standard di legalità.

[18] Sul trattamento dei dati personali da parte delle amministrazioni pubbliche come fattispecie di esercizio del potere, cfr. *ibidem*: "il trattamento di dati personali è ad esempio strettamente necessario per lo svolgimento di una determinata funzione pubblica, il che quindi giustifica la raccolta degli stessi anche coattivamente attraverso l'acquisizione d'ufficio in forza del principio inquisitorio (…) In tali casi *il soggetto interessato è spogliato della possibilità di autodeterminarsi* in ordine al rilascio del consenso", 138 (corsivi aggiunti).

3. Il dual legality standard *e la sua concreta declinazione*

1. Perché mettere a tema uno standard legale duale?

La ricostruzione del regime di trattamento dei dati in termini di *dual legality standard*, con riferimento al regime derivante dal GDPR, muove da due considerazioni, una di carattere storico-positivo e l'altra di carattere sistematico-applicativo. Sul piano storico-positivo, occorre considerare il fatto che il regolamento europeo mira a costruire un *framework* normativo destinato a sostituire quello determinato dall'adozione della precedente direttiva 95/46/CE e dal suo recepimento nei diversi ordinamenti degli Stati membri. Come si è visto, per altro, sul piano dei contenuti (e con particolare riferimento alla identificazione dei presupposti di liceità del trattamento) il regolamento risulta molto fedele alla disciplina precedente. Nella vigenza della direttiva, tuttavia, proprio il momento del recepimento aveva costituito l'occasione per "integrare" il sistema di tutela dei dati personali nell'ambito di ciascun sistema legislativo nazionale. L'esito di questo "momento" è stata una significativa differenziazione delle legislazioni nazionali. Al momento dell'entrata in vigore del regolamento – pertanto – coesistono sul territorio dell'Unione una molteplicità di sistemi di tutela dei dati personali, ciascuno frutto di un adattamento dei principi della direttiva ai diversi contesti giuridici nazionali[1]. In tema di trattamento dei dati per l'esercizio di compiti di

[1] Come la Commissione chiarisce nella relazione annessa alla proposta di regolamento (COM(2012) 11 final), il presupposto giustificativo dell'intervento mediante lo strumento di massima armonizzazione legislativa, il regolamento, è rappresentato dal fatto che "Pur rimanendo valido in termini di obiettivi e principi, *il quadro giuridico attuale non ha impedito la frammentazione delle modalità di applicazione della protezione dei dati personali nel territorio dell'Unione*, né ha eliminato l'incertezza giuridica e la diffusa percezione nel pubblico che le operazioni on line comportino notevoli rischi" (p. 2) ; ancora "Nel corso delle consultazioni sull'impostazione generale la grande maggioranza degli interpellati ha convenuto che i principi generali rimangono validi (…) *Aspre critiche ha suscitato l'attuale frammentazione*

interesse pubblico, tale fase di adattamento ha consentito agli Stati membri di adeguare principi e criteri della direttiva nell'ambiente giuridico-amministrativo dell'ordinamento domestico. Come detto, in questo processo, il tema del *potere pubblico* speso dalle amministrazioni e dagli altri soggetti che esercitino funzioni pubbliche *implicitamente connesso* al trattamento di dati personali ha finito inevitabilmente per essere assorbito e sistematizzato alla stregua dei principi caratteristici di ciascun ordinamento, proprio in virtù del processo di recepimento e della intermediazione del legislatore interno. In questo modo, con l'entrata in vigore del GDPR, si osservano e si confrontano, sul piano storico-positivo, due diversi *standard legali* connessi al trattamento dei dati personali per l'esercizio di compiti di interesse pubblico. Da una parte, con riferimento a ciascun sistema legale "domestico", il parametro di legalità frutto del recepimento della direttiva. Uno standard legale che – in ragione dell'indispensabile intermediazione del legislatore interno – finisce per essere integrato entro i criteri ed i caratteri propri dell'ordinamento di destinazione. Dall'altra, lo standard legale disegnato dal GDPR, e idoneo a trovare diretta, immediata applicazione in quegli stessi ordinamenti nazionali. Uno standard legale, quest'ultimo, caratterizzato in modo specifico e distintivo, e non necessariamente in linea con lo standard che identifica i requisiti di liceità dell'esercizio del potere pubblico nei diversi contesti domestici. Come si è visto, anzi, con riferimento al sistema della legalità amministrativa nell'ordinamento nazionale italiano, la clausola di *necessarietà* che caratterizza lo standard del GDPR risulta difforme dalle esigenze del principio di legalità, per come interpretato e vigente nell'ordinamento nazionale, anche tenuto conto dei margini di applicazione della teoria dei poteri impliciti. Anche per questa ragione, il legislatore del regolamento, in relazione al regime del trattamento dei dati personali per l'esercizio di compiti di interesse pubblico, si è trovato di fronte ad una opzione di politica del diritto particolarmente rilevante, ed impegnativa, anche tenuto conto della più tradizionale *deference* dell'ordinamento comunitario nei confronti dei sistemi nazionali di diritto amministrativo. Una *deference* fortemente radicata nel modello originario del sistema dei trattati, che però ha mantenuto una forte

della protezione dei dati personali nell'Unione, in particolare degli operatori economici che hanno chiesto una maggiore certezza giuridica e l'armonizzazione delle norme sulla protezione dei dati personali" (p. 4); pertanto "Il *regolamento è considerato lo strumento più idoneo* per definire il quadro giuridico per la protezione dei dati personali nell'UE. *L'applicabilità diretta di un regolamento ai sensi dell'articolo 288 del TFUE ridurrà la frammentazione giuridica* e offrirà maggiore certezza giuridica grazie all'introduzione di una serie di norme di base armonizzate, migliorando la tutela dei diritti fondamentali delle persone fisiche e contribuendo al corretto funzionamento del mercato interno" (p. 6) (corsivi aggiunti).

impronta anche nelle stagioni evolutive successive dell'ordinamento, comunitario prima e dell'Unione dopo. Infatti, poiché l'esecuzione "amministrativa" del diritto "comunitario" è stata tradizionalmente (ed ancora è, largamente) affidata alle amministrazioni degli Stati membri, questi ultimi hanno potuto preservare il diritto delle amministrazioni (il diritto amministrativo interno). Ciò, come noto, non ha impedito al diritto comunitario e unionale di esercitare una enorme influenza sui diritti amministrativi nazionali, realizzando anche fenomeni e percorsi di significativa convergenza tra modelli un tempo molto distanti tra loro[2]. Ciò che però non ha comportato una loro uniformazione – sotto l'egida del primato del diritto dell'Unione. Non solo perché tale processo è sostanzialmente impedito proprio dalla strategia dell'integrazione, che mediante il metodo comunitario o *funzionalista*, tende a non mettere formalmente in discussione la sovranità dei paesi membri. Ma anche perché la stessa integrazione si fonda sulla salvaguardia di queste differenze, laddove gli strumenti di integrazione non passano esclusivamente attraverso l'uniformazione (legislativa) o l'unificazione (delle strutture amministrative di governo), ma anche attraverso i meccanismi dell'*equivalenza*, che invece presuppongono proprio la *differenziazione* di regole, principi, istituti, tra i sistemi amministrativi nazionali[3]. Si aggiunga, poi, che la clausola di salvaguardia delle identità costituzionali – inserita nel trattato di Lisbona – costituisce l'esplicito riconoscimento e la salvaguardia del pluralismo giuridico che connota il composito ordinamento dell'Unione europea[4].

In tale contesto, al momento del passaggio ad una più forte integrazione della disciplina a tutela dei dati personali (e di più intensa promozione della libera circolazione di questi dati all'interno dei confini dell'Unione), si è trattato di scegliere se procedere ad uniformare i presupposti di liceità di trattamento dei dati personali per l'esecuzione di compiti di interesse pubblico, ovvero se – diversamente – salvaguardare la differenziata attitudine dei diritti amministrativi nazionali (e delle relative discipline positive) a regolare i requisiti per l'attribuzione e l'esercizio del potere pubblico, anche con riferimento a quello speso nel trattare i dati personali per finalità di interesse pubblico. Come noto, ne è scaturita una soluzione di compromesso, nella quale i due standard legali sono entrambi posti nella condizione (potenziale) di disciplinare la materia *de qua*, secondo un criterio che vede nella clausola di

[2] Cfr. *supra* la dottrina richiamata alla nota n. 3 del cap. 2.

[3] Sul principio di equivalenza come modalità di governo della diversità alternativo all'uniformazione, cfr. Torchia L. (2006), *Il governo delle differenze. Il principio di equivalenza nell'ordinamento europeo*, Bologna.

[4] Vecchio F. (2012), *Primazia del diritto europeo e salvaguardia delle identità costituzionali: effetti asimmetrici dell'europeizzazione dei controlimiti*, Torino; Faraguna P. (2015), *L'identità nazionale nell'Unione europea come problema e come soluzione*, il Mulino.

necessarietà lo standard legale di *default* (ad applicazione generalizzata e residuale, in virtù della diretta efficacia ed applicabilità delle disposizioni del regolamento, ivi compresa quella di cui all'art. 6, par. 1, lett. e)), salvo però che lo Stato membro non scelga di approfittare dei margini di adattamento aperti alla legislazione nazionale dalle clausole all'uopo inserite nello stesso art. 6, nei paragrafi 2 e 3. Pertanto, anche sotto il profilo sistematico-applicativo, si confrontano *due standard legali*: quello (im)posto dal regolamento (la *necessary clause*), e quello (facoltativo) che ciascuno Stato membro ha la possibilità di delineare e di modulare, nell'ambito dei margini di adattamento aperti dallo stesso regolamento. Tali margini di adattamento rispetto allo standard uniforme (nell'ottica sistematico-applicativa) costituiscono in effetti la diretta conseguenza della dinamica storico-positiva, ovvero dell'affermarsi – in seno all'Unione – di una molteplicità di approcci regolatori differenziati in ordine al regime legale del trattamento dei dati personali per l'esercizio di compiti di interesse pubblico, in esito del recepimento della direttiva. Sul punto, per altro, il GDPR è del tutto esplicito, laddove l'art. 6, par. 2 consente agli Stati membri non solo di *introdurre* ma anche (appunto) di *mantenere* "disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, letter[a] … e)". Va anche ricordato che tale clausola è stata introdotta a partire dagli emendamenti elaborati dal Consiglio[5], mentre il testo della proposta iniziale dalla Commissione, così come la posizione adottata dal Parlamento europeo, non la contemplavano affatto. Non è un caso che questa esigenza sia venuta dalle rappresentanze degli esecutivi nazionali, interpreti principali di quelle specificità e sensibilità maturate nelle legislazioni e nei regimi di diritto amministrativo nazionali nei quali la tutela dei dati personali era stata recepita, adattata, inquadrata. Il duplice standard legale è quindi anche l'effetto, l'esito di un processo di progressiva uniformazione del diritto europeo a tutela dei dati personali, e della "resistenza" opposta dai regimi nazionali di diritto amministrativo; ma anche l'espressione della ricerca di un punto di equilibrio *necessario*, tenuto conto non solo del livello di integrazione effettivamente conseguibile in tale contesto, ma anche delle caratteristiche strutturali del modello istituzionale dell'Unione, che poggia su sistemi amministrativi nazionali. Tale punto di equilibrio assegna essenzialmente agli Stati membri l'ultima parola circa il regime a tutela dei dati personali connesso al trattamento per finalità di interesse pubblico. Mentre lo standard delineato dalla *necessary clause* dell'art. 6(1), lett. e) del regolamento costituisce in certo senso il livello essenziale ed uniformemente

[5] Cfr. Roßnagel, A., Nebel, M., & Richter, P. (2015). *Was bleibt vom Europäischen Datenschutzrecht. Überlegungen zum Ratsentwurf der DS-GVO*, ZD, 455.

applicabile a tutela dei dati personali, gli Stati membri dispongono di un (facoltativo, ma significativo) margine di adattamento, in base al quale gli ordinamenti domestici possono comporre e modulare un differente standard di legalità, per adattarlo alle esigenze e alle caratteristiche della legislazione amministrativa nazionale. Si noti come, in modo del tutto coerente con questo approccio, gli istituti di cooperazione tra le autorità nazionali di controllo come pure il meccanismo del «meccanismo dello sportello unico» (*one stop shop*) non risultano operanti quando "*quando il trattamento è effettuato da autorità pubbliche o da organismi privati nell'interesse pubblico*"; anzi, il regolamento è esplicito nel dichiarare che in questi casi l'unica autorità di controllo competente a esercitare i poteri a essa conferiti a norma del presente regolamento sia l'autorità di controllo dello Stato membro in cui l'amministrazione o l'organismo privato incaricato dell'esercizio di funzioni pubbliche si trovino a trattare i dati personali (considerando 127 e 128): in questo modo si accorda un meccanismo di salvaguardia della differenziazione applicativa (in coerenza con il margine di adattamento riconosciuto a ciascuno stato membro), piuttosto che non dell'uniformità.

2. I caratteri dello standard uniforme/residuale: la *necessary clause*

2.1. La base legale ai sensi del regolamento: il referente del trattamento "necessario"

Nella declinazione della *necessary clause*, per come prefigurata dal regolamento quale presupposto di liceità per il trattamento dei dati personali ai fini dell'esercizio di compiti e poteri pubblici, un primo elemento da inquadrare e decodificare è il *referente* in vista del quale il trattamento dei dati personali si configura in quanto *trattamento necessario*. Sul piano della *identificazione oggettiva* di questo referente, il regolamento (così come pure la direttiva) utilizza una nozione di *funzione pubblica* di carattere tendenzialmente *oggettivo*, formulata cioè in relazione ai caratteri della attività per l'esecuzione e/o l'esercizio della quale il trattamento risulta necessario. Tale attività è identificata con due locuzioni che, come si già avuto modo di sottolineare, risultano complementari proprio perché la relativa declinazione vale a identificare (e ricomprendere) tutte le attività *oggettivamente* "di interesse pubblico", o perché preordinate al perseguimento di interessi pubblici (anche nell'ipotesi in cui tale attività non comporti l'esercizio di poteri pubblici), o perché caratterizzate dalla spendita di un potere pubblicistico (ed in

questo caso, l'attinenza dell'esercizio del potere con il perseguimento di interessi pubblici è da intendersi come implicita nell'attribuzione del potere). La formula è invece volutamente neutra per quanto riguarda la natura *soggettiva* del titolare del trattamento, potendo questi essere un soggetto formalmente pubblico o un soggetto formalmente privato investito dell'esecuzione di un compito di interesse pubblico e/o investito dell'esercizio di un pubblico potere. Ciò che rileva non è *chi* eserciti l'attività, ma di *che tipo* di attività si tratti. Qui vanno fatte due notazioni. Non mancano nel testo del regolamento plurimi richiami ad una nozione (invece) *soggettiva* del potere pubblico o della pubblica amministrazione, a cominciare proprio dalla disposizione che detta i presupposti di liceità del trattamento. Infatti, la nozione (soggettiva) di autorità pubblica è utilizzata per escludere che il presupposto di liceità di cui all'art. 6, par. 1, lett. f) possa trovare applicazione con riguardo alle "autorità pubbliche nell'esecuzione dei loro compiti". Si tratta di una precisazione importante, sotto molteplici profili. In primo luogo, ribadisce il carattere *oggettivo* della nozione formulata nella precedente lett. e), in quanto l'autorità pubblica (*in senso soggettivo*) è solo uno dei soggetti che possono essere investiti dell'esecuzione di compiti di interesse pubblico; ai soggetti formalmente privati che lo fossero, la possibilità di avvalersi del presupposto di liceità del trattamento in quanto necessario al perseguimento del legittimo interesse del titolare non può invece essere esclusa. Inoltre, la precisazione rivela come il GDPR sia allineato ad una lettura complessiva che nega alle *autorità pubbliche* la capacità di elaborare *autonomamente* l'interesse pubblico da perseguire, poiché quest'ultimo è sempre, in prima battuta, indicato *dall'esterno*. Dunque, le autorità pubbliche sono configurate nel regolamento sulla tutela dei dati personali quali soggetti integralmente *serventi* interessi pubblici che sono loro indicati: tali autorità sono chiamate a darvi esecuzione, anche mediante l'investitura di poteri pubblici. Ciò che rimanda alla centralità di quella dimensione *funzionalizzante* della legalità, quella che con la terminologia dei diritti nazionali potremmo declinare come *legalità-indirizzo*, o *mission de service public*, mediante la quale l'ordinamento positivo seleziona ovvero elabora le finalità e gli intessi *pubblici*, e li indica alle amministrazioni, affidando loro il compito di perseguirne la cura. Questa centralità della *legalità-indirizzo*[6] è del tutto comprensibile nell'economia della *necessary clause*: è solo con riferimento alle finalità da perseguire che è possibile verificare se ed in che misura il trattamento dei dati personali risulti effettivamente necessario (ma sulla nozione di *necessarietà*, vedi subito *infra*, al paragrafo successivo). Ciò che ci consente di sciogliere un'apparente

[6] Sulla nozione di "legalità-indirizzo", si veda, per tutti, Marzuoli C. (1982), *Principio di legalità e attività di diritto privato della pubblica amministrazione*, Milano.

ambiguità del testo del regolamento. Sul piano sintattico, infatti, la formulazione della lett. e), sembra riferire il parametro della necessarietà (del trattamento) solo all'esecuzione dei compiti di interesse pubblico, mentre il nesso con "l'esercizio di pubblici poteri" appare più sfumato. La formula impiegata nel testo della versione italiana è "trattamento (…) connesso all'esercizio di pubblici poteri", ma identiche sono le considerazioni che possono emergere dalla lettura del testo in francese ("le traitement… est relevant de l'exercice de l'autorité publique"). Che però il nesso giustificativo del trattamento dei dati personali sia sempre la *necessarietà*, anche con riferimento all'esercizio del potere pubblico, lo chiariscono sia elementi di interpretazione sistematica (la centralità della *clausola di necessarità* conferimento a tutti i presupposti di liceità del trattamento), sia le versioni in altre lingue (a cominciare dal testo in lingua inglese "processing is necessary (…) in the exercise of official authority"), sia il testo del considerando 45[7]. Ciò, per altro, ci consente di sottolineare come l'identificazione dell'interesse pubblico perseguito costituisca l'elemento indispensabile per l'operatività della clausola di necessarietà anche quando questa abiliti il trattamento di dati personali in funzione dell'esercizio di pubblici poteri. Infatti, l'investitura di un potere pubblico, in sé e per sé considerata, non è in grado di illuminare quali trattamenti risultino necessari al suo esercizio, se non si completa la fattispecie mediante l'evidenziazione degli interessi e delle finalità in vista delle quali quel potere è attribuito. D'altra parte, è proprio in ragione di questa struttura (che si compone essenzialmente di *una finalità* e *dei poteri necessari per il suo conseguimento*) che si è potuta inquadrare la clausola di *necessarietà* entro lo schema dei *poteri impliciti*.

2.2. Il ruolo della base giuridica

Ai sensi dell'art. 6, par. 3, la base su cui si fonda il trattamento dei dati di cui all'art. 6, par. 1, lett. e) deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento. Sotto questo profilo, alla luce della conformazione della clausola di necessità, si può senz'altro affermare che ciò che la base giuridica deve disporre (per risultare idonea ad abilitare il presupposto di liceità) è l'affidamento al titolare

[7] "È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro (…)", dove si evince in modo chiaro che il requisito della necessarietà è parimenti da riferirsi ad entrambi gli elementi della fattispecie (*per* l'esecuzione di un compito svolto nel pubblico interesse e *per* l'esercizio di pubblici poteri).

del trattamento dell'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri. In altre parole, ciò che rileva ai fini della integrazione della base giuridica – in relazione al presupposto di liceità di cui all'art. 6(1), lett. e) – è la dimensione della *legalità-indirizzo*, che è esercitata in modo esplicito nel caso dell'affidamento dell'esecuzione di compiti di interesse pubblico, e può risultare invece *implicita* nel caso della (nuda) attribuzione di poteri pubblici. In altre parole, l'assegnazione (ad una pubblica autorità o altro soggetto), da parte del diritto dell'Unione o del diritto dello Stato membro, di un compito di interesse pubblico (e/o di un potere pubblicistico) costituisce la base giuridica su cui si fonda il trattamento dei dati personali. Si noti che, alla stregua di quanto chiarito al considerando 41 del regolamento, il riferimento a una "base giuridica" non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Piuttosto, devono essere rispettate alcune condizioni oggettive: la base giuridica o misura legislativa dovrebbe essere chiara, precisa e accessibile e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo.

Tale base giuridica, così delineata, costituisce il parametro rispetto al quale ricavare e/o identificare la finalità del trattamento. Si tratta di un passaggio essenziale, dal momento che il *principio di limitazione della finalità* costituisce il principio cardine attorno al quale è costruito l'edificio della tutela dei dati personali, nel sistema del GDPR[8]. In effetti, i meccanismi di tutela dei dati personali muovono dal presupposto per cui ogni dato personale reca (deve recare) con sé una finalità (determinata, esplicita e legittima) che ne ha giustificato la raccolta: ogni successivo trattamento da parte del titolare deve risultare non incompatibile con tale finalità (art. 5, par. 1, lett. b)), così

[8] Sul principio di limitazione del trattamento, cfr. von Grafenstein M. (2018), *The Principle of Purpose Limitation in Data Protection Laws. The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Baden-Baden. "Like a guardian angel, the original purpose of a personal data collection is supposed to accompany the data through whatever processing life throws at them to ensure that all activities are at least compatible with what the data were originally collected for (referred to as the principle of 'purpose limitation')", così Drechsler, L. C. (2023). "What purpose is left for purpose limitation as a guiding principle of the General Data Protection Regulation after Case C- 268/21, Norra Stockholm Bygg AB v Per Nycander AB?", in *https://eulawlive.com*, 15 marzo 2023 (accesso 15 maggio 2023); per una disanima delle diverse funzioni di legittimazione e tutela dispensate dal principio di limitazione del trattamento, e per una analisi della giurisprudenza rilevante in material della Corte di giustizia, si veda già Brouwer, E. R. (2011), *Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation*, in Besselink L. F. M., Prechal S., & Pennings F. (eds.), *The Eclipse of the Legality Principle in the European Union*, 273-294.

che *la finalità* del trattamento costituisce *giustificazione* e *limite* di ogni trattamento. Giustificazione, perché il presupposto di liceità del trattamento "incorpora" *sempre* il principio di finalità del trattamento, sia che si tratti del consenso dell'interessato[9], sia che si tratti delle altre ipotesi, tutte basate sulla clausola della necessarietà[10]. Limite, perché i dati acquisiti e trattati dal titolare per una (o più) di queste finalità, potranno essere ulteriormente utilizzati solo se i trattamenti successivi/ulteriori saranno caratterizzati da finalità non incompatibili con quella iniziale[11].

Vanno sottolineati i termini peculiari nei quali opera – in questo caso – l'*identificazione* della finalità del trattamento. Infatti, ai sensi dell'art. 6, par.

[9] Infatti, il consenso che integra un idoneo e lecito presupposto al trattamento è quello espresso dall'interessato rispetto al trattamento dei propri dati personali per una o più specifiche finalità (art. 6(1), lett. a): la *finalità specifica* – quindi – costituisce elemento necessario ed integrante del meccanismo che autorizza il trattamento dei dati personali fondato sul consenso dell'interessato.

[10] La clausola di necessarietà, nelle diverse fattispecie in cui è declinata in altrettanti presupposti del trattamento dall'art. 6 del regolamento, si basa infatti sul nesso di strumentalità (necessaria) che intercorre tra il trattamento cui è sottoposto il dato personale dell'interessato ed il compimento, la realizzazione, la cura di una serie di interessi qualificati (l'esecuzione di un contratto di cui l'interessato è parte (lett. b)); l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (lett. c)); la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (lett. d)); 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)); il perseguimento del legittimo interesse del titolare del trattamento o di terzi (lett. f)). Il compito e/o la realizzazione di ciascuna di queste azioni (preordinate a dare soddisfazione ad una serie di interessi) costituisce – dunque – la finalità dei trattamenti così autorizzati.

[11] Il vincolo imposto dal principio di *limitazione della finalità* può essere derogato (art. 6, par. 4) solo con un atto legislativo dell'Unione o dello stato membro, e soltanto se il trattamento così disposto costituisce una misura necessaria e proporzionata in una società democratica, giustificata dall'esigenza di salvaguardare gli obiettivi esplicitati all'art. 23, par. 1 del regolamento (ossia: la sicurezza nazionale; la difesa; la sicurezza pubblica; 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; 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; la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri esercitati per la salvaguardia dei predetti interessi pubblici; la tutela dell'interessato o dei diritti e delle libertà altrui; l'esecuzione delle azioni civili). Tuttavia, anche in questo caso, tale misura legislativa deve contenere – tra le altre cose – disposizioni specifiche riguardo alle finalità del trattamento in questione (art. 23, par. 2, lett. a)). Di recente, la Corte del Lussemburgo ha chiarito che la considerazione dei diritti degli interessati concorre alla valutazione (rimessa al giudice nazionale) circa il carattere necessario e proporzionato di una misura legislativa *in deroga* al principio di limitazione della finalità del trattamento, adottata ai sensi dell'art. 6(4): cfr. Corte di giustizia, causa C-268/21.

3, "*la finalità del trattamento* (…) per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), *è necessaria* per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Dunque, è lo stesso nesso di *strumentalità necessaria* a identificare la finalità del trattamento, mentre la base giuridica (con la quale – lo si è visto – è operato l'affidamento al titolare del trattamento dell'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri) funge da referente esterno, è lo "scopo" per il conseguimento del quale il trattamento può essere effettuato, qualora tale trattamento sia configurabile come *mezzo necessario* rispetto a tale fine. Ciò significa che non è indispensabile – nell'economia della *necessary clause* – che la *base giuridica* determini o indichi esplicitamente la finalità del trattamento[12]. Piuttosto, *quale sia la finalità* del trattamento si ricaverà (anche in termini impliciti[13]) accertando/verificando il nesso di strumentalità tra il trattamento effettuato dal titolare e l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri a esso affidati in virtù della base giuridica[14]. Dunque, il nesso di *strumentalità necessaria* che intercorra tra il trattamento effettuato dal titolare e l'esecuzione del compito di interesse pubblico assolve ad una pluralità di funzioni: esso identifica *la finalità* del trattamento effettuato ed al tempo stesso contribuisce ad integrare il *presupposto di liceità* di tale trattamento.

[12] "Il legislatore europeo ha cioè ritenuto che, quando la base giuridica del trattamento risiede nella esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, una esplicitazione in sede legislativa della finalità del trattamento non sia necessaria: ciò pare confermato anche dai Considerando nn. 41 e 45 del regolamento, oltre che da una lettura sistematica del medesimo art. 6 GDPR e, in particolare, da un confronto tra l'art. 6, par. 1, lett. e) – ove la valutazione del trattamento come necessario e inevitabile è rimessa alla discrezionalità della pubblica amministrazione e l'art. 6, par. 1, lett. c), che viceversa autorizza il trattamento dei dati quando il titolare deve adempiere un obbligo legale, nel qual caso è appunto la legge a valutare *ex ante* se un trattamento sia necessario e inevitabile", così Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, in (eds.) Pajno A., Donati F., Perrucci A., I*ntelligenza artificiale e diritto: una rivoluzione? Vol. 1: Diritti fondamentali, dati personali e regolazione*, Bologna, 395-96.

[13] Così Frenzel E.M. (2018), *Rechtmäßigkeit der Verarbeitung*, in Paal B.P., Pauly D.A., *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, C.H. Beck, Munich, 86.

[14] Cfr. Corte di giustizia, *Puškár* (C-73/16): "l'obiettivo del trattamento dei dati personali è indissolubilmente collegato, nell'ambito di applicazione dell'articolo 7, lettera e), della direttiva 95/46, con i compiti affidati al responsabile del trattamento. L'attribuzione di detti compiti a quest'ultimo deve pertanto ricomprendere chiaramente l'obiettivo del trattamento in questione" punto 110.

2.3. Principio di limitazione della finalità ed esercizio di funzioni pubbliche

L'identificazione della finalità è un passaggio essenziale, dal momento che anche con riferimento al trattamento dei dati per l'esecuzione di compiti di interesse pubblico opera il principio di limitazione della finalità. Un principio particolarmente rilevante in questo contesto, dal momento che l'esercizio dei poteri e dei compiti di interesse pubblico si va caratterizzando in modo sempre più rilevante per un uso strategico, sistematico ed integrato delle banche dati pubbliche, quali infrastrutture informative e conoscitive, da mettere al servizio dell'intero sistema pubblico, a prescindere dalla ubicazione e dalla titolarità della banca dati stessa. L'interconnessione tra le banche dati, mediante la quale realizzare e abilitare la fruibilità del patrimonio informativo all'interno del sistema pubblico, costituisce un obiettivo (di riforma) di lunga data, e muove nella direzione di considerare il sistema pubblico come un insieme integrato, nell'ambito del quale le informazioni sono raccolte da alcuni attori e poi rese disponibili agli altri, secondo una logica per la quale l'informazione andrebbe acquisita una sola volta (il principio del «*once only*», promosso a livello dell'Unione[15] e recepito come misura strutturale e trasversale di riforma nel PNRR[16] e fatto proprio anche nel processo di digitalizzazione del ciclo di vita dei contratti pubblici per come delineato nel nuovo Codice dei contratti adottato nella primavera del 2023, anche in applicazione dello stesso PNRR)[17]. Il principio di fruibilità delle banche dati

[15] Cfr. il *Piano d'azione dell'UE per l'eGovernment 2016-2020*, COM(2016) 179 final.

[16] Cfr. PNRR, Investimento 1.3: Dati e interoperabilità: "La trasformazione digitale della PA si prefigge quindi di cambiare l'architettura e le modalità di interconnessione tra le basi dati delle amministrazioni affinché l'accesso ai servizi sia trasversalmente e universalmente basato sul principio "once only", facendo sì che le informazioni sui cittadini siano a disposizione "una volta per tutte" per le amministrazioni in modo immediato, semplice ed efficace, alleggerendo tempi e costi legati alle richieste di informazioni oggi frammentate tra molteplici enti. Investire sulla piena interoperabilità dei dataset della PA significa introdurre un esteso utilizzo del domicilio digitale (scelto liberamente dai cittadini) e garantire un'esposizione automatica dei dati/attributi di cittadini/residenti e imprese da parte dei database sorgente (dati/attributi costantemente aggiornati nel tempo) a beneficio di ogni processo/servizio "richiedente". Si verrà a creare una "Piattaforma Nazionale Dati" che offrirà alle amministrazioni un catalogo centrale di "connettori automatici" (le cosiddette "API" – Application Programming Interface) consultabili e accessibili tramite un servizio dedicato, in un contesto integralmente conforme alle leggi europee sulla privacy, evitando così al cittadino di dover fornire più volte la stessa informazione a diverse amministrazioni", 93.

[17] Il "principio dell'unicità dell'invio" è alla base dell'architettura informativa che presiede alla piena digitalizzazione del ciclo di vita dei contratti pubblici, che informa il Codice dei contratti pubblici approvato con il d.lgs. 31 marzo 2023, n. 36, ed è declinato all'art. 19 *(Principi e diritti digitali)*.

detenute, alimentate e gestite dalle singole amministrazioni a beneficio di tutte le altre amministrazioni coinvolge anche *i dati personali* gestiti, così che – almeno in linea *tendenziale* – le amministrazioni dovrebbero evitare di raccogliere presso l'interessato i dati e le informazioni di cui abbisognano per l'esercizio delle rispettive funzioni, ma dovrebbero piuttosto procurarsele accedendo alla banca dati che le conserva stabilmente. Non è questa la sede in cui è possibile indagare le trasformazioni organizzative, tecniche ed operative che la realizzazione di questo modello comporta o impone (a cominciare, per fare solo gli esempi più significativi, dalla identificazione, istituzione ed implementazione della basi di dati di interesse nazionale di cui all'art. 60 del Codice dell'amministrazione digitale[18]; o la effettiva abilitazione della Piattaforma Digitale Nazionale dei Dati di cui all'art. 50-ter del medesimo Codice[19]); è sufficiente sottolineare che – nell'ottica di questo modello – le amministrazioni saranno poste nella condizione di progettare e gestire modalità di esercizio delle proprie funzioni alimentate anche dall'accesso e dall'utilizzo di dati personali tratti direttamente dai sistemi informativi di altre amministrazioni[20]. In tale contesto, il principio di *limitazione della finalità* si configura come un vincolo alla concreta realizzazione di queste soluzioni, dal momento che va sempre verificata la *compatibilità* (o la *non incompatibilità*) tra la finalità del trattamento successivo e quella che ha giustificato/supportato la sua raccolta. Nell'ambito dello standard legale costruito attorno alla clausola di necessarietà, il vincolo imposto dal principio di limitazione appare particolarmente significativo, dal momento che finisce per operare come limite a una perfetta, piena circolazione e/o integrazione (sotto il profilo funzionale) del patrimonio informativo pubblico. Infatti, il requisito di liceità – integrato dal nesso di strumentalità del trattamento con

[18] Le basi di dati nazionali sono, ai sensi dell'art. 60, comma 1 del CAD "basi di dati affidabili, omogenee per tipologia e contenuto, rilevanti per lo svolgimento delle funzioni istituzionali delle Pubbliche amministrazioni e per fini di analisi. Esse costituiscono l'ossatura del patrimonio informativo pubblico, da rendere disponibile a tutte le PA, facilitando lo scambio di dati ed evitando di chiedere più volte la stessa informazione al cittadino o all'impresa"

[19] La Piattaforma Digitale Nazionale Dati è un'infrastruttura tecnica funzionale ad abilitare lo scambio e la fruibilità del patrimonio informativo pubblico tra le componenti del sistema, attraverso la messa a disposizione e l'utilizzo, da parte dei soggetti accreditati, di interfacce di programmazione delle applicazioni (API), così da rendere interoperabili i sistemi informativi delle pubbliche amministrazioni e dei gestori dei servizi pubblici.

[20] Sul punto, cfr. Falcone M. (2023), *Ripensare il potere conoscitivo pubblico. La conoscenza amministrativa con i big data e gli algoritmi*, Napoli, in corso di pubblicazione.; nonché Boschetti B. (2022), *La transizione della pubblica amministrazione verso il modello Government as a platform*, in Lalli A. (ed.), *L'amministrazione pubblica nell'era digitale*, Torino, 1- 44); Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, cit., 389 ss.

l'esercizio della funzione pubblica – risulta arricchito dal profilo della compatibilità della finalità del trattamento stesso, quando i dati *non sono raccolti presso l'interessato*, ma tratti dal sistema informativo di un'altra amministrazione (e quindi il trattamento di configura non come quello "iniziale", ma come quello "successivo"). Sotto questo profilo, l'identificazione della finalità del trattamento (strettamente interrelata, come si è visto, con il compito di interesse pubblico cui tale trattamento risulta strumentale) finisce per essere decisiva, ai fini della valutazione della liceità del trattamento stesso. E tuttavia va anche sottolineato che, poiché tale condizione di liceità si risolve in un giudizio di compatibilità tra due termini (la *finalità iniziale* e *quella successiva*), la sua verifica in concreto dipende (anche) dalle modalità con le quali è formulata e identificata la finalità iniziale (quella che supporta la raccolta "iniziale" del dato personale). Sotto questo profilo, cioè, occorre anche tenere conto di come è formulato ed inteso il compito di interesse pubblico cui sia preordinata la raccolta dei dati personali. Un conto, infatti, è la identificazione della finalità connessa alla raccolta iniziale presso la banca dati di una amministrazione che eserciti *funzioni pubbliche specifiche* (e finali), di erogazione di funzioni e servizi pubblici; altra cosa, invece sarebbe la identificazione della finalità connessa alla raccolta iniziale presso una banca dati (magari centralizzata) esplicitamente preordinata a realizzare la raccolta di informazioni "omogenee per tipologia e contenuto" e caratterizzata da specifici requisiti di qualità (congruità, aggiornamento, accuratezza, etc.) e la cui *funzione sia (anche) quella di rendere tali informazioni disponibili alle altre amministrazioni* in vista dell'esercizio delle rispettive funzioni[21]. In questo secondo caso, il giudizio di compatibilità sarebbe il risultato di un confronto tra un parametro non solo (e non tanto) "più ampio" (o generico),

[21] A questo fine, si potrebbe ragionare sull'effetto determinato dalla costituzione delle richiamate "Basi di dati di interesse nazionale", costituite esattamente allo scopo di allineare e rendere disponibili le informazioni (ivi compresi i dati personali) a tutte le componenti del sistema pubblico per l'esercizio delle rispettive funzioni, Emblematico, in questo senso, è il caso dell'ANPR. La banca dati è stata costituita (presso il ministro dell'Interno) mediante la centralizzazione organizzativa di un patrimonio informativo in precedenza gestito (e detenuto) in modo decentrato presso i comuni. La disciplina della banca dati prevede che i dati siano resi disponibili ai comuni i dati contenuti nell'ANPR per l'esercizio delle funzioni istituzionali dei comuni (con una formulazione che è certo è *determinata*, ma non così *specifica*: "L'ANPR assicura ai comuni la disponibilità dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, e mette a disposizione dei comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale", art. 62, comma 3 del CAD)", come pure delle altre amministrazioni ("L'ANPR assicura ai soggetti di cui all'articolo 2, comma 2, lettere a) e b), l'accesso ai dati contenuti nell'ANPR", *ibidem*).

ma piuttosto *coerente* con le esigenze funzionali finalità e del trattamento *successivi*. Tale considerazione consente di riflettere sul fatto che il vincolo imposto dal principio di limitazione della finalità ha un impatto che dipende *anche* da come è configurata la (o le) finalità del trattamento iniziale (la raccolta del dato). Una considerazione particolarmente rilevante nell'ambito dell'esercizio delle funzioni pubbliche (e dei trattamenti di dati personali a ciò preordinate), in considerazione del fatto che se è vero che il regolamento, come già sottolineato, qualifica la finalità come *determinata*, *esplicita* e *legittima* (art. 5(1), lett. b)), nonché *specifica* (art. 6(1), lett. a) è pure vero che la *identificazione* della finalità nell'ambito dell'esercizio delle funzioni pubbliche dipende in particolare dalla tipologia di compiti, funzioni e poteri la cui esecuzione è affidata alle pubbliche amministrazioni (o agli altri soggetti che ne siano investiti), e che la formulazione di tali compiti (e il relativo affidamento) è effettuata in prima battuta dal legislatore, con ciò che ne consegue in termini di ampiezza e consistenza del potere legislativo così impegnato e speso.

In ogni caso, perché il presupposto di liceità sia integrato, non è sufficiente che il nesso di strumentalità sia verificato (e che la finalità del trattamento sia così identificata); occorre che la relazione di strumentalità sia qualificabile come *necessaria* (al conseguimento dello scopo). Di qui l'importanza della nozione di *necessarietà* applicabile.

2.4. Il concetto di necessarietà

Il nesso di strumentalità che deve *connettere* il trattamento dei dati personali con l'esecuzione di un compito di interesse pubblico o con l'esercizio di pubblici poteri di cui sia investito il titolare del trattamento, deve caratterizzarsi nei termini della *necessarietà*. Si tratta, a prima vista, della formulazione di un valore "soglia" in ordine all'intensità di tale relazione di strumentalità, qualcosa che – parafrasando le parole utilizzate dall'Autorità di controllo del Regno Unito – si colloca a metà strada tra una relazione di mera *utilità* ed una di stretta *indispensabilità*[22]. In ogni caso, l'identificazione di

[22] "Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose", cfr. *Guide to Data Protection*, *Lawful basis for processing*, in https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#when. Non è forse sorprendente che fin dalla sua introduzione nella Costituzione statunitense, la definizione operativa di *ne-*

quanto debba essere intenso il nesso di strumentalità per rispondere alla soglia della *strumentalità necessaria* si presta a margini di interpretazione, non soltanto perché essa dipende anche dagli altri elementi in gioco e di cui il nesso di strumentalità costituisce il connettore, nonché dal contesto specifico in cui assume rilievo, ma anche in ragione della complessità della nozione stessa, in sé e per sé considerata.

Se si guarda alla giurisprudenza della Corte di giustizia (la più rilevante, in materia) si può constatare, all'apparenza, un progressivo aggravamento dell'intensità del nesso di strumentalità richiesto per completare il requisito di necessità del trattamento. Mentre in una prima sentenza (in applicazione, per altro, della direttiva), la Corte – nell'affrontare *ex professo* il concetto di *necessity* – fa riferimento ad una serie variegata di elementi differenti utili ad integrare il requisito di necessità, più di recente altre sentenze (emesse in applicazione della corrispondente disposizione presente nel GDPR) fanno riferimento, invece, ad un criterio soglia formulato in termini di *stringente necessarietà* ("*strictly necessary*"), in ragione del quale il requisito del nesso di strumentalità si avvicina (fino quasi a coincidere con) al quello di *indispensabilità*. Per le ragioni di cui diremo meglio più avanti, tuttavia, una lettura in termini di progressivo aggravamento del requisito di necessità non appare del tutto persuasiva, tenuto conto delle caratteristiche specifiche dei casi decisi, e delle indicazioni più generali che da questi possono essere tratte. Conviene, pertanto, analizzare rapidamente questi casi, così da trarne alcune utili indicazioni.

In *Heinz Huber vs Bundesrepublik Deutschland* (causa C-524/06), in sede di domanda di pronuncia pregiudiziale, il Tribunale amministrativo superiore della Nord Renania-Vestfalia chiedeva alla Corte di giustizia (tra le altre cose) se la raccolta generale ed il successivo trattamento di dati personali di cittadini dell'Unione in un registro centralizzato degli stranieri, quale strumento posto al servizio delle autorità incaricate di applicare la normativa sul

cessità – come clausola di attribuzione ed esercizio di un potere (in quel caso, della confederazione rispetto alle competenze degli stati) – si sia mosso attorno alla medesima alternativa (e pervenendo ai medesimi risultati); cfr. Barnett R. E. (2003), "The Original Meaning of the Necessary and Proper Clause", in *University of Pennsylvania Journal of Constitutional Law*, 2, 183 ss: "I will show that the choice between the meanings of "necessary" inherited from John Marshall's discussion in *McCulluch v. Malyland* – that of "indispensably requisite" on the one hand and merely "convenient" on the other – is undercut by the available evidence. Rather, the truth lies somewhere in between (…) This evidence suggests that, while it is a mistake to equate "necessary" with "convenient," neither was it as stringent a standard as connoted by the terms "indispensably" or "absolutely" necessary. Instead, the original meaning of necessity creates the requirement of a degree of means-end fit somewhere between these two extremes" (184, 208).

diritto di soggiorno, fosse compatibile con il requisito concernente la necessità, di cui all'art. 7, lett. e), della direttiva 95/46. Nel rispondere al quesito, la Corte ha avuto modo di chiarire alcuni punti fondamentali. In primo luogo, tenuto conto dell'obiettivo di garantire un livello di tutela equivalente in tutti gli Stati membri, la Corte statuisce che la nozione di necessità come risultante dall'art. 7, lett. e), della direttiva 95/46 – che mira a delimitare con precisione l'ipotesi in cui il trattamento di dati personali finalizzato all'esercizio di compiti di interesse pubblico sia lecito – non può avere un contenuto variabile in funzione degli Stati membri; piuttosto, *la nozione di necessità va considerata una nozione autonoma del diritto comunitario*, che deve essere interpretata in maniera tale da rispondere pienamente alla finalità della direttiva. Si tratta di una affermazione di notevole rilievo, anche in considerazione del fatto che è stata pronunciata in applicazione della disciplina posta con lo strumento della direttiva, come tale fisiologicamente soggetto ad un margine di applicazione e differenziazione a livello statale. La Corte, invece, esprime una netta preferenza per una nozione *radicata nel diritto dell'Unione*, suscettibile di essere applicata in modo uniforme nei diversi contesti ordinamentali nazionali: una indicazione che vale a maggior ragione in costanza di una disciplina di contenuto sostanzialmente identico, ma trasposta nella fonte regolamentare. Ai fini della articolazione del *dual legality standard*, ciò comporta che in caso di diretta applicazione del requisito di liceità di cui all'art. 6(1)(e), il nesso di strumentalità necessaria va inteso in accordo con questa specifica declinazione e non è invece soggetto ad adeguamento/differenziazione sul piano dell'interpretazione giurisprudenziale da parte del giudice domestico. Il che però lascia anche intendere che, in presenza di una clausola di adattamento come quella di cui all'art. 6(2), lo Stato membro potrebbe avere dei margini di manovra al fine di *adeguare* e *precisare* le condizioni per l'applicazione di questo requisito[23].

[23] A conferma, cfr. quanto statuito più di recente dalla Corte di Giustizia, nella causa *Norra Stockholm Bygg AB* (C- 268/21): quando si tratti di dare applicazione a discipline nazionali basate sulla clausola di adattamento di cui all'art. 6(3), "i trattamenti di dati personali sono leciti a condizione che costituiscano misure necessarie e proporzionate in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23 del GDPR che essi perseguono. Ne consegue che, al fine di procedere alla verifica di tali requisiti, un giudice nazionale è tenuto a prendere in considerazione gli interessi contrapposti in gioco quando valuta l'opportunità di ordinare la produzione di un documento contenente dati personali di terzi. *A tal riguardo, occorre sottolineare che l'esito della ponderazione che il giudice nazionale deve effettuare può variare in funzione sia delle circostanze di ciascun caso di specie sia del tipo di procedimento di cui trattasi*" (cfr. punti 45-47). Circa l'idoneità insita nella disciplina di adeguamento di alternare il modo di atteggiarsi del requisito di *necessarietà*, torneremo *infra*, nel capitolo conclusivo.

In secondo luogo, la Corte chiarisce che il requisito di necessità va interpretato alla luce del principio di minimizzazione ("occorre tuttavia rilevare che siffatto registro non può contenere informazioni diverse da quelle a tal fine necessarie"), che concorre così a perimetrare dall'interno il novero e la tipologia dei dati personali suscettibili di essere trattati in coerenza con la clausola di necessarietà. Infine, la Corte ha modo di argomentare che il requisito di necessità è integrato anche nel caso in cui il trattamento consista nella centralizzazione di una serie di informazioni già detenute in modo decentralizzato, perché "la centralizzazione di tali dati può risultare necessaria (…) se contribuisce ad un'applicazione più efficace" dei compiti assegnati all'amministrazione[24]. In questo modo, il contributo in termini di maggiore efficacia nell'esercizio della funzione pubblica integra il requisito di necessità. Si tratta, in effetti, di una statuizione di grande momento, dal momento che introduce un elemento di bilanciamento, utile a costruire un test di necessarietà in presenza di soluzioni di trattamento *meno intrusive*: se il trattamento risulta *più intrusivo* rispetto alle alternative, ma consente di predisporre una soluzione *più efficace* ai fini dell'adempimento del compito di interesse pubblico, allora può risultare un trattamento idoneo ad integrare il requisito di *necessità*[25].

In *Puškár* (causa C-73/16) il giudice del rinvio (la Corte suprema della Repubblica slovacca) aveva domandato se la direttiva 95/46 e gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea fossero da interpretare nel senso che essi ostano a un trattamento dei dati personali realizzato dalla Direzione delle Finanze e dall'Ufficio Crimini dell'amministrazione finanziaria – trattamento finalizzato alla riscossione delle imposte e alla lotta alla frode fiscale – consistente nella compilazione di un elenco di persone fisiche che opererebbero in qualità di prestanome, in assenza del consenso di tali soggetti. In tale caso, dunque, la liceità del trattamento sarebbe dipesa dall'integrazione del requisito di necessità di tale trattamento per l'esecuzione dei compiti di riscossione delle imposte e di contrasto alla frode fiscale. Nel rispondere a tale quesito, la Corte reitera il richiamo al principio di proporzionalità e tuttavia tale principio viene declinato in termini parzialmente diversi, e più restrittivi rispetto al caso precedente. "A tale proposito – nota

[24] Cfr. C-524/06, punti 61-62.

[25] In questo senso, la Corte sembra costruire il test di *necessarietà* sulla scorta di un giudizio di proporzionalità tra efficacia del trattamento e *limitazione*/*compressione* delle esigenze di tutela dei dati personali, così echeggiando l'approccio dell'ICO ("a targeted and proportionate way of achieving a specific purpose", *loc. ult. cit.*); sul punto, vedi più diffusamente G. Black-L. Stevens (2013), *Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest*, in *SCRIPTed*, 10:1, disponibile in http://script-ed.org/?p=835

la Corte – è importante fare attenzione al rispetto del principio di proporzionalità. La tutela del diritto fondamentale al rispetto della vita privata a livello dell'Unione esige, infatti, che deroghe e le restrizioni alla tutela dei dati personali intervengano entro i limiti dello stretto necessario"[26]; la declinazione del principio di proporzionalità nei termini di una verifica della *stretta necessità* del trattamento, prende corpo nelle indicazioni formulate al giudice del rinvio. Questi dovrà infatti "verificare se la redazione dell'elenco controverso e l'iscrizione in quest'ultimo del nome delle persone interessate siano atte a conseguire gli obiettivi perseguiti dalle stesse e se non sussistano altri mezzi meno restrittivi per raggiungere tali obiettivi". Come si vede, nel criterio di verifica così formulato non viene *esplicitato* (a differenza del caso precedente) un criterio di bilanciamento che tenga conto anche della effettività/efficacia del trattamento in questione. Tuttavia, tale criterio di bilanciamento pare ancora sussistere – sebbene in termini *impliciti*: infatti, l'eventuale sussistenza di mezzi meno intrusivi sarebbe suscettibile di privare il trattamento in questione del carattere della necessarietà solo nel caso in cui tali mezzi si dimostrassero idonei a conseguire i *medesimi obiettivi*. Tale maggiore cautela da parte del giudice si spiega perché il trattamento in questione (l'inserimento in una lista di soggetti "sospetti") comporta *di per sé* dei rischi di lesione dei diritti della persona[27]. Tuttavia, anche considerati questi rischi, il giudice non esclude per ciò solo l'integrazione della clausola di necessarietà, la cui verificazione viene però circondata di molteplici cautele e condizioni[28].

Due più recenti casi si sono conclusi invece negando l'integrazione del requisito di necessità a due tipologie di trattamento tra loro molto simili. In

[26] Cfr. C-73/16, punti 111-112.

[27] "L'inclusione in tale elenco potrebbe, per esempio, nuocere alla sua reputazione e incidere sui suoi rapporti con le autorità fiscali. Allo stesso tempo, tale menzione potrebbe ledere la presunzione di innocenza di tale persona, sancita dall'articolo 48, paragrafo 1, della Carta, nonché la libertà d'impresa – ai sensi dell'articolo 16 della Carta – delle persone giuridiche collegate alle persone fisiche iscritte nell'elenco controverso", *ivi* punti n. 114.

[28] Come si legge a chiusura della sentenza, il presupposto di liceità basato sul trattamento necessario ai fini dell'esercizio di funzioni pubbliche deve essere interpretato "nel senso che esso non osta a un trattamento dei dati personali da parte delle autorità di uno Stato membro ai fini della riscossione delle imposte e della lotta alla frode fiscale, come quello a cui si procede con la redazione di un elenco di persone del tipo oggetto del procedimento principale, senza il consenso delle persone interessate, a condizione, da un lato, che a tali autorità siano stati affidati compiti di interesse pubblico dalla normativa nazionale ai sensi di detta disposizione, la redazione di tale elenco e l'iscrizione in quest'ultimo del nome delle persone interessate siano effettivamente idonee e necessarie al raggiungimento degli obiettivi perseguiti e sussistano elementi sufficienti per presumere che le persone interessate figurino a ragione in tale elenco e, dall'altro lato, che siano soddisfatte tutte le condizioni di liceità di tale trattamento dei dati personali imposte dalla direttiva 95/46.", *ivi* punto 125-3).

Latvijas Republikas Saeima (penality points) (causa C-439/19) il quesito è stato interpreto dalla Corte di Giustizia come volto a verificare se il trattamento dei dati personali consistente nel rendere *accessibile al pubblico mediante la pubblicazione su un portale* il registro in cui sono iscritti i punti di penalità inflitti ai conducenti di veicoli per infrazioni stradali fosse da considerato lecito alla luce di tutte le disposizioni di tale regolamento e, in particolare, alla luce del principio di proporzionalità. Per rispondere a tale quesito, la Corte ha inquadrato il trattamento in questione (per altro disposto da una disposizione di legge) nell'ambito della fattispecie di cui all'art. 6, par. 1, lett. e), ed ha quindi proceduto a valutare se, nel caso di specie, fosse soddisfatto il requisito di necessità del trattamento. Il test applicato – nella sua configurazione astratta – non appare dissimile (nella sua formulazione schematica) da quello prefigurato già prefigurato nelle cause C-524/06 e C-73/16. Infatti, la Corte ribadisce che "il requisito di necessità non è soddisfatto quando l'obiettivo di interesse generale considerato può ragionevolmente essere raggiunto in modo *altrettanto efficace* mediante altri mezzi *meno pregiudizievoli* per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei diritti personali garantiti agli articolo 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di simili dati devono avere luogo nei limiti dello stretto necessario"[29]. Come si vede, ad avviso della Corte il *requisito di necessità* va ancora verificato sulla base di un bilanciamento che accerti l'idoneità di altri mezzi meno pregiudizievoli a conseguire risultati *altrettanto efficaci*: l'efficacia del trattamento nel conseguire l'obiettivo di interesse pubblico, quindi, gioca ancora un ruolo essenziale. Nel fare concreta applicazione di tale criterio di bilanciamento, il giudice prende però in considerazione "la gravità dell'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali" determinati dalla specifica tipologia del trattamento in questione, consistente nella *comunicazione al pubblico* dei punti di penalità accumulati in dai conducenti dei veicoli per infrazioni stradali. Infatti, la comunicazione al pubblico e la conoscibilità generalizzata di tali dati personali "può suscitare la disapprovazione sociale e comportare la stigmatizzazione della persona interessata"[30]. La sensibilità dei dati in questione e la gravità dell'ingerenza nei diritti fondamentali prodotta dalla specifica tipologia del trattamento (*la comunicazione al pubblico*) comportano dunque una più severa, stringente considerazione del requisito di necessità: è la stessa Corte che procede a verificare l'esistenza di mezzi alternativi giudicati meno invasivi (perché non comportano la comunicazione al pubblico delle

[29] Cfr. C-439/19, punto 110 (corsivi aggiunti).
[30] *Ivi*, punto 112.

penalizzazioni comminate ai conducenti dei veicoli), come sperimentati in diversi contesti ordinamentali. La mancata considerazione di tali soluzioni alternative (in sede di istruttoria legislativa) fa ritenere alla Corte "non (…) dimostrato che un siffatto sistema di comunicazione dei dati personali relativi ai punti di penalità inflitti per infrazioni stradali sia necessario per raggiungere il suddetto obiettivo"[31].

Nella causa *Vyriausioji tarnybinės etikos komisija* (C-184/20) viene in causa la normativa nazionale lituana che impone la pubblicazione sul sito Internet di un agenzia pubblica dei dati contenuti nelle dichiarazioni di interessi privati di persone fisiche che lavorano nel servizio pubblico nonché di dirigenti di associazioni o di enti percettori di fondi pubblici, al fine "di conciliare gli interessi privati delle persone che lavorano nel servizio pubblico e gli interessi pubblici della società, di assicurare la prevalenza dell'interesse pubblico al momento dell'adozione di decisioni, di garantire l'imparzialità delle decisioni adottate e di prevenire il verificarsi e il diffondersi della corruzione nel servizio pubblico"[32]. Tale misura di trasparenza in funzione di prevenzione della corruzione è inquadrata dalla Corte di giustizia come assolvimento di un obbligo legale (art. 6, par. 1, lett. c) del GPDR), circostanza che consente alla Corte di non indagare la questione sotto lo specifico profilo della fattispecie di cui alla lett. e) (pure prospettata dal giudice remittente). Tuttavia, dati i profili di analogia tra le due fattispecie, con specifico riferimento alla clausola di necessarietà, l'analisi della sentenza è comunque interessante, ai nostri fini. In particolare, il giudice ripete quanto già affermato in *Latvijas Republikas Saeima (Penalty points)*, di poco precedente. In termini astratti, la Corte ribadisce che il requisito di necessità è soddisfatto quando l'obiettivo di interesse generale considerato *non può ragionevolmente essere conseguito in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati*, in particolare per i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti agli articoli 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di simili dati devono applicarsi nei limiti dello *stretto necessario*. L'applicazione di tale massima al caso di specie consente al giudice di fare applicazione del principio di minimizzazione ad integrazione e specificazione del requisito di necessità[33], come pure di argomentare circa l'effettiva presa in considerazione di soluzioni alternative, altrettanto efficaci ma meno invasive[34]. Analogo è poi il ruolo giocato dalla specifica considerazione riservata al livello di intensità ("*seriousness of the interference*") dell'interferenza con i diritti fondamentali della persona (di

[31] *Ivi*, punto 113.
[32] Cfr. C-184/20, punto 24.
[33] *Ivi*, punto 93.
[34] *Ivi*, punti 85-91.

cui agli art. 7 e 8 della Carta). L'intensità del pregiudizio è connessa, per un verso, alla natura particolarmente sensibile dati personali in questione (informazioni sugli interessi economici privati), dall'altra alla modalità di trattamento (la pubblicazione sul sito internet), tale per cui tali dati personali risultano "liberamente accessibili su Internet all'insieme del grande pubblico e, di conseguenza, a un numero potenzialmente illimitato di persone"[35]: il combinato disposto di questi elementi comporta per gli interessati il rischio di *profilazione*[36] e di esposizione ad azioni intrusive o anche di natura criminale[37]. Di qui la conclusione per cui il trattamento in questione "costituisca un'ingerenza grave nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali degli interessati"[38]. È proprio la gravità di questa ingerenza a determinare l'esito del bilanciamento, dal momento che essa non riesce ad essere compensata da un apprezzabile surplus di *efficacia* della misura del trattamento consistente nella pubblicazione via internet dei dati sugli interessi economici e finanziari personali, rispetto a soluzioni meno invasive[39].

2.5. Clausola di necessarietà e ingerenza nei diritti fondamentali

La sequenza cronologica appena richiamata sembra, dunque, disegnare un *crescendo rossiniano*: non solo il requisito di necessità, da una configurazione più aperta, perché integrata dal criterio di efficacia del trattamento, muove nella direzione di una configurazione più rigida ed esigente, declinata

[35] *Ivi*, punti 102-103.

[36] "La gravità di una simile ingerenza può risultare ulteriormente accresciuta dall'effetto cumulativo dei dati personali oggetto di una pubblicazione come quella di cui al procedimento principale, dal momento che la loro combinazione consente di tracciare un ritratto particolarmente dettagliato della vita privata delle persone interessate", *ivi*, punto 101.

[37] "la pubblicazione di detti dati può, ad esempio, esporre gli interessati a operazioni ripetute di pubblicità mirata e a iniziative a carattere commerciale, o addirittura a rischi di azioni criminali" *ivi*, punto 104.

[38] *Ivi*, punto n. 105.

[39] "è necessario constatare che la pubblicazione in rete della maggior parte dei dati personali contenuti nella dichiarazione di interessi privati di qualsiasi direttore di un ente percettore di fondi pubblici, come quella di cui al procedimento principale, non soddisfa i requisiti di un bilanciamento equilibrato. Infatti, rispetto a un obbligo di dichiarazione unito a un controllo del contenuto della medesima esercitato dalla commissione superiore, di cui spetta allo Stato membro interessato garantire l'efficacia dotando detto organo dei mezzi necessari a tal fine, una simile pubblicazione rappresenta una lesione considerevolmente più grave dei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta, senza che tale aggravamento possa essere compensato dagli eventuali benefici che potrebbero derivare dalla pubblicazione dell'insieme di tali dati ai fini della prevenzione dei conflitti di interessi e della lotta alla corruzione", ivi, punto n 112.

nei termini della *stretta necessarietà* (nella quale il criterio di efficacia sembra avere minore o nessuna cittadinanza), ma, all'esito dei giudizi, la Corte appare sempre meno propensa ad ammettere la liceità dei trattamenti oggetto delle cause principali, in quanto fondati sull'applicazione del presupposto di liceità di cui all'art. 6, par. 1, lett. e). Tuttavia, una più attenta considerazione delle circostanze specifiche oggetto dei giudizi ci consente di leggere non solo in modo più equilibrato lo sviluppo di questa giurisprudenza (riconoscendole un tasso significativo di coerenza interna), ma anche di trarre alcune indicazioni particolarmente preziose per la nostra indagine. Infatti, il maggiore rigore applicato dalla Corte non pare, invero, dipendere da una differente configurazione del *requisito di necessità*, che – anzi – pare mantenere nel tempo uno schema sostanzialmente stabile. Anche quando ricorre alla formula lessicale della "stretta necessità" (su cui però vedi subito *infra*), il giudizio della Corte resta ancorato al modulo della *proporzionalità*: la circostanza che siano immaginabili o concretamente disponibili mezzi meno intrusivi di quelli sperimentati mediante il trattamento dei dati oggetto di giudizio non impedisce – di per sé – di identificare e considerare soddisfatta la relazione di strumentalità necessaria; occorre – infatti – che tali mezzi meno pregiudizievoli siano anche idonei a conseguire gli obiettivi di interesse generale in modo altrettanto efficace[40]. Pertanto, è possibile riconoscere un nucleo essenziale utile a identificare la relazione di strumentalità necessaria, un nucleo caratterizzato dall'integrazione con principio di minimizzazione e dal ruolo riconosciuto all'*efficacia* del trattamento, quale parametro di legittimazione a fronte di eventuali soluzioni alternative, pure meno intrusive. Ciò che muta, nei diversi casi considerati da questa giurisprudenza, è piuttosto la *tipologia* del trattamento oggetto di giudizio, e di conseguenza l'impatto che tale tipologia di trattamento è suscettibile di determinare in termini di serietà e gravità del pregiudizio arrecato al diritto alla tutela dei dati personali. Determinante, sotto questo profilo, è che la finalità di interesse pubblico sia adempiuta mediante la *comunicazione al pubblico* ovvero mediante *la diffusione tramite pubblicazione in rete* dei dati personali, dal momento che è la generalizzata accessibilità o disponibilità dei dati personali così realizzata a concorrere in modo decisivo alla *serietà/gravità* della compressione del diritto alla tutela dei dati personali[41].

[40] Questo schema di test utile a verificare la relazione di strumentalità necessaria è affermato in tutte le sentenze analizzate: cfr. C-524/06, punto n. 62; C-73/16, punto n. 113; C-439/19, punto n. 110; C-184/20, punto n. 85.

[41] Il criterio che riconduce la gravità dei potenziali pregiudizi a quelle tipologie di trattamento che comportano l'accessibilità generalizzata dei dati è chiaramente strutturato nella giurisprudenza della corte, tant'è che lo ritroviamo anche in decisioni in cui l'oggetto di causa non prevede questa tipologia di trattamento; come si legge in *Puškár*, per "verificare se la

Questa circostanza ci consente anche un'ulteriore osservazione: come si è detto, qualsiasi trattamento dei dati personali comporta – alla luce del diritto alla tutela dei dati personali – una incisione/compressione di una sfera giuridicamente protetta; pertanto, l'apprezzamento, da parte della Corte di Giustizia, di differenti gradazioni quanto alla serietà/gravità dell'incisione operata da *differenti tipologie* di trattamento[42] fornisce alcune indicazioni che è utile e necessario mettere a sistema. La comunicazione al pubblico, la pubblicazione, la diffusione via internet di dati personali costituisce, agli occhi della Corte, una tipologia trattamento che – di per sé – rappresenta un fattore di *grave* incisione nella sfera giuridica degli interessati. Così *grave* da chiamare in causa presupposti e criteri di bilanciamento *ulteriori* rispetto a quelli che (già) caratterizzano e sono incorporati nella clausola di *necessarietà* di cui all'art. 6, par. 1, lett. e). In questi casi, infatti, Corte chiama in causa esplicitamente i meccanismi di bilanciamento di cui all'art. 52, comma 1 della Carta dei diritti fondamentali dell'UE, quelli cioè che presidiano la possibilità di apportare limitazioni ai diritti fondamentali, meccanismi che – a giudizio della Corte – trovano espressione nella clausola contenuta in chiusura dell'art. 6, par. 3 dello stesso regolamento[43], dove si tratta della base giuridica del trattamento di cui alle lett. c) ed e) ("Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito"). Identica emersione ed espressione di questa diversa accezione del requisito di *necessità* si trova all'art. all'art. 23, par. 1 del regolamento (anche per come richiamato dall'art. 6, par. 4)[44].

redazione dell'elenco controverso sia necessaria all'espletamento dei compiti di interesse pubblico di cui al procedimento principale [occorre] tenere conto, in particolare, della finalità esatta della redazione dell'elenco controverso, degli effetti giuridici a cui sono sottoposte le persone che vi sono iscritte e *del carattere pubblico o meno di tale elenco*", cfr. C. 73/16, punto n. 111 (corsivo aggiunto).

[42] Il fatto che la Corte di giustizia riconosca diverse graduazioni della gravità delle limitazioni al diritto protetto dall'art. 8 della Carta dei diritti fondamentali, a seconda della tipologia di trattamento dei dati in questione, è sottolineato da Pitruzzella G. (2022), "Dati fiscali e diritti fondamentali", in *Diritto e pratica tributaria internazionale*, 2, 668: "Allo stesso modo, l'accesso di autorità pubbliche a tali informazioni costituisce un'interferenza nel diritto Carta, comportando il processo di dati personali. Questa ingerenza, a seconda del tipo di dati trasmetti e della loro ampiezza, costituisce un'ingerenza di diversa intensità, che può spaziare in uno spettro da 'non grave' a 'grave' a 'molto grave', con ripercussioni sull'applicazione del test di proporzionalità fondamentale alla protezione dei dati personali previsto dall'art. 8 della Carta".

[43] Cfr. C-184/20, punto n. 69.

[44] L'art. 23, par. 1 autorizza il diritto dell'Unione o dello Stato membro di limitare "mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza

È invece elemento significativo che tale richiamo all'art. 52, par. 1 della Carta non venga operato nelle altre due sentenze (nelle quali il trattamento effettuato è di tipologia differente da quella della comunicazione al pubblico/diffusione), nelle quali il criterio di apprezzamento del trattamento è ricondotto unicamente a quanto disposto all'art. 6, par. 1, lett. e). Il che, evidentemente, non può significare che – in questo secondo caso – non sia in questione un bilanciamento tra la tutela dei dati personali e gli interessi pubblici curati/eseguiti mediante il trattamento, ma piuttosto che nei due casi il bilanciamento avviene secondo uno schema in parte differente, e che il discrimine tra l'applicazione dell'uno e dell'altro possa essere individuato nel superamento di un valore-soglia circa la *serietà/gravità* della limitazione sofferta dalla tutela dei dati personali. Una sovrapposizione tra i due criteri di valutazione (e – al limite – la loro confusione) può derivare dalla circostanza che in entrambi casi gioca un ruolo un criterio declinato nei termini della *necessarietà strumentale* (da articolare secondo il principio di proporzionalità); infatti, anche le limitazioni dei diritti fondamentali "possono essere apportate (…) solo laddove siano *necessarie* e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui" (art. 52, par. 1 della Carta). E tuttavia, nei due casi la necessarietà strumentale svolge un ruolo differente: nel caso del presupposto di liceità, il *requisito di necessità* è un carattere predicato con riferimento al *trattamento dei dati* (*i.e.*, è lecito il trattamento che è necessario all'esecuzione di un compito di interesse pubblico), nel caso dell'art. 52, par. 1 della Carta, il *requisito di necessità* indica la misura entro la quale sono considerate ammissibili le limitazioni ai diritti e alle libertà fondamentali sanciti dalla Carta. La distinzione, anche concettuale, tra i due meccanismi è stata opportunamente ribadita anche dall'EDPS[45].

Alla luce della giurisprudenza appena analizzata, si può allora desumere quanto segue. Nell'ambito dell'applicazione del diritto dell'Unione, quando

dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare" i rilevanti diritti e interessi (anche pubblici) *ivi* elencati alle lettere da a) a j); l'art. 6, par. 4 autorizza invece l'atto "legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia" dei medesimi diritti e interessi elencati all'articolo 23, a trattare i dati personali per una finalità ulteriore, diversa ed *incompatibile* rispetto a quella in vista della quale erano stati raccolti in origine, quando non sia stato acquisito il consenso dell'interessato.

[45] "'*Necessity*' is also a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU secondary law. However, necessity of processing operations in EU secondary law and necessity of the limitations on the exercise of fundamental rights refer to different concepts"; cfr. EDPS (2016), *Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights. Background paper*.

venga in questione un trattamento dei dati giustificato dall'esecuzione di compiti di interesse pubblico o in ragione dell'esercizio di poteri pubblici, il *presupposto base* di liceità del trattamento è quello (attualmente) disegnato dall'art. 6, par. 1, lett. e) del GDPR, secondo le caratteristiche che abbiamo descritto più in alto. Tale regime *costituisce già un bilanciamento tra le esigenze di tutela dei dati personali ed il soddisfacimento/la cura/il perseguimento di interessi pubblici* (quale specifica, distinta, declinazione dell'interesse a garantire la circolazione di tali dati[46]), un criterio che potremmo definire *de minimis*, che si applica alle intromissioni nel diritto alla tutela dei dati personali che – proprio in ragione dell'applicazione di tale regola – vengono a qualificarsi come intromissioni di minore entità/gravità, e come tali già risolte dal bilanciamento incorporato nel GPDR[47]. Quando il grado e la

[46] In effetti, come per altro noto, il GDPR non costituisce una disciplina di sola garanzia e tutela delle esigenze di protezione dei dati personali, esso risponde anche all'esigenza di "libera circolazione di tali dati" (art. 1, par. 1). Pertanto, nel suo complesso la disciplina posta dal regolamento va intesa come un equilibrio regolatorio tra queste due esigenze (come per altro implicitamente richiesto già all'art. 16 del TFUE e dall'art. 39 del TUE). Nella misura in cui una disciplina uniforme abbatte le barriere alla circolazione, la scelta della tipologia di fonte mediante la quale disporre le regole (il regolamento) costituisce di per sé una misura di a tutela della circolazione; e, tuttavia, poiché anche i principi, i singoli istituti e le regole procedurali poste a tutela dei dati costituiscono anch'essi una potenziale barriera/ostacolo alla libera circolazione dei dati, anche l'ampiezza, la profondità ed il livello di tutela assicurati dalle disposizioni del regolamento rappresentano il punto di caduta in termini di contemperamento tra queste esigenze. Ciò che vale, pertanto, anche con riferimento alla regola di legittimazione del trattamento dei dati per l'esercizio di compiti di interesse pubblico. Il fatto che il regolamento assegni agli Stati membri i margini di adeguamento/adattamento di cui si è discusso comporta (in questo senso) che gli Stati dispongono del margine di manovra per alterare questo bilanciamento, ma non anche che lo spazio residuo non coperto da queste discipline ulteriori non sia presidiato (e riempito di significato) dall'esigenza di tutela della libera circolazione dei dati. Il che vale, a ben vedere, anche per la circolazione dei dati *all'interno del settore pubblico*. Infatti, la *necessary clause* fissata all'art. 6(1)e) costituisce lo *standard* di base anche per il trattamento dei dati che consiste nella comunicazione dei dati da un'amministrazione all'altra. In assenza di una disciplina nazionale di adattamento, essa segna il punto di equilibrio (stabilito dal GPDR) tra tutela dei dati personali e circolazione dei dati all'interno del settore pubblico; in presenza di una disciplina di adattamento, il punto di equilibrio tra le due esigenze sarà (eventualmente) fissato da questa diversa regola (su cui, vedi *infra* gli esempi illustrati nel par. 4 del presente capitolo), ma resterà un punto di equilibrio. Con riferimento a "the dual objectives of european data regulation", Lynskey conclude che "data protection is probably best characterized as hybrid regulation, or a 'cluster concept'" (cfr. Lynskey O. (2015), *The Foundations of EU Data Protection Law*, cit., 75). Cfr. anche Balducci Romano F. (2015), "La protezione dei dati personali nell'Unione Europea tra libertà di circolazione e diritti fondamentali dell'uomo", *Rivista italiana di diritto pubblico comunitario*, 2016, 1619-1660.

[47] Si noti che a tale bilanciamento corrisponde il riconoscimento ai titolari del trattamento del *potere* di trattare dati altrui (e agli interessati la condizione di correlativa *soggezione*, con-

serietà di incisione/limitazione del diritto alla tutela dei dati personali superano una certa *soglia*, il criterio di bilanciamento "sale di livello", e viene in qualche modo assorbito nell'ambito dell'operatività dell'art. 52, comma 1 della Carta. Dall'analisi della giurisprudenza, possiamo individuare almeno *due livelli* di ingerenza/gravità, con distinte conseguenze. Nel caso di gravità intermedia (determinata dai rischi connessi alle caratteristiche del trattamento effettuato e dei dati oggetto di tale trattamento), le conseguenze apprezzabili possono essere identificate in un irrigidimento del criterio di proporzionalità e – soprattutto – nella circostanza per cui il giudice sembra richiedere che la base legale *ricomprenda in modo chiaro, se non esplicito, gli obiettivi del trattamento in questione*[48]. In altre parole, al crescere della serietà della limitazione sofferta dalla tutela dei dati personali (in particolare, anche in ragione della quantità dei dati trattati), sembra ridursi il margine di manovra dell'amministrazione nel *desumere* in modo *implicito*, alla stregua del solo criterio della *strumentalità necessaria*, i trattamenti lecitamente realizzabili.[49] In tale caso, cioè, (quanto i dati trattati siano una quantità sufficientemente ampia, dato il contesto in cui si svolge il trattamento), sarà necessario che la base giuridica espliciti la finalità del trattamento e il tipo di dati che possono essere trattati: ciò che però non implica ancora che questa

sistente nel subire il trattamento dei dati personali a prescindere dal consenso). Tale bilanciamento – fissato nella disciplina del GDPR – a sua volta corrisponde all'esigenza, perseguita da questa disciplina, di conciliare l'esigenza di tutela dei dati personali con l'altra esigenza, quella di assicurare che questi possano essere trattati per esigenze di interesse pubblico. Il riconoscimento di una serie di diritti in capo all'interessato, da esercitarsi nei confronti del titolare del trattamento – anche all'interno di questa condizione di *soggezione* – confermano lo schema descrittivo di una quota di potere (attribuita dalla normativa *de qua* in capo al titolare del trattamento) che viene esercitato nei confronti di una sfera giudica protetta. Sul punto, e con specifico riferimento alla relazione che si instaura tra titolari di trattamenti connessi all'esercizio di funzioni pubbliche ed interessati, vedi le considerazioni, già richiamate, formulate da Carullo G. (2020), "Trattamento di dati personali da parte delle pubbliche amministra-zioni e natura del rapporto giuridico con l'interessato", *cit.*, *passim*. In termini analoghi (sebbene non con specifico riferimento ai titolari che esercitano funzioni pubbliche) cfr. Piraino F. (2017), "Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", in *Nuove leggi civ. comm.*, 2, par. 3.

[48] Cfr. C-73/16, punto n. 110.

[49] "In generale, più i trasferimenti di dati sono generalizzati, ampi e permanenti, più la base legislativa deve essere solida, dettagliata ed esplicita, poiché tali trasferimenti di dati rappresentano un'interferenza maggiore nella salvaguardia della protezione dei dati. Al contrario, più le richieste di comunicazione sono discrete e limitate – di solito in relazione a uno o pochi interessati soltanto, o anche in relazione a una quantità limitata di dati – più è probabile che tali richieste possano essere eseguite a livello di singole richieste amministrative, rimanendo la clausola di abilitazione legislativa piuttosto ampia e generica", così le conclusioni dell'Avvocato generale, causa C-175/20, par. 81, senza tuttavia che tale base giuridica consistere in atto legislativo dell'assemblea.

base giuridica sia costituita da un atto *formalmente* legislativo: l'amministrazione può cioè concorrere in questo senso, mediante propri atti, ad integrare la base giuridica, mediante la predisposizione di indicazioni chiare, la cui applicazione sia prevedibile e vincolante per i consociati, e che indichino le finalità dei trattamenti e i dati che ne sono oggetto[50].

Il livello più elevato di gravità è identificabile nella *tipologia* di trattamento dei dati corrispondente alla *comunicazione al pubblico* (sotto forma di accessibilità generalizzata, ovvero di pubblicazione o diffusione via internet): qui è la specifica tipologia di trattamento a determinare il grado (elevato) di "*seriousness*" della limitazione sofferta dal diritto alla tutela dei dati personali, in ragione del fatto che alla potenziale dispersione dei dati personali corrispondono rischi connessi all'uso ulteriore di tali informazioni (con impatti imprevedibili e potenzialmente dannosi a carico degli interessati). A questo livello di gravità consegue un effetto principale, ovvero che la base giuridica del trattamento deve *prevedere esplicitamente la tipologia del trattamento*[51] e consistere *in un atto legislativo*[52], mentre l'applicazione del criterio di *necessità* assume i suoi caratteri più stringenti, nei quali il criterio di efficacia della soluzione di trattamento cessa di svolgere un ruolo effettivo nel bilanciamento, mentre diventano assorbenti i motivi connessi alla astratta percorribilità di misure alternative (anche meno efficaci, ma) meno invasive.

Va per altro notato che, proprio l'indispensabilità di un atto legislativo, comporta anche un'ulteriore conseguenza, ovvero che il trattamento così *disposto dalla legge*, soprattutto quando si traduce in un obbligo di pubblicazione/diffusione dei dati personali mediante la rete, finisce per poter essere inquadrato non solo nella fattispecie di cui all'art. 6, par. 1, lett. e) del GDPR, ma anche nella fattispecie di cui alla lett. c) (ossia, un trattamento necessario

[50] Cfr. *ivi*, par. 81-82, nonché Corte di giustizia, C.175/20, par. 68-69.

[51] In questo stesso senso, si veda il Parere della Corte (Grande Sezione) del 26 luglio 2017 (Parere 1/15): "Si deve aggiungere che il requisito secondo cui eventuali limitazioni all'esercizio dei diritti fondamentali devono essere previste dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione all'esercizio del diritto interessato".

[52] Questo elemento è chiarito in modo efficace, ad esempio, nelle *Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies* (General Secretariat of the Council To: Working Party on Fundamental Rights, Citizens Rights and Free Movement of Persons), 2014, dove si afferma che "This means that the limitation must be provided for in one of the Union binding legal acts referred to in Article 288 TFEU adopted in accordance with the relevant Treaty provisions. In addition, following the case law of the Court regarding the essential/non-essential elements of a legislative act, the seriousness of an interference with the fundamental rights may require the direct involvement of the Union legislature, i.e. that the rules on the limitation of the fundamental rights at stake should be set out in the legislative act itself (or basic act) and not left for adoption through a delegated or an implementing act".

per adempiere un obbligo legale al quale è soggetto il titolare del trattamento), come abbiamo visto accadere con riferimento alla causa C-184/20[53]. Sotto questo profilo, è consolidata la giurisprudenza della Corte di giustizia che tende ad ammettere le limitazioni al diritto alla tutela dei dati personali conseguenti ad obblighi di pubblicazione/diffusione via web (disposti per finalità di tutela del diritto alla trasparenza amministrativa) solo in esito ad un giudizio di *stretta indispensabilità* della misura[54], secondo un approccio diverso da quello adottato ad esempio più di recente dalla Corte costituzionale italiana, che ha invece optato per l'applicazione di un meno rigido criterio di ragionevolezza[55].

3. Il margine di manovra disponibile degli Stati membri e l'integrazione di standard legali ulteriori

Lo standard legale disegnato dalla *necessary clause* costituisce dunque lo schema di base, indicato nel GDPR, per il trattamento dei dati personali per l'esercizio di compiti di interesse pubblico. Nello stesso art. 6 del regolamento sono però contenute anche le clausole che aprono la possibilità agli Stati membri di "mantenere o introdurre" disposizioni specifiche per adeguarne l'applicazione. Tenuto conto della *natura della fonte* e degli obiettivi avevano spinto il legislatore dell'Unione a sostituire la direttiva con un regolamento, le clausole contenute all'art. 6, ai paragrafi 2 e 3, rivestono una funzione specifica, quella di aprire spazi di manovra (*margin of discretion*) ai legislatori nazionali, spazi altrimenti preclusi. Pertanto, con riferimento al regime giuridico del trattamento dei dati personali ai fini dell'esercizio di funzioni di interesse pubblico, il GDPR mantiene sostanzialmente un assetto di co-regolazione UE-Stati membri.

Un primo punto di interesse è capire quale ampiezza abbia questo spazio di manovra, e – soprattutto – che tipo di rapporto si instaura con le disposi-

[53] Cfr. *ivi* il punto n. 71.

[54] Cfr. CGUE, *Volker und Markus Schecke* (C-92/09) e *Hartmut Eifert* (C-93/09), punto n. 81.

[55] Cfr. Corte cost. n. 20/2019, su cui – proprio con riferimento alle diversità di approccio rispetto alla giurisprudenza della Corte di giustizia, sia consentito rinviare a Ponti B. (2019), "Il luogo adatto dove bilanciare. Il 'posizionamento' del diritto alla riservatezza e alla tutela dei dati personali *vs* il diritto alla trasparenza nella sentenza n. 20/2019", in *Istituzioni del Federalismo*, 2, 529 ss.; nonché Pollicino O. e Repetto G. (2019), "Not to be Pushed Aside: the Italian Constitutional Court and the European Court of Justice", in *VerfBlog*, 2/27, disponibile in https://verfassungsblog.de/not-to-be-pushed-aside-the-italian-constitutional-court-and-the-european-court-of-justice

zioni del GDPR, non solo quelle più direttamente rilevanti, ossia il presupposto di liceità disegnato dalla *necessary clause*, ma con l'intero impianto del regolamento. In particolare, si tratta di capire se il margine di manovra assegnato agli Stati membri vada inteso come margine di specificazione che assuma il livello di tutela assicurato ai dati personali con la *necessary clause*, come una soglia minima-essenziale, rispetto alla quale i legislatori nazionali sono autorizzati a intervenire, nel rispetto del GDPR, solo per arricchire, aggiungere, precisare i requisiti che rendono lecito il trattamento dei dati personali a fini dell'esercizio di compiti di interesse pubblico. In questo senso, lo spazio di manovra accordato al legislatore nazionale andrebbe letto come abilitato solo ad *aggiungere*, *arricchire* e *completare* il quadro dei presupposti e delle condizioni di trattamento dei dati a tali fini, mentre lo standard legale complessivamente disegnato dal GDPR andrebbe considerato come una soglia minima al di sotto della quale non sarebbe consentito scendere. Il dato positivo, tuttavia, non risulta del tutto perspicuo – sotto questo profilo. In effetti, il testo dell'art. 6, par. 2 sembra puntare nella direzione indicata, dal momento che le disposizioni più specifiche che possono essere adottate per adeguare l'applicazione delle norme di cui al par. 1, lett. e), sono disposizioni volte a determinare "*con maggiore precisione requisiti specifici* per il trattamento e *altre misure atte a garantire* un trattamento lecito e corretto". Il legislatore locale, quindi, pare autorizzato ad introdurre misure a precisazione dei requisiti (già) indicati nel GDPR, ovvero a introdurne misure *ulteriori*, *aggiuntive*, a garanzia di un trattamento lecito e corretto. Questa lettura, però, pare in qualche modo contraddetta (o, comunque, alterata in ordine alla *direzione* dello spazio di manovra disponibile) da alcuni termini impiegati, invece, nel successivo par. 3. Qui, infatti, con riferimento alla base giuridica su cui si fonda il trattamento dei dati, si dice che essa "potrebbe contenere disposizioni specifiche per *adeguare* l'applicazione delle norme del presente regolamento: tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX.". Per un verso, la lista degli ambiti già coperti dalle disposizioni del GDPR in cui il legislatore dello Stato membro è autorizzato ad intervenire nel declinare la base giuridica del trattamento di cui al par. 1, lett. e) è cospicua (e, per altro, solo esemplificativa, dato che è introdotta dalla locuzione "tra cui"); ma è l'uso del termine "adattare" (*to adapt*, nella versione in lingua inglese; *adaptér*, in

quella francese), a suscitare perplessità, dal momento che si tratta di una locuzione *neutra*, che non implica (a differenza di "precisare"), una specifica direzione all'azione di *adeguamento* della disciplina *de qua*. Quindi, in teoria, l'adattamento potrebbe anche consistere nella adozione di una misura idonea a derogare *in peius* il livello di garanzia stabilito dalla corrispondente disciplina del GDPR. Per fare un esempio, in materia di *limitazione della finalità*, la disciplina nazionale potrebbe introdurre una regola meno stringente di quella ad esempio indicata all'art. 6, par. 4, nel quale sono indicati i criteri da utilizzare per verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti. Inoltre, occorre considerare che è lo stesso regolamento che – per il perseguimento degli interessi e delle esigenze elencate all'art. 23 – acconsente alla legge dello stato membro di apportare limitazioni agli obblighi (posti in capo ai titolari del trattamento, con particolare riferimento per quelli di cui all'art. 5) e ai diritti (degli interessati), purché la "limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica". Ciò comporta che, – se la finalità del trattamento può essere inquadrata in uno degli interessi/esigenze elencate all'art. 23(1) – la misura di adattamento potrebbe anche comportare una *reformatio in peius* dei requisiti e degli standard fissati dal GDPR[56].

In dottrina, si è notato che questa contraddizione sarebbe da intendersi come solo apparente, dal momento che solo il par. 2 conterrebbe una *delegation of power* agli Stati membri: in questo senso, il par. 3 andrebbe letto come "*as a limitation of the statutory exceptions*", e quindi come una specificazione del paragrafo precedente (il cui contenuto e la cui "direzione" non potrebbe quindi contraddire)[57]. Tuttavia, questa lettura appare smentita, quantomeno sotto il profilo della prassi, da alcune scelte operate proprio dagli Stati membri in applicazione di suddette clausole (vedi subito *infra*), così che l'ambiguità del testo resta in qualche modo confermata. Per altro, non appare comunque agevole, in via generale, distinguere tra *precisazione* e *adattamento*, anche tenuto conto del fatto che agli Stati membri sembrano da riconoscersi margini più consistenti in sede di esecuzione (anche sul piano

[56] Per una applicazione in concreto di questo schema argomentativo, anche con riferimento al trattamento dei dati personali di cui all'art. 6(1)(e), cfr. Corte di giustizia, C-269/21 *Norra Stockholm Bygg AB*, cit.

[57] Wagner J. e Benecke A. (2016), "National legislation within the framework of the gdpr", in *European Data Protection Law Review (EDPL)*, 2(3), 353-361, in part. 354-355. In termini analoghi, mentre la disposizione di cui all'art. 6(2) conterrebbe una clausola che abilita una disciplina interna ad *integrazione* rispetto a quella del regolamento, quella di cui all'art. 6(3) conterrebbe invece una clausola che abilita una disciplina interna di sola *attuazione*, così Pizzetti F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. II, Torino, 18.

della normativa interna), sia in ragione del fatto che è lo stesso atto normativo a qualificarsi come "*general regulation*", sia perché le esigenze di coerenza e di comprensibilità della disciplina nazionale (a specificazione, adattamento o anche limitazione – ove consentito – delle disposizioni del GDPR) possono giustificare la riproduzione di parti del testo del regolamento (i cd. *repetitive content*) negli atti normativi nazionali, ciò che è invece generalmente proibito sulla base di una giurisprudenza consolidata[58]. Si deve, inoltre, considerare la circostanza – già più volte sottolineata – per cui il GDPR interviene a valle di un lungo periodo nel quale le legislazioni nazionali, in recepimento della direttiva 95/46/CE, si sono stratificate, e che la clausola contenuta al par. 2 è diretta esplicitamente non solo a consentire agli Stati membri di *introdurre* nuove disposizioni, ma anche di *mantenere* quelle esistenti. In altre parole, sebbene in astratto lo schema del *dual legality standard* possa essere ricostruito (con ottimi argomenti sistematici) nel senso di riconoscere alla *necessary clause* un ruolo di chiusura del sistema, aperto però a soluzioni nazionali *specifiche* e *più garantiste*, il quadro effettivo deve fare i conti non solo con le concrete scelte operate dai paesi membri nell'utilizzare i margini di manovra concessi, ma anche con le oggettive condizioni di contesto.

4. Tipologie e approcci del *dual legality standard*

4.1. Uno sguardo alle discipline di adeguamento GDPR

L'adozione del GDPR ha costretto i Paesi membri a mettere mano alle rispettive discipline interne in materia di tutela dei dati personali, al fine di allineare il quadro normativo interno. Un'analisi selettiva, concentrata sui profili relativi al trattamento dei dati personali per l'esercizio di compiti di interesse pubblico, può essere utile per evidenziare come – a seconda delle

[58] *Ibidem*, 358-361. Notevoli, in effetti, possono essere le problematiche connesse alla leggibilità del testo normativo, nella misura in cui si scelga una strada differente rispetto all'integrazione *ripetitiva* di pezzi del GDPR nella disciplina interna. Segnala queste difficoltà, con riferimento alla legislazione francese di allineamento al GDPR, Tambou O. (2018), "France: the french approach to the gdpr implementation", in *European Data Protection Law Review (EDPL)*, 4(1), 88-94, in part. 89-90, ma analoghe difficoltà sono rimarcate in esito all'allineamento della disciplina italiana ("con il risultato che oggi come oggi non esiste un unico testo leggibile, intellegibile e comprensibile dal quale ricavare il contenuto normative. È sempre necessaria una sfibrante opera d'interpretazione per ricostruire la norma vigente per effetto di un gioco pressoché continuo di rinvii che rende praticamente indispensabile l'impiego di una tavola sinottica", così Francario F. (2021), "Protezione dei dati personali e pubblica amministrazione", in *giustiziainsieme.it*, par. 4, disponibile al sito https://shorturl.at/jmL29 (1.5.2023).

strategie adottate dagli Stati membri – il *dual legality standard* possa essere concretamente declinato. Infatti, poiché il margine di manovra è nella disponibilità dello Stato membro, a seconda di come questo spazio viene effettivamente utilizzato, ci troveremo davanti a declinazioni variabili dello standard legale, frutto dell'interazione/integrazione tra le regole poste dallo standard *di base* (la *necessary clause*) e le regole poste a livello nazionale. Ne emergono strategie molto differenziate, che non è qui possibile nemmeno tratteggiare nella loro complessità, anche perché ciascuna di queste risente in modo particolare di una serie di fattori complessi, ed ulteriori, rispetto al solo dato positivo[59]. Piuttosto, si procederà a cogliere da alcuni specifici esempi, alcuni modelli di utilizzo del margine di manovra, che appaiono significativi anche come parametro di confronto rispetto alle scelte compiute dal legislatore nazionale italiano.

Una prima distinzione di massima va operata tra normative interne *verticali*, volte a disciplinare l'esercizio di funzioni specifiche o compiti determinati, e discipline o disposizioni di carattere *trasversale*, che invece si riferiscono ad aspetti più o meno circoscritti del trattamento dei dati personali, e che risultano applicabili a intere classi di funzioni pubbliche (più o meno ampie). Nel primo caso, le singole discipline possono contenere anche indicazioni molto precise e su numerosi e qualificanti aspetti del trattamento dei dati personali rilevanti per l'esercizio di una specifica funzione pubblica. La numerosità di discipline particolari con queste caratteristiche è certamente indice dell'attenzione e del rilievo che la tutela dei dati personali riveste nell'ambito di uno dato ordinamento nazionale. È il caso ad esempio, dell'ordinamento tedesco, nel quale il coordinamento anche solo *formale* con il GDPR della legislazione esistente ha comportato l'adozione di un migliaio di emendamenti specifici, relativi ad un complesso di circa centocinquanta leggi diverse[60]. Analogo è il caso austriaco, dove due successivi interventi legislativi hanno provveduto ad allineare al GDPR, complessivamente, circa duecentoventi atti legislativi[61]. Appare però più interessante – ai fini del nostro studio – concentrare l'attenzione su quegli interventi di carattere generale e trasversale, introdotti (oppure riproposti, ovvero adattati) in seguito, per effetto o con l'occasione dell'adozione del GDPR. Infatti, da queste

[59] Per una panoramica delle legislazioni nazionali di allineamento al GDPR, si v. Mc Cullagh K., Tambou O., Bourton S. (2019), *National adaptations of the GDPR*, Blogdroiteuropéen, disponibile all'indirizzo https://hal.science/hal-03521416

[60] Questi dati sono riportati in Etteldorf C. (2019), "Germany revisited: the second data protection adaption and implementation act", *European Data Protection Law Review (EDPL)*, 5(3), 397-403, in part. 397.

[61] Cfr. Leissler G., Reisinger P., Böszörmenyi J. (2019), *National Adaptations of the GDPR in Austria*, in Mc Cullagh K., Tambou O., Bourton S. (eds.), *National Adaptations of the GDPR*, Collection Open Access Book, Blogdroiteuropeen, Luxembourg February 2019, 37.

scelte emerge in modo *più evidente* l'adozione di questa o quella opzione in termini di adattamento, integrazione, modifica dello *standard legale* uniforme (quello delineato dalla *necessary clause*), mediante un utilizzo del margine di manovra di carattere *sistemico*, e quindi idoneo ad evidenziare i caratteri dello *standard legale* adottato in sede locale. Procediamo quindi a evidenziare solo alcune di queste scelte, tratte da distinti ordinamenti statali, che appaiono esemplari sotto questo profilo.

a) regimi differenziali per specifiche tipologie di dati

La storica, risalente disciplina francese di tutela dei dati personali è stata radicalmente modificata, ed in parte significativa abrogata, per allinearne i contenuti al GDPR[62]. Il nuovo testo dell'art. 30 della *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, introduce una disciplina relativa al trattamento di una specifica tipologia di dati personali, ossia quei dati che ricomprendono il *numéro d'inscription des personnes au répertoire national d'identification des personnes physiques* (cioè il codice identificativo di iscrizione all'anagrafe). La disciplina in questione stabilisce che con un decreto del Conseil d'État, previo parere della CNIL, vengano determinate le categorie di responsabili del trattamento che possono trattare i dati che ricomprendono il *numéro d'inscription*, nonché le finalità per il perseguimento delle quali questi trattamenti possono essere effettuati. Tuttavia, tale regime non si applica quando i medesimi dati sono oggetto di trattamento*:* 1) per finalità esclusive di statistica ufficiale, ad opera del servizio statistico ufficiale; 2) per finalità esclusive di ricerca scientifica o storica; ovvero, 3) per trattamenti finalizzati ad erogare i servizi di amministrazione elettronica di cui all'*ordonnance* n. 2005-1516 dell'8 dicembre 2005 relativa agli scambi elettronici tra gli utenti e le autorità amministrative e tra le stesse autorità amministrative. Analogo approccio si può constatare con riferimento alla categoria *des données concernant la santé des personnes*: fissazione di un regime specifico per il trattamento della categoria dei dati[63], e previsione di un regime (semplificato) in deroga, quando il trattamento sia svolto da organismi che esercitano compiti di interesse pubblico (identificati con apposito provvedimento del ministro della salute) che abbiano per finalità la risposta in via d'urgenza ad una *alerte sanitaire* ai sensi del *Code de la santé*

[62] Cfr. Tambou O. (2018), "France: the french approach to the gdpr implementation", cit.; Id. (2019), *The French Adaptation of the GDPR*, in Mc Cullagh K., Tambou O., Bourton S. (eds.), *National Adaptations of the GDPR*, cit., 52.

[63] Tale regime è definito nella *section 3 du chapitre III du titre II, Loi n° 78-17 du 6 janvier 1978*.

publique[64]. In entrambi questi casi, è significativo notare che la strategia normativa consiste nel ricavare, all'interno di un regime generale di trattamento di una specifica tipologia o categoria di dati, un sub-regime *in deroga*, giustificato anche dall'esigenza di abilitare l'erogazione di servizi amministrativi telematici/digitali (nel caso del *numéro d'inscription*) o servizi di sanitari d'urgenza (nel caso dei dati idonei a rivelare lo stato di salute). Si noti che, ad esempio, anche la disciplina danese contiene una misura specifica di autorizzazione di trattamento della medesima tipologia di dati[65].

b) misure trasversali di trasparenza del trattamento dei dati per fini di interesse pubblico

Ancora nella disciplina francese troviamo una misura trasversale, diretta a fare trasparenza su alcune tipologie di trattamenti, ed in particolare: 1) i trattamenti di interesse per la sicurezza dello Stato, la difesa o la pubblica sicurezza o il cui scopo è la prevenzione, l'indagine, l'osservazione o il perseguimento di reati o l'esecuzione di condanne penali o misure di sicurezza.; nonché: 2) il trattamento di dati personali effettuato per conto dello Stato, nell'esercizio delle sue prerogative di pubblico potere, che riguardano dati genetici o dati biometrici necessari per l'autenticazione o la verifica dell'identità delle persone. In entrambi questi casi, quando il trattamento sia effettuato anche con mezzi automatizzati, la CNIL deve rendere disponibile sul proprio sito, in formato aperto e riutilizzabile, una serie dettagliata di informazioni concernenti tali trattamenti[66]. Si tratta, come si vede, di una misura trasversale di carattere aggiuntivo, che arricchisce il regime di trattamento per alcune specifiche finalità o per alcune tipologie di dati oggetto di trattamento, che mira a rendere conoscibile l'esistenza e le caratteristiche di trattamenti automatizzati che – per le finalità perseguite (sicurezza e difesa dello Stato, pubblica sicurezza) o

[64] Cfr. *ivi*, l'art. 67.

[65] Ai sensi del *Data protection act* danese del 2018, le autorità pubbliche sono autorizzate a trattare i dati relativi ai numeri di identificazione per finalità di identificazione univoca o come codice ti classificazione dei fascicoli (cfr. legge n. 502 de 23 maggio 2018).

[66] Si tratta, in particolare, delle seguenti informazioni: - l'atto che decide la creazione del trattamento; - la finalità del trattamento e, ove applicabile, il nome; - l'identità e l'indirizzo del titolare del trattamento o, se quest'ultimo non è stabilito nel territorio nazionale o in quello di altro Stato membro dell'Unione Europea, quelli del suo rappresentante - la funzione della persona o del servizio con cui si esercita il diritto di accesso previsto dagli articoli 49, 105 e 119; - le categorie di dati personali oggetto di trattamento, nonché i destinatari e le categorie di destinatari autorizzati a riceverne comunicazione; - se rilevanti, i trasferimenti di dati personali previsti verso uno Stato non membro dell'Unione Europea. Cfr. art. 36 Loi n° 78/1978.

per l'oggetto del trattamento (dati genetici o dati biometrici necessari per l'autenticazione o la verifica dell'identità delle persone) – sono ritenuti particolarmente rilevanti, in termini non solo di compressione del diritto alla tutela dei dati personali, ma anche della sfera di libertà e dignità della persona.

c) misure trasversali relative alla circolazione dei dati personali all'interno del settore pubblico

Significativo il caso della misura introdotta nella disciplina belga di adeguamento al GDPR[67]. Si noti come nella disciplina nazionale precedentemente in vigore ogni trattamento automatizzato o semi-automatizzato da chiunque effettuato, ivi compresi quelli effettuati a fini di esercizio di funzioni pubbliche, doveva essere comunicato preventivamente alla *Commission de la protection de la vie privée* (CPVP)[68]. Come noto, in attuazione del principio di *responsabilizzazione* di cui all'art. 5, par. 2 del regolamento, le autorità nazionali di protezione hanno perduto buona parte dei rispettivi poteri di autorizzazione preventiva, così che anche il sistema di comunicazione preventiva (mediante il quale la CPVP era posta in condizione di avere notizia delle iniziative e delle soluzioni adottate dai responsabili del trattamento, e di poter intervenire di conseguenza mediante l'esercizio di poteri di indagine, interdittivi e sanzionatori) era destinato a venire meno. Nell'utilizzare il margine di manovra assicurato dall'art. 6(2) del GDPR, il legislatore belga ha introdotto un meccanismo di natura trasversale, volto a regolamentare la circolazione dei dati all'interno del settore pubblico, e quindi la trasmissione e lo scambio dei dati *tra* amministrazioni. L'esigenza di presidiare questa specifica (e rilevante) tipologia di trattamento dei dati era stata sottolineata, nel corso della elaborazione della nuova disciplina, dal Conseil d'État, che aveva avuto modo di rimarcare come "*un transfert de données d'une autorité publique à une autre constitue une ingérence dans le droit à la protection de la vie privée des personnes concernées. En vertu de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, tel qu'interprété par une jurisprudence constante de la Cour constitutionnelle, pareille ingérence doit notamment reposer sur une base légale, être proportionnée par rapport à l'objectif poursuivi et être organisée de manière suffisamment précise pour être*

[67] Cfr. la *Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

[68] Cfr. l'art. 17 della *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*.

prévisible pour le citoyen"[69], sottolineando l'esigenza di provvedere alla "*mise en place d'un cadre législatif consciencieux pour les échanges de données à caractère personnel*"[70]. La misura introdotta a riguardo prevede che il trasferimento di dati personali debba essere *formalizzato* (per ciascun tipo di trattamento) mediante la stipulazione di un protocollo tra l'amministrazione di origine della trasmissione e quella destinataria, previa consultazione dei rispettivi DPO; tali pareri devono essere allegati al protocollo, che deve indicare le motivazioni per le quali i pareri dei DPO non siano stati eventualmente assecondati. Il protocollo deve essere pubblicato sul sito internet di ciascuna delle amministrazioni coinvolte. La disposizione prevede anche una lunga lista di potenziali contenuti del protocollo (che riflettono l'esigenza di conformare lo scambio dei dati ai principi del regolamento). Tuttavia, l'indicazione non è tassativa, potendo le amministrazioni scegliere di comune accordo quali informazioni e prescrizioni inserire effettivamente all'interno del protocollo. Tale scelta del legislatore è stata oggetto di vivaci critiche da parte del Conseil d'État e della CPVP, che hanno indicato nel carattere opzionale dei contenuti del protocollo una contraddizione con il *principio costituzionale di legalità*. Si noti che la misura del protocollo non sostituisce la base di liceità del trattamento fondata sulla *clausola di necessarietà* (che anzi è esplicitamente richiamata nella disposizione della legge), ma la integra. Si vede pertanto anche qui, all'opera, la dinamica del *dual legality standard*: la base legale di liceità del trattamento fissata dal regolamento è integrata con una misura volta a stabilire alcune salvaguardie, connesse alla circolazione dei dati personali nell'ambito del sistema pubblico. Tali esigenze si spiegano, per altro, in ragione della progressiva adesione del sistema informativo pubblico belga al principio organizzativo della *collecte unique des données à caractère personnel*[71], un principio di architettura informativa che presuppone come fisiologica e continua la circolazione delle informazioni tra le amministrazioni. Pare quindi evidente il tentativo, da parte del legislatore belga, di trovare un compromesso tra le esigenze di favorire questo indirizzo di riforma e quelle di mantenere un presidio (giocato essenzialmente in termini di *trasparenza*) rispetto ad una tipologia di

[69] Cfr. il parere della sezione legislativa del Conseil d'État sul progetto di legge, 5 settembre, 68616/21.

[70] Knockaert M. (2019), "La loi du 30 juillet 2018: l'échange de données à caractère personnel au sein du secteur public", *Revue du droit des technologies de l'information*, 74, 5-24, in part. 7-8.

[71] Cfr. Knockaert M. (2019), op. cit., 6 ss., nonché Degrave E. (2017), *L'administration belge organisée en réseaux : réutilisation des données à caractère personnel et protection de la vie privée*, in Auby J. B. e De Gregorio V., a cura di, *Données urbaines et smart cities*, Berger-Levrault, 184-187, Id. (2014), *L'e-Gouvernement et la protection de la vie privée : Légalité, transparence et contrôle*, Bruxelles.

trattamento idonea a determinare un'ingerenza rilevante nei diritti e nelle libertà dei cittadini.

Nella legislazione tedesca[72]– che dedica una specifica attenzione al trattamento dei dati che consista nel trasferimento di dati da un ente pubblico ad altro ente pubblico – il presidio rispetto alle dinamiche di integrabilità generalizzata delle banche dati pubbliche appare più robusto, dal momento che le misure trasversali a riguardo lo autorizzano solo in determinati casi, esplicitamente elencati (per altro declinati secondo lo schema della *necessary clause*)[73]. Anche in questo caso, dunque, il *dual legality standard* opera in termini di integrazione tra il livello di tutela definito in termini uniformi dal regolamento, ed un livello ulteriore, aggiunto dalla legislazione nazionale. Si noti che il meccanismo così implementato (l'esplicita autorizzazione del trasferimento di dati tra soggetti pubblici, con il conseguente, implicito divieto in tutti gli altri casi) non impedisce che il trasferimento possa essere realizzato anche nei casi non contemplati dalla norma *de qua*, ma impone che tale trattamento sia esplicitamente previsto dalla legge[74]. L'uso del margine di adattamento, realizza così un sistema *composito*, si direbbe *misto*. La medesima tipologia di trattamento (il trasferimento dei dati da un'amministrazione ad un'altra) in alcune circostanze – selezionate nella legislazione *generale* –

[72] Cfr. Bundesdatenschutzgesetz (BDSG), adottato nel luglio del 2017 ed entrato in vigore insieme al GDPR, il 25 maggio del 2018. La legislazione federale tedesca, che al pari di molte altre discipline nazionali, ha dato attuazione anche alla Direttiva UE n. 680/2015 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, con riferimento, nella parte in cui si occupa di trattamenti dei dati per l'esercizio di funzioni pubbliche trova applicazione (sotto il profilo soggettivo) solo con riferimento alle amministrazioni federali, o alle amministrazioni dei *lander*, quando questi applicano la legislazione federale. Negli altri casi, infatti, la competenza a disciplinare tale materia, con riferimento all'esercizio delle funzioni amministrative dei *lander* e degli altri livelli amministravi territoriali, spetta alla legislazione regionale (cfr. art. 1).

[73] Ai sensi dell'art. 25(1) del BDSG "Il trasferimento di dati personali da enti pubblici a enti pubblici è consentito se è necessario per l'ente trasferente o il terzo a cui i dati sono trasferiti per svolgere i propri compiti e sono soddisfatte le condizioni che consentirebbero il trattamento ai sensi dell'art. 23. La terza parte a cui vengono trasferiti i dati deve trattare i dati trasferiti solo per lo scopo per il quale sono stati trasferiti": per il dettaglio delle circostanze contemplate nell'art. 23 del BDSG, si vedano le note immediatamente successive. Si noti che la deroga copre anche le categorie di dati particolari di cui all'art. 9 del GDPR, purché siano soddisfatte anche le condizioni che autorizzano il loro trattamento, sia ai sensi dello stesso art. 9, sia ai sensi dell'art. 22 del BDSG.

[74] Come si evince anche dalle modalità con le quali il BDSG regola i rapporti di precedenza con le altre leggi federali che rechino misure di protezione dei dati personali; cfr. l'art. 1(2): "Le altre leggi federali sulla protezione dei dati prevalgono sulle disposizioni della presente legge. Se tale legislazione non disciplina in modo definitivo o per nulla una questione disciplinata dalla presente legge, allora si applica la presente legge".

è sottoposta al presupposto di liceità del trattamento formulato secondo la *necessary clause*, mentre in tutte le altre circostanze il presupposto di liceità è rimesso ad un più stringente principio di legalità.

d) misure trasversali relative alla limitazione di finalità del trattamento

Un'ulteriore misura di carattere trasversale che troviamo nelle legislazioni di allineamento al GDPR riguarda un altro aspetto centrale nei meccanismi che caratterizzano il trattamento dei dati personali per l'esercizio di compiti di interesse pubblico, ovvero l'uso ulteriore dei dati personali raccolti e detenuti nei patrimoni informativi pubblici, anche per finalità diverse da quelle che ne avevano giustificato la raccolta. La digitalizzazione delle informazioni, la circolazione e lo scambio di dati tra le componenti di ciascun sistema pubblico, l'interoperabilità dei sistemi informativi, come pure le tecnologie che consentono di mettere a frutto questa capacità di raccolta, integrazione e combinazione delle banche dati, nonché le stesse esigenze di gestione efficiente dei servizi, sono tutti fattori che cospirano nella direzione di rendere fisiologico e continuo il trattamento secondario delle informazioni, compresi i dati personali. Come si è già avuto di sottolineare, il pieno sviluppo di queste potenzialità tendenzialmente confligge con il principio di limitazione della finalità trattamento, in base al quale gli usi successivi ed ulteriori dei dati personali per finalità differenti da quelle che ne avevano giustificato la raccolta è lecito solo se questi due ordini di finalità sono tra loro non incompatibili. Alcune discipline hanno introdotto misure specifiche, di carattere trasversale, finalizzate a rimuovere o attenuare il vincolo che deriva dal principio di limitazione della finalità, modulando tale deroga in vari modi: vediamone alcuni casi esemplari. La disciplina federale tedesca elenca una serie di circostanze nelle quali il trattamento dei dati personali, per finalità diverse, è comunque consentito. Si tratta di una lista eterogenea di circostanze, in cui la *ratio* della deroga al principio di limitazione finalità del trattamento è di natura mutevole: per un verso, la deroga serve ad assicurare meglio gli interessi dell'interessato[75]; in altri casi, invece, la deroga è funzionale ad assicurare maggiore efficacia nel perseguimento di alcuni interessi

[75] Cfr. l'art. 23(1)1 del BDSG, che autorizza le amministrazioni pubbliche a trattare per uno scopo diverso da quello per il quale i dati sono stati raccolti, quando ciò sia evidentemente nell'interesse dell'interessato e non vi sia motivo di ritenere che l'interessato negherebbe il consenso se fosse a conoscenza della diversa finalità.

pubblici[76]. La disciplina chiarisce che tale deroga al principio di limitazione della finalità del trattamento copre anche l'eventuale trasferimento di dati da una amministrazione ad un'altra che risulti necessario in tali circostanze[77]. Va notato che la disciplina federale tedesca previgente contemplava già misure analoghe, sì che in questo caso il margine di manovra pare sfruttato anche allo scopo di *mantenere* operative tali disposizioni. Va poi sottolineato come, nel declinare tali ipotesi di deroga, il legislatore tedesco mutui lo schema della *necessary clause*, che così finisce per essere applicato – a livello della legislazione di uno stato membro – anche quale meccanismo di *disattivazione* o *attenuazione* rispetto alla operatività di un principio del GDPR.

La legge di allineamento al GDPR approvata dalla Grecia contiene misure analoghe a quelle della normativa tedesca, con riferimento alla possibilità per le amministrazioni pubbliche di riutilizzare dati personali per finalità diverse da quelle per le quali i dati erano stati originariamente raccolti, sia quanto allo schema autorizzatorio (con il ricorso alla *necessary clause*), sia quanto alla selezione delle circostanze in cui la deroga al principio di limitazione della finalità del trattamento viene abilitata[78]. Tale opzione regolatoria,

[76] Cfr. l'art. 23(1)2- del BDSG, che autorizza le amministrazioni pubbliche a trattare per uno scopo diverso da quello per il quale i dati sono stati raccolti, quando: - sia necessario verificare le informazioni fornite dall'interessato perché vi è motivo di ritenere che tali informazioni non siano corrette; - il trattamento sia necessario a prevenire un danno sostanziale per il bene comune o una minaccia per la sicurezza pubblica, la difesa o la sicurezza nazionale; salvaguardare preoccupazioni sostanziali del bene comune; o per garantire entrate fiscali e doganali; - il trattamento sia necessario al perseguimento di illeciti penali o amministrativi, all'esecuzione o all'esecuzione di sanzioni o provvedimenti educativi o disciplinari di cui alla legge sul tribunale per i minorenni o per l'esecuzione di sanzioni pecuniarie; - il trattamento sia necessario per prevenire una grave lesione dei diritti altrui; - il trattamento sia necessario per esercitare poteri di vigilanza e controllo, per effettuare audit o analisi organizzative del titolare; ciò vale anche per il trattamento svolto ai fini della formazione e verifica dell'apprendimento da parte del responsabile del trattamento, purché non sia in conflitto con i legittimi interessi dell'interessato.

[77] Infatti, l'ultimo periodo dell'art. 25(1) del BDSG chiarisce che "il trattamento per altri scopi è consentito solo se sono soddisfatte le condizioni di cui all'art. 23". La deroga, per altro copre anche le categorie di dati particolari di cui all'art. 9 del GDPR, purché siano soddisfatte anche le condizioni che autorizzano il loro trattamento, sia ai sensi dello stesso art. 9, sia ai sensi dell'art. 22 del BDSG.

[78] Ai sensi dell'art. 24 della legge n. 4624 del 29 agosto 2019 – legge sull'autorità ellenica per la protezione dei dati, misure per l'attuazione del GDPR e recepimento della direttiva sulla protezione dei dati in relazione all'applicazione della legge (direttiva (UE) 2016/680) e altre disposizioni – il trattamento di dati personali da parte di enti pubblici per una finalità diversa da quelle per cui sono stati raccolti è consentito qualora tale trattamento sia necessario per l'esecuzione dei compiti loro assegnati e a condizione che sia necessario: - per la verifica delle informazioni fornite dall'interessato, in quanto dati, in quanto vi sono ragionevoli motivi per ritenere che tali informazioni non siano corrette; - per la prevenzione di rischi per la sicurezza

tuttavia, è stata criticata dalla locale autorità di garanzia di protezione dei dati personali, perché ritenuta non compatibile con la disciplina del GDPR[79].

Differente invece è il meccanismo previsto nella disciplina danese, sebbene lo scopo sia analogo (alleggerire i vincoli derivanti dal principio di limitazione della finalità del trattamento). Secondo questa disposizione, ciascun ministro, con riferimento alla rispettiva amministrativa di competenza, può con proprio atto, sentito il ministro della giustizia, autorizzare le amministrazioni a riutilizzare dati personali per finalità diverse da quelle per le quali i dati sono stati raccolti, senza tenere conto dei profili di compatibilità. La deroga al principio di finalità del trattamento può essere applicata con riferimento a tutti i trattamenti relativi alle funzioni ed ai compiti esercitati per la salvaguardia degli interessi di cui all'art. 23 del GDPR. Con il medesimo meccanismo, i ministri competenti possono anche autorizzare le amministrazioni a trattare i dati genetici e i dati idonei a rivelare lo stato di salute di cui all'art. 9 del GDPR, per finalità diverse da quelle per cui tali dati sono stati raccolti, ma solo se queste seconde, ulteriori finalità risultano compatibili con quelle originarie[80]. Anche nel caso della legislazione danese (in combinato disposto con lo standard di *base* fissato dal GDPR), non vi è dubbio che la misura introdotta concorre a definire uno standard legale *ad hoc*, che si discosta in modo significativo da quello vigente in precedenza. In effetti la disposizione amplia lo spazio disponibile alle autorità pubbliche per trattare i dati personali e di comunicarli ad altre autorità pubbliche, in deroga al principio di limitazione della finalità del trattamento. Nell'assetto legislativo previgente, infatti, i trattamenti di dati personali per finalità diverse da quelle iniziali dovevano essere autorizzati con una legge parlamentare.

nazionale, la difesa sicurezza nazionale, alla difesa o alla pubblica sicurezza, o per assicurare le entrate fiscali e doganali; - per il perseguimento di reati; - per la prevenzione di gravi danni ai diritti di un'altra persona; - la produzione di statistiche ufficiali. Anche in questo caso, la deroga copre parimenti le categorie di dati particolari di cui all'art. 9 del GDPR, purché siano soddisfatte sia le condizioni che autorizzano il loro trattamento ai sensi dello stesso art. 9, sia le condizioni integrate all'art. 22 della disciplina nazionale *de qua*. Il testo della legge, con traduzione a cura dell'autorità nazionale di protezione dei dati è disponibile presso il sito dell'autorità: www.dpa.gr.

[79] "…according to the HDPA, Articles 24 and 25 establish bases to process personal data for purposes other than initially collected (see HDPA Opinion 1/2020). The HDPA takes the position that the GDPR does not authorize national law to establish new legal bases for processing other than those in GDPR Article 6. The HDPA does not consider these provisions a necessary and proportionate measure to safeguard the objectives stated in GDPR Article 23. Therefore, according to the HDPA, Articles 24 and 25 are not in line with the GDPR", cfr. Patsalia T. e Kalogiannis V. (2021), "Greek Implementation of the GDPR", *Thompson Reuters Practical Law*, giugno 2021, testo disponibile al sito: https://shorturl.at/dquxR (5.5.2023).

[80] Cfr. l'art. 5 (3) della legge danese n. 502 de 23 maggio 2018 (Data protection act).

4.2. Gli spazi di composizione dello standard legale di trattamento a fini di esercizio di compiti di interesse pubblico

La sintetica rassegna di alcune delle misure di carattere *trasversale* adottate nelle legislazioni di alcuni Stati membri, in occasione dell'allineamento al GDPR – misure che sfruttano il margine di adattamento che le clausole del regolamento assegnano alle legislazioni degli Stati membri nel declinare il regime applicabile al trattamento dei dati personali per finalità di interesse pubblico – consente di formulare alcune osservazioni. In primo luogo, le scelte operate dai legislatori nazionali confermano – in concreto – l'ipotesi interpretativa del *dual legality standard*. Le misure trasversali analizzate, infatti, si caratterizzano proprio perché – muovendo dallo standard legale di base rappresentato dalla *necessary clause* fissata all'art. 6(1)(e) del regolamento – costruiscono regimi regolatori di carattere *composito* e *modulare*. Il legislatore sceglie a seconda dei casi la misura che ritiene più opportuna per dare soddisfazione a determinati interessi o risposta ad esigenze più o meno specifiche (l'esigenza di assicurare una ampia capacità di trattamento a certe tipologie di dati; l'esigenza di assecondare le dinamiche di integrazione dei sistemi informativi secondo il principio, variamente declinato, del *once only*; oppure, al contrario: l'esigenza di *presidiare* questi processi; l'esigenza di attenuare il vincolo del principio di limitazione della finalità del trattamento quantomeno, con riferimento ad alcune funzioni pubbliche, e così via), e procede per addizioni, *fine tuning* – ma anche, a volte, per sottrazioni. Sicché, il regime di trattamento dei dati personali a fini di esercizio di funzioni pubbliche costituisce la risultante all'integrazione tra lo standard legale *uniforme*, disegnato dal GDPR, e le misure adottate a livello nazionale. L'analisi ci ha mostrato anche che il margine di adattamento è utilizzato in modo coerente con lo scopo per il quale è stato assicurato/mantenuto, anche nel *framework* regolatorio del GDPR: ciascun paese adotta le misure di *adattamento* con modalità e secondo stili regolatori disomogenei, perché destinati ad integrarsi ed interagire con lo specifico contesto normativo, istituzionale, ed organizzativo proprio di ciascun paese; e questo anche quando le misure sembrano puntare ai medesimi obiettivi, o rispondere ad analoghe esigenze.

Un secondo elemento che emerge dall'analisi riguarda la *direzione* concretamente assunta dalle integrazioni introdotte a livello nazionale al *legal standard* del GDPR. Infatti, in alcuni dei casi che abbiamo osservato, le misure si caratterizzano per un *alleggerimento* di alcuni vincoli derivanti dal GDPR. In altri termini, il margine concesso dall'art. 6, parr. 2 e 3, è stato interpretato da alcuni Stati membri anche come spazio per calibrare il regime di trattamento dei dati personali per l'esercizio di compiti di interesse pub-

blico non solo mediante *precisazione* dello standard uniforme (e, quindi, tramite un qualche arricchimento e/o irridigidimento dei presupposti di liceità delineati dal GDPR), ma anche mediante *alleggerimento* di alcuni di questi vincoli. Il caso delle misure per favorire l'utilizzo secondario dei dati personali fuori dai vincoli imposti dal principio di limitazione della finalità è – sotto questo profilo – esemplare. Certamente, in questi casi gli Stati membri si sono potuti giovare della clausola di adattamento di cui all'art. 6, par. 4, ma è significativo notare che: 1) quando lo hanno fatto, hanno riconosciuto ai soggetti pubblici e/o all'esercizio di compiti di interesse pubblico spazi maggiori e più significativi entro cui avvantaggiarsi del regime in deroga; e 2) hanno esplicitamente collegato questa deroga anche al trattamento consistente nel trasferimento di dati tra amministrazioni. Nel complesso, dunque, le clausole di adattamento concesse agli Stati membri sono state utilizzate anche in modo *strategico*, così che il regime di trattamento dei dati personali a fini di esercizio di funzioni pubbliche che ne deriva, non si risolve semplicemente in un arricchimento/aggravamento (più o meno accentuato) del regime di base, ma ne realizza un'effettiva ricalibratura.

4. Il dual legality standard *nell'ordinamento nazionale italiano: l'esplorazione del margine di manovra*

1. Prima del GDPR: il trattamento dei dati personali per l'esercizio di funzioni pubbliche nella disciplina di recepimento della direttiva

La disciplina nazionale italiana di recepimento[1] della direttiva 95/46/CE dedicava alcuni specifici articoli ai trattamenti effettuati dai soggetti pubblici (ad esclusione degli enti pubblici economici), con ciò per altro adottando un criterio essenzialmente *soggettivo* per l'individuazione del campo di applicazione di questa specifica disciplina[2]. Il trattamento dei dati personali è ammesso "soltanto per lo svolgimento delle funzioni istituzionali"[3], senza però menzionare il criterio di necessarietà, così che il rapporto di strumentalità che fonda la liceità del trattamento da parte dei soggetti pubblici appare retto da criteri meno stringenti di quelli indicati nella direttiva (dov'era invece già declinata la clausola di *strumentalità necessaria*); la direttiva tuttavia, come già notato, ha operato anche come criterio interpretativo rispetto della disci-

[1] Come noto, la direttiva è stata recepita nell'ordinamento nazionale ad opera l. 31 dicembre 1996, n. 675; le norme sul trattamento da parte dei soggetti pubblici sono stato poi trasposte nel Codice in materia di protezione dei dati personali (di seguito Codice), d.lgs. 30 giugno 2003, n. 196: la nostra analisi si concentrerà sulle disposizioni di quest'ultimo testo (non troppo dissimili, in effetti, da quelle contenute nella originaria disciplina di recepimento). In dottrina, si vedano i commenti agli artt. 18-19 (Troiano P.), 20 (Sanna P.) 21 (Misserini F.) e 22 (Pieraccini M. B.), in Bianca C. M., Busnelli F. D. (2007), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (codice della privacy)*, Padova, 456-540; nonché Cardarelli F., Sica S., Zeno-Zencovich V. (2004), *Il codice dei dati personali: temi e problemi*, Milano.

[2] Cfr. gli art. da 18 a 22 del Codice, articoli poi abrogati dal d.lgs. 10 agosto 2018, n. 101, con il quale è stato effettuato l'allineamento e l'adeguamento della disciplina interna al GDPR.

[3] Cfr. art. 18, comma 2 del Codice.

plina interna, e non mancano infatti pareri del Garante che – già prima dell'entrata in vigore del GDPR – declinano il criterio di legittimazione all'uso dei dati per l'esercizio di funzioni pubbliche in termini di strumentalità *necessaria*[4]. Tuttavia, quantomeno con riferimento ai trattamenti di dati personali cosiddetti "comuni", il criterio di strumentalità pare anche condizione sufficiente di legittimazione, dal momento che la disciplina esclude che il trattamento sia impedito dal fatto che una norma di legge o di regolamento non preveda "espressamente" quel trattamento[5]. Questo significa che il criterio di legittimazione fondato sulla strumentalità (allo svolgimento delle funzioni pubbliche) ammetteva trattamenti che non fossero esplicitamente previsti, ma che risultassero *implicitamente* a ciò strumentali. Con la notevole eccezione, però, dei trattamenti che consistessero nella *comunicazione ad altri soggetti pubblici*, per i quali era invece necessaria una disposizione normativa (di legge o di regolamento) che li prevedesse (espressamente); in assenza di tale norma, questa tipologia di trattamento poteva essere effettuata se fosse risultata "comunque necessaria per lo svolgimento di funzioni istituzionali", ed era sottoposta comunque all'onere di previa comunicazione al Garante e ad un periodo di latenza di quarantacinque giorni, fatte salve le diverse indicazioni formulate dallo stesso Garante[6]. Invece, per i trattamenti consistenti nella *comunicazione a soggetti privati* (o a enti pubblici economici), oppure consistenti nella *diffusione*, il trattamento era ammesso esclusivamente se previsto da una norma di legge o di regolamento[7].

Il trattamento dei dati sensibili da parte di soggetti pubblici era consentito "solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite"[8]. Si tratta di una disposizione molto interessante, non solo perché impone uno *standard* di legalità particolarmente stringente (la disposizione di legge deve specificare espressamente *quali dati* possono essere trattati; *quali siano i trattamenti eseguibili*, e *quali siano le finalità di interesse pubblico perseguite*), ma anche perché offre indicazioni *a contrario* sullo *standard* applicabile al trattamento dei dati comuni. Anche in questo caso, la norma stabilisce le procedure che possono essere attivate, rispettivamente, qualora la norma di legge si limiti

[4] Cfr. ad esempio il parere n. 9 ottobre 2006 [doc. web n. 1353472];

[5] Cfr. art. 19, comma 1: "Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente".

[6] Cfr. art. 19, comma 2.

[7] Cfr. art. 19, comma 3.

[8] Cfr. art. 20, comma 1.

ad indicare solamente la finalità di interesse pubblico[9], oppure nemmeno quella[10]. In entrambi i casi, l'integrazione del quadro di legittimazione al trattamento avviene mediante l'adozione di atti regolamentari da adottarsi previo parere del Garante, che è pure chiamato a selezionare (all'occorrenza) le attività che perseguono finalità di rilevante interesse pubblico, tra quelle che la legge affida alla cura dei soggetti pubblici. Sostanzialmente analoghe le previsioni concernenti il trattamento dei dati giudiziari[11]. Infine l'art. 22 recava la disciplina specifica relativa alle (più stringenti ed esigenti) modalità di trattamento dei dati sensibili e giudiziari.

In sintesi, si può affermare che il regime di trattamento dei dati personali da parte di soggetti pubblici per lo svolgimento delle loro funzioni disciplinato Codice prima dell'avvento del GDPR si articolava sostanzialmente in tre differenti tipologie di sub-regimi: il regime di trattamento dei dati comuni (retto dal presupposto di liceità fondato sullo clausola di strumentalità); il regime applicabile agli specifici trattamenti della comunicazione e diffusione di dati comuni (retto invece da un principio di legalità, legislativa o regolamentare) ed infine il regime di trattamento dei dati sensibili e giudiziari (retto da un principio di espressa riserva di legge, per quanto concerne i tipi di dati che possono essere trattati; i trattamenti eseguibili; le finalità di rilevante interesse pubblico perseguite). Al Garante era affidato il compito di presidiare i meccanismi di *flessibilizzazione* dei criteri di legittimazione, in eventuale supplenza di indicazioni legislative carenti o assenti.

2. Dopo il GDPR: la sperimentazione del margine di manovra nella direzione della stretta legalità

Al fine di allineare l'ordinamento interno al GDPR, il parlamento vara una delega poi esercitata con l'emanazione del d.lgs. 101/2018, che compie la scelta di mantenere quantomeno sotto il profilo *formale* il contenitore del Codice privacy, ampiamente svuotato però dei suoi contenuti, per effetto delle numerose, sistematiche abrogazioni apportate per "lasciare spazio" alla diretta applicazione delle norme del GDPR[12], fatti salvi i necessari coordina-

[9] Cfr. art. 20, comma 2.

[10] Cfr. art. 20, comma 3

[11] Cfr. art. 21.

[12] La legge di delegazione europea n. 163 del 2017 aveva stabilito, all'art. 13 comma 3, i seguenti criteri direttivi:

"a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati

menti. Il testo dei criteri di delega non sembra autorizzare *modifiche innovative*, che non siano giustificate dalla necessità di abrogare le disposizioni incompatibili con il regolamento, dare attuazione a disposizioni dello stesso regolamento non direttamente applicabili, o da ragioni di mero coordinamento (tra le norme del GDPR e quelle "superstiti"). Tuttavia, le disposizioni introdotte con riferimento al trattamento dei dati giustificato dall'esecuzione di compiti di interesse pubblico non appaiono del tutto coerenti con questi criteri. Da una parte, le specifiche dedicate a questa materia (artt. 18-22) sono abrogate. Ne sono introdotte (ma in una differente collocazione) delle altre, che però in ragione dello specifico contenuto (vedi subito *infra*) non appaiono disposizioni di mero coordinamento, né sembrano intervenire "per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento", dal momento che – come abbiamo già osservato – le clausole di cui all'art. 6, parr. 2 e 3 facoltizzano l'intervento della disciplina nazionale di adattamento/precisazione, ma non la impongono come necessaria[13]. Pertanto, il decreto legislativo di "allineamento" contiene in effetti anche quelle scelte *discrezionali*[14] (*opening clause*) che il regolamento consente di adottare in questa specifica materia.

personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse".

[13] Una considerazione tanto più fondata, nella misura in cui la disciplina allora vigente (quella di cui agli art. 18-22 del Codice) poteva essere *mantenuta* senza che questo comportasse alcun problema in termini di compatibilità con lo standard di base determinato dal GDPR; esprime questa opinione, ad esempio D'Ancona S. (2018), "Scambio di dati tra le pubbliche amministrazioni e principio di buona amministrazione nel diritto comunitario e nazionale. Interferenze colle norme sulla privacy. Reg UE n. 679/2016", in *Rivista italiana di diritto pubblico comunitario*, 3/4, 587-627, in spec. 621: "Il margine di 'libertà' attribuito al legislatore nazionale è tale per cui diventa prevedibile che, gli Stati membri, compresa l'Italia, non cambino di molto le regole che avevano fissato negli impianti normativi attuativi della Direttiva 95/46, soprattutto negli ambiti dove l'autonomia procedurale è più ampia (tra cui le norme in materia di trattamento dati personali da parte di Pubbliche Amministrazioni)".

[14] Di questa circostanza pare perfettamente consapevole il legislatore delegato: nella relazione illustrativa di accompagnamento allo schema di decreto si dice "In particolare, l'articolo

Si tratta, in effetti, di scelte di carattere *innovativo*, rispetto all'assetto disegnato negli articoli da 18 a 22 del Codice privacy. In primo luogo, il criterio distintivo fondato sulla natura *soggettiva* dei titolari del trattamento viene abbandonato, in favore di una adesione al criterio *oggettivo* utilizzato da regolamento, sia mediante rinvio alle sue disposizioni pertinenti (cfr. art. 2-ter, commi 1 e 2), sia – infine – mediante l'espressa formulazione impiegata ("l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", come declinato nell'art. 2-ter, comma 3). Quanto ai presupposti del trattamento, la nuova disciplina interna utilizza i margini di manovra secondo una direzione di *netto irrigidimento* di tali presupposti, rispetto sia alla disciplina interna precedente, sia rispetto allo standard legale del GDPR[15]. Con riferimento al trattamento dei dati personali diversi da quelli particolari o giudiziari (quelli che per comodità possiamo continuare a definire dati personali *comuni*), l'art. 2-ter sancisce che "La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento"[16]. La formulazione potrebbe lasciare aperti – in effetti – alcuni spazi interpretativi, dal momento che, come abbiamo avuto modo di notare, il ruolo della base giuridica – per come declinato proprio nell'art. 6, par. 3, lett. b) – è quello (e solo quello) di individuare ed affidare al titolare del trattamento l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri (cfr. la lettura critica delle scelte del legislatore del 2018 di Pelino E. (2019), *Sub art. 2-ter d.lgs.*

2-ter detta specificazioni in merito alla 'Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri', nell'esercizio dello spazio di discrezionalità previsto dall'articolo 6, 2° comma, del regolamento che lascia agli Stati membri la possibilità di mantenere o introdurre disposizioni più specifiche con riguardo ai trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" (cfr. p. 6).

[15] La commissione incaricata di stendere lo schema di decreto legislativo di armonizzazione della legislazione nazionale al GDPR "has set out that the processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority is only legal if it is provided for by national laws or regulations. Since processing for the above mentioned purposes should be carried out for collective and general interests and is directed at higher needs, *this provision severely restricts the cases when personal data can be legally processed*. This means that only primary and, when it is explicitly provided by law, secondary sources of law can be adequate to set out a processing for public interest purposes: in other words, soft law or customary law are not sufficient to this aim and cannot be an adequate legal basis according to Article 6(3)b) GDPR", così Finocchiaro G. (2018), "Italy: the legislative procedure for national harmonisation with the gdpr", *European Data Protection Law Review (EDPL)*, 4(4), 496-499, in part. 498; questo passaggio può essere letto come una sorta di interpretazione autentica dal momento che l'autrice ha presieduto la commissione tecnica che ha elaborato gli interventi normativi poi confluiti nel d.lgs. 101/2018 (corsivo aggiunto).

[16] Cfr. Cardarelli F. (2021), *Comm. sub. art. 2-ter Codice Privacy*, in D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (eds.), *Codice della privacy e data protection*, Milano, 1011 ss.

196/2003, in (eds.) Bolognini L., Pelino E., *Codice della disciplina privacy*, Milano, 97 ss.). In questo senso, la scelta del legislatore potrebbe essere intesa nel più limitato senso di limitare alla sola fonte di rango legislativo (e a quella regolamentare, ma previa delega espressa nella fonte legislativa) tale ruolo. Una riserva alla fonte legislativa del tutto coerente con il principio di legalità, sia per quanto concerne l'attribuzione del potere (legalità garanzia), sia per quanto concerne l'indicazione all'amministrazione dei fini di interesse generale da perseguire (legalità-indirizzo). Entro queste coordinate, e compiuta questa attribuzione (da un atto fonte che integri la categoria così prescritta/abilitata), l'identificazione della finalità del trattamento, come pure di quali dati trattare e secondo quali modalità, resterebbe attratta (per effetto della diretta applicabilità del GDPR) nello standard legale della clausola della *necessarietà*: sarebbe l'esistenza di una relazione di *strumentalità necessaria* a consentire di identificare e legittimare tali elementi. Tuttavia, l'interpretazione prevalente del disposto normativo, fornita in particolare dal Garante nell'emanazione di avvisi e pareri sugli atti di regolamentazione secondaria[17], ovvero in sede di audizione su atti normativi di fonte primaria, è andata in diversa direzione, valorizzando in particolare la nuova formula adottata nel Codice posta a confronto con quella previgente. Mentre in precedenza si statuiva che il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari fosse consentito *anche in mancanza di una norma di legge o di regolamento che lo prevedesse espressamente*, la nuova formulazione utilizza l'avverbio *esclusivamente*, ciò che è stato inteso nel senso di attrarre nella base giuridica non solo *la qualificazione della fonte* ("esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento"), ma anche ciò che in precedenza poteva restare fuori dalla fonte legislativa ("Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito (…) anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente"). In base a questa lettura, pertanto, la base giuridica (legislativa, o regolamentare, se a ciò espressamente abilitata) non può limitarsi ad individuare ed affidare al titolare del trattamento l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri, ma deve (quantomeno) prevedere espressamente quale trattamento (di quali dati, e per quale finalità) possa essere realizzato. Come si vede, si tratta di una ricostruzione che valorizza il dato orizzontale dell'evoluzione della legislazione

[17] Si vedano, a titolo di esempio, il parere n. 263 dell'8 luglio 2021 su di uno schema di regolamento di disciplina delle modalità di realizzazione e gestione della banca dati delle strutture ricettive e degli immobili destinati alle locazioni [doc. web n. 9688040], nonché il parere n. 138 del 20 giugno 2019 su uno schema di decreto del Ministro del lavoro e delle politiche sociali in materia di Sistema informativo del Reddito di cittadinanza [doc. web n. 9122428].

interna[18], piuttosto che non la lettura integrata tra standard legale di base e disposizioni nazionali di adattamento[19]. Una conferma autorevole ed in qualche modo "autentica" della prevalenza di questa opzione interpretativa, anche con specifico riferimento al vincolo per cui è nella base giuridica che deve essere *esplicitata* (e quindi, espressa) la finalità del trattamento, l'ha fornita lo stesso Garante, in occasione del cambio di regime legislativo avvento nell'autunno del 2021[20] (su cui vedi subito *infra*).

[18] Cfr. Cardarelli F. (2021), *Comm. sub. art. 2-ter Codice Privacy*, cit., 1018: "Questa soluzione (che suscita comunque alcune perplessità rispetto alle disposizioni del regolamento europeo) è frutto di un delicato compito di raccordo che il legislatore delegato ha ritenuto di dover svolgere, alla luce della rigidità della previsione del comma 1 (si ripete, pienamente giustificabile sul piano formale) e della indicazione europea (contenuta nel par. 2 dell'art. 6 del Regolamento) sulla facoltà di 'mantenere' in vita disposizioni dotate di maggiore specificità, e quindi legittimando una sorta di continuità normativa tra l'impianto del vecchio Codice rispetto al nuovo".

[19] Come si è osservato, si tratterebbe di "una lettura del GDPR che priva d'efficacia immediatamente precettiva la previsione recata dall'art. 6 lett. e), secondo la quale 'l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento' è una è una delle possibili basi giuridiche che consentono di ritenere lecito il trattamento", così Francario F. (2022), "Protezione dei dati personali e pubblica amministrazione", cit., par. 6.1. Tale interpretazione dell'art. 2 ter del Codice, nell'attuazione dell'art 6(3) del GDPR è stata ritenuta in dottrina "eccessivamente restrittiva" da Pizzetti F. (2021), *La parte I del Codice novellato*, in Pizzetti F. (eds.), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 92.

[20] In sede di audizione, infatti, il presidente dell'autorità Garante per la protezione dei dati personali ribadiva "il vincolo di determinatezza, *esplicitazione*, legittimità e compatibilità delle finalità, che *devono essere inscritte nella base giuridica*, sancito dagli artt. 5, par. 1, lett. b), e 6, p. 4, del Regolamento", con ciò chiarendo l'interpretazione per cui la base giuridica deve prevedere ed esplicitare il trattamento cui è possibile sottoporre i dati e la sua finalità. A conferma, il testo della audizione soggiunge che "laddove l'intenzione del Governo, attraverso l'intervento in commento, sia quella di andare di là da tale impostazione e di prevedere che *il semplice perseguimento di un interesse pubblico è di per sé sufficiente a costituire base giuridica del trattamento*, egualmente, la corretta collocazione della disposizione avrebbe dovuto essere il comma 1 dell'art. 2-ter. Questo avrebbe potuto prevedere chiaramente che la base giuridica di un trattamento da parte di un soggetto pubblico per il perseguimento delle proprie finalità istituzionale può essere la legge, un regolamento, un atto amministrativo generale *o la semplice strumentalità del trattamento alle sue finalità istituzionali*". *A contrario*, ciò conferma che – secondo questa lettura – il testo dell'art. 2-ter, nella versione precedente alla sua modifica intervenuta nel corso del 2021, imponeva invece che la base giuridica prevedesse espressamente il trattamento (e la sua finalità). Ancora, nel medesimo passaggio, si osservava che, volendo *invece* optare per una legittimazione del trattamento su base meramente strumentale (ovvero in accordo alla clausola di *strumentalità necessaria*) "in tale ultima evenienza – a mio avviso non strettamente strumentale al perseguimento delle dichiarate finalità di semplificazione –la compatibilità con l'ordinamento europeo dei trattamenti di dati personali avviati da un soggetto pubblico sulla base di tale disposizione risulterà, inesorabilmente, da accertare caso per caso giacché, l'ordinamento europeo, esige sempre e comunque – quale che sia l'impostazione del diritto nazionale in fatto di

La disciplina, così interpretata, determina un ulteriore effetto. Mentre nell'assetto precedente lo specifico trattamento consistente nella comunicazione dei dati ad altre amministrazioni (a fini di esercizio di funzioni pubbliche) risultava *più presidiato* rispetto alle altre tipologie di trattamento (perché richiedeva che la comunicazione fosse espressamente prevista dalla normativa), nell'assetto disegnato dal d.lgs. 101/2010 lo è *di meno* (perché l'assenza di una previsione normativa che lo contempli esplicitamente può essere supplita, entro i confini della necessarietà strumentale, dalla procedura attivata con la previa comunicazione al Garante[21]). Una circostanza che comunque segnala il progressivo maturare di una sensibilità più attenta alle esigenze di circolazione e integrazione del patrimonio informativo pubblico. Sostanzialmente inalterato è il regime relativo al trattamento consistente nella diffusione dei dati personali, anche perché in questo caso la necessità di una base legislativa che preveda espressamente tale trattamento, ad integrare il presupposto di liceità di tale trattamento, costituisce un dato sostanzialmente imposto dalla giurisprudenza della Corte di giustizia.

Nell'art. 2-sexies[22] sono invece specificati i presupposti di trattamento dei dati particolari (quelli di cui all'art. 9 del GDPR), ad eccezione dei dati genetici, biometrici e dei dati relativi alla salute, per il quale vale il regime un

fonte giuridica legittimante il trattamento – che il trattamento, *nella sua finalità e nelle sue modalità, sia trasparente, prevedibile, noto ai cittadini*" (corsivi aggiunti). Un passaggio argomentativo *significativo*, perché per un verso conferma le caratteristiche che sono proprie dello standard legale abilitato dalla clausola di *necessarietà*; per altro verso, spiega bene le ragioni dell'opzione interpretativa adottata per leggere la versione originaria del testo dell'art. 2-ter (quella precedente alle modifiche intervenute nel 2021): assicurare che finalità e modalità del trattamento connesso all'esercizio di compiti di interesse pubblico siano conoscibili, prevedibili e noti prima *al momento dell'affidamento del compito all'amministrazione*, e quindi esplicitati nella norma che dispone tale affidamento. Un'esigenza di trasparenza e prevedibilità del *potere* (quello speso nel trattare i dati) che si traduce in un vincolo di più stringente legalità rispetto allo standard abilitato dalla clausola di necessarietà.

[21] Cfr. il testo originario dell'art. 2-ter, comma 2 del Codice, come introdotto dal d.lgs. 101/2018 ("La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1 [cioè, se espressamente prevista dalla legge, o dal regolamento, in base alla legge, secondo l'interpretazione della norma adottata dal Garante]. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati").

[22] Su cui si veda Cortese F. (2021), *Comm. sub. art. 2-sexies Codice Privacy*, in D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (eds.), *Codice della privacy e data protection*, Milano, 1043 ss.

ulteriore regime ad hoc, delineato al successivo art. 2 septies). Rispetto all'assetto precedente, ciò che si osserva è una sorta di codificazione ordinatrice dei motivi di interesse pubblico rilevante che giustificano il trattamento dei dati particolari (motivi raccolti ed elencati nelle lett. da a) a dd) del comma 2), mentre viene contemporaneamente meno la possibilità – in capo al Garante – di selezionare ed esplicitare ulteriori motivi di interesse pubblico rilevante, traendoli dalla normativa vigente (come era invece possibile in precedenza). Anche in questo caso, dunque, si osserva una modifica in direzione di un irrigidimento dello *standard legale*.

Un'ulteriore misura che occorre segnalare, relativa al regime di trattamento dei dati personali per l'esercizio di compiti di interesse pubblico declinato dal legislatore nazionale italiano, è l'attivazione di competenza in capo all'autorità nazionale di controllo, con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del GDPR. In questi casi, infatti, sulla base di una clausola di adattamento aperta dallo stesso regolamento[23], il Codice (come modificato) prevede che il Garante – a fronte della segnalazione da parte del titolare del trattamento[24] – possa prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad attuare; tali misure possono essere elaborate con riferimento ad uno specifico trattamento, ovvero mediante provvedimenti di carattere generale adottati d'ufficio[25]. Si tratta di una deviazione rispetto al principio di *accountability* di cui all'art. 5, par. 2 del regolamento: i trattamenti che presentano rischi elevati, ma solo quando siano finalizzati all'esecuzione di compiti di interesse pubblico, sono fatti oggetto di indicazioni specifiche (vincolanti) formulate *ex ante* da parte dell'autorità di controllo, piuttosto che soggetti al regime di piena *accountabilty* (in virtù del quale è compito del titolare assicurare la conformità del trattamento al regime del GDPR ed è suo onere comprovarlo[26]).

[23] Cfr. art. 36, par. 5 del GDPR.

[24] La segnalazione, ai sensi dell'art. 36, par. 1 del regolamento, è dovuta nel caso in cui il trattamento presenti rischi elevati ai sensi dell'art. 35: ("Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio").

[25] Cfr. art. 2-quinquiesdecies del Codice, come introdotto dal d.lgs. 101/2018.

[26] "il Regolamento lascia un ampio grado di autonomia a coloro che sono chiamati ad attuarne le disposizioni, bilanciando tale libertà di scelta con la responsabilità di creare un modello che sia in grado di rispondere effettivamente e tempestivamente alle esigenze di tutela (3). Per questo motivo, al cuore del nuovo Regolamento sui dati ci sono tre principi: accountability (art. 5 GDPR), data protection by design e by default (art. 25 GDPR)", così Fiorentino L., (2018), "Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche", in *Giornale Dir. Amm.*, 6, 690 ss.

Complessivamente, nell'ottica della chiave di lettura del *dual legal standard*, l'intervento operato nell'ambito della disciplina di allineamento al GDPR si segnala come un'ipotesi *hard* di sperimentazione del margine di manovra accordato agli Stati membri dalle clausole di precisazione/adattamento di cui all'art. 6, par. 2 e 3 del GDPR (e non solo di quelle, come si è appena visto). Il regime introdotto con gli art. 2-ter e seguenti del Codice appare più rigido e garantista, sia rispetto all'analogo regime disciplinato, sempre nel Codice, agli art. 18-22, sia se posto a confronto con il regime di base disegnato dal regolamento. Nel caso di specie, cioè, il *dual legality standard* prende corpo mediante una quasi integrale sostituzione (dei termini oggettivi) del regime del GDPR – modulato sulla *necessary clause* – con uno standard legale caratterizzato piuttosto in termini di *strict legality*. Poco se non alcuno spazio è riservato all'ipotesi di *poteri impliciti*, dal momento che – anche con riferimento al trattamento dei dati personali comuni – la disciplina di adattamento interna (e l'interpretazione operata dall'autorità di controllo nazionale) finisce per imporre la previsione esplicita in norma di legge (o di regolamento, se così previsto dalla legge) del trattamento da effettuarsi e delle sue finalità. L'unica, parziale, eccezione si può osservare con riferimento allo specifico (ma strategico) trattamento consistente nella comunicazione di dati personali comuni fra titolari che effettuano trattamenti per l'esecuzione di compiti di interesse pubblico; solo in questo caso – ed in assenza di una espressa previsione normativa – la comunicazione è ammessa quando è *comunque necessaria* per lo svolgimento di compiti di interesse pubblico, sebbene anche in questo caso la disciplina preveda alcune cautele ulteriori (che fanno perno sulla possibilità che l'autorità di controllo imponga misure ulteriori a garanzia degli interessati).

3. L'inversione di rotta: la disciplina nazionale adotta la *necessary clause*

3.1. Le condizioni di contesto in cui sono maturate le modifiche al Codice privacy in materia di trattamento dei dati per l'esercizio di funzioni pubbliche

Come noto, la disciplina nazionale relativa al trattamento dei dati personali per l'esercizio di funzioni pubbliche è stata oggetto di una significativa modifica a pochi anni di distanza dalla sua più recente ricalibratura (analizzata nel paragrafo precedente). Tali modifiche sono intervenute in circostanze abbastanza peculiari, così come peculiari sono state anche le condizioni di contesto che – in qualche modo – hanno favorito quella che si può

senz'altro definire una "inversione di rotta". Alcuni fattori di contesto sono maturati per effetto della pandemia da Covid-19, e dalle considerazioni elaborate nel corso della gestione delle misure di contrasto alla diffusione del contagio e alla mitigazione dei suoi effetti, sia sul piano strettamente sanitario, che più in generale con riferimento ai contraccolpi sociali ed economici prodotti anche per effetto delle misure di contrasto applicate, oltre che in ragione del rallentamento complessivo dell'economia mondiale. La necessità di dover intervenire sotto la spinta dell'urgenza ha – per un verso – fatto premio rispetto alla possibilità di conservare integre (quantomeno, con riferimento alla gestione della fase emergenziale più acuta) le garanzie a tutela dei trattamenti dei dati personali, anche di quelli più sensibili. All'inizio della pandemia sono state così disposte misure, dichiaratamente di carattere emergenziale, di temporaneo alleggerimento delle regole di trattamento dei dati personali, anche sensibili, gestiti in ambito sanitario. La "semplificazione" della tutela dei dati personali nell'emergenza sanitaria è stata, dunque, finalizzata a rendere più agevole e veloce lo scambio di informazioni tra le autorità sanitarie, sviluppando così la sorveglianza territoriale, così da rendere più efficace il contenimento dell'epidemia[27]. Ampio dibattito, anche nell'arena dell'opinione pubblica, ha suscitato la fase di progettazione e realizzazione della *app* di tracciamento dei contatti a rischio di contagio (cd. *Immuni*), dibattito che ha travalicato i confini nazionali (in ragione degli sforzi compiuti a livello europeo per abilitare una soluzione tecnologica compatibile con i principi a tutela dei dati personali), ma che nel contesto nazionale ha costituito anche occasione per dibattere e ridiscutere l'equilibrio tra esigenze di tutela dei dati personali e (più o meno presuntamente) contrapposte

[27] Per una prima ricostruzione delle modifiche del quadro di tutela dei dati personali giustificato per ragioni di gestione dell'emergenza determinata dall'epidemia di covid-19, si veda il *Rapporto ISS COVID-19. Protezione dei dati personali nell'emergenza COVID-19*, n. 42/2020, nonché la raccolta dei provvedimenti del Garante, disponibile all'indirizzo https://www.garanteprivacy.it/temi/coronavirus. In dottrina, Poletti D. (2020), "Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza", in *Persona e Mercato*, 2, 65-76; Cecili M. e Cardone M. (2020), "Osservazioni sulla disciplina in materia di tutela dei dati personali in tempi di Covid-19. L'Italia e i modelli sudcoreano, israeliano e cinese: opzioni a confronto", in *Nomos*, 1, 47; Vari F. e Piergentili F. (2021), "'To no other end, but the... Safety, and publick good of the People': le limitazioni alla protezione dei dati personali per contenere la pandemia di Covid-19", in *Rivista AIC*, 328-342. Più in generale, sulla pandemia come fattore di innesco per avviare "una riflessione più ampia sulle questioni fin qui evidenziate, la quale consenta, in tempi ragionevoli, di pervenire ad un'accettabile "quadratura", in primis a livello costituzionale, tra potere pubblico, riservatezza e consenso al trattamento dei dati personali", cfr. Tigano F. (2022), "Protezione dei dati e pubblica amministrazione: alcuni spunti di riflessione", in *Diritto e società*, 2, 413-432, in part. 432, nonché Palladini V. (2022), "Il ruolo del Garante per la protezione dei dati personali nell'emergenza sanitaria", in *Osservatorio costituzionale*, 2/153-178.

esigenze di efficiente, semplice e rapida predisposizione di strumenti e soluzioni per il contrasto alla pandemia[28]. Un dibattito che (al di là della condivisibilità *nel merito* delle obiezioni e delle perplessità sollevate nei confronti del livello di tutela assicurato ai dati personali, tanto più che il contesto emergenziale avrebbe dovuto sconsigliare una generalizzazione di tali considerazioni ai tempi "non straordinari") ha contribuito a mettere sotto i riflettori la disciplina nazionale a tutela dei dati personali, anche in termini critici[29]. Tuttavia, la pandemia è stata anche l'occasione per attirare l'attenzione su ritardi e debolezze organizzative di più lunga data, anche con particolare riferimento ai processi di digitalizzazione, interazione ed integrazione del patrimonio informativo pubblico. Nel frattempo, venivano maturando, per un verso, alcuni interventi di riforma incidenti sull'organizzazione delle banche dati pubbliche, la loro interconnessione e l'interoperabilità dei sistemi informativi (cui si è già fatto cenno: su tutte la concretizzazione delle basi di dati di interesse nazionale e la prospettiva della loro interoperabilità tramite l'abilitazione del Piattaforma Digitale Nazionale dei Dati, che sembrano aver poi trovato nel PNRR il punto di caduta per la relativa, effettiva implementazione[30]) e che intendono promuovere una più rapida, snella, automatica circolazione dei dati all'interno del settore pubblico; per altro verso, si consoli-

[28] Una disamina (critica) dei provvedimenti adottati dal Garante nel periodo di emergenza da covid-19, in relazione ad una serie di misure connesse alla gestione della pandemia si trova in Francario F. (2022), "Protezione dei dati personali e pubblica amministrazione", cit., par. 5.2-5.4.

[29] Anche in dottrina, le questioni connesse alla realizzazione della *app* di tracciamento hanno costituito l'occasione per un dibattito particolarmente ampio; cfr., *ex multis*, Cinque A. (2021), "'Privacy', 'big-data' e 'contact tracing': il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute", *La Nuova Giurisprudenza Civile Commentata*, 957-968; D'Arcangelo L. (2020), "'Contact tracing' e protezione dei dati nella fase 2 dell'epidemia da Covid-19 (anche nel rapporto di lavoro)", in *giustiziacivile.com*, 5, 1 ss.; Pertot T. (2020), "*Immuni* e tracciamento digitale: fra protezione dei dati personali, problemi di efficacia e qualche prospettiva futura", *Le Nuove leggi civili commentate*, 5, 1131-1165; Crespi S. (2020), "Applicazioni di tracciamento a tutela della salute e protezione dei dati personali nell'era Covid-19: quale (nuovo) bilanciamento tra diritti?" *Eurojus*, 3, 218-255; Latte S. (2020), "Immuni: framing and first considerations one month from the start", *European Journal of Privacy Law & Technologies*, 2, 362-373; Pizzetti F. (2020), "Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti", in *MediaLaws*, 2, 11-33; Colapietro C. , Iannuzzi A. (2020), "'App' di 'contact tracing' e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali", in *dirittifondamentali.it*, 2, 772-803.

[30] Sottolineano la connessione tra esigenze di attuazione del PNRR e modifiche al Codice privacy, tra gli altri: Buttarelli G. (2022), *L'interoperabilità dei dati nella Pubblica Amministrazione*, in Bontempi V. (eds.), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, Roma, 140 ss. e, *ivi*, Sgueo G., *I servizi pubblici digitali*, spec. 122-123.

dava la consapevolezza che andassero colte le opportunità offerte dalle metodologie di analisi dei dati che presuppongono la capacità di integrare e combinare insieme fonti di dati diverse, spesso distribuite su più attori pubblici[31]. Anche questi fattori inducevano a una riflessione circa l'adeguatezza del *framework* normativo posto a tutela dei dati personali nell'assecondare queste linee di tendenza, proprio in considerazione del fatto che il legislatore dispone di un *margine di manovra* significativo, come detto, per adattare tali regole in diverse direzioni[32].

3.2. Le modifiche introdotte con il decreto «capienze»

Le modifiche al Codice sono state inserite nell'ambito del d.l. 8 ottobre 2021, n. 139, meglio noto come decreto «capienze», dal momento che tra i suoi contenuti principali vi era la rimodulazione della capienza di esercizio di alcune tipologie di impianti destinati ad ospitare lo svolgimento di attività culturali, sportive e ricreative, per effetto dell'andamento della curva dei contagi.

Si è trattato di un intervento che – per quanto evidentemente ispirato anche da logiche ed esigenze maturate nel corso dell'emergenza (come visto) – si distacca dai precedenti interventi legislativi finalizzati alla gestione dell'emergenza, perché introduce delle modifiche che operano e valgono *a regime*, e quindi non si presentano come ad efficacia limitata nel tempo, o astrette in specifici ambiti/settori di applicazione. Si tratta, quindi, di modifiche ordinamentali di enorme impatto, dal momento che modificano in modo permanente aspetti fondamentali del regime di uso dei dati personali nell'ambito del settore pubblico, per il perseguimento di finalità e compiti di interesse pubblico.

[31] Circa le prospettive aperte all'esercizio del potere conoscitivo pubblico dall'applicazione delle tecniche di elaborazione dell'intelligenza artificiale, cfr. Falcone M. (2023), *Ripensare il potere conoscitivo pubblico. La conoscenza amministrativa con i big data e gli algoritmi*, Napoli, cit. *passim*, per la declinazione, nel PNRR, delle esigenze di 'buona amministrazione' proprio nei termini della interconnessione delle banche dati e la promozione della *big data analytics* anche nel settore pubblico, sia consentito rinviare a Ponti B. (2022), "Le diverse declinazioni della 'Buona amministrazione' nel PNRR", in *Istituzioni del federalismo*, 2, 401-418.

[32] Lo stesso presidente del Garante per la protezione dei dati personali, in sede di audizione sulla conversione in legge, soggiungeva che "il fine perseguito dal Governo attraverso il decreto-legge è adeguare l'ordinamento interno, nel doveroso rispetto di quello europeo, alle esigenze di celerità caratteristiche della fase storica che stiamo vivendo, così da consentire il raggiungimento degli ambiziosi obiettivi del PNRR, fra l'altro in termini di trasformazione digitale del Paese".

Le novità introdotte vanno tutte, si può ben dire, nel senso di rendere più agevole l'uso dei dati personali da parte degli attori del settore pubblico. Si tratta, in altre parole, di un intervento finalizzato ad allentare i vincoli, presenti nella disciplina nazionale di recepimento/contorno, anche alla luce dei notevoli spazi di manovra effettivamente resi disponibili al legislatore nazionale dalle norme del GDPR, in questo specifico ambito.

Vediamole più nel dettaglio, concentrandoci sui testi finali, quelli risultanti dalle modifiche al decreto-legge introdotte in sede di conversione, e che hanno tenuto conto anche dai contributi istruttori acquisti in quella sede, a partire dall'audizione del Garante.

3.2.1. I presupposti di liceità del trattamento dei dati comuni (verso la necessary clause*)*

Con riferimento al trattamento dei dati personali comuni, le modifiche apportate all'art. 2-ter del codice operano su due livelli.

In primo luogo, viene modificato ed integrato il primo comma, nel quale sono specificate/precisate le basi giuridiche che fondano il trattamento dei dati personali a fini di esercizio di funzioni pubbliche. Il testo che ne risulta ("*La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita da una norma di legge o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali*") contiene due importanti novità. Viene eliminato l'avverbio "esclusivamente", che – come si è potuto constatare nel paragrafo precedente – ha rappresentato l'elemento testuale idoneo ad *attrarre* all'interno della fonte normativa l'esplicitazione della finalità e della modalità del trattamento, così da realizzare una clausola di stretta legalità per quanto concerne i presupposti di liceità del trattamento. Inoltre, tra le basi giuridiche che legittimano il trattamento dei dati, alla legge (e al regolamento, nei casi previsti dalla legge) sono aggiunti gli "atti amministrativi generali". Sul piano sintattico, va notato che questi ultimi non sembrano costituire un atto fonte cui la legge debba delegare la capacità di intervento (come nel caso dei regolamenti), ma sembrano rappresentare un ulteriore *base giuridica*, ad integrazione delle precedenti. Da queste due modifiche, considerate congiuntamente, derivano conseguenze notevoli. Venuto meno il polo attrattivo determinato dall'avverbio "esclusivamente" ed aggiunta la possibilità di fondare il trattamento (anche) sulla base giuridica consistente negli atti amministrativi generali (atti, per definizione, di carattere non normativo), lo standard legale risultante smette di caratterizzarsi nei termini della *stretta legalità*. Certamente, una base giuridica fondata sulla fonte

legislativa continuerà a essere indispensabile – per quanto riguarda la conformità allo standard legale *di diritto interno*[33] – quando all'amministrazione sia affidato l'esercizio di un potere (in ossequio al principio di legalità garanzia), o comunque per quanto concerne l'indicazione delle finalità da perseguire (legalità-indirizzo), come anche in quei casi – sul fronte dello standard legale di *diritto dell'Unione* – selezionati ed evidenziati dalla giurisprudenza della Corte di giustizia, e consistenti essenzialmente nell'esercizio di funzioni pubbliche che implicano si concretizzano mediante la comunicazione al pubblico di dati personali. E tuttavia, il fatto che la base legale possa articolarsi *anche* sugli atti amministrativi generali adottati dal titolare del trattamento, comporta che alcuni elementi potranno essere individuati ed esplicitati in questa ulteriore sede. Mentre, cioè, spetterà alla legge individuare le *finalità generali*, *i compiti di interesse pubblico* assegnati alla PA (e, eventualmente, conferire i poteri pubblici a ciò deputati), l'esplicitazione di quali trattamenti effettuare, su quali dati, per quali finalità potrà essere assolta anche nell'atto amministrativo generale. Si tratta di un contributo di *flessibilizzazione* del presupposto di liceità di grande momento, poiché l'atto amministrativo generale costituisce uno strumento giuridico che è sostanzialmente *nella disponibilità dell'amministrazione titolare del trattamento*, così che questa potrà procede, con proprio atto, tanto alla *specificazione* e *precisazione* del compito di interesse pubblico cui il trattamento è (strumentale), quanto alla individuazione ed esplicitazione degli ulteriori elementi che integrano la clausola di necessarietà strumentale (quali trattamenti, quali dati, quali finalità). Al tempo stesso, la circostanza per cui questi elementi sono destinati ad essere evidenziati in un atto amministrativo generale, comporta anche la possibilità di esercitare una verifica e un controllo circa la rispondenza di questi elementi al canone di liceità imposto dal GDPR. In questo senso, l'adozione dell'atto amministrativo generale, quale strumento utile a integrare la base giuridica, risponde ad una serie di esigenze. Costituisce un elemento di *trasparenza*, mediante il quale sarebbero integrati quei requisiti di chiarezza, precisione, e prevedibilità di applicazione che il considerando (41) del regolamento indica quali attributi che devono caratterizzare la base giuridica[34]. Costituisce veicolo mediante il quale l'amministrazione *rende*

[33] Ciò che per altro è anche oggetto anche di specifica considerazione nel regolamento, che al considerando n. 41 chiarisce che "Qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, *fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato*" (corsivi aggiunti).

[34] Cfr. considerando n. 41: "tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la «Corte di giustizia») e della Corte europea dei diritti dell'uomo".

conto delle scelte effettuate in ordine al rispetto dei principi e dei criteri di legittimazione dei trattamenti effettuati, sulla base del principio di responsabilizzazione di cui all'art. 5, par. 2 del regolamento. Rappresenta elemento di garanzia di conformità del trattamento, anche in quanto oggetto di verifiche da parte dell'autorità nazionale di controllo e punto di riferimento per l'attivazione della tutela giurisdizionale. Come si comprende, siffatta articolazione della base giuridica dei trattamenti effettuati per l'esecuzione di compiti di interesse pubblico apre la porta alla configurabilità di trattamenti articolati su basi giuridiche la cui integrazione spetta anche alla stessa amministrazione che li pone in essere.

Nella misura in cui – secondo lo schema ricostruttivo proposto più in alto (cfr. cap. 2, par. 2.4) – il trattamento dei dati personali si risolve sempre in una incisione nella sfera giuridica del titolare, che – in assenza di previo consenso – si configura come l'esercizio di un *potere giuridico*, questo schema si approssima in modo significativo a quello del potere implicito (che trova esternazione e conformazione in un atto che è proprio della stessa amministrazione che esercita tale potere, e quindi si configura, in questo senso, come un potere auto-attribuito). Quindi, la fattispecie di cui all'art. 2-ter, comma 1, come riformulata dal d.l. 139/2021, appare molto più allineata rispetto allo *standard legale* che caratterizza l'art. 6, par. 1, lett. e) del regolamento, nella misura in cui assegna all'amministrazione la capacità e gli strumenti (gli atti amministrativi generali) utili per individuare e specificare gli elementi del trattamento di dati personali strumentale all'esercizio di una funzione pubblica.

Tuttavia, l'intervento di "alleggerimento" non si è limitato a questa – pure significativa – modifica, relativa alla qualificazione delle basi giuridiche abilitanti il trattamento. Dopo il comma 1 dell'art. 2-ter del Codice, è stato inserito un comma 1-bis, il cui schema – nel declinare un'ulteriore fattispecie di presupposto legittimante il trattamento dei dati personali – risponde invece in modo del tutto fedele al modello della *necessary clause*. La disposizione si caratterizza per una qualificazione molto scrupolosa dei titolari del trattamento che possono avvalersi di questo titolo di legittimazione, secondo un criterio che – questa volta – appare di carattere prettamente *soggettivo*, mediante il quale sono individuate le pubbliche amministrazioni che possono avvalersene (ossia, le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196); e i soggetti in forma societaria che – parimenti – possono farvi ricorso (ossia, le società a controllo pubblico statale o, limitatamente ai gestori di servizi pubblici, locale, di cui all'articolo 16 del testo unico in materia di società a partecipazione pubblica, di cui al decreto

legislativo 19 agosto 2016, n. 175, con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato). Il presupposto di liceità del trattamento è formulato in questi termini: "Fermo restando ogni altro obbligo previsto dal Regolamento e dal presente codice, il trattamento dei dati personali [*da parte dei soggetti di cui sopra*] è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse[i] attribuiti". Come si vede, la formula ricalca fedelmente quella utilizzata nel GDPR, mentre l'avverbio "*anche*" (che fa evidentemente riferimento a quanto statuito nel comma precedente) vale a chiarire che si tratta di un titolo abilitativo che si aggiunge a quello individuato nel comma 1 del medesimo articolo.

Circa i caratteri e la portata di un presupposto di liceità così formulato, vale quanto già detto a proposito della *necessary clause* di cui all'art. 6, par. 1, lett. e) del regolamento, anche per quanto concerne la rispondenza allo schema (di legittimazione) di ipotesi di *poteri impliciti* nel trattamento dei dati personali ai fini dell'esercizio di compiti di interesse pubblico. Sono altresì interessanti le clausole di salvaguardia inserite all'inizio e alla fine del comma ("Fermo restando ogni altro obbligo previsto dal Regolamento e dal presente codice (…). In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento". Infatti, l'inserimento di questi passaggi tradisce una lettura del rapporto tra regolamento e norma legislativa interna, innescata dalle clausole di cui all'art. 6, par. 2 e 3, tale per cui l'attivazione dello spazio di manovra (a prescindere dalla latitudine delle disposizioni poi adottate) varrebbe quasi a *schermare del tutto* tale ambito materiale (quello relativo al trattamento dei dati personali funzionale all'esercizio di compiti di interesse pubblico) dalla diretta applicabilità delle disposizioni del regolamento. Così ché, per salvaguardare l'applicabilità delle disposizioni del regolamento sarebbe necessario farne esplicito richiamo (e salvezza, appunto) nella normativa interna. Una lettura che non appare del tutto persuasiva, dal momento che l'apertura di margini di precisazione e adattamento al legislatore nazionale non vale certo (di per sé) a *disattivare* la prescrittività (nella forma della diretta applicabilità ed efficacia) delle pertinenti disposizioni del regolamento, mentre l'effetto di *deroga* a tale disciplina, derivante dalla concreta formulazione delle discipline nazionali così adottate, opera solo nella misura in cui questa disciplina si discosti dal (ovvero integri, arricchisca effettivamente il) quadro normativo disegnato nel GDPR; infatti, negli spazi di potenziale differenziazione non coperti dalla disciplina nazionale di adattamento, continuano a trovare combinata, coerente applicazione

le disposizioni del GDPR, secondo quel meccanismo di integrazione (residuale) che abbiamo descritto più in alto. Per fare un esempio, poiché la disciplina nazionale (così come riformulata dal d.l. n. 139/2021, nel testo convertito) nulla dice a proposito del principio *di limitazione della finalità del trattamento* (che pure rappresenta uno degli aspetti sui quali la disciplina nazionale potrebbe intervenire, a mente dell'art. 6, par. 3 del regolamento), continuerebbero a trovare applicazione le indicazioni formulate, a questo riguardo, nell'art. 6, par. 4, anche qualora la disciplina nazionale non le avesse esplicitamente richiamate per farle salve (come invece fa). E tuttavia, anche considerate le evidenze che abbiamo tratto dall'analisi della disciplina introdotta in altri ordinamenti, circa le modalità di esercizio del margine di manovra (cfr. *supra*, cap. 3, par. 4), queste indicazioni "di salvaguardia" non risultano del tutto prive di utilità (e di effetto). Per un verso, esse – sebbene possano apparire ripetitive o ridondanti – sono di ausilio i fini di una chiara lettura ed interpretazione del quadro normativo vigente ed applicabile[35]; inoltre, indirizzano l'interprete, scongiurando il rischio che i "vuoti" possano essere letti ed interpretati come deroga *implicita*. Pertanto, resta confermata la lettura per la quale il presupposto di liceità disegnato all'art. 2-ter, comma 2, va applicato integrando le indicazioni ivi formulate con le pertinenti disposizioni del regolamento.

3.2.2. I presupposti di liceità della comunicazione dei dati personali comuni (verso l'integrabilità delle banche dati pubbliche)

Anche per effetto delle modifiche introdotte al comma 2 dell'art. 2-ter, il regime applicabile alla *comunicazione* dei dati personali "comuni" fra titolari che effettuano trattamenti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è del tutto parificata al regime appena descritto: pertanto, la comunicazione potrà avvenire (lecitamente), sia in ragione di una base giuridica così come prevista ai sensi del

[35] Come è stato efficacemente notato "the different opening clauses of the GDPR which allow national legislation are a strong indication for the legality of Member State acts with repetitive content (…) Insofar as provisions of the GDPR are modified by national measures in the scope of application of the GDPR's opening clauses, a complex multi-level system arises. This has far reaching consequences for legal clarity (…) In order to restore legal clarity in this multi-level system, it must be possible for the national legislator to repeat at least parts of the European Regulation in its national acts to clarify to what extent the national measures replace the European Regulation and to what extent the European Regulation remains applicable", Wagner J. and Benecke A. (2016), "National legislation within the framework of the gdpr", cit., 360.

comma 1 (e, pertanto, anche qualora finalità del trattamento e dati trattati siano identificati in atti amministrativi generali); sia perché "necessaria ai sensi del comma 1-bis". Dunque, anche con riferimento a quegli specifici trattamenti dei dati (la comunicazione fra titolari che esercitano funzioni pubbliche) che sono funzionali ad abilitare la *circolazione* e l'*integrazione* dei patrimoni informativi pubblici, il regime di trattamento dei dati personali viene flessibilizzato mediante la riconduzione della relativa disciplina al modello della *necessary clause*: il che pare del tutto coerente con alcune delle esigenze di contesto che abbiamo segnalato più in alto[36]. Si noti, a questo proposito, che l'espressione utilizzata identifica la specifica tipologia di comunicazione che avvenga tra soggetti che trattano dati *per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, a significare che, per un verso, il soggetto da cui origina la comunicazione deve avere il controllo di quei dati in ragione dell'esercizio di una funzione pubblica; dall'altro, che il destinatario della comunicazione deve ricevere quei dati in funzione dell'esercizio di un compito di interesse pubblico. Vale la pena di sottolineare che, con riferimento a questa tipologia di trattamento, le modifiche introdotte al comma 2 dell'art. 2-ter non ribadiscono (come invece viene fatto nel testo del coma 1-bis) il richiamo al rispetto di "ogni altro obbligo previsto dal regolamento", né la specifica salvaguardia dell'art. 6. Una circostanza che è probabilmente priva di effetti concreti (per le ragioni già esposte) e che tuttavia appare significativa della volontà (o quantomeno, del malcelato desiderio) del legislatore di "liberare" il trattamento che abilita la circolazione dei dati personali all'interno del settore pubblico e l'integrazione dei diversi corpi informativi da limiti, condizioni e presidi avvertiti come *eccessivi* (e che pure, nel regime precedente alle modifiche, risultava comunque un po' meno *rigido* di quello riservato a tutte le altre tipologie di trattamento).

[36] Cfr. il par. 3.1 di questo capitolo. Si noti che con l'adozione della *necessary clause*, il presupposto di liceità quanto alla tutela dei dati personali (anche per quanto concerne la comunicazione dei dati personali all'interno del settore pubblico) finisce per risultare del tutto allineato alla regime legislativo che regola la comunicazione/circolazione dei dati tra pubbliche amministrazioni, come delineato nell'art. 50, comma 2 del CAD, ai sensi del quale "Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato *sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente*, senza oneri a carico di quest'ultima": il presupposto che giustifica la fruizione del dato da parte dell'amministrazione richiedente (*i.e.* la *strumentalità necessaria*) è il medesimo che ne autorizza la comunicazione, nel caso si tratti di un dato personale "comune" (fatta salva la verifica di compatibilità delle finalità del trattamento).

3.2.3. I presupposti di liceità della diffusione dei dati personali comuni (una deroga allo standard legale dell'Unione?)

Le modifiche introdotte con riferimento, invece, al trattamento di dati che siano detenuti in ragione dell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e che consista nella *diffusione* di dati personali ovvero nella *comunicazione a soggetti che intendano trattarli per altre finalità* (ossia, per finalità che non corrispondano all'esercizio di un compito di interesse pubblico), risultano invero *problematiche*. Il regime, anche qui, è allineato a quello indicato ai commi 1 e 1-bis, salvo che – ma solo qualora si faccia cioè ricorso a quest'ultima ipotesi (la *necessary clause*) – occorre darne notizia al Garante almeno dieci giorni prima dell'inizio della diffusione o della comunicazione. L'applicazione tanto della *necessary clause* (comma 1-bis) quanto della base giuridica *non legislativa* (comma 1) appare problematica, perché sembra elidere la necessità (quantomeno, con riferimento alla diffusione, nonché alla comunicazione che consegua all'esercizio di un diritto di accesso azionabile da chiunque) che questo tipo di trattamento sia disciplinato *dalla legge*, sia con riferimento alla identificazione delle categorie di dati oggetto di diffusione/comunicazione, sia con riferimento alla stessa tipologia di trattamento. Insomma, per questa tipologia di trattamento, l'ammissibilità di poteri impliciti pare da escludersi, non solo per effetto del principio di legalità (sul fronte del diritto interno), ma anche alla luce della giurisprudenza della Corte di giustizia, già richiamata (cfr. il cap. 3, par. 2.5). La serietà e la gravità del pregiudizio alla tutela dei dati personali determinato da questa specifica modalità di trattamento, infatti, richiede necessariamente (quantomeno) che esso sia previsto e disposto con una norma di legge espressa[37]. Pertanto, delle due l'una: o questo regime è ricostruito ed interpretato alla luce di tali esigenze (ma allora questa formulazione risulterebbe *inutiliter data*), oppure effettivamente il legislatore (nell'esercizio del margine di manovra accordato dal regolamento) avrebbe delineato un regime che opererebbe in deroga non tanto rispetto al regolamento, quanto piuttosto rispetto alla declinazione dello *standard legale* definito in sede giurisprudenziale (sul fronte del diritto dell'Unione), in diretta applicazione del diritto alla tutela dei dati personali, come sancito dall'art. 8 della Carta dei diritti fondamentali dell'UE. Un uso "estremo" del margine di manovra, che spinge forse la disciplina nazionale (nella declinazione concreta

[37] Già con riferimento alla versione precedente della disposizione che abilita la diffusione dei dati personali da parte dell'amministrazione, e quindi sotto un regime informato alla *strict legality rule*, sono state sollevate critiche con riferimento all'ambiguità del testo normativo. In particolare, appariva "di difficile decifrazione il trattamento 'per altre finalità'" (cfr. Cardarelli F. (2021), *Comm. sub. art. 2-ter Codice Privacy*, cit., 1023).

del *dual legalty standard*) oltre la soglia di compatibilità con l'ordinamento dell'Unione, e la espone, pertanto, al rischio di censura in quella sede.

3.2.4. I presupposti di liceità del trattamento dei dati particolari (verso l'autonomia operativa dei titolari del trattamento)

Anche per quanto concerne il trattamento dei dati particolari di cui all'art. 9 del regolamento si registrano alcune significative innovazioni, e sempre nel senso dell'alleggerimento dei presupposti di trattamento. Immutate le altre condizioni e presupposti trattamento già contemplali all'art. 2-sexies, una prima innovazione concerne l'indicazione (anche qui) degli atti amministrativi generali, accanto alla legge o al regolamento, quale base giuridica atta ad autorizzare il trattamento di tali categorie di dati. Anche qui, l'innovazione non è di poco momento. Dal momento, infatti, che i motivi di interesse pubblico rilevante sono raccolti ed elencati al comma 2 del medesimo articolo, tale modifica consente alle amministrazioni (cui siano attribuiti compiti e poteri in funzione del perseguimento di tali interessi) di elaborare per proprio conto (mediante l'adozione di atti amministrativi generali) le disposizioni 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* (fatte salve le specifiche ulteriori garanzie, rimante immutate, disposte dall'art. 2-septies con riferimento ai dati genetici, biometrici e relativi alla salute). Infatti, tali amministrazioni non dipendono più dalla previa fissazione in legge (o nel regolamento, ma sulla base della legge) dei requisiti necessari (quali, appunto, la specificazione dei tipi di dati che possono essere trattati, delle operazioni eseguibili e del motivo di interesse pubblico rilevante, nonché delle misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato), potendo invece procedere loro stesse a fissare tali requisiti, con propri atti.

Inoltre, sempre all'art. 1-sexies, è stato introdotto il comma 1-bis che muove nella direzione di realizzare un *framework normativo* utile a favorire l'interconnessione e la circolazione dei dati sanitari, ivi compresi quelli raccolti nel Fascicolo sanitario elettronico, da porre a supporto dell'esercizio delle funzioni di programmazione, governo e gestione a opera dei diversi

attori del sistema sanitario nazionale, come indicati nella disposizione in parola. Il presupposto introdotto al fine di abilitare questa finalità di trattamento è la pseudonimizzazione dei dati. Parallelamente, mediante l'abilitazione dell'interconnessione di tali informazioni con altri dati di natura non sanitaria[38], si è predisposto il quadro giuridico finalizzato a favorire la implementazione della misura M6 del PNNR[39]. Tutti questi interventi sono animati dalla consapevolezza, maturata in particolare nel corso della pandemia, delle gravi carenze che affliggono il sistema informativo posto a supporto delle funzioni di salute (e le altre attività strumentali e a queste connesse) nel nostro paese. Un'analisi della frammentazione e dell'inefficienza dei diversi (e non comunicanti) flussi informativi che alimentano le diverse articolazioni funzionali del sistema nazionale, indica che anche queste soluzioni sono ancora considerate parziali e insufficienti[40].

In ogni caso, proprio le norme adottate con riferimento ai presupposti di trattamento dei dati sanitari dimostrano la stretta connessione che intercorre tra le circostanze, le carenze e le esigenze evidenziatesi nel corso della vicenda pandemica e gli interventi di "semplificazione" o alleggerimento introdotti con il d.l. n. 139/2021[41]. Esigenze pressanti e non rinviabili, come

[38] Cfr. l'art. 7 del d.l. 19 maggio 2020, n. 34, convertito, con modificazioni, dalla legge 17 luglio 2020, n. 77, sono apportate le seguenti modificazioni, come introdotto dall'art. 9, comma 4 del decreto «capienze».

[39] La Missione 6 salute (M6) del PNRR contiene tutti gli interventi a titolarità del Ministero della Salute suddivisi in due componenti: la componente M6C1 – Reti di prossimità, strutture e telemedicina per l'assistenza sanitaria territoriale (a sua volta articolata negli interventi: Case della Comunità e presa in carico della persona; Casa come primo luogo di cura e telemedicina:; Rafforzamento dell'assistenza sanitaria intermedia e delle sue strutture (Ospedali di Comunità)); e la componente M6C2 – Innovazione, ricerca e digitalizzazione del Servizio Sanitario (a sua volta articolata nelle misure: Aggiornamento tecnologico e digitale; Formazione, ricerca scientifica e trasferimento tecnologico).

[40] Cfr. Consiglio Superiore di Sanità, *Proposta per lo schema di Riforma dei Sistemi Informativi Sanitari*, 2022, testo disponibile al sito: https://www.salute.gov.it/imgs/C_17_pubblicazioni_3223_allegato.pdf

[41] Come indicato nella relazione di accompagnamento al d.d.l. di conversione, le misure introdotte dall'art. 9 del d.l. 139/2019 sono volte "ad allineare le previsioni del codice in materia di protezione di dati personali, di cui al decreto legislativo 30 giugno 2003, n.196 al rispetto delle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nell'ottica di semplificare il quadro e valorizzare le attività e i compiti di interesse pubblico svolti dalle pubbliche amministrazioni o dalle società a controllo pubblico statale per finalità di pubblico interesse, oltre che nell'adozione e attuazione delle riforme e misure previste dal PNRR", cfr. A.S. 2409, relazione, 11. Anche il presidente del Garante per la protezione dei dati personali, nell'audizione resa in sede di conversione in legge, ha sottolineato "il fine, complessivamente sotteso alla riforma, di semplificazione del quadro normativo e delle relative regole procedurali".

testimoniano le specifiche disposizioni introdotte per assicurare la loro immediata operatività[42], o per rassicurare i responsabili del trattamento rispetto alle conseguenze connesse al trattamento dei dati[43].

3.2.5. Il ridimensionamento del ruolo del Garante

Le misure di alleggerimento così introdotte si traducono anche in un oggettivo depotenziamento del ruolo del Garante[44]. Viene meno, come detto, il ruolo di *filtro* per quanto concerne la comunicazione di dati comuni tra titolari di trattamenti svolti a fini pubblici. Si aggiunga che, con l'abrogazione dell'art. 2-quinquiesdecies (introdotto dal d.lgs 101/2018), viene esclusa la consultazione preventiva del Garante in caso di trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati; a tale consultazione era correlato, come si è visto, il potere del Garante di prescrivere *ex ante* misure e accorgimenti a garanzia dell'interessato che il titolare era tenuto ad adottare[45]. In questo modo, i trattamenti finalizzati

[42] Ai sensi dell'art. 9, comma 5 del d.l. 139/2021, come convertito il l. n. 205/2021, infatti gli articoli concernenti il trattamento effettuato per l'esecuzione di compiti di interesse pubblico, come risultanti dalle modifiche introdotte, "si applicano anche ai casi in cui disposizioni di legge già in vigore stabiliscono che i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, la finalità del trattamento nonché le misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato e i suoi interessi sono previsti da uno o più regolamenti".

[43] Il decreto introduce infatti un trattamento di maggior favore per i titolari di trattamenti "pubblici": infatti, mentre la disciplina generale prevede che l'avvio di una procedura per l'adozione di provvedimenti correttivi e sanzionatori vada notificata al titolare o al responsabile delle presunte violazioni, *salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare*, per quanto riguarda invece i titolari dei trattamenti per l'esecuzione di compiti di interesse pubblico, tale notifica può essere omessa solo in casi molto più circoscritti ("esclusivamente nel caso in cui il Garante abbia accertato che le presunte violazioni hanno già arrecato e continuano ad arrecare un effettivo, concreto, attuale e rilevante pregiudizio ai soggetti interessati al trattamento, che il Garante ha l'obbligo di individuare e indicare nel provvedimento, motivando puntualmente le ragioni dell'omessa notifica)". Se mancano tali presupposti (e la notifica non è stata inviata), il provvedimento sanzionatorio eventualmente adottato è accertato dal giudice come inefficace; cfr. art.9, comma 5 del d.l. n. 139/2021, come convertito in l. n. 205/2021.

[44] Per una rilettura contestualizzata delle ragioni del ridimensionamento del ruolo del Garante, cfr. Palladini V. (2022), "Il ruolo del Garante per la protezione dei dati personali nell'emergenza sanitaria", cit., *passim*; cfr. anche Sartoretti C. (2021), "Le authorities al tempo del covid-19. Riflessioni sul ruolo delle autorità indipendenti: modello in declino o consolidato?", in *DPCE Online*, 47/2, disponibile al sito: https://www.dpceonline.it/index.php/dpceonline/article/view/1347 (15.5.2023).

[45] Il Garante è stato così privato di una "funzione particolarmente penetrante" (così Palla-

all'esecuzione di compiti di interesse pubblico sono stati ricondotti entro la piena operatività del principio di responsabilizzazione, che disloca sul titolare l'onere e le responsabilità di conformare il trattamento ai vincoli, ai requisiti e alle esigenze imposte dal GDPR.

3.3. Dalla identificazione del (mutevole) dual standard *all'analisi dei suoi effetti*

In definitiva, tutti gli interventi di revisione delle disposizioni relative al trattamento dei dati personali finalizzati all'esercizio di funzioni di interesse pubblico introdotti dal d.l. n. 139/2021 si caratterizzano nel senso di assicurare una più ampia autonomia operativa e di iniziativa alle amministrazioni nel procedere al trattamento dei dati, quando tale trattamento risulti necessario per l'esecuzione di un compito di interesse pubblico (o per l'esercizio di un potere pubblico). Il significativo allentamento dei presupposti di stretta legalità che caratterizzavano le disposizioni introdotte dal d.lgs n. 101/2018 e la più decisa preferenza per il meccanismo di abilitazione/giustificazione di tali operazioni di trattamento fondato sulla *necessary clause* consentono alle amministrazioni (*rectius*, a tutti i titolari di compiti e di poteri connessi con l'esercizio di funzioni pubbliche) di poter procedere con maggiore agio a completare/integrare il quadro degli elementi necessari per effettuare il trattamento (a partire dalla individuazione ed esplicitazione della finalità del trattamento, dei dati da trattare e delle operazioni da effettuare), senza dover dipendere dalla (ed attendere una) previa espressa identificazione di tali elementi nella norma (di legge o di regolamento, sulla base della legge). Una soluzione che passa per l'adozione di atti amministrativi generali, da parte delle amministrazioni titolari del trattamento, ovvero (per i soli dati "comuni") anche in assenza di tali atti amministrativi generali, purché il trattamento risulti necessario per l'esecuzione del compito di interesse pubblico[46].

dini V. (2022), "Il ruolo del Garante per la protezione dei dati personali nell'emergenza sanitaria", cit., 156. Secondo Bombardelli M. (2022), *Dati personali (Tutela)*, cit., mentre "il Garante si può trovare a disporre di poteri di fatto molto penetranti (…) il cui esercizio può interferire con l'attività di perseguimento dei fini istituzionali delle amministrazioni (…) alcune delle possibili aree di sovrapposizione sono per altro di recente state rimosse con la modifica dell'art. 2-ter del d.l. n. 196/2013 operata con il d.l. n. 139/2021" (377 e nota n. 157).

[46] Nel caso dell'attivazione della clausola di necessarietà di cui all'art. 2-ter, comma 1-bis del Codice, la opportuna evidenziazione di quegli stessi elementi (la finalità del trattamento, i dati da trattati e le operazioni effettuate), dovrà seguire logiche e modalità di verificazione differenti, connesse ad uno paradigma giustificativo che si modella (come detto) sullo schema dei *poteri impliciti*; in questo senso, è interessante prendere nota di quanto sottolineato dal presidente del Garante per la protezione dei dati personali in occasione dell'audizione svolta

Nel capitolo seguente, analizzeremo alcuni casi di studio, utili ad evidenziare l'impatto determinato da questo significativo cambio di direzione, nel passaggio, cioè, da uno standard legale del trattamento caratterizzato in termini di *stretta legalità*, ad uno caratterizzato da una più netta apertura nella direzione della *necessary clause* e, comunque, da una maggiore autonomia operativa in capo ai titolari di trattamento finalizzati all'esecuzione di compiti di interesse pubblico.

Nel capitolo finale, anche alla luce degli elementi emersi, proveremo a riflettere sulle configurazioni assunte dal principio di legalità, per come abilitate dai due standard legali osservati in azione.

nel corso della discussione del disegno di legge di conversione del d.l. n. 139/2021, a proposito dell'intenzione del Governo di stabilire che la base giuridica di un trattamento da parte di un soggetto pubblico per il perseguimento delle proprie finalità istituzionale può essere la legge, un regolamento, un atto amministrativo generale *o la semplice strumentalità del trattamento alle sue finalità istituzionali*; osserva il presidente: "Mi sia, peraltro, consentito segnalare che, in tale ultima evenienza – a mio avviso non strettamente strumentale al perseguimento delle dichiarate finalità di semplificazione – la compatibilità con l'ordinamento europeo dei trattamenti di dati personali avviati da un soggetto pubblico sulla base di tale disposizione risulterà, inesorabilmente, *da accertare caso per caso* giacché, l'ordinamento europeo, esige sempre e comunque – quale che sia l'impostazione del diritto nazionale in fatto di fonte giuridica legittimante il trattamento – che il trattamento, nella sua finalità e nelle sue modalità, sia trasparente, prevedibile, noto ai cittadini. E tale requisito, ovviamente, non appare sempre facilmente integrabile in assenza anche di un semplice atto amministrativo generale che disponga e disciplini il trattamento" (corsivi aggiunti).

5. Tre casi di studio

1. Sperimentare soluzioni conoscitive strumentali all'esercizio delle funzioni di prevenzione della corruzione amministrativa (primo caso di studio)

1.1. L'esigenza di dotare una funzione nuova di adeguati supporti e strumenti conoscitivi

La predisposizione e messa in opera di un sistema ordinamentale strutturato di prevenzione della corruzione ha posto immediatamente in rilievo l'esigenza di disporre di adeguati strumenti conoscitivi che consentissero di leggere in modo più adeguato il fenomeno che si intendeva regolamentare (a fini di prevenzione). Infatti, era oramai venuta a maturazione una certa insoddisfazione rispetto agli indici di percezione dei fenomeni corruttivi, che pure avevano contribuito ampiamente all'affermarsi di una cultura attenta e sensibile al fenomeno della corruzione[1]. Una insoddisfazione motivata non in termini ideo-

[1] Sul punto, sia consentito rinviare a Ponti B. (2018) *Oltre la percezione: concretizzare le potenzialità conoscitive degli indicatori basati sull'elaborazione degli hard data di fonte amministrativa*, in (eds.) Ponti B. e Gnaldi M., *Misurare la corruzione oggi. Obiettivi, metodi, esperienze*, Milano 47-58, nonché Tartaglia Polcini G. (2018), *La corruzione tra realtà e rappresentazione. Ovvero: come si può alterare la reputazione di un paese*, Bologna; Mazzoni M., Stanziano A., Recchi L. (2017), "Rappresentazione e percezione della corruzione in Italia. Verso una strumentalizzazione del fenomeno", in *Comunicazione politica*, 1, 99-118; Andersson S., Heywood P. M. (2009), "The Politics of Perception: Use and Abuse of Transparency International's Approach to Measuring Corruption", in *Political Studies*, 57, pp. 746-767, Charron N. (2015), "Do corruption measures have a perception problem? Asses-sing the relationship between experiences and perceptions of corruption among citizens and experts", in *European Political Science Review*, 1-25, Lambsdorff J. (2006), "Measuring corruption – the

logici o accademici, ma piuttosto dalla consapevolezza che – una volta predisposto un sistema di istituti volti ad operare in modo capillare[2] – occorre affiancare a indici sintetici di livello nazionale (quali il CPI di Transparency International, su tutti), altri strumenti conoscitivi di carattere disaggregato (sul piano territoriale, funzionale, organizzativo), indispensabili in primo luogo per verificare precisione, adeguatezza ed efficacia degli istituti messi in campo[3]. Sotto questo profilo, l'esigenza conoscitiva è innanzitutto una esigenza propria della fase di progettazione dell'anticorruzione, tanto a livello decentrato, quanto a livello di autorità nazionale di regolazione. La disciplina legislativa è esplicita nel richiedere (come per altro pare necessario che sia) che i momenti di pianificazione siano preceduti, accompagnati e seguiti da analisi quantitative e qualitative volte a indentificare tutti quegli elementi di conoscenza della realtà utili a calibrare ed integrare tra loro gli istituti, tenendo conto delle condizioni specifiche del contesto in cui l'amministrazione opera (analisi di contesto). Per altro, tali elementi conoscitivi integrano in modo permanente la funzione di progettazione, nella misura in cui consentono una verifica delle misure (ed un successivo aggiornamento/aggiustamento) non episodica o meramente "volontaristica", ma (anche) razionalmente fondata sulla registrazione dei dati di fatto rilevanti, di come questi si sono "mossi" (anche) per effetto del dispiegamento degli strumenti di prevenzione.

Dunque, nel momento in cui la funzione di prevenzione si è tradotta in un sistema concreto ed operativo di strumenti giuridici, si è posto il tema di come implementare e migliorare la funzionalità di tale sistema, potendo di-

validity and precision of subjective indicators (Cpi)", in (eds) C. Sampford, A. Shacklock, C. Connors, F. Galtung, *Measuring Corruption*, Aldershot, Ashgate, 81-99; Liu T., Juang W., Yu C. (2023), "Understanding Corruption with Perceived Corruption: The Understudied Effect of Corruption Tolerance", in Public Integrity, 25/2, 207-219.

[2] Sul sistema di prevenzione della corruzione edificato con la legge 6 novembre 2012, n. 190 e con decreti legislativi attuativi, si vedano, *ex multis*, Carloni E. (2023), *L'anticorruzione. Politiche, regole, modelli*, Bologna; Cantone R. (2020), *Il sistema della prevenzione della corruzione*, Torino; D'Alberti M. (2017), *Corruzione e pubblica amministrazione*, Napoli; Nunziata M. (2017), *Riflessioni in tema di lotta alla corruzione: rimedi preventivi e repressivi*, Roma; Cantone R., Merloni F. (2015), *La nuova Autorità nazionale anticorruzione*, Torino; Nicotra I. A. (2016), *L'Autorità Nazionale Anticorruzione: tra prevenzione e attività regolatoria*, Torino; (eds.) Mattarella B. G. e Pelissero M. (2013), *La legge anticorruzione. Prevenzione e repressione della corruzione*, Torino.

[3] Circa la necessità di calibrare gli interventi di prevenzione e contrasto ai fenomeni di corrusione amministrativa con riferimento alle caratteristiche specifiche delle diverse realtà territoriali ed amministrative, si veda Barone A. (2016), *Territorio e politiche anticorruzione*, in Scoca F.G. e Di Sciascio A. (eds.), *Le proprietà pubbliche: tutela, valorizzazione e gestione*, Napoli, 113-134.

sporre di un apparato conoscitivo adeguato all'esercizio delle relative funzioni. A questo fine, l'ANAC, a seguito di uno studio preliminare[4], ha attivato un progetto sperimentale[5], con l'obiettivo specifico di contribuire alla elaborazione di indicatori di carattere quantitativo e quali-quantitativo, utili all'esercizio delle funzioni di prevenzione amministrativa della corruzione amministrativa, e più in generale funzionali ad accrescere gli strumenti di conoscenza dei fenomeni di deviazione patologica dell'esercizio delle funzioni pubbliche e della cd. *maladministration*. Alcuni aspetti di questo progetto forniscono elementi di particolare interesse, e pertanto costituiscono il nostro primo caso di studio.

Disporre di adeguati strumenti conoscitivi costituisce un elemento strategico sia con riferimento alla fase di progettazione e riprogettazione dell'anticorruzione, sia un fattore utile (quando non, necessario) per una effettiva gestione degli strumenti di prevenzione, nella loro concreta, diuturna applicazione. Infatti, molti istituti di prevenzione della corruzione agiscono rispetto a un contesto operativo caratterizzato da *asimmetrie informative* rilevanti e strutturali (a scapito dell'amministrazione interessata a prevenire il verificarsi di condizioni favorevoli alla corruzione/*maladministration*), che devono essere in qualche modo colmate al fine di far valere in modo efficace tali istituti. In linea generale, lo scopo degli istituti della trasparenza (come anche quello del *whistleblowing*) è proprio quello di abilitare una maggiore conoscenza (diffusa), così che i fatti rilevanti possano essere messi in rilievo, ed eventualmente gestiti in modo conseguente. Tuttavia, nella misura in cui gli istituti della trasparenza (diffusione obbligatoria tramite siti web e accesso generalizzato) consistono nel rendere disponibili in modo generalizzato determinate informazioni, essi assolvono solo *in parte* alla funzione di colmare l'asimmetria informativa, dal momento che a tale scopo l'informazione non deve solo essere disponibile, ma anche opportunamente gestita/trattata. Ciò perché una cosa è la *disponibilità* delle informazioni, altra cosa (ulteriore passaggio) è la possibilità di estrarre *conoscenza* da queste informazioni. Pertanto, è non solo del tutto fisiologico, ma è anche strettamente funzionale all'efficace dispiegamento degli strumenti di prevenzione

[4] Cfr. ANAC, *Analisi istruttoria per l'individuazione di indicatori di rischio corruzione e di prevenzione e contrasto nelle amministrazioni pubbliche*, 2014, disponibile al sito https://shorturl.at/otST8 (consultato il 4.5.2023).

[5] Progetto PON "Misurazione del rischio di corruzione a livello territoriale e promozione della trasparenza" (2018-2023): le informazioni sul progetto sono disponibili a questo sito: https://www.anticorruzione.it/-/misurazione-territoriale-del-rischio-corruzione-e-promozione-della-trasparenza-progettopon-1#p1. I risultati del progetto (cruscotto indicatori di rischio a livello territoriale e centro di documentazione) sono disponibili in questo sito: https://www.anticorruzione.it/misura-la-corruzione. L'autore di questo studio ha partecipato al progetto come esperto esterno senior.

che il sistema di anticorruzione possa disporre di strumenti di trasparenza mediante i quali attivare quella capacità conoscitiva utile (indispensabile?) sia in fase di progettazione che in fase di gestione concreta degli strumenti di prevenzione della corruzione.

Entro queste coordinate, nella definizione delle strategie di prevenzione della corruzione, ai meccanismi connessi alla *trasparenza orizzontale* (quella attivata a partire dal controllo diffuso operato mediante accesso e utilizzo dei dati resi disponibili pubblicamente – mediante gli istituti della pubblicità obbligatoria e del diritto di accesso generalizzato), è venuta maturando la necessità di affiancare strumenti di *trasparenza verticale*. Ovvero, di mettere a punto strumenti idonei ad attivare una capacità conoscitiva *interna* all'amministrazione, utile per mettere a punto meccanismi di analisi e monitoraggio da impiegare a fini di prevenzione. L'effettiva disponibilità di questa capacità conoscitiva è presupposta da molti degli istituti che caratterizzano il sistema di prevenzione della corruzione. Si pensi alla funzione di indirizzo esercitata dall'Autorità nazionale anticorruzione mediante la predisposizione e l'aggiornamento del PNA. È del tutto evidente che questa funzione – con la quale, tra l'altro, si forniscono alle amministrazioni indicazioni su come predisporre i piani di prevenzione e su come gestire i diversi istituti connessi – può essere esercitata in modo efficace solo se si dispone di una adeguata, aggiornata, sistematica conoscenza delle dinamiche che caratterizzano *effettivamente* il fenomeno che si intende regolamentare (a fini preventivi), la distribuzione territoriale dei rischi, le correlazioni con dati/elementi che può fornire indicazioni in questo senso. Ancora, si pensi alla necessità che il piano triennale di prevenzione, che ogni amministrazione è tenuta a formulare ed aggiornare, tenga conto delle effettive caratteristiche in cui quella amministrazione si trova a operare, in relazione alle funzioni esercitate. Nel piano, tale funzione è assolta (in particolare) in sede di ricostruzione del c.d. *contesto esterno*, che si caratterizza proprio perché rappresenta il compendio informativo, formulato e tarato sulle specifiche esigenze dell'amministrazione, sulla base del quale sono raccolte ed evidenziate tutta una serie di informazioni ed elementi che poi incidono nella predisposizione, articolazione ed organizzazione degli istituti di prevenzione. Rispetto alle critiche spesso formulate in dottrina circa l'eccessivo formalismo degli istituti di prevenzione "calati dall'alto", proprio l'esercizio della funzione conoscitiva che dovrebbe accompagnare la predisposizione del piano costituisce il primo e principale elemento utile – invece – a rendere il piano adatto (e rispondente) alle esigenze di quella specifica amministrazione. Sotto questo profilo, il governo dell'anticorruzione fornisce un ottimo esempio di come la *trasparenza verticale* rappresenti un compendio utile, spesso necessario, per l'esercizio *effi-*

cace ed *effettivo* delle funzioni pubbliche[6]. *Trasparenza verticale* da intendersi, in questo senso, come la capacità di *conoscenza e comprensione* che matura all'interno dell'amministrazione, mediante l'elaborazione di informazioni che tendenzialmente sono già nella disponibilità dell'amministrazione stessa (o che sono disponibili nell'ambito del sistema pubblico, complessivamente inteso), e da cui possono emergere indicazioni preziose. L'uso del termine "*verticale*" sta ad indicare anche che il processo, la dinamica conoscitiva si sviluppa su più livelli ed ambiti del sistema amministrativo: sia perché le informazioni elaborate (o *elaborande*) sono tratte da livelli differenti, sia perché i risultati della elaborazione possono contribuire all'esercizio di una funzione che vede coinvolti plurimi livelli di governo. Si pensi (appunto) al caso dell'anticorruzione, la cui funzione conoscitiva riverbera sia sulle funzioni di indirizzo che su quelle di progettazione e gestione dell'anticorruzione a livello locale; oppure, si pensi alle funzioni di controllo della spesa pubblica, o alle funzioni di coordinamento, nel dispiegamento di politiche pubbliche che coinvolgano diversi livelli di governo. In tutti questi casi, la disponibilità di informazioni (provenienti da fonti informative differenti, e differentemente collocate in termini di raccolta, titolarità, accesso) è un prerequisito essenziale per consentire alle stesse amministrazioni coinvolte di poterle elaborare, sia per conoscere e comprendere meglio il contesto in cui sono chiamate ad operare, sia per conoscere e comprendere come effettivamente queste istituzioni operano nell'esercizio dei rispetti compiti.

Con specifico riferimento all'esercizio delle funzioni di indirizzo, programmazione e gestione a fini di prevenzione della corruzione, utilizziamo l'esempio fornito dal Progetto PON "*Misurazione del rischio di corruzione a livello territoriale e promozione della trasparenza*" come caso di studio per analizzare l'impatto del regime di trattamento dei dati personali a fini di esercizio di funzioni pubbliche, secondo le declinazioni del *dual legality standard*, così come sperimentate nell'ordinamento nazionale.

Come si legge nello studio preliminare del progetto:

> Un aspetto di fondamentale importanza per la corretta implementazione del sistema di indicatori proposti riguarda la disponibilità di dati di base dettagliati ed affidabili. A questo riguardo è utile distinguere 3 tipologie di banche dati sulle quali la costruzione degli indici può essere basata. Una prima tipologia riguarda *le banche dati ANAC già*

[6] Sotto questo profilo, l'integrazione dei cicli operativi finalizzati alla prevenzione della corruzione, alla misurazione della performance, alla efficiente allocazione delle risorse organizzative, realizzata mediante l'introduzione del *Piano Integrato di Attività e Organizzazione*-PIAO, ad opera dell'art. 6 del decreto legge n. 80 del 9 giugno 2021, ha contribuito ad esaltare il ruolo svolto dalle attività conoscitive preliminari che le amministrazioni attuano in vista della predisposizione, aggiornamento e verifica delle funzioni di programmazione.

esistenti e immediatamente disponibili. Tra questi ci si intende riferire, ad esempio, alla banca dati interna dell'ANAC (BDNCP) ed alle banche dati costituite presso le singole stazioni appaltanti, e gestite dai singoli Responsabili di Prevenzione alla Corruzione (RPC). Una seconda tipologia di dati si riferisce, invece, a *banche dati esterne all'ANAC, ma facilmente acquisibili grazie alla collaborazione manifestata nel corso dei tavoli del gruppo di lavoro* da enti quali l'ISTAT, la Banca d'Italia, la Corte dei Conti, Ministero dell'Interno, Ministero della Giustizia, la Presidenza del Consiglio dei Ministri, e al contributo di vari enti pubblici non economici, agenzie, regioni, comuni, Aziende sanitarie locali, Aziende ospedaliere, IRCCS, Università, Camere di commercio industria artigianato e agricoltura e Unioni regionali. Nel considerare questa seconda tipologia di dati non vanno certamente sottostimati i problemi che si presenteranno in fase di costruzione del data-base, dovuti alla integrazione delle varie fonti. Tra questi vanno ricordati i problemi derivanti dalla diversa affidabilità delle fonti, i problemi di dati mancanti, i problemi derivanti dalla non perfetta comparabilità del dato, i problemi connessi alla diversa definizione delle unità (ad esempio territoriali), i problemi derivanti dal diverso supporto informatico o linguaggio di programmazione utilizzato ed i problemi di *coupling* tra unità elementari derivanti da errori ed imprecisioni nella fase di immissione dei dati (…)

Già in fase di progettazione, erano chiare le difficoltà che sarebbero potute emergere in relazione alla integrabilità di banche dati in titolarità di amministrazioni diverse tra loro. Il progetto aveva, però, chiaro fin dal principio che la *trasparenza verticale* richiede la disponibilità (all'uso) di informazioni che difficilmente si ritrovano concentrate/allocate presso un'unica amministrazione, e che pertanto un requisito indispensabile per poter ottenere quel tipo di conoscenza necessaria per completare e rendere operativamente efficace il sistema della prevenzione della corruzione è costituito dalla messa in comune o, se si vuole, della circolazione delle informazioni all'interno del sistema pubblico complessivamente inteso. Senza questo prerequisito, infatti, viene sostanzialmente meno un presupposto che – sebbene non sufficiente – è evidentemente necessario per poter estrarre dal patrimonio informativo quella conoscenza *utile*, nel senso già indicato poco sopra, perché funzionalmente connessa (a diversi livelli) con il concreto esercizio della *mission* di prevenzione della corruzione.

Accanto a questo compito di carattere generale e trasversale, il progetto si era dato *secondo obiettivo* – che in effetti può essere riguardato anche come caso di studio particolare rispetto all'osservazione generale relativa alle esigenze conoscitive/trasparenza verticale – quello di *verificare presupposti e condizioni per lo sviluppo di un indicatore finalizzato alla rilevazione/verifica del conflitto d'interessi*, nonché fornire supporto per il test di alcune soluzioni concrete di sviluppo dell'indicatore.

Una caratteristica specifica di questa seconda linea progettuale era (come vedremo) che il suo sviluppo avrebbe richiesto necessariamente il trattamento di dati personali. Per questa ragione esso costituisce un caso di studio ideale per verificare come il regime giuridico a tutela dei dati personali impatti sulle condizioni di praticabilità effettiva di soluzioni di trasparenza verticale basate sulla condivisione e sull'uso dei dati.

1.2. Gli ostacoli alla condivisione dei dati del patrimonio informativo pubblico

L'esigenza di mettere a sistema i dati in titolarità (o nella stabile disponibilità) di diverse amministrazioni ha trovato una risposta sul piano procedurale tramite la sottoscrizione di un protocollo d'intesa tra ANAC e numerose amministrazioni centrali, protocollo stipulato proprio allo scopo di creare una cornice istituzionale utile a promuovere e legittimare il processo di individuazione delle fonti informative da utilizzare (anche in combinazione tra loro, e con quelle già nella disponibilità di ANAC) per elaborare gli strumenti di *trasparenza verticale*, nelle loro diverse accezioni e declinazioni, ma comunque utili alle finalità della prevenzione della corruzione.

Tuttavia, nonostante le risorse organizzative dedicate proprio al confronto con le amministrazioni coinvolte, per la concreta condivisione di informazioni, sostanzialmente in nessun caso la firma del protocollo d'intesa si è poi tradotta in una conseguente acquisizione/messa in comune di basi di dati da mettere a servizio della elaborazione di indicatori di prevenzione della corruzione. I fattori che hanno cospirato verso questo esito sono molteplici: qui ci concentreremo in particolare sulle dinamiche effettivamente osservabili – che in effetti hanno rappresentato un caso davvero interessante di *law in action*.

1.2.1. Il dato di partenza: organizzazione dell'informazione e pluralismo organizzativo

Non è certamente questa la sede per inquadrare *funditus* il tema della proprietà/appartenenza dei dati, con riferimento al sistema degli enti pubblici[7].

[7] Cfr. Marongiu D. (2008), "I dati delle pubbliche amministrazioni come patrimonio economico nella società dell'informazione", in *Informatica e diritto*, 1-2, 355-368; Ponti B. (2008), *Titolarità e riutilizzo dei dati pubblici*, in (eds.) Id., *Il regime dei dati pubblici*, Rimini,

Tuttavia, per poter procedere è utile inquadrare gli elementi essenziali che caratterizzano il *dato di partenza*, quello per il quale i dati pubblici non risultano in titolarità del sistema pubblico unitariamente considerato, ma piuttosto a ciascuna singola amministrazione/ente pubblico. Un dato di fatto (e di diritto, come vedremo tra poco) che costituisce la premessa che spiega, poi, la necessità di individuare e praticare meccanismi idonei a consentire che i dati *di qualcuno* siano messi in comune o nella disponibilità *di qualcun altro*, al fine di essere utilizzabili (e concretamente utilizzati). I dati sono evidentemente nella disponibilità dell'amministrazione che li raccoglie, li acquisisce, ovvero che li forma, in quanto necessari ai fini dell'esercizio delle proprie funzioni[8]. Questo insieme di dati, raccolti/acquisiti/formati, viene poi conservato, in modo organizzato, per consentirne la reperibilità e l'utilizzo ai fini della medesima o correlata funzione. I dati sono quindi conservati, gestiti e resi disponibili secondo una specifica strutturazione, e vanno così a comporre un insieme organizzato secondo criteri predefiniti, la *banca dati*. Per effetto di questo dato di fatto (giuridicamente qualificato dalla strumentalità della effettiva disponibilità del dato all'esercizio della funzione), si determina quella relazione di appartenenza che viene declinata dal diritto positivo in termini *titolarità*, che riguarda quindi piuttosto le banche dati (che danno organizzazione e forma alle informazioni elementari raccolte e conservate). Al di là dei profili dominicali della relazione di appartenenza – che pure esistono e trovano riscontro, ad esempio, nella disciplina giuridica che tutela la proprietà intellettuale sulle banche dati, ma anche altri diritti (i cd. diritti connessi, di cui alla direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati, che prescindono dal profilo dell'originalità/innovatività della banca dati) – va subito sottolineato che la titolarità di (banche) dati in capo a soggetti pubblici porta con sé una serie di *doveri*, connessi tanto alla garanzia della qualità ed integrità dei dati "posseduti"[9], tanto alla tutela dei dati personali ivi contenuti, tanto con riferimento alle esigenze di accesso qualificato di altre amministrazioni[10]. Le amministrazioni, in altre parole – ed al di là della eventuale disciplina legislativa specifica dettata con riferimento ad una

213-252; Rovati A. M. (2011), "Prime note su proprietà intellettuale e riutilizzo dei dati pubblici", in *Informatica e diritto*, 1-2, 153-184; Sappa C. (2011), "Diritti di proprietà intellettuale e dati pubblici nell'ordinamento italiano", in *Informatica e diritto*, 1-2, 185-197;

[8] Per tutti, cfr. Guerra M. P. (1996), *Funzione conoscitiva e pubblici poteri*, Milano e Levi F. (1967), *L'attività conoscitiva della pubblica amministrazione*, Torino.

[9] Cfr. Carloni E. (2009), "La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata", in R*ivista trimestrale di diritto pubblico*, 1, 155-186.

[10] Cfr. Ponti B. (2008), *Titolarità e riutilizzo dei dati pubblici*, cit.; nonché Guerra M. P. (2005), "Circolazione dell'informazione e sistema informativo pubblico: profili giuridici dell'accesso interamministrativo telematico. Tra Testo Unico sulla documentazione amministrativa e codice dell'amministrazione digitale", in *Dir. pubbl.*, 525 ss.

specifica tipologia/classe, o singola banca dati – in quanto titolari di banche dati sono destinatarie di una serie di doveri che disciplinano e (quindi) limitano la effettiva disponibilità del bene in questione (la banca dati) e dei suoi contenuti (le informazioni ivi raccolte), anche con riferimento all'effettivo potere di disposizione su tale bene. Per altro, va anche considerato che le informazioni costituiscono un bene immateriale, e come tale si configurano *naturaliter* come bene non rivale, talché (a differenza di quanto accade ai beni materiali) il loro uso da parte di qualcuno non consuma né deteriora il bene stesso, che risulta in effetti illimitatamente replicabile. Infine, occorre considerare che la categoria dei beni immateriali non è contemplata tra quelle cui fa riferimento la disciplina codicistica relativa al regime giuridico dei beni di appartenenza di amministrazioni pubbliche (artt. 810 e ss.), così che appare del tutto problematica la riconducibilità del regime dei beni pubblici a tali classi di beni (si veda, in questo senso, la relazione della Commissione Rodotà per la modifica delle norme del codice civile in materia di beni pubblici, che raccomandava invece l'esplicito riferimento alla categoria dei beni immateriali, così da ricomprendere nel novero dei beni assoggettati al regime dei beni pubblici anche "le informazioni pubbliche"[11]). Con la conseguenza che il sistema di doveri ed obblighi che accompagnano la titolarità delle banche dati, si esercita su beni che sono comunemente inquadrati (salva specifica e differente disposizione legislativa) come afferenti al patrimonio *disponibile*.

Sulla base di queste coordinate, possiamo inquadrare un primo profilo – potremmo dire preliminare – relativo a come le informazioni si distribuiscono all'interno del sistema pubblico, sotto il profilo giuridico: le informazioni raccolte, gestite ed archiviate sono costituite in banche dati di titolarità di una specifica amministrazione, così che le banche dati "appartengono" alle singole amministrazioni, secondo una geografia della titolarità di tali beni che è modellata sull'assetto pluralistico del sistema organizzativo pubblico. A conferma di questo assetto pluralistico, si notino gli sforzi prodotti dal legislatore nazionale per ottenere l'effetto di rendere allineati/unitari e disponibili alcuni corpi informativi che sono effettivamente gestiti in modo distribuito (pluralismo), nell'esercizio della funzione di coordinamento dei dati di cui all'art. 117 Cost., secondo comma, lett. r)[12]. Si veda, in particolare,

[11] Cfr. relazione finale Commissione Rodotà - per la modifica delle norme del Codice civile in materia di beni pubblici: https://shorturl.at/boKT6 (4 maggio 2023).

[12] Sulla funzione di coordinamento, in quanto funzionale all'integrazione dei patrimoni informativi delle amministrazioni pubbliche, sia consentito rinviare a Ponti B. (2008), *I dati di fonte pubblica: coordinamento, qualità e riutilizzo*, in (eds.) Merloni F., *La trasparenza amministrativa*, Milano, 405-442, nonché a Lazzaro F. (2011), "Coordinamento informativo e pubbliche amministrazioni", in *Istituzioni del federalismo*, 3, 659-681.

la nozione di "Base di dati di interesse nazionale", di cui all'art. 60 e seguenti del CAD. Tali linee di intervento legislativo presuppongono un quadro che necessita di essere "tenuto insieme", proprio in ragione dell'assetto pluralistico e di come questo si proietta su titolarità e gestione delle banche dati (pubbliche).

Su questo dato preliminare, tuttavia, sono andati costruendosi abitudini ed attitudini delle amministrazioni pubbliche, che hanno trovato riscontro nelle dinamiche di sviluppo del caso di studio che stiamo analizzando e che potremmo articolare – per comodità espositiva – in quattro punti distinti (sebbene vi siano tra loro molte correlazioni ed interferenze reciproche): l'*atteggiamento proprietario*; i *silos informativi*; il *sistema degli incentivi*; la *qualità dei dati*. A questi si aggiunge un fattore ulteriore, che possiamo individuate nelle ricadute della disciplina a tutela dei dati personali, che – per le ragioni che chiariremo meglio in seguito – rappresenta *sia una causa remota* che *un fattore recente* che incide in modo significativo sulla condivisione dei dati *tra amministrazioni*.

1.2.2. I "silos" informativi

Con questa metafora (quella dei *silos*) si fa riferimento ad una modalità di raccolta, gestione ed archiviazione dei dati che viene realizzata dall'amministrazione con riferimento alle proprie esigenze conoscitive e funzionali, senza che nell'operazione di definizione delle caratteristiche della banca dati (modalità di raccolta del dato, elementi informativi raccolti, individuazione dei metadati, formati di codifica, etc.) si tenga conto delle esigenze di scambio/circolazione delle informazioni anche a beneficio di altre amministrazioni, e di sistemi differenti. In presenza di un sistema caratterizzato in termini pluralistici (vedi sopra) ed in assenza di una forte/effettiva funzione di coordinamento informativo, tale assetto è aperto ad esiti di dispersione/frammentazione informativa, nella misura in cui i sistemi informativi delle singole amministrazioni vengono a costruirsi (come è ovvio che sia) in modo tale da rispondere alle esigenze specifiche di quella amministrazione, sviluppando linguaggi non standardizzati, metodologie e formati di codifica differenziati, semantiche non omogenee, etc. In questo modo, i sistemi informativi finiscono (*effettivamente*) per essere strutturati in modo tale da rendere tecnicamente complessa se non proibitiva la condivisione di dati, informazioni e/o processi con gli altri sistemi informativi. Di qui l'immagine del silos, un sistema di immagazzinamento che eroga in verticale (a favore dell'amministrazione di appartenenza, fuor di metafora), ma che non è in grado

di trasferire/condividere il contenuto con altri silos (altri sistemi informativi), in orizzontale.

Circa l'attualità di questo tema, sia sufficiente ricordare che "superare l'approccio a 'silos' storicamente adottato dalla Pubblica amministrazione e per favorire la realizzazione di un vero e proprio sistema informativo della Pubblica amministrazione" costituiva uno degli obiettivi strategici ancora nel Piano triennale dell'informatica nella pubblica amministrazione per il triennio 2017-2019[13], a significare che la organizzazione dell'informazione con effetto *silos* costituisce tutt'ora la realtà effettiva in larghissima parte del sistema informativo pubblico, ed un problema aperto[14].

Sul fronte del caso di studio che stiamo analizzando, il tema della incomunicabilità "tecnica" tra sistemi informativi è emerso più volte, nell'interlocuzione tra le amministrazioni partner del protocollo di intesa, quando è stato analizzato il tema del formato dei dati da mettere a disposizione del progetto. Detto in altri termini, si è avuta la possibilità di verificare "con mano" ed in "presa diretta" le conseguenze dei ritardi accumulati dalla funzione di indirizzo e coordinamento nel settore dell'informatica pubblica. Banalmente: la decisione se raccogliere e/o collegare una specifica informazione, nell'alimentare una banca dati, può rivelarsi una scelta decisiva, nel caso in cui quell'informazione (si pensi al codice fiscale o alla partita iva, per fare un esempio) finisca per costituire il punto di aggancio per collegare tra loro elementi informativi diversi/disparati.

[13] Cfr. Piano triennale per l'informatica nella pubblica amministrazione 2017-19, in part. il cap. 2 "Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione": https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2017-2019/doc/02_modello-strategico-di-evoluzione-dell-ict-della-pa.html (15.5.2023).

[14] In questo senso, un passo decisivo è stato compiuto con il superamento della logica di condivisione del patrimonio informativo fondato sul previo accordo tra le amministrazioni coinvolte (secondo il modello impostato nel testo originario 58 del CAD), mediante l'adozione di una logica differente, fondata sulla abilitazione di una infastruttura di sistema finalizzata ad abilitare l'interoperabilità dei sistemi informativi. Tale infrastruttura – la Piattaforma Digitale Nazionale Dati (PDND) di cui all'art. 50-ter del CAD – si fonda sulla standardizzazione delle interfacce di programmazione delle applicazioni (API), è gestita in modo centralizzato (presso la Presidenza del Consiglio dei ministri) ed opera come strumento di coordinamento informativo ed informativo ai sensi dell'art. 117, secondo comma, lett. r) Cost. Tuttavia, questo diverso approccio alla condivisione dei dati è per il momento solo *disegnato*: la sua concreta attuazione è, ad esempio, oggetto di specifiche misure del PNRR (cfr. la Missione Digitalizzazione, innovazione e sicurezza nella PA" (M1C1), nonché la linea d'investimento Investimento 1.3: "Dati e interoperabilità") ed è anche alla base del processo di completa digitalizzazione del ciclo di vita dei contratti pubblici che costituisce l'infrastruttura operativa (ancora da completare, sul piano operativo) del nuovo Codice dei contratti, approvato con d.lgs. 36 del 2023.

Allo stesso modo, le modalità di codifica dell'informazione rappresentano un prerequisito per rendere possibile il transito e l'utilizzo di una informazione da un sistema informativo all'altro. Si è così avuto modo di constatare come – con specifico riferimento a plurime banche oggetto di indagine e confronto – alcune analisi sarebbero risultate di difficile (e, quindi, dispendiosa) fattibilità, proprio in ragione della mancanza di "anelli di congiunzione", ovvero in ragione di specifiche tecniche quanto ai *formati* differenziate e non interoperabili. Il problema dei "silos" ha numerose ricadute. Per un verso, esso rende più onerosa e dispendiosa l'operazione di condivisione delle informazioni (dal momento che impone – per la sua realizzazione – un intervento di adeguamento di una delle basi di dati in questione). Dall'altro, costituisce anche un vincolo, una coazione a "perpetuare" nella medesima logica. Le difficoltà determinate da una infrastruttura conoscitiva composta di tanti "silos" finiscono infatti per rappresentare un incentivo a fare conto solo sulle proprie/rispettive risorse informative, attivando un circolo vizioso.

1.2.3. L'atteggiamento proprietario

Si è già fatto cenno al peculiare *mix* che caratterizza il regime giuridico che definisce la relazione di "appartenenza" delle banche dati alle amministrazioni titolari. Si è anche potuto constatare come tale regime giuridico – che pure prevede una serie di qualificanti doveri in capo ai titolari dei corpi informativi, ivi compresi doveri specifici di accesso/condivisione dei dati – mantiene una impronta *dominicale* di fondo, che su di un piano più ancora culturale che strettamente giuridico, si ripercuote nell'atteggiamento, nella postura dei titolari, quando si tratta di gestire tale bene. Di conseguenza, nella misura in cui le informazioni sono considerate un *asset*, l'ottica in cui si pone il titolare è più spesso quella dello "sfruttamento" (nel senso della messa a valore) piuttosto che non quella della condivisione.

Come noto, questa postura ha trovato a lungo (e trova ancora, in qualificati casi) riscontro nella prassi di cessione dei dati al mercato contro un prezzo, ossia nella commercializzazione del patrimonio informativo. Una pratica che è stata progressivamente erosa, prima dalla disciplina europea sul riutilizzo dell'informazione del settore pubblico, quindi dall'affermarsi delle politiche di apertura dei dati pubblici (open data), approcci regolatori che hanno finito per convergere nella direttiva 2019/1024 "*on open data and the re-use of public sector information*", così che attualmente gli spazi di commercializzazione dei dati pubblici sono (almeno sotto il profilo giuridico) residuali ed in via di progressivo esaurimento. Sul piano delle relazioni in-

terne al sistema pubblico – invece – l'atteggiamento proprietario ha mantenuto una presa rilevante: l'idea di mettere a "profitto" gli assetti informativi si traduce – su questo fronte – nel prevalere di logiche di scambio. Alla stregua di questo atteggiamento, la cessione/condivisione del patrimonio informativo avviene solo nella misura in cui la controparte ha qualcosa da cedere "in cambio". Si noti – per altro – che un atteggiamento di questo genere ha alcune evidenti giustificazioni, laddove l'amministrazione si trova a dover far fronte a significativi investimenti per mantenere e sviluppare l'infrastruttura informativa e relative applicazioni, in un contesto recente caratterizzato – da una parte – da una generalizzata contrazione della spesa per investimenti e – dall'altra – dalla sostanziale elisione del canale di ammortamento connesso alla commercializzazione del patrimonio informativo (in conseguenza della logica *open data*). Non deve sorprendere – in altri termini – che amministrazioni costrette a far fronte a significativi investimenti in condizioni di stringenti vincoli di bilancio e a risorse calanti (basti qui richiamare la stagione delle riforme "costo zero"), non vedano di buon occhio la condivisione gratuita di patrimoni così faticosamente conservati e sviluppati. Si tratta di elementi su cui occorre riflettere, anche in prospettiva, se si vuole effettivamente uscire dalle secche di questa logica.

Il caso di studio ha fornito testimonianze notevoli di questo atteggiamento, e delle dinamiche che lo hanno alimentano, con ricadute che si collocano su uno spettro ampio di situazioni concrete. Da una parte, infatti, ci sono quelle amministrazioni che gli investimenti (finanziari, organizzativi, procedurali) li hanno fatti, e che in fondo sono restie a condividere in termini "altruistici" il *dividendo* di questo lavoro; ma, dall'altra, vi sono anche amministrazioni che non investono da molti anni, e in cui la ritrosia a condividere è dettata anche dalla consapevolezza della grave insufficienza/deficienza dell'infrastruttura informativa e dei servizi connessi. Il caso di studio rappresenta quindi un osservatorio particolarmente interessate per osservare gli effetti combinati di vincoli di bilancio/contrazione spese per investimento, calati all'interno di un contesto già scarsamente predisposto ad operare in ottica cooperativa e di sistema.

1.2.4. Il sistema degli incentivi

Sostanzialmente omogeneo alla motivazione illustrata nel paragrafo che precede, un distinto ordine di ragioni che spiega la difficoltà a interagire in modo collaborativo/cooperativo nella condivisione del patrimonio informativo, può essere individuato nell'assetto degli incentivi connessi alla scelta

se operare in modo cooperativo o, piuttosto, competitivo. Infatti, occorre tenere presente che la condivisione/messa a disposizione dei dati ad altra amministrazione (sebbene motivata da accordi formali e da obiettivi comuni) comporta che l'attività di uso dei dati ed i relativi risultati finiscono per essere evidenziati in capo all'amministrazione capofila, con la conseguenza che i servizi che operano nell'amministrazione "cedente" possono percepire tale *outcome* come un disconoscimento del proprio ruolo. Inoltre, anche gli incentivi di carriera possono giocare un ruolo importante, in questo senso: un progetto realizzato in autonomia – e di cui i dirigenti responsabili possono accreditare la responsabilità esclusiva – comporta una visibilità certamente maggiore da quella derivante dalla partecipazione ad un progetto più ampio, con diverso capofila. Anche in questo caso, quindi, le motivazioni a supporto di questo tipo di strategia non mancano. Possono così innescarsi dinamiche competitive che si sovrappongono a quelle collaborative, depotenziando queste ultime.

Il caso di studio consente di osservare bene questa dinamica. In effetti, almeno uno tra gli importanti partner del protocollo d'intesa – protocollo volto a dare base giuridica e istituzionale alla collaborazione e alla condivisione/messa in comune dei dati a beneficio degli obiettivi del progetto – ha promosso in modo autonomo attività di ricerca e sviluppo che avevano per oggetto i medesimi set di dati che avrebbero dovuto essere condivisi per lo sviluppo del progetto e, per finalità, proprio quella di sviluppare e testare un indicatore di rischio di corruzione nel settore degli appalti pubblici, iniziativa che in termini formali è stata svolta e presentata all'esterno come del tutto svincolata dal protocollo d'intesa (quasi come se il progetto e l'annesso protocollo d'intesa non esistessero). Dunque, un esempio di *competizione* in luogo della *collaborazione*, che contribuisce a testimoniare delle difficoltà che si incontrano nel promuovere e realizzare progetti, servizi e strumenti fondati sulla collaborazione e la condivisione del patrimonio informativo.

1.2.5. La qualità dei dati

Un ultimo fattore che si intende illustrare è quello connesso alla (molto) variabile qualità dei dati dislocati nei diversi corpi informativi che, nel caso di studio analizzato, si volevano mettere a fattor comune. Nel caso illustrato nel paragrafo precedente, l'attivazione della dinamica competitiva era anche supportata dalla consapevolezza del partner relativamente alla buona qualità del data set in questione e del valore aggiunto che questa qualità portava con sé in termini di potenzialità conoscitive da sfruttare. Ma la qualità del dato, se invece che percepita come buona è invece considerata carente o scarsa,

può attivare motivazioni che – sebbene differenti – conducono al medesimo risultato, ossia l'avversione alla effettiva condivisione (dei dati). Infatti, un'amministrazione consapevole di disporre di basi di dati di scarsa qualità, poco affidabili, o anche deficitarie sotto il profilo delle modalità di raccolta (e quindi difettose in termini di congruità, consistenza ed esattezza), avrà una scarsissima se non nulla propensione a procedere effettivamente ad una condivisione di quei dati, perché (comprensibilmente) preoccupata dai probabili contraccolpi (in termini reputazionali e di responsabilità giuridica). Nella logica dei silos, un *data base* di scarsa qualità può essere gestito come un problema *interno* ("lavare i panni sporchi in casa", secondo un noto adagio); al contrario, la messa in comune rappresenta un'occasione di socializzazione dei ritardi e delle inadeguatezze che caratterizzano quel *data set* e chi ne è titolare, che determina la potenziale *rottura* dei meccanismi di gestione interna del problema, e una emersione di esso all'attenzione generale (effetto di trasparenza). Il caso di studio dà modo di osservare anche questo tipo di dinamiche.

1.2.6. La distribuzione / deconcentrazione del patrimonio informativo come meccanismo strutturale di garanzia delle libertà e dei dati personali

L'ultimo fattore da analizzare (non certo per ordine di importanza, e non solo in considerazione dell'oggetto della nostra indagine) è quello connesso alla tutela dei dati personali. Nel corso di questo studio abbiamo già avuto modo di riflettere sui presupposti normativi e sui requisiti di legittimazione che devono sorreggere il ricorso a trattamenti di dati personali detenuti dalla pubblica amministrazione, applicabili anche alle operazioni finalizzate alla elaborazione di indicatori e strumenti utili per la prevenzione della corruzione (quando sia rilevante il trattamento di dati personali). Ciò che il caso di studio consente di osservare è che le esigenze di tutela dei dati personali – oggi così centrali e impattanti rispetto alla modalità di acquisizione e trattamento – sono anche uno dei fattori che hanno contribuito a determinare – *storicamente* – l'architettura distribuita e deconcentrata dei *data set*, all'interno del sistema pubblico complessivamente considerato. Infatti, già agli albori dei processi di informatizzazione è maturata la consapevolezza che la concentrazione di informazioni disponibili a un medesimo soggetto abilitasse (sia in termini attuali, allora, sia in termini di potenzialità ancora inespresse) un *potere conoscitivo* idoneo a incidere in modo significativo sulle

libertà e sui diritti dei cittadini, con rilevantissimi rischi di loro limitazione, condizionamento, manipolazione, negazione[15].

Dunque, già negli anni '70 del secolo scorso veniva posta all'ordine del giorno la necessità di provvedere affinché fosse impedito allo Stato (al sistema pubblico considerato nel suo insieme) di realizzare una concentrazione dei dati personali raccolti e trattati per l'esercizio delle funzioni amministrative, mediante una illimitata integrazione delle basi di dati ovvero una loro illimitata/non presidiata circolazione, proprio a protezione e a garanzia della libertà dei consociati.

Sotto questo profilo, la *dispersione* del patrimonio informativo pubblico, e la sua "originaria" deconcentrazione, in ragione della distribuzione delle banche dati tra i diversi enti e amministrazioni pubbliche in ragione della competenza funzionale e territoriale, costituisce *di per sé* una prima forma di garanzia avverso i rischi connessi ad una ipotetica immediata disponibilità di un insieme vasto, eterogeneo, ma organizzato e concentrato, di dati personali; così che il sistema di tutela dei dati si muoverà nel senso di interdire tale concentrazione, come pure di presidiare l'eventuale circolazione, sulla base del *principio di finalità* (del trattamento). Si noti, dunque, che fin dal principio, i meccanismi approntati a tutela delle libertà e dei dati personali ha guardato con favore alla separazione tra le banche dati pubbliche, tollerando/ammettendo invece la circolazione solo entro il quadro di legittimazione offerto dal principio di finalità (sorretto da quello di legalità). Sotto questo profilo, dunque, la tutela dei dati personali emerge da subito quale fattore che regolamenta in modo rilevante la possibilità di condivisione del patrimonio informativo pubblico, ponendosi come uno dei *formanti* che sottopone a condizioni di legittimità l'operazione di trasmissione/circolazione/condivisione della frazione di una banca dati rilevante ai fini della tutela dei dati personali.

Vale la pena sottolineare, per ora in via del tutto incidentale, che la condizione di pluralismo organizzativo, pluralismo delle banche dati, struttura deconcentrata nella distribuzione dei *data set* contenenti dati personali ha condotto ad una soluzione che ha privilegiato – con riferimento al settore pubblico e per le ragioni indicate qui sopra – meccanismi di controllo preventivo della concentrazione delle banche dati, disincentivando (o, piuttosto, escludendo radicalmente) la costituzione di sistemi accentrati di raccolta e gestione dei dati personali detenuti dal sistema pubblico.

La storia più recente si è incarica di dimostrare che – diversamente – con riferimento al settore privato, gli strumenti predisposti a tutela dei dati per-

[15] Cfr. *supra*, gli autori citati alla nota n. 1 del cap. 1.

sonali (e delle libertà personali), muovendosi all'interno di contesti organizzativi diversi, e in applicazione di principi differenziati di legittimazione alla raccolta e all'uso dei dati personali (il principio del consenso; il perseguimento del legittimo interesse del titolare del trattamento) non hanno impedito la costituzione di grandi (enormi) concentrazioni di dati personali (in termini di disponibilità), concentrando l'attenzione piuttosto sulla *regolamentazione dell'uso di tali dati*. Un elemento di asimmetria[16] tra contesto pubblico e contesto privato che – come vedremo in seguito – non è privo di ricadute, anche con riferimento alle modalità concrete di realizzazione di strumenti per la realizzazione della trasparenza verticale a fini di prevenzione della corruzione.

1.3. Il conflitto d'interessi come istituto di prevenzione della corruzione amministrativa, esigenze di trasparenza verticale e trattamento dei dati personali

1.3.1. I meccanismi di prevenzione basati sul rilievo del conflitto d'interessi

La disciplina del conflitto di interessi, per come introdotta/modificata/irrobustita dal complesso intervento normativo che fa capo alla legge 190/2012, costituisce uno dei principali strumenti di *prevenzione* dei fenomeni corruttivi, dal momento che – in ragione della sua strutturazione, della sua dinamica – esso mira ad *impedire* il concretizzarsi di situazioni tali da comportare il rischio di un pregiudizio per la cura dell'interesse pubblico, senza che acquisti diretto rilievo anche la circostanza che tale pregiudizio si verifichi in termini concreti[17]. Il che è perfettamente coerente con la finalità

[16] Sul punto, cfr. Falcone M. (2023), *Ripensare il potere conoscitivo pubblico. La conoscenza amministrativa con i big data e gli algoritmi*, cit., in part. Il cap. 1; ma sia anche consentito rinviare a Ponti B. (2021), *Informazione pubblica, trasparenza e potere conoscitivo: come proseguendo sui percorsi indicati da Francesco Merloni*, in Pioggia A., Carloni E., Ponti B. (eds.), *Studi in onore di Francesco Merloni*, Torino, 207-222.

[17] Sul conflitto d'interessi, cfr. Cantone R. e Merloni F. (2019), "Conflitti di interesse: una diversa prospettiva", in *Dir. pubbl.*, 886 ss.; Lubrano E. (2018), *Il conflitto di interessi nell'esercizio dell'attività amministrativa*, Torino; Presutti, L. (2018), "Il conflitto di interessi come causa di esclusione nel nuovo codice", in *Urbanistica e appalti*, 4, 548; Federico G. (2018), *Il conflitto di interessi nell'esercizio del potere amministrativo*, Torino; Iudica, G. (2016), *Il conflitto di interessi nel diritto amministrativo*, Torino; Lalli, A., Moreschini, A., Ricci, M. (2019), *L'ANAC e la disciplina dei conflitti di interessi*, Napoli; Id. (2019), *La prassi dell'Anac in materia di conflitto di interessi*, Napoli; Frego Luppi S. A. (2013), "L'obbligo di astensione nella disciplina del procedimento dopo la legge n. 190 del 2012", in *Dir. amm.*,

dell'istituto, che dovrebbe appunto prevenire, ossia "venire prima" (in termini logici, non solo cronologici) dell'evento dannoso/pregiudizievole che si intende scongiurare. Il nucleo del conflitto d'interessi – tipico delle relazioni di agenzia – consiste nella situazione in cui, nello svolgimento di un'attività, un individuo sia tenuto a realizzare (o collaborare alla realizzazione di) un c.d. *interesse primario* che pertiene ad altri (tipicamente, l'interesse pubblico cui è funzionalizzata l'attività oggettivamente rilevante a tali fini), interesse che può trovarsi *in contrasto* o in condizioni di *non compatibilità* con un interesse personale. In tale circostanza, l'agente potrebbe essere indotto a dare preferenza alla soddisfazione del proprio interesse particolare/personale, e così facendo potrebbe arrecare un pregiudizio alla cura/al perseguimento dell'interesse pubblico. La disciplina del conflitto d'interessi si atteggia tipicamente come meccanismo di prevenzione dal momento che opera per impedire che tale situazione (quella del conflitto d'interessi) possa determinarsi, mediante la *disqualification* (variamente declinata) dell'agente portatore dell'interesse personale in contrasto con quello pubblico. La *disqualification* costituisce la soluzione tipica per la risoluzione del conflitto d'interessi, e consiste nella misura (di diversa intensità, vedi subito *infra*) per cui l'agente viene rimosso dallo svolgimento dell'attività in questione.

Si consideri, a questo proposito, che gli istituti che danno corpo alla disciplina del conflitto d'interessi – così inquadrato – si configurano come altrettanti strumenti di rafforzamento della imparzialità soggettiva del funzionario/agente. È del tutto fisiologico (doveroso, anzi) che l'amministrazione – quando agisce – debba tenere conto degli interessi in gioco. Gli schemi normativi dell'organizzazione e dell'azione danno forma alle modalità fisiologiche (perché legittime) in cui avviene questa interazione. Pertanto (e in base a una schematizzazione utile a fini descrittivi) gli interessi presenti nella società, nel mercato, nella realtà concreta, possono incidere sull'esercizio della funzione o in conformità a tali schemi normativi, oppure in modo difforme. Gli istituti a tutela dell'imparzialità soggettiva, che la legislazione anticorruzione ha rafforzato o introdotto *ex novo*, rispondono alla logica del canone di imparzialità come meccanismo teso a *escludere* quegli interessi (che si pongano oggettivamente in contrasto con l'interesse pubblico) che *per le modalità attraverso le quali si manifestano*, sono suscettibili di incidere sull'esercizio della funzione amministrativa in modo ritenuto patologico. Tale patologia consiste, appunto, nella circostanza che nel medesimo soggetto (l'agente) convivano il dovere/ il compito di perseguire l'interesse

694 ss.; Contessa, C. (2017), "Circa la nozione in senso funzionale del conflitto d'interessi nel codice dei contratti", in *Urbanistica e appalti*, 6, 824; Berrettini, A. (2020); "Conflitto di interessi e contratti pubblici: un difficile equilibrio tra (in)certezza del diritto e tassatività delle situazioni conflittuali", in *Federalismi.it*, 7, 1-30.

pubblico, e l'essere portatore di un distinto interesse che si pone oggettivamente in contrasto con tale interesse pubblico. Tale circostanza è considerata *patologica* perché considerata un rischio per la tenuta dell'interesse pubblico, dal momento che l'interesse secondario di cui è portatore l'agente potrebbe far deviare il corso dell'azione amministrativa, piegandola al soddisfacimento dell'interesse personale (a discapito dell'interesse pubblico)[18].

[18] Va sottolineato che l'identificazione e la modulazione delle circostanze nelle quali il conflitto d'interessi acquista carattere *patologico* per l'ordinamento è rimessa al rilievo che tale condizione assume in termini di diritto positivo, e al trattamento che le viene riservato. Nella disciplina anticorruzione (legge 190/2012 e decreti legislativi attuativi), ad esempio, viene dato rilievo al conflitto d'interessi *potenziale*, che si verifica ogni qualvolta un interesse pubblico di cui sia portatore o "canale di trasmissione" (vedi subito *infra*) il funzionario pubblico risulti in potenziale contrasto con l'interesse pubblico primario, a prescindere da ogni altra considerazione circa la consistenza o la gravità di questo contrasto, o circa l'eventualità concreta che l'interesse in potenziale conflitto possa trovare soddisfazione senza pregiudicare la soddisfazione dell'interesse primario. Si tratta di una scelta di diritto positivo, che dipende cioè dalle modalità con le quali l'ordinamento seleziona le ipotesi in cui la condizione di conflitto d'interessi acquista un profilo *patologico*. Per avvedersene, è significativo osservare quanto accaduto di recente con riferimento alla declinazione della nozione di conflitto d'interessi nel settore dei contratti pubblici. Nel Codice appena "rimpiazzato" (d.lgs. 50/2016 e s.m.i.), la declinazione della nozione di conflitto d'interessi era formulata in termini particolarmente ampi: ("Si ha conflitto d'interesse quando il personale di una stazione appaltante o di un prestatore di servizi che, anche per conto della stazione appaltante, interviene nello svolgimento della procedura di aggiudicazione degli appalti e delle concessioni o può influenzarne, in qualsiasi modo, il risultato, ha, direttamente o indirettamente, un interesse finanziario, economico o altro interesse personale che può essere percepito come una minaccia alla sua imparzialità e indipendenza nel contesto della procedura di appalto o di concessione", art. 42, comma 2). Il conflitto si verificava quando l'interesse personale (economico, finanziario o di altro genere) dell'agente addetto alla procedura poteva essere percepito come una minaccia alla sua imparzialità ed indipendenza di giudizio. Inoltre, tale condizione – così declinata – acquistava rilievo *sempre*, *in ogni caso* ("le stazioni appaltanti prevedono misure adeguate per contrastare le frodi e la corruzione nonché per individuare, prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione degli appalti e delle concessioni, in modo da evitare qualsiasi distorsione della concorrenza e garantire la parità di trattamento di tutti gli operatori economici" (art. 42, comma 1). Il rilievo attribuito al conflitto d'interessi nel nuovo Codice dei contratti (d.lgs. 31 marzo 2023, n. 36) appare significativamente diverso; ciò perché nella sua declinazione positiva ha inciso (esplicitamente) il peso riservato al principio del *risultato*, così come declinato nell'art. 1. Il testo dell'art. 16 recita infatti: "si ha conflitto di interessi quando un soggetto che, a qualsiasi titolo, interviene con compiti funzionali nella procedura di aggiudicazione o nella fase di esecuzione degli appalti o delle concessioni e ne può influenzare, in qualsiasi modo, il risultato, gli esiti e la gestione, ha direttamente o indirettamente un interesse finanziario, economico o altro interesse personale che può essere percepito come una minaccia concreta ed effettiva alla sua imparzialità e indipendenza nel contesto della procedura di aggiudicazione o nella fase di esecuzione. (…) In coerenza con il principio della fiducia e per preservare la funzionalità dell'azione amministrativa, la percepita minaccia all'imparzialità e indipendenza deve essere provata da chi invoca il conflitto sulla base di presupposti specifici e documentati e deve riferirsi a interessi effettivi, la cui soddisfazione sia conseguibile solo subordinando un

Come detto, la *risoluzione* della patologia è configurata in termini di *disqualification*, ovvero la *rimozione* dell'agente dallo svolgimento dell'azione amministrativa. Tale rimozione può riguardare un singolo affare, quando il conflitto si presenta come episodico/contingente, e si declina quindi nei termini dell'*obbligo di astensione*, ovvero di *divieto di accesso a incarichi esterni*. Quanto invece il conflitto tra gli interessi si configura come stabile/strutturale, la prevenzione del conflitto d'interessi si traduce in istituti quali l'*incompatibilità* e (alcune ipotesi di) *inconferibilità*.

Come detto, gli istituti di prevenzione che fanno perno sul conflitto d'interessi si concentrano sul profilo della imparzialità soggettiva del funzionario (in termini di escludenti), perché è sul funzionario che si scaricano gli interessi in conflitto, ed è il funzionario stesso che può costituire il "canale di ingresso" degli interessi devianti (perché in contrasto con quello pubblico).

Facciamo un esempio che può aiutare a inquadrare nel concreto una situazione di conflitto d'interessi. Prendiamo quindi in considerazione alcuni funzionari che, per incarico ricoperto/attività svolta, sono chiamati a perseguire un interesse pubblico *primario* che possiamo declinare (in termini generali) "tutela della salute" e, più in particolare "appropriata prescrizione dei farmaci e dei dispositivi medici".

Prendiamo poi in considerazione una serie di interessi, soggettivamente configurati, che si pongono in potenziale contrasto con l'interesse pubblico primario. Le aziende produttrici di farmaci e/o di dispositivi medici sono fisiologicamente interessate alla massimizzazione del profitto, anche mediante la massimizzazione delle vendite, ciò che pone il loro interesse in potenziale conflitto con l'interesse (pubblico) ad un approvvigionamento *appropriato* di farmaci e dispositivi medici. La clinica convenzionata può essere interessata a erogare il massimo possibile di prestazioni, e anche in questo caso tale interesse si pone in contrasto con quello pubblico (approvvigionamento appropriato). Discorso analogo può essere fatto per il medico del servizio sanitario che esercita in *intramoenia*, nella misura in cui l'interesse a effettuare

interesse all'altro". Come si vede, in primo luogo, la minaccia all'imparzialità del funzionario che rende *patologica* la condizione di conflitto d'interessi è solo quella sia apprezzabile come "concreta ed effettiva", e pertanto deve essere provata da chi la invoca "sulla base di presupposti specifici e documentati". Inoltre, l'interesse particolare che minaccia quello primario (perché in contrasto con esso) deve essere un interesse effettivo e la cui soddisfazione implichi la subordinazione dell'interesse primario. Si nota, dunque, un restringimento delle condizioni di rilievo del conflitto d'interessi, che acquista carattere patologico in un insieme di circostanze più limitato rispetto alla declinazione precedente. Ciononostante, permane in capo alla stazione appaltante il dovere adottano misure adeguate a individuare, prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione ed esecuzione degli appalti" (art. 16, comma 3).

visite durante l'esercizio dell'intramoenia può risultare in contrasto con l'interesse dell'azienda ad utilizzare in modo pieno le energie e le risorse professionali del medico quale dipendente del servizio sanitario.

Prendiamo uno di questi interessi *potenzialmente* in contrasto con l'interesse pubblico, e formuliamo una serie di ipotesi di situazioni di conflitto d'interessi, con riferimento a uno specifico funzionario/incarico, ad esempio: il dirigente dell'assessorato regionale alla salute che si occupa della fornitura di farmaci.

Ipotesi 1. Il dirigente regionale è fratello dell'amministratore delegato di una azienda del settore farmaceutico coinvolta nella procedura negoziale per l'attivazione di un progetto di partenariato pubblico-privato (ppp) per la progettazione, realizzazione e gestione di una piattaforma per l'acquisto dinamico dei farmaci. Istituto: astensione del dirigente dalla procedura.

Ipotesi 2. La moglie del dirigente regionale è titolare di una srl che detiene il controllo di fatto di una società attiva nel settore delle protesi ortopediche. La società partecipa alla gara indetta dalla regione per la stipulazione di un accordo quadro per l'approvvigionamento di protesi a beneficio di un IRCSS. Istituto: il dirigente si astiene dalle attività di definizione del bando.

Ipotesi 3. Il dirigente regionale viene contattato da una azienda del settore farmaceutico per l'affidamento di un incarico di consulenza. Istituto: divieto di accesso all'incarico esterno.

Ipotesi 4. Il dirigente regionale fino a 6 mesi prima della nomina (incarico dirigenziale ad esterni) è stato amministratore di un'azienda convenzionata con il sistema sanitario regionale. Istituto: inconferibilità (d.lgs. 39/2013: provenienza da enti di diritto privato regolati o finanziati dalle pubbliche amministrazioni. L'incarico dirigenziale non poteva essere assegnato).

Si noti come l'interesse personale del funzionario può entrare *direttamente* in conflitto con l'esercizio della funzione (si pensi al caso dell'*intramoenia*) ma più spesso è il *canale* attraverso il quale hanno ingresso altri, ulteriori interessi, che sono in conflitto con quello primario. Nell'ipotesi 1 e 2, l'interesse proprio del dirigente è la relazione di parentela e di coniugio, e questo interesse non è di per sé in contrasto con l'interesse pubblico: il punto è che tale relazione può costituire canale di ingresso ed incisione sull'interesse pubblico a favore dell'interesse di cui sono portatori il fratello o la consorte del funzionario. Anche nel caso dell'ipotesi 3, l'interesse del dirigente regionale (accedere ad un incarico esterno al fine di poter ricevere il relativo compenso e consolidare la relazione con l'azienda che conferisce tale incarico) non è di per sé in contrasto con l'interesse pubblico all'appropriato approvvigionamento dei farmaci (semmai può entrare in contrasto con l'interesse dell'amministrazione datore di lavoro ad ottenere dal dirigente una pre-

stazione lavorativa ottimale); tuttavia, questo interesse personale può costituire il canale di ingresso / incisione sull'interesse pubblico da parte dell'azienda del settore farmaceutico. Pertanto, gli istituti del conflitto d'interessi rendono *rilevante un reticolo di interessi in cui il funzionario/l'agente è coinvolto*, e che vanno al di là dei soli interessi strettamente personali dell'agente, per arrivare a dare rilievo agli ulteriori interessi (che si pongano in conflitto con l'interesse pubblico) di cui l'agente costituisce non tanto il diretto titolare, ma piuttosto il "canale di trasmissione", oppure, per leggerla in altro modo, il nodo di connessione.

1.3.2. I meccanismi di emersione e di enforcement del conflitto d'interessi

L'istituto del conflitto d'interessi come strumento di prevenzione mira, come detto, ad evitare che si concretizzino le situazioni di rischio potenziale di deviazione dell'interesse primario in favore degli interessi in conflitto con esso. Tale istituto, nelle sue diverse declinazioni, è quindi efficace (ai fini della *prevenzione*) se è in grado di intercettare le situazioni di conflitto di interessi che si verificano effettivamente, così da poter innescare le misure di *disqualification* previste dalla normativa.

Perché siano intercettate, *occorre che le situazioni di conflitto d'interessi siano conosciute*. Nel quadro ordinamentale attuale tale esigenza viene assolta mediante i meccanismi di cosiddetta *autodichiarazione*, mediante la richiesta da parte dell'amministrazione di dichiarazioni sostitutive di certificazione o sostitutive dell'atto di notorietà da parte del soggetto interessato, dichiarazioni attestanti l'assenza di situazioni di conflitto d'interessi (comunque declinate), ovvero mediante l'imposizione di obblighi di informazione in capo all'agente relativamente ai rapporti di collaborazione suoi, di suoi parenti o affini entro il secondo grado, del coniuge o del convivente, con soggetti privati in qualunque modo retribuiti, e intrattenuti in periodi recenti, con specifico (anche se non esclusivo) riguardo ai rapporti intercorsi o che intercorrano con soggetti che abbiano interessi in attività o decisioni inerenti alle funzioni pubbliche a lui affidate; più in generale, tramite l'obbligo di segnalare tali situazioni. Poiché, per altro, il conflitto d'interessi può sorgere anche con riferimento a interessi di carattere non economico, il dovere di comunicazione riguarda anche l'eventuale adesione o partecipazione ad associazioni o organizzazioni, a prescindere dal loro carattere riservato o meno, i cui ambiti di interesse possano interferire con lo svolgimento dell'attività d'ufficio. Anche nel caso di astensione (un dovere che ricade in capo al soggetto direttamente interessato), la relativa decisione deve essere comunicata

per iscritto all'amministrazione di appartenenza, con la specificazione della situazione di conflitto che viene in rilievo.

Come si vede, in tutti questi casi è il soggetto direttamente interessato dalla situazione di conflitto di interessi a darne informazione all'amministrazione. Il che è certamente rispondente ad un canone di appropriatezza, dal momento che – nella generalità dei casi – è il soggetto interessato ad avere (migliore, piena, e precisa) conoscenza della situazione in questione. Tuttavia, tale meccanismo di emersione del conflitto d'interessi rivela anche la strutturale condizione di *asimmetria informativa* in cui si trova ad operare l'amministrazione, costretta (per le citate ragioni di appropriatezza conoscitiva) a ricorrere alle dichiarazioni dei soggetti interessati per avere contezza delle situazioni di conflitto d'interessi, così da potervi porre rimedio secondo quanto indicato dalla disciplina normativa. Come noto, il meccanismo di *enforcement* del dovere di fornire alle amministrazioni informazioni veritiere ed accurate circa l'esistenza di circostanze che possano configurare l'esistenza di un conflitto d'interessi è connesso alle modalità con cui tali obblighi di informazione devono essere assolti (quelle disciplinate dal T.U. sulla documentazione amministrativa, agli artt. 46 e 47). Per un verso, le dichiarazioni mendaci rese in tali sedi sono suscettibili di determinare responsabilità penali in capo all'autore. Dall'altro, l'amministrazione dispone di specifici poteri di verifica della veridicità delle dichiarazioni rese e dei fatti attestati, mediante l'istituto dell'accertamento d'ufficio, anche mediante la consultazione diretta degli archivi dell'amministrazione certificante.

Tuttavia, tali soluzioni non risolvono il problema (strutturale) dell'asimmetria informativa che intercorre tra amministrazione procedente e soggetto interessato dalla situazione di conflitto d'interessi, ma lo spostano solo più a valle, al momento cioè dell'effettuazione delle verifiche (di veridicità e completezza) da operarsi sulle dichiarazioni rese. Infatti, in tale sede si ripropone la medesima condizione di partenza dell'amministrazione che effettua il controllo, ossia quella di un deficit strutturale di conoscenza circa i fatti in rilievo.

Si noti che tale condizione cospira anche nel senso di rendere meno effettivo/efficace il meccanismo di emersione dei conflitti d'interesse. In effetti, la cogenza del sistema delle autodichiarazioni e successivi controlli di veridicità poggia sull'effetto di deterrenza prodotto dalle paventate conseguenze (anche penali) delle dichiarazioni mendaci eventualmente rese. Ora, tale effetto di deterrenza risulterebbe *nei fatti* quasi del tutto svuotato di efficacia/cogenza, se le amministrazioni non fossero poste in condizione di poter verificare in modo efficace, efficiente ed effettivo la veridicità delle dichiarazioni rese. Detto in altri termini, pochi avrebbero effettivamente timore di rendere dichiarazioni mendaci o incomplete se vi fosse consapevolezza del

fatto che l'amministrazione non dispone della capacità e dei mezzi per effettuare in modo effettivo i controlli e le verifiche[19].

1.3.3. La trasparenza verticale come meccanismo di compensazione dell'asimmetria informativa in materia di conflitto d'interessi

La rapida disamina del conflitto d'interessi (un istituto affatto centrale e strategico nell'economia dei meccanismi di *prevenzione* della corruzione) ci ha ricordato che tale situazione coinvolge una pluralità di interessi, che fanno perno in modo reticolare sull'agente incaricato o partecipe dell'esercizio di funzioni o attività di rilievo pubblico, così da rendere rilevanti interessi in contrasto con l'interesse pubblico veicolati o canalizzati dalla sfera personale dell'agente.

L'analisi dei meccanismi di rilevazione ed *enforcement* delle situazioni di conflitto d'interessi ci ha mostrato come il pieno dispiegamento delle potenzialità di tale istituto di prevenzione sono in qualche modo ostacolate o indebolite dalla condizione di strutturale asimmetria informativa delle amministrazioni, con riferimento alla capacità di conoscenza delle situazioni di conflitto di interessi. Una condizione che rende meno efficaci i meccanismi di deterrenza connessi alle procedure di verifica circa la veridicità (la completezza e la congruenza) delle dichiarazioni rese dai soggetti interessati, circa l'esistenza (o l'assenza) di situazioni di conflitto.

Vi è quindi un'*esigenza da soddisfare*, e c'è uno spazio da riempire: dotare l'amministrazione di strumenti conoscitivi idonei a colmare o quantomeno ridurre tale asimmetria informativa, realizzando le condizioni per dispiegare una capacità conoscitiva idonea ad aumentare efficacia ed effettività dei meccanismi di prevenzione fondati sulla evidenziazione e gestione del conflitto d'interessi.

Il caso di studio ha mosso in questa direzione: verificare cioè la possibilità di mettere a frutto le informazioni disponibili nel sistema amministrativo

[19] Come è stato sottolineato, "the lack of control of submission and ineffective verification of declarations undermine the importance of Asset and Interest Declaration (AID)" cfr. Bajpai R. e Myers B. (2020), *Enhancing Government Effectiveness and Transparency the Fight Against Corruption*, Word Bank, 235. Questo tema e questa esigenza sono stati posti in termini espliciti dalle stesse amministrazioni. In particolare, la Conferenza delle Regioni e delle Province Autonome, nel parere al Piano nazionale anticorruzione 2019, parere pure favorevole, ha però esplicitamente richiesto che fossero "fornite maggiori indicazioni in merito alle modalità di controllo delle autodichiarazioni rese, sia in materia di conflitto di interessi che di altre misure di prevenzione specifiche che ne rappresentano una derivazione. In particolare, le modalità operative (…) andrebbero meglio esplicitate anche in considerazione delle implicazioni attinenti la protezione dei dati personali" (parere 24 ottobre 2019).

complessivamente considerato, al fine di progettare, elaborare e testare strumenti di *trasparenza verticale*, così da dotare le amministrazioni di autonome e efficaci capacità conoscitive utili a far emergere e/o verificare l'esistenza di situazioni di conflitto d'interessi.

Per fare anche qui un esempio, si pensi all'istituto del *pantouflage* (o *revolving door*), ossia quella forma di incompatibilità successiva, introdotta nell'ordinamento nazionale con la legge 190/2012, e che vieta ad un agente pubblico, nel triennio successivo all'esaurimento del rapporto di pubblico impiego, di intrattenere rapporti con le imprese che operino nei settori coperti/regolati negli ultimi tre anni di servizio. Perché questo istituto possa efficacemente operare, sono necessarie un certo numero/tipologia di informazioni (informazioni anagrafiche, informazioni commerciali, previdenziali, bancarie, tributarie, etc.), ma la loro (*mera*) disponibilità non è anche sufficiente: occorre che dette informazioni siano gestire/trattate perché emerga all'attenzione (sia, cioè, conosciuta) una determinata circostanza, quella ad esempio che integri in concreto la fattispecie vietata dalla norma. Solo in questo caso, l'asimmetria informativa che caratterizza strutturalmente la situazione dell'ex dipendente e dell'impresa (da una parte) – che conoscono già quella circostanza di fatto – e dell'amministrazione, dall'altra – che non la conosce – può essere colmata, così da ottenere effettiva trasparenza sulla situazione di fatto, con l'attivazione delle misure e delle conseguenze del caso. Com'è evidente, la mera disponibilità delle informazioni utili allo scopo (nominativo/Part. IVA/settore di attività dell'impresa, informazioni presenti nel registro delle imprese; versamenti previdenziali da impresa a ex dipendente, registro INPS; prelievo IRPEF su compenso, presente nell'anagrafe tributaria; ruolo/incarico dell'ex dipendente nel periodo precedente alla cessazione dal servizio, informazione disponibile presso l'ente di appartenenza, etc.) per quanto necessaria, non è sufficiente. Occorre che le informazioni rilevanti e pertinenti siano messe in relazione tra loro, in funzione dello specifico istituto considerato, così da diventare significative[20]. Il

[20] Per una declinazione della nozione di trasparenza che non si ferma alla sola disponibilità/conoscibilità delle informazioni (che pure è indispensabile), me che metta a tema anche la capacità di estrarre un significato, una *comprensione* circa l'oggetto osservato, sia consentito rinviare a Ponti B., "La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi", *Diritto dell'informazione e dell'informatica*, 2, 2019, 383-422. In questo senso, si veda di recente la esplicazione della nozione di trasparenza fornita nella relazione al Codice dei contratti adottato con il d.lgs. 36/2023, con riferimento all'art. 20 (Principi in materia di trasparenza) "Per trasparenza amministrativa deve intendersi la *comprensibilità* e la conoscibilità dall'esterno dell'attività finalizzate a realizzare imparzialità e buon andamento dell'azione amministrativa e a rendere maggiormente chiare e credibili le scelte rivolte alla cura dell'interesse generale", 42 (corsivo aggiunto).

sistema della prevenzione della corruzione ha – per un verso – scommesso/investito sulla capacità della società di contribuire a questa attività. Di qui il senso degli istituti della trasparenza amministrativa (obblighi di pubblicazione e accesso generalizzato): abilitare la disponibilità diffusa delle informazioni, perché – su iniziativa dei diversi corpi sociali interessati a farlo – i dati siano analizzati (in modo più o meno approfondito, sistematico, strutturato) così da individuare, segnalare ed esporre casi di corruzione (trasparenza orizzontale). Ma contemporaneamente è emersa anche la consapevolezza che quel contributo (per quanto fondamentale, ed in effetti ineliminabile, dal momento che gli istituti della trasparenza corrispondono al soddisfacimento di un diritto di libertà del cittadino, e quindi si giustificano in quanto tali, a prescindere dall'efficacia concreta in termini di prevenzione della corruzione[21]) non poteva essere considerato sufficiente (di per sé) a realizzare/soddisfare le esigenze conoscitive "di sistema", per una serie di ragioni concorrenti. In primo luogo, perché il contributo della trasparenza diffusa tende ad essere – per sua natura (e salvo eccezioni) – episodico, territorialmente disomogeneo, discontinuo, e guidato dagli interessi e dalle priorità che gli attori della società civile si danno, nell'esercizio della rispettiva autonomia. In secondo luogo, perché non tutte le informazioni che sono nella effettiva disponibilità del settore pubblico (il *patrimonio informativo pubblico* complessivamente inteso) possono essere anche essere rese disponibili alla conoscenza e all'uso generalizzati, dal momento che una parte consistente di tale patrimonio è costituito da dati personali, con ciò che ne consegue in termini di limiti al trattamento che consista nella diffusione al pubblico (lo si è già potuto constatare[22]). Tali informazioni – se ne ricorrono i presupposti e i requisiti – possono però essere utilizzate (e riutilizzate) all'interno del settore pubblico, sempre a fini conoscitivi.

Una volta chiarito l'obiettivo, emerge immediatamente all'attenzione la circostanza per cui uno strumento idoneo a consentire di rilevare ed evidenziare possibili situazioni di conflitto d'interessi, o quantomeno a fornire una

[21] Così Cons. Stato, Ad. Plen. n. 10/2020 "nell'accesso civico generalizzato si ha un accesso dichiaratamente finalizzato a garantire il controllo democratico sull'attività amministrativa, nel quale il c.d. *right to know*, l'interesse individuale alla conoscenza, *è protetto in sé*, se e in quanto non vi siano contrarie ragioni di interesse pubblico o privato, ragioni espresse dalle cc.dd. eccezioni relative di cui all'art. 5-bis, commi 1 e 2, del d. lgs. n. 33 del 2013", par. 22.3 del considerato in diritto; "Non solo, peraltro, l'accesso civico generalizzato, nel quale la trasparenza si declina come "accessibilità totale" (Corte cost., 21 febbraio 2019, n. 20), *è un diritto fondamentale, in sé* (…), ivi, par. 23.1 (corsivi aggiunti).

[22] Cfr. *supra* il cap. 3, par. 2.5, con specifico riferimento alla giurisprudenza della Corte di giustizia relativa al requisito di stretta necessarietà applicato alle ipotesi di diffusione di dati personali al pubblico, anche con specifico riferimento alle misure esplicitamente rivolte alla prevenzione della corruzione, come nel caso esaminato in C-184/20.

rappresentazione del reticolo di interessi che fa capo ad un determinato agente richiede di disporre e trattare (anche, soprattutto) *dati personali*, per altro dislocati in banche dati allocate presso plurime amministrazioni. Infatti, poiché lo strumento conoscitivo in questione mira a consentire di ricostruire, evidenziare e rappresentare le reti di interessi che fanno capo all'agente, tale risultato può essere conseguito, evidentemente, solo mediante il trattamento di dati personali, cioè, elementi informativi – quali la titolarità di una impresa, la partecipazione azionaria, la relazione di parentela, etc. – che siano riferibili ad una persona identificata o identificabile.

1.4. Mappatura delle reti di interessi e trattamento dei dati personali per l'esercizio delle funzioni di prevenzione della corruzione

Una volta identificato il compito di interesse pubblico (verifica delle dichiarazioni sull'insussistenza delle condizioni di conflitto d'interessi) e l'esigenza connessa al suo esercizio in concreto (dotare le amministrazioni di uno strumento per supportarne l'esercizio), il passo successivo, sul piano pratico, è consistito nell'immaginare quale soluzione conoscitiva potesse rispondere a questa esigenza. Tale soluzione (sul piano ancora puramente speculativo) è stata individuata nella elaborazione di una mappatura degli interessi che fanno al soggetto dichiarante, predisposta in modo tale che, una volta identificati e selezionati gli interessi primari in gioco in una circostanza specifica, la mappa possa evidenziare se vi siano legami (archi) con interessi che risultino qualificabili come in contrasto o incompatibili con l'interesse primario. Un simile strumento istruttorio, qualora disponibile, consentirebbe di utilizzare in modo più efficiente ed efficace le risorse organizzative dedicate alla verifica (delle dichiarazioni attestanti l'assenza) del conflitto d'interessi, dal momento che – evidenziando in termini di *red flag* le situazioni che si presentano come potenzialmente integranti tali condizioni – consentirebbero di indirizzare le necessarie verifiche ed acquisizioni documentali solo dove esistano fondati sospetti (fondati, nel senso di basati sull'analisi preliminare delle reti di interessi fornita dalla mappatura). L'esperienza maturata dal caso di studio ha consentito di apprezzare i diversi aspetti problematici connessi alla effettiva realizzabilità di un simile strumento di supporto conoscitivo/istruttorio. Sul piano tecnico, la necessità di condurre studi esplorativi per verificare quale tecnica di analisi delle informazioni possa risultare più coerente ed efficace rispetto allo scopo. Sul piano ingegneristico, elaborare sistemi di identificazione, qualificazione e standardizzazione della complessa, variegata, differenziata dimensione degli interessi pubblici affidati alla cura delle amministrazioni, necessaria per realizzare una tassonomia che consenta

di ridurre la complessità (senza per altro mortificarla o eluderla) così da abilitare le procedure automatizzare di elaborazione della mappatura del reticolo di interessi. Sul piano conoscitivo, l'identificazione delle fonti di informazione da utilizzare per compiere la elaborazione. Tutti aspetti con elevata interdipendenza reciproca, così che uno studio di fattibilità si presenta come una missione particolarmente complessa da realizzare.

Dal punto di vista del presente studio, tuttavia, gli aspetti interessanti sono quelli connessi all'effettivo grado di *fattibilità giuridica* di una simile soluzione, sotto il profilo – in particolare – della compatibilità con il quadro giuridico che legittima il trattamento di dati personali a fini di esercizio di compiti di interesse pubblico. Ciò che è interessante osservare, nel caso di specie, è l'interazione tra il quadro giuridico nazionale (nelle sue recenti mutazioni) rispetto all'effettivo grado margine di iniziativa disponibile alle amministrazioni, così da verificare *in vivo*, come il quadro normativo che legittima il trattamento dei dati personali incide sulle concrete dinamiche operative sperimentate dalle amministrazioni.

1.4.1. La mappatura dei conflitti d'interesse sotto la strict legality rule

Il nucleo dei dati personali necessari per elaborare la mappatura di cui sopra è costituito da dati personali *comuni* (si tratta di dati anagrafici e di dati relativi agli interessi economici – settori di attività delle imprese, struttura di proprietà e di controllo delle società, partecipazioni azionarie, dati catastali); pertanto si può ragionare facendo riferimento al relativo regime giuridico applicabile. La tipologia di trattamento in questione di configura, *prima facie*, come un'ipotesi di profilazione, stando al GDPR, che ricomprende nella definizione "qualsiasi forma di trattamento automatizzato di dati personali (…) per valutare determinati aspetti personali relativi a una persona fisica (…) gli interessi (…) di detta persona fisica"[23]. Tuttavia, poiché lo strumento è immaginato fin dall'inizio come supporto rispetto all'esercizio di compiti di approfondimento istruttorio, verifica ed accertamento che restano in capo ai funzionari addetti, non si tratterebbe di una decisione basata *unicamente* sul trattamento automatizzato, con le conseguenze del caso[24].

[23] Cfr. art. 4, n. 4) del GDPR, ma vedi anche WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 6 febbraio 2018.

[24] Nel GDPR, infatti, il trattamento automatizzato che si configuri come (o determini) una profilazione dell'interessato rileva a vari fini. In primo luogo, l'esistenza di un processo decisionale automatizzato, compresa la profilazione va reso trasparente nell'informativa (art. 13 e 14) insieme ad informazioni significative sulla logica utilizzata, nonché circa l'importanza e

Come detto, i requisiti di legittimazione del trattamento fissati alla stregua della *strict legaly rule* dal d.lgs. 101/2018 comportavano che la norma (di legge o, nei casi previsti dalla legge, di regolamento) non potesse limitarsi ad affidare all'amministrazione il compito di interesse pubblico, ma dovesse anche prevedere espressamente (quantomeno) quale trattamento potesse essere effettuato e la sua finalità. Procediamo allora alla identificazione del quadro normativo rilevante, con riferimento all'attribuzione ed all'esercizio dei compiti oggetto del caso di studio.

Con riferimento ai compiti di prevenzione della corruzione amministrativa, anche con specifico riferimento al rilievo del conflitto d'interessi, il riferimento va fatto tanto ai compiti volti ad assicurare in modo coordinato, l'attività di controllo, di prevenzione e di contrasto della corruzione e dell'illegalità nella pubblica amministrazione affidati all'ANAC (art. 1, comma 1 della l. n. 190/2012), tra i quali anche il compito di *analizzare le cause e i fattori della corruzione e di individuare gli interventi che ne possono favorire la prevenzione e il contrasto* (comma 2), poteri che trovano forma specifica (ma non esclusiva) di concretizzazione nell'adozione ed aggiornamento deliano nazionale anticorruzione (PNA); tanto ai compiti delle singole amministrazioni che – mediante l'elaborazione del piano triennale di prevenzione della corruzione e della trasparenza amministrativa (PTPCT) – valutano i rischi specifici cui sono esposte e formulano le strategie di programmazione e di gestione ai fini dell'applicazione degli istituti di prevenzione al tale specifico contesto organizzativo, anche elaborando misure aggiuntive (art. 1, commi da 5 a 9 della l. n.190/2012). Tra gli istituti la cui applicazione è oggetto di programmazione ad opera del PTPCT, figurano tutti quelli che fanno perno sul conflitto d'interessi (obblighi di comunicazione e di pubblicità; dovere di astensione, regolamentazione dell'accesso agli incarichi esterni, incompatibilità, inconferibilità, codice di comportamento).

le conseguenze previste di tale trattamento per l'interessato; inoltre, nell'esercizio del suo diritto di accesso (art. 15) l'interessato ha diritto di conoscere dal responsabile analoghe informazioni; l'interessato ha diritto, per motivi connessi alla sua situazione particolare, di opporsi al trattamento di profilazione che lo riguardi ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), ed in ogni caso, qualora i dati personali siano trattati per finalità di marketing diretto (art. 21). Infine, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (art. 22, con le eccezioni stabilite al par. 2 del medesimo articolo); cfr. Spangaro A. (2022), "Il concetto di profilazione tra 'direttiva madre' e GDPR, in *Giurisprudenza italiana*, 7, 1579-1587; Lagioia F., Sartor G. (2020), "Profilazione e decisione algoritmica: dal mercato alla sfera pubblica", in *federalismi.it*, 11, 85-110; Rizzuto I. (2018), "Le nuove frontiere del 'digital marketing': dalla profilazione alla manipolazione 'online' nell'ambito politico alla luce del GDPR", in *Ciberspazio e Diritto*, 1-2, 99-120.

Con riferimento, invece, ai doveri di comunicazione e dichiarazione dei conflitti d'interessi e i connessi compiti di verifica, si devono richiamare quantomeno le seguenti norme:

- l'art. 53, comma 7 del d.lgs. 165/2001 prevede che: "I dipendenti pubblici non possono svolgere incarichi retribuiti che non siano stati conferiti o previamente autorizzati dall'amministrazione di appartenenza. Ai fini dell'autorizzazione, l'amministrazione verifica l'insussistenza di situazioni, anche potenziali, di conflitto di interessi."
- l'art. 20 del d.lgs. 39 del 2013 ("Dichiarazione sulla insussistenza di cause di inconferibilità o incompatibilità") prevede che "1. All'atto del conferimento dell'incarico l'interessato presenta una dichiarazione sulla insussistenza di una delle cause di inconferibilità di cui al presente decreto. 2. Nel corso dell'incarico l'interessato presenta annualmente una dichiarazione sulla insussistenza di una delle cause di incompatibilità di cui al presente decreto. 3. Le dichiarazioni di cui ai commi 1 e 2 sono pubblicate nel sito della pubblica amministrazione, ente pubblico o ente di diritto privato in controllo pubblico che ha conferito l'incarico. 4. La dichiarazione di cui al comma 1 è condizione per l'acquisizione dell'efficacia dell'incarico. 5. Ferma restando ogni altra responsabilità, la dichiarazione mendace, accertata dalla stessa amministrazione, nel rispetto del diritto di difesa e del contraddittorio dell'interessato, comporta la inconferibilità di qualsivoglia incarico di cui al presente decreto per un periodo di 5 anni";
- l'art. 6 del d.p.r. n. 62/2013 (Comunicazione degli interessi finanziari e conflitti d'interesse), prevede che: "1. Fermi restando gli obblighi di trasparenza previsti da leggi o regolamenti, il dipendente, all'atto dell'assegnazione all'ufficio, informa per iscritto il dirigente dell'ufficio di tutti i rapporti, diretti o indiretti, di collaborazione con soggetti privati in qualunque modo retribuiti che lo stesso abbia o abbia avuto negli ultimi tre anni, precisando:
  - se in prima persona, o suoi parenti o affini entro il secondo grado, il coniuge o il convivente abbiano ancora rapporti finanziari con il soggetto con cui ha avuto i predetti rapporti di collaborazione;
  - se tali rapporti siano intercorsi o intercorrano con soggetti che abbiano interessi in attività o decisioni inerenti all'ufficio, limitatamente alle pratiche a lui affidate. 2. Il dipendente si astiene dal prendere decisioni o svolgere attività inerenti alle sue mansioni in situazioni di conflitto, anche potenziale, di interessi con interessi personali, del coniuge, di conviventi, di parenti, di affini entro il secondo grado. Il conflitto può riguardare interessi di qualsiasi natura, anche non patrimoniali, come quelli derivanti dall'intento di voler assecondare pressioni politiche, sindacali o dei superiori gerarchici."
- L'art. 77 (Commissione giudicatrice) del Codice dei contratti (d.lgs. 50/2016, disciplina applicabile in costanza del vigore delle modifiche al Codice privacy introdotte con il d.lgs. 101/2018), al comma 9 stabilisce che: "Al mo-

mento dell'accettazione dell'incarico, i commissari dichiarano ai sensi dell'articolo 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, l'inesistenza delle cause di incompatibilità e di astensione di cui ai commi 4, 5 e 6. Le stazioni appaltanti, prima del conferimento dell'incarico, accertano l'insussistenza delle cause ostative alla nomina a componente della commissione giudicatrice di cui ai commi 4, 5 e 6 del presente articolo, all'articolo 35-bis del decreto legislativo n. 165 del 2001 e all'articolo 42 del presente codice. La sussistenza di cause ostative o la dichiarazione di incompatibilità dei candidati devono essere tempestivamente comunicate dalla stazione appaltante all'ANAC ai fini della cancellazione dell'esperto dall'albo e della comunicazione di un nuovo esperto";

- l'art. 42. (Conflitto di interesse) del Codice degli appalti ((d.lgs. 50/2016, disciplina applicabile in costanza del vigore delle modifiche al Codice privacy introdotte con il d.lgs. 101/2018) stabilisce che: "1. Le stazioni appaltanti prevedono misure adeguate per contrastare le frodi e la corruzione nonché per individuare, prevenire e risolvere in modo efficace ogni ipotesi di conflitto di interesse nello svolgimento delle procedure di aggiudicazione degli appalti e delle concessioni, in modo da evitare qualsiasi distorsione della concorrenza e garantire la parità di trattamento di tutti gli operatori economici.

Con riferimento, invece, alle norme che disciplinano le modalità di esercizio dei compiti di verifica delle dichiarazioni, va fatto riferimento alle seguenti:

- *Dichiarazioni sostitutive dell'atto di notorietà*. I soggetti interessati comunicano all'amministrazione notizie concernenti stati, qualità personali o fatti che siano a loro diretta conoscenza mediante dichiarazione resa e sottoscritta dagli interessati medesimi, ai sensi dell'art. 47 del dpr 445/2000 ("Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"), osservando delle modalità di cui all'art. 38 del medesimo dpr.
- *Accertamenti d'ufficio*. Ai sensi dell'art. 43 del dpr 445/2000, le amministrazioni sono autorizzate ad accedere ed a consultare direttamente le banche dati detenute da altre amministrazioni per effettuare il controllo sulle dichiarazioni sostitutive presentate dai cittadini.

In particolare, l'art. 43 così recita:

- 1. Le amministrazioni pubbliche e i gestori di pubblici servizi sono tenuti ad acquisire d'ufficio le informazioni oggetto delle dichiarazioni sostitutive di cui agli articoli 46 e 47, nonché tutti i dati e i documenti che siano in possesso delle pubbliche amministrazioni, previa indicazione, da parte dell'interessato, degli elementi indispensabili per il reperimento delle informazioni o dei dati

richiesti, ovvero ad accettare la dichiarazione sostitutiva prodotta dall'interessato. (L) 2. Fermo restando il divieto di accesso a dati diversi da quelli di cui è necessario acquisire la certezza o verificare l'esattezza, si considera operata per finalità di rilevante interesse pubblico, ai fini di quanto previsto dal decreto legislativo 11 maggio 1999, n. 135, la consultazione diretta, da parte di una pubblica amministrazione o di un gestore di pubblico servizio, degli archivi dell'amministrazione certificante, finalizzata all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive presentate dai cittadini. Per l'accesso diretto ai propri archivi l'amministrazione certificante rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente. (L). 3. L'amministrazione procedente opera l'acquisizione d'ufficio, ai sensi del precedente comma, esclusivamente per via telematica (L). Al fine di agevolare l'acquisizione d'ufficio di informazioni e dati relativi a stati, qualità personali e fatti, contenuti in albi, elenchi o pubblici registri, le amministrazioni certificanti sono tenute a consentire alle amministrazioni procedenti, senza oneri, la consultazione per via telematica dei loro archivi informatici, nel rispetto della riservatezza dei dati personali. 5. In tutti i casi in cui l'amministrazione procedente acquisisce direttamente informazioni relative a stati, qualità personali e fatti presso l'amministrazione competente per la loro certificazione, il rilascio e l'acquisizione del certificato non sono necessari e le suddette informazioni sono acquisite, senza oneri, con qualunque mezzo idoneo ad assicurare la certezza della loro fonte di provenienza. (R) 6. I documenti trasmessi da chiunque ad una pubblica amministrazione tramite fax, o con altro mezzo telematico o informatico idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale (R)."

Nessun dubbio, dalla lettura delle norme, che la disciplina affidi alle amministrazioni il compito di prevenire la corruzione; strumentale all'esercizio di questa funzione è l'istituto del conflitto d'interessi, che è oggetto di plurimi obblighi di dichiarazione in capo ai funzionari pubblici ed è anche oggetto dei specifici compiti conoscitivi e di verifica in capo all'amministrazione, sia con riferimento alla diretta individuazione delle situazioni di conflitto d'interessi, sia (indirettamente) mediante l'esercizio dei compiti di verifica circa la veridicità del contenuto delle dichiarazioni che i funzionari sono tenuti a presentare.

Se però andiamo a verificare quali trattamenti di dati personali sono esplicitamente previsti dalla normativa *de qua* e per quali *finalità*, a supporto delle attività di individuazione (del conflitto d'interessi) o di verifica (della veridicità delle dichiarazioni), ci avvediamo che le uniche indicazioni utili fanno riferimento alle *finalità* di verifica delle dichiarazioni rese (art. 46 d.p.r.

445/2000), nelle modalità dell'accesso cd. inter-amministrativo[25] (art. 43). Quanto alla finalità del trattamento, è abilitato l'accesso inter-amministrativo al fine di controllare le informazioni rese nelle dichiarazioni. La finalità è quindi solo quella di avere riscontro (in sede di controllo) dell'esattezza delle informazioni rese. Un trattamento che, evidentemente, non è in grado di risolvere il problema dell'asimmetria informativa di cui si è detto, dal momento che l'amministrazione potrà al limite verificare quanto *effettivamente dichiarato* dall'interessato. Non vi sono, invece, indicazioni circa un trattamento dei dati a fini di supporto istruttorio, ovvero trattamenti che abbiano la (diversa, preliminare) finalità di indicare all'amministrazione *cosa eventualmente andare a verificare e accertare*, che non sia stato dichiarato o che sia stato dichiarato in modo non veritiero. Né, pertanto, sono previste le relative modalità operative (che ovviamente sono molto diverse da quelle mediante le quali si opera l'accesso di cui all'art. 43 del d.p.r. 445/2000). Tali finalità e tali trattamenti non sono nemmeno contemplati nelle altre discipline indagate, a supporto delle attività di individuazione e/o verifica dell'esistenza di situazioni di conflitto d'interessi (presenti sia nel d.lgs. 165/2001, in riferimento alle procedure di autorizzazione degli incarichi esterni; sia nel d.lgs 39/2013, quanto alle dichiarazioni sull'insussistenza di situazioni di incompatibilità/inconferibilità; sia nel codice dei contratti). Per altro, va anche constatato che la cosa non è così sorprendente: infatti, sino alle modifiche introdotte con il d.lgs. 101/2018, il regime di trattamento dei dati personali comuni definito dal Codice era sostanzialmente riconducibile allo schema della *necessary clause*, così che l'espressa previsione in legge dei trattamenti e delle relative finalità non era indispensabile a legittimarne la realizzazione. Invece, a seguito dell'introduzione di un regime di *strict legality*, i trattamenti giustificati solo in termini di *strumentalità necessaria*, ma non anche coperti da esplicita previsione nella norma, risultano impraticabili.

Il caso di studio ne fornisce plastica testimonianza. Dati i vincoli esistenti, il progetto è, in effetti, riuscito a progredire meglio e di più nell'elaborazione di indicatori che non richiedessero il trattamento di dati personali. Tuttavia, è utile sottolineare (a conferma della pregnanza degli ostacoli *ulteriori*, rispetto ai vincoli imposti dal regime a tutela dei dati personali) che la più ampia parte delle informazioni utilizzate a tali fini non è stata fornita dalle amministrazioni coinvolte, sulla base del protocollo d'intesa che ha dato il via al progetto. Piuttosto, il progetto si è avvalso e messo a frutto numerosi

[25] Sul punto, cfr. Guerra M.P. (2005), "Circolazione dell'informazione e sistema informativo pubblico: profili giuridici dell'accesso interamministrativo telematico", cit., 525-571.

e diversi *data set* resi disponibili in *open data* da molte amministrazioni, anche esterne al protocollo d'intesa. Una circostanza affatto significativa, non solo delle difficoltà già segnalate più in alto, ma anche del fatto che le politiche di apertura dei dati pubblici risultano funzionali anche ad agevolare la circolazione e la fruizione di tali informazioni anche all'*interno del sistema pubblico*, e per il soddisfacimento delle sue *specifiche esigenze*[26]. Ed infatti, quella parte di progetto ha sviluppato la sperimentazione fino al punto di pubblicare una serie di indicatori territoriali di rischio corruttivo resi *già disponibili* all'uso delle amministrazioni pubbliche (e non solo)[27].

Diverso è il caso per quanto concerne la sperimentazione dell'indicatore utile alla verifica del conflitto d'interessi. In questo caso, le verifiche di fattibilità hanno dovuto fare i conti, innanzitutto, con il vincolo imposto dalla *strict legality rule* introdotta con il d.lgs. 101/2018. A parte lo studio di alcune significative esperienze maturate nel contesto giuridico di altri Stati membri dell'UE (sia per quanto riguarda *in generale* il trattamento dei dati a fini di esercizio di funzioni pubbliche, sia per quanto concerne trattamenti finalizzati proprio alla prevenzione della corruzione e della *maladministration*), lo sviluppo in concreto di soluzioni operative – anche solo di carattere sperimentale – era escluso proprio in virtù della carenza di un'adeguata base giuridica. In effetti, il progetto mirava a concludersi mediante la formulazione di indicazioni *al legislatore* circa le opzioni regolatorie da tenere presenti per consentire di abilitare strumenti conoscitivi basati (anche) sul trattamento di dati personali.

1.4.2. La mappatura dei conflitti d'interesse sotto la necessary clause

Tuttavia, nel corso del progetto sono intervenute le modifiche al Codice, che hanno alterato in modo così significativo il quadro normativo che presiede al trattamento dei dati personali per l'esecuzione di compiti di interesse pubblico. Ciò ha rappresentato (anche se i tempi residui disponibili erano molto limitati) una finestra di opportunità, dal momento che l'adozione della *necessary clause* sembrava invece fornire un utile presupposto di liceità del trattamento, quantomeno per avviare alcune prime fasi di sperimentazione di

[26] Per una risalente indicazione circa le potenzialità dei dati aperti per incentivare la circolazione del patrimonio informativo all'interno del sistema pubblico, sia consentito rinviare a Ponti B., "Il patrimonio informativo pubblico come risorsa: i limiti del regime italiano di riutilizzo dei dati delle pubbliche amministrazioni", *Diritto pubblico*, n. 3, 2007, 991-1014.

[27] Tali indicatori possono essere consultati e calcolati direttamente dagli utenti mediante all'accesso all'apposita sezione costituita nella piattaforma di ANAC: https://www.anticorruzione.it/gli-indicatori

una soluzione per la mappatura del conflitto d'interessi. Non è questa la sede per dare conto dei *risultati* di questa prima fase di sperimentazione[28]. Ciò che qui è invece interessante notare è l'effetto determinato dalle modifiche del quadro normativo. L'amministrazione ha potuto assumere direttamente l'iniziativa della sperimentazione, individuare le basi dati da applicare alla sperimentazione, commissionare e sovraintendere alla realizzazione di un prototipo per le mappature, muovendo da un sottoinsieme di dati su cui svolgere i test di sperimentazione.

Avere la possibilità di svolgere almeno una prima fase di sperimentazione ha consentito all'amministrazione di verificare una serie di ipotesi di base, di testare la fattibilità di sistemi di standardizzazione degli interessi primari, esaminare e discutere varie metodologie utili per selezionare e qualificare gli interessi in contrasto con l'interesse primario, saggiare l'effettiva potenzialità della soluzione nell'identificare ed evidenziare le *red flag*, individuare le strategie e le opzioni più opportune per impostare le ulteriori fasi di sviluppo.

Avere la possibilità di sperimentare (anche mediante simulazione) le capacità conoscitive abilitate dal trattamento di mappatura a fini di supporto istruttorio alla verifica del conflitto d'interessi, consente oggi di poter valutare con cognizione di causa rischi e opportunità derivanti dalla combinazione di data set di diversa provenienza (ANPR, Registro delle imprese, Catasto, Istat, etc.), ma anche di disporre già di alcune prime indicazioni circa la concreta fattibilità, e le opzioni per la sua ulteriore implementazione. Ovviamente, la possibilità di disporre più agevolmente dei presupposti di liceità (dal momento che le fattispecie di cui all'art. 2-ter, comma 1 e comma 1 bis consentono all'amministrazioni di *attivarsi*, come il caso di studio dimostra) non esaurisce, né risolve di per sé tutte le (altre, rilevanti) questioni relative alla compatibilità del trattamento con la disciplina a tutela dei dati personali. Ma evidentemente modifica in modo significativo le *regole del gioco*: e su questi profili (anche muovendo dagli elementi osservati nella *law in action*) tornare nel capitolo conclusivo di questo lavoro.

[28] Cfr. la sezione di documentazione del portale Anac dedicato ai risultati del progetto: https://www.anticorruzione.it/studi-e-documenti-utili

2. Il contrasto dell'evasione fiscale e gli strumenti di elaborazione dei profili di rischio da parte dell'Agenzia delle Entrate (secondo caso di studio)

Il secondo caso di studio che intendiamo indagare riguarda il trattamento di dati personali (di varia provenienza) per l'individuazione dei profili di rischio di evasione ed elusione fiscale, a supporto delle attività dell'Agenzia delle Entrate finalizzate all'emersione della base imponibile: anche questa vicenda (il cui punto di partenza è costituito dalle disposizioni inserite all'art. 11 del d.l. 6 dicembre 2011 n. 201, cosiddetto "salva Italia", convertito con modificazioni dalla legge 22 dicembre 2011 n. 214) è stata scelta perché le dinamiche evolutive che hanno caratterizzato la progressiva realizzazione delle soluzioni di analisi e la relativa (recente) messa a regime, consentono di osservare gli effetti dei diversi regimi legali relativi al trattamento che si sono succeduti nel tempo, come pure di osservare l'interazione tra gli attori in gioco, nei diversi contesti regolatori così abilitati.

L'angolo visuale prescelto muove dell'esigenza di attrezzare l'amministrazione tributaria di strumenti di indagine e di analisi utili a individuare i contribuenti che presentino profili di rischio più significativi, in modo da poter indirizzare le risorse dedicate alla verifica e all'accertamento in modo più efficiente ed efficace. Si tratta un angolo di visuale interessante, sotto molteplici aspetti. In primo luogo, perché comporta la messa in opera di strumenti volti a irrobustire ed innovare la capacità conoscitiva dell'amministrazione[29]. In secondo luogo, perché indica la volontà del legislatore di attrezzare e qualificare le capacità conoscitive dell'amministrazione fiscale mediante il ricorso alle più recenti tecniche di analisi dei dati[30], in accordo con una tendenza generalizzata sul piano internazionale[31]. In terzo luogo, perché

[29] Cfr. Fransoni G. (2020), *Le indagini tributarie. Attività e poteri conoscitivi nel diritto tributario, Giappichelli*, Torino; Falcone M. (2023), *Ripensare il potere conoscitivo pubblico. La conoscenza amministrativa con i big data e gli algoritmi*, cit.

[30] Cfr. Guidara A. (2023), "Accertamento dei tributi e intelligenza artificiale: prime riflessioni per una visione di sistema", in *Dir. e Prat. Trib.*, 2, 384; Uricchio A. (2019), "Robot tax: modelli di prelievo e prospettive di riforma", in *Giur. It.*, 7, 1657 ss.; Conigliaro M. (2020), "RecoveryFund: verso la riforma fiscale con innovazione digitale, big data, tracciabilità e tassazione per cassa", in *Fisco*, 40, 4850 ss.

[31] Faúndez-Ugalde A., Mellado-Silva R., Aldunate-Lizana E. (2020), "Use of artificial intelligence by tax administrations: An analysis regarding taxpayers' rights in Latin American countries", in *Computer Law & Security Review*, 38; Ribes Ribes A. (2020), "La inteligencia artificial al servicio del «compliance tributario», in *Revista española de derecho financiero*, 2020, 125 ss.; Shakil M. H., Tasnia M. (2022), *Artificial Intelligence and Tax Administration in Asia and the Pacific*, in (eds.) Hendriyetty N., Evans C., Kim C. J., Taghizadeh-Hesary F., *Taxation in the Digital Economy New Models in Asia and the Pacific*, 45-55; de la Feria R. e Grau Ruiz M.A. (2022), "The Robotisation of Tax Administration", in M.A. Grau Ruiz (eds.),

il soddisfacimento di queste finalità (e la realizzazione dei relativi strumenti) implica il trattamento (plurimi trattamenti, a dire il vero) di dati personali[32]. Già la disciplina introdotta nel 2011 disponeva l'acquisizione di ulteriori informazioni (movimenti ed ogni altra informazione e operazione relativa ai rapporti finanziari intrattenuti con banche, istituti di credito, imprese d'investimento, organismi di gestione del risparmio nonché ogni altro operatore finanziario[33]) all'Anagrafe tributaria, in modo tale da agevolare "per l'elaborazione con procedure centralizzate, secondo i criteri individuati con provvedimento del Direttore della medesima Agenzia, di specifiche liste selettive di contribuenti a maggior rischio di evasione"[34].

I profili toccati dall'interazione tra amministrazioni coinvolte (Agenzia e Ministero delle finanze), autorità di controllo (il Garante privacy) e legislatore sono molteplici, e tutti di grande rilievo. Di seguito ne selezioniamo i principali, per evidenziare come il *framework* normativo relativo al regime di trattamento dei dati personali abbia concorso in modo decisivo a tracciare il percorso di progressiva implementazione di tale strumento.

Interactive Robotics: Legal, Ethical, Social and Economic Aspects, Cham, § III; Hadwick D. e Lan S. (2021), "Lessons to Be Learned from the Dutch Childcare Allowance Scandal: a Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany", cit.; Amparo Gran Ruiz M. (2022), "Fiscal Transformations due to AI and Robotization: Where Do Recent Changes in Tax Administrations, Procedures and Legal Systems Lead Us?", in *Northwestern Journal of Technology and Intellectual Property*, 19, 4, 325-363.

[32] Pertanto, il trattamento dei dati personali fiscali (e non solo) a fini di indagine ed accertamento tributari – anche con specifico riferimento all'applicazione di tecniche di elaborazione di intelligenza artificiale – ed i riflessi in materia di tutela dei dati personali, costituisce un ambito di evidente interesse (ai nostri fini); in letterature, cfr. Francioso C. (2023)., "Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela", in *Rassegna tributaria*, 1, 47-94; Farri F. (2020), "Digitalizzazione dell'amministrazione finanziaria e diritti dei contribuenti", in *Rivista di diritto tributario*, 6, 115-139; Santoro A. (2019), *Nuove frontiere per l'efficienza dell'amministrazione fiscale: tra analisi del rischio e problemi di privacy*, in Arachi G. e Baldini M. (eds.), *La finanza pubblica italiana. Rapporto 2019*, Bologna, 66 ss.; Ragucci G. (2019), "L'analisi del rischio di evasione in base ai dati dell'archivio dei rapporti con gli intermediari finanziari: prove generali dell'accertamento "algoritmico"?", in *Riv. tel. dir. trib.*, disponibile al sito https://shorturl.at/vFOQ4 (5.5.2023); Marcheselli A., Ronco S. (2022), "Dati personali, Regolamento GDPR e indagini dell'Amministrazione finanziaria: un modello moderno di tutela dei diritti fondamentali?", in *Rivista di diritto tributario*, I, 97 ss.; G. Pitruzzella, "Dati fiscali e diritti fondamentali", cit.; Carinci A. (2019), "Fisco e privacy: storia infinita di un apparente ossimoro", in *Fisco (Il)*, 46, 4407 ss.

[33] Cfr. l'art. 11, comma 2 del d.l. 201/2011, che richiama i rapporti finanziari di cui all'articolo 7, sesto comma del d.p.r. 605/1973.

[34] Cfr. l'art. 11, comma 4 del d.l. 201/2011, nel testo convertito in legge (l. n. 214 del 22 dicembre 2011).

2.1. L'acquisizione dei dati all'Anagrafe dei tributi

Un primo profilo riguarda gli aspetti del trattamento in questione che attengono all'acquisizione dei dati alla banca dati di destinazione (l'*Anagrafe dei rapporti finanziari*). Nel primo parere[35] espresso dal Garante sulla prima bozza di provvedimento attuativo del Direttore dell'Agenzia delle Entrate, il Garante formula numerose osservazioni (e riserve).

Una prima (di carattere generale) riguarda la preoccupazione in "riferimento all'eccezionale concentrazione presso l'anagrafe tributaria di un'enorme quantità di informazioni personali"; a questo proposito, il Garante formula dei dubbi circa "l'integrale acquisizione e duplicazione presso l'anagrafe tributaria di una moltitudine di dati che, laddove necessari a fini di accertamento, risultano già disponibili all'amministrazione finanziaria attraverso la procedura delle indagini finanziarie che consente la puntuale e dettagliata acquisizione di tutte le informazioni finanziarie dei contribuenti", mentre invece "secondo le valutazioni effettuate dall'Agenzia, tali dati sarebbero tutti necessari ai fini dell'elaborazione con procedure centralizzate". Come si vede, ciò che viene messo in dubbio è il profilo di *necessarietà* del trattamento consistente nella raccolta a fini di *centralizzazione* del patrimonio informativo. Si noti che tale profilo, oggetto di osservazione, risultava già esplicitato e coperto sul piano normativo quanto al *modello di trattamento*, dal momento che è proprio la disposizione legislativa a stabilire che le informazioni così acquisite, insieme a quelle già raccolte e gestite nell'Anagrafe tributaria "sono utilizzate dall'Agenzia delle Entrate per l'elaborazione con procedure centralizzate, secondo i criteri individuati con provvedimento del Direttore della medesima Agenzia, di specifiche liste selettive di contribuenti a maggior rischio di evasione". In altri termini, il parere del Garante non fa che sottolineare (a più riprese) la circostanza per cui la *espressa previsione legislativa* di una determinata modalità di trattamento (in questo caso, l'acquisizione e la centralizzazione delle informazioni in questione) non comporta, di per sé sola, la soddisfazione del requisito di *necessarietà*; anzi, le considerazioni espresse dal Garante confermano come la legittimazione mediante previsione legislativa espressa risponde ad una logica *non coincidente* e, quindi, *alternativa* rispetto a quella che è propria del nesso di strumentalità necessaria. Si tratta di un elemento di riflessione prezioso, sul quale sarà utile e necessario tornare nelle nostre conclusioni.

Una seconda osservazione attiene invece ai profili di sicurezza connessi alla raccolta periodica (presso gli operatori finanziari) delle informazioni per poter procedere alla loro trasmissione all'Anagrafe, nonché ai canali utilizzati

[35] Cfr. il parere n. 145 del 17 aprile 2012, doc. web n. 1886775.

per effettuare tali trasmissione; anche qui il Garante formula molte e dettagliate osservazioni, sottolineando i profili di rischio connessi a ciascun passaggio, ed analizzando anche le caratteristiche tecniche delle applicazioni allora in uso per la trasmissione dei dati dagli operatori finanziari all'Anagrafe tributaria. Con la tecnica del parere favorevole, ma condizionato, il Garante formula così significative richieste di modifica ed integrazione dello schema di provvedimento. Questo secondo ordine di considerazioni risponde, invero, ad una precisa indicazione dello stesso legislatore, che aveva demandato al provvedimento di attuazione dell'Agenzia delle Entrate, previo parere del Garante, di stabilire "le modalità della comunicazione (…)" e di "prevedere adeguate misure di sicurezza, di natura tecnica e organizzativa, per la trasmissione dei dati e per la relativa conservazione". In questo senso, il parere del Garante opera nel senso di assicurare una verifica preventiva del parametro fissato con legge e che i provvedimenti dell'amministrazione sono chiamati ad integrare.

2.2. La tipologia di trattamento

Segue, per iniziativa della stessa amministrazione titolare del trattamento, un periodo di sperimentazione, durante il quale le tecniche di analisi sono testate su un ristretto campione di contribuenti, prima relativamente all'anno fiscale 2013, sperimentazione poi estesa al 2014 e 2015. I dati utilizzati per testare l'efficacia del nuovo modello di analisi erano quelli contenuti nell'Archivio dei rapporti finanziari[36] (come alimentato con le nuove informazioni raccolte in base al d.l. 201/2011), unitamente ai redditi e alle spese desumibili dalle informazioni contenute nell'Anagrafe tributaria. Durante questo periodo è proseguito il dialogo tra amministrazione titolare del trattamento e Garante, in ordine agli aspetti di sicurezza e tutela dei diritti degli interessati,

[36] L'Archivio dei rapporti finanziari è una sezione dell'Anagrafe tributaria che contiene informazioni: (i) sui conti correnti e gli altri rapporti finanziari del contribuente o a sua disposizione in virtù di deleghe o procure (parte anagrafica); (ii) sulle relative movimentazioni contabili in forma aggregata; sul saldo iniziale e finale; per alcune tipologie di conto, anche sulla giacenza media annua; e, infine, sulle eventuali operazioni effettuate al di fuori di un rapporto continuativo con l'intermediario (parte contabile). Istituito nel 1991, limitatamente alla parte anagrafica, e ampliato nel 2011 con la sezione contabile, l'Archivio avrebbe dovuto rendere più efficiente l'attività di controllo sulle imposte dirette e l'Iva, ma la sua attuazione è stata piuttosto travagliata", (cfr. Francioso C. (2023)., Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela", cit., par. 3.3); un travaglio complesso, anche in ragione delle obiezioni sollevate dal Garante con riferimento agli atti secondari di attuazioni di cui ci occupiamo subito di seguito (ma vedi anche Santoro A. (2019), *Nuove frontiere per l'efficienza dell'amministrazione fiscale: tra analisi del rischio e problemi di privacy*, cit.).

senza però che gli esiti della fase di sperimentazione si traducessero in applicativo operante "a regime". Per "sbloccare" la situazione si assiste ad uno *scatto in avanti*, che è connotato dall'integrazione legislativa della base giuridica del trattamento, operata nella legge di bilancio per il 2020. Si tratta di un passaggio significativo, ai nostri fini. Poiché l'intenzione è quella di allargare il novero delle basi di dati sui quali svolgere le indagini, anche al fine di applicare un *set* ulteriore e più ampio di tecniche analitiche (su cui, vedi subito *infra*), in vigenza della *strict legality rule* (siamo alla fine 2019) si rende indispensabile un aggiornamento del quadro normativo, sia per immettere nel trattamento le nuove basi di dati, sia per aggiornare la finalità di trattamento. Sotto il primo profilo, la nuova disposizione annette all'analisi finalizzata alla selezione dei profili "le altre banche dati" dell'Agenzia delle Entrate; sotto il secondo profilo, la stessa disposizione aggiunge alla finalità di "individuare criteri di rischio utili per far emergere posizioni da sottoporre a controllo" quella di "incentivare l'adempimento spontaneo"[37]. Per altro, già in precedenza il quadro legislativo pertinente era stato oggetto di integrazione, al fine di indicare in modo espresso ulteriori finalità per il trattamento dei dati di cui all'Anagrafe tributaria[38]. Notevole è pure l'indicazione in legge della possibilità di ricorrere alla *pseudonimizzazione*, quale misura di attenuazione dei rischi connessi al trattamento. Anche in questa scelta si leggono bene gli effetti di un regime ispirato alla *strict legality rule*: l'attrazione alla fonte legislativa di opzioni (certamente importanti) che ben potrebbero essere operate in sedi differenti (in applicazione dei criteri già formulati dal GDPR, a cominciare dal principio di minimizzazione).

[37] Cfr. l'art. 1, comma 682 della l. 27 dicembre 2019, n. 160, ai sensi del quale "Per le attività di analisi del rischio di cui all'articolo 11, comma 4, del decreto-legge 6 dicembre 2011, n. 201 (…) con riferimento all'utilizzo dei dati contenuti nell'archivio dei rapporti finanziari (…) l'Agenzia delle Entrate, anche previa pseudonimizzazione dei dati personali, si avvale delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui dispone, allo scopo di individuare criteri di rischio utili per far emergere posizioni da sottoporre a controllo e incentivare l'adempimento spontaneo".

[38] Cfr. l'art. 11, comma 4 del d.l. n. 201/2011 come integrato dal d.l. 6 luglio 2012, n. 95 conv. in l. 7 agosto 2012, n. 135, "Le medesime informazioni sono altresì utilizzate ai fini della semplificazione degli adempimenti dei cittadini in merito alla compilazione della dichiarazione sostitutiva unica di cui all'articolo 4 del decreto legislativo 31 marzo 1998, n. 109, nonché in sede di controllo sulla veridicità dei dati dichiarati nella medesima dichiarazione".

2.3. Machine learning*, conoscenza aggiuntiva e tutela dei dati personali*

La formulazione dei *criteri di analisi* mediante i quali individuare i contribuenti che presentino indicazioni di rischio più elevato di evasione/elusione, così da indirizzare in modo più mirato e consistente le attività di controllo e di accertamento, ha rappresentato a lungo il principale elemento di "dissidio" tra l'Agenzia delle Entrate e il Garante, come emerge in controluce dalla sequenza e dalla lettura dei pareri di quest'ultimo, oltre che dalla letteratura. Si tratta di un dissidio che ha ragioni di carattere strutturale, che riflette in modo particolarmente significativo una delle principali *impasse* cui è esposta la disciplina di tutela dei dati personali, quando è posta a confronto con uno dei paradigmi conoscitivi che caratterizzano alcune tecniche di elaborazione basate sul *machine learning*. Infatti, nella misura in cui finalità del trattamento e minimizzazione costituiscono principi cardine della tutela dei dati personali, essi entrano in collisione (forse irrimediabile) con quelle tecniche di acquisizione di conoscenza *nuova*, perché aggiuntiva ed inaspettata, realizzata mediante gli *algoritmi di machine learning*; queste sono metodologie di analisi connotate dalla capacità di far emergere, evidenziare, identificare delle correlazioni *non immediatamente evidenti*, e *non scontate* tra diversi elementi informativi (elementi che più sono numerosi e diversificati, meglio rispondono alle esigenze funzionali di queste tecniche analitica: c.d. *big data analysis*). Dal nostro angolo di osservazione, ciò comporta che la conoscenza *aggiuntiva* è un *prodotto*, un *output* di questo processo analitico, che non può essere *preventivato*, predeterminato. Né con riferimento alla possibilità di stabilire *ex ante* quali tipologie, quantità, varietà di dati risultano utili all'evidenziazione di una certa correlazione significativa; né con riferimento (pertanto) alla finalità per la quale quel dato trattamento risulterà utile, strumentale, necessario[39].

[39] In dottrina, questa "incompatibilità" tra le tecniche di elaborazione dei *big data* basate sul *machine learning* (ed in particolare, sul *deep learning* non supervisionato) è stata variamente evidenziata, cfr. Zarsky T. (2017), "Incompatible: The GDPR in the Age of Big Data", in *Seton Hall Law Review*, 47, 4(2), https://ssrn.com/abstract=3022646 (01.04.2023); Froomkin A. M. (2019), "Big Data: Destroyer of Informed Consent", in *Yale Journal of Health Policy, Law, and Ethics*, https://ssrn.com/abstract=3405482_ (01.04.2023); Hahn I. (2021), "Purpose Limitation in the Time of Data Power: Is There a Way Forward?", in *European Data Protection Law Review*, 7, 1, 31-44; Cate F.H., e Mayer-Schönberger V. (2013), "Notice and consent in a world of Big Data", in *International Data Privacy Law*, 3, 67-73; Hildebrandt M. (2013), "Slaves to Big Data. Or Are We?", in *IDP: revista d'Internet, dret i política*, 17, 27-44; D'Ippolito G. (2018), "Il principio di limitazione delle finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data", in *Il diritto dell'informazione e dell'informatica*, n. 6, 943-987.

I segni di questa intima contraddizione si rintracciano già nel primo parere emesso dal Garante, il cui oggetto erano (per la verità) soltanto gli aspetti relativi all'acquisizione dei dati rapporti finanziari all'Anagrafe tributaria.

Alla luce di quanto stabilito nello schema, infatti, la raccolta di tali dati riferiti alla totalità dei contribuenti è finalizzata unicamente all'elaborazione con procedure centralizzate delle liste selettive di contribuenti a maggior rischio di evasione, secondo i criteri che dovranno essere successivamente individuati con provvedimento del Direttore dell'Agenzia (art. 11, comma 4, del citato decreto-legge). Le posizioni, così individuate, saranno segnalate per l'avvio delle attività di controllo fiscale.

Al riguardo, il parere sottolinea che *l'individuazione di criteri astratti volti ad analizzare il comportamento del contribuente*, soprattutto laddove effettuati sulla base di numerose tipologie di dati presenti in anagrafe tributaria, presenta rischi specifici per i diritti fondamentali e la libertà, nonché la dignità degli interessati, che richiedono la previsione di adeguate garanzie, fermo restando il divieto di adottare atti o provvedimenti amministrativi fondati unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato (artt. 14 e 17 del Codice).

Nell'occasione dell'espressione del parere, pertanto, considerati i predetti rischi che comporta una *siffatta attività di classificazione del contribuente*, *il Garante ritiene necessario che l'Agenzia gli sottoponga, ai fini di una verifica preliminare, il provvedimento del Direttore dell'Agenzia delle Entrate con il quale vengono definiti i criteri per l'elaborazione delle liste* al fine di individuare eventuali misure e accorgimenti idonei a garantire l'applicazione dei principi in materia di protezione dei dati personali (artt. 14 e 17 del Codice), fermo restando l'obbligo di notificazione al Garante ai sensi dell'art. 37, comma 1, lett. d), del Codice.[40]

Dunque il Garante chiede all'Agenzia di conoscere, una volta che li avrà elaborati, i criteri mediante i quali procederà a selezionare le liste di contribuenti con profilo di rischio maggiore, per poterli sottoporre a verifica preliminare. In questa richiesta, oltre a un fraintendimento relativo alla tipologia strumento istruttorio che si intende elaborare[41], è espressa la volontà di ope-

[40] Cfr. il parere n. 145 del 17 aprile 2012, doc. web n. 1886775, punto E), corsivi aggiunti.

[41] Nel considerare criticamente l'opzione della raccolta dei dati, lo stesso parere aveva stigmatizzato la "duplicazione presso l'anagrafe tributaria di una moltitudine di dati che, laddove necessari a fini di accertamento, risultano già disponibili all'amministrazione finanziaria attraverso la procedura delle indagini finanziarie che consente la puntuale e dettagliata acquisizione di tutte le informazioni finanziarie dei contribuenti"; un passaggio nel quale si scorge un'aporia logica. Infatti, se l'analisi dei dati serve a capire quando e dove fare l'indagine, non può evidentemente svolta mediante degli strumenti utilizzabili solo *nell'ambito di una indagine già in essere*; così Santoro A. (2019), "Più che i pagamenti elettronici serve il profilo dell'evasore", in *lavoce.info*, 24.09.2019, disponibile al sito: https://lavoce.info consultata il 5 maggio 2023.

rare un controllo sulle logiche applicate all'elaborazione, così da poter verificare il rispetto dei principi del trattamento, quali minimizzazione e finalità del trattamento, a tutela dei diritti fondamentali degli interessati. Questa richiesta continuerà ad essere ribadita in tutte le successive occasioni di interlocuzione con l'Agenzia delle Entrate, nel corso dello sviluppo progressivo della sperimentazione[42], segno che a questa domanda il Garante non ha mai ottenuto una risposta. La ragione di questa mancata risposta sta proprio nel fatto che l'applicazione delle tecniche di *deep learning* sono incompatibili con l'applicare i criteri di minimizzazione dei dati e di limitazione delle finalità del trattamento, dal momento che il criterio di selezione resta in gran parte *opaco*, come anche il peso ed il ruolo che ciascun dato in *input* ha giocato in funzione della conoscenza abilitata dall'*output*.

Non è dunque casuale che, una volta chiarito ed esplicitato questo punto – ciò che è avvenuto nel contesto del "rilancio" avvenuto con la l. n. 160/2019, con l'impostazione dei nuovi criteri di analisi, e l'ampliamento delle basi di dati oggetto di trattamento mediante espressa disposizione legislativa – il Garante abbia smesso di porre la domanda, prendendo atto – piuttosto – che quel modello conoscitivo così applicato "consente di calcolare degli indicatori di rischio fiscale – *anche non noti a priori*"[43]. Le "misure da adottare" per gestire, escludere o mitigare i rischi cui sono esposti gli interessati non posso essere valutate a priori, ma "devono essere valutate in concreto, vale a dire tenendo in considerazione le caratteristiche delle banche dati di volta in volta utilizzate e i modelli di analisi impiegati"; e pertanto "è necessario che l'Agenzia verifichi e documenti, nel rispetto del principio di *accountability*, le scelte effettuate in ordine all'individuazione delle banche dati utilizzate per la creazione del *dataset* di analisi e dei modelli di analisi

[42] Cfr. il parere n. 861 del 15 novembre 2012 [doc. web n. 2099774]; n. 321 del 20 luglio 2017 [doc. web n. 6843736]; n. 58 del 14 marzo 2019 [doc. web n. 9106329].

[43] Cfr. il provvedimento n. 276 del 30 luglio 2022, avente ad oggetto la *Valutazione di impatto sulla protezione dati relativa al trattamento "Analizzare rischi e fenomeni evasivi/elusivi tramite l'utilizzo dei dati contenuti nell'Archivio dei rapporti finanziari e l'incrocio degli stessi con le altre banche dati di cui dispone l'Agenzia delle entrate"- Articolo 1, comma 684, della legge 27 dicembre 2019, n. 160 - 30 luglio 2022*, [doc. web n. 9808839], dove viene chiarito che il trattamento è condotto sulla base di un'"analisi stocastica", una "tecnica di analisi che, sfruttando algoritmi supervisionati e non supervisionati di modellazione statistica e *machine learning*, consente di calcolare degli indicatori di rischio fiscale - *anche non noti a priori* - che possono: a) fungere da input per l'analisi deterministica; b) essere utilizzati per ridurre la platea di riferimento per le analisi deterministiche, individuando i soggetti che presentano caratteristiche di particolare anomalia; b) essere usati per graduare il livello di rischiosità fiscale dei contribuenti presenti nel data set di controllo; c) misurare preventivamente, attraverso l'impiego di opportune tecniche, il livello di accuratezza delle analisi, riducendo in tal modo l'incertezza dei risultati, e, pertanto, la probabilità di selezionare falsi positivi", punto 2.

impiegati, comprovando di aver adeguatamente individuato e gestito i rischi per i diritti e le libertà degli interessati"[44].

Lo *standard di legalità* si è così già spostato da una verifica *a priori* (coerente con un modello di legalità in cui la garanzia è attratta e dislocata nella base giuridica) ad una *a posteriori*, nella quale gioca un ruolo essenziale il principio di *accountability* (ed il confronto continuo, analitico, *caso per caso*, con il contesto operativo rilevante). E, in effetti, questi ultimi pareri del Garante sono già successivi al cambio di regime realizzato nel 2021.

2.4. L'allentamento del regime di trattamento dei dati e la messa a regime dello strumento di data analysis *per il contrasto dell'evasione*

Nella tarda primavera del 2022, il sistema di verifica dei rapporti finanziari (Ve.R.A. nell'acronimo utilizzato nella circolare dell'Agenzia delle Entrate) esce finalmente dalla fase di sperimentazione, per diventare *a regime* uno strumento di supporto istruttorio[45] alle attività di controllo dell'evasione[46]. Non è affatto casuale che il passaggio dalla fase di sperimentazione a

[44] Cfr. *ivi*, punto 4.

[45] La dottrina è particolarmente attenta nel sottolineare come dall'effettiva caratterizzazione dello strumento in termini di *supporto istruttorio* (e non invece di implicita ed *immediata* decisione di accertamento), passi la preservazione di un indispensabile e corretto bilanciamento con le esigenze di tutela dei diritti del contribuente, e nell'evidenziare i rischi connessi al superamento di questa di questa caratterizzazione: cfr. Francioso C. (2023)., "Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela", cit.; Farri F. (2020), "Digitalizzazione dell'amministrazione finanziaria e diritti dei contribuenti, cit.; Marcheselli A., Ronco S. (2022), "Dati personali, Regolamento GDPR e indagini dell'Amministrazione finanziaria: un modello moderno di tutela dei diritti fondamentali?", cit. In effetti, lo stesso Garante ha evidenziato il rischio che i funzionari delle Direzioni regionali, che potrebbero integrare l'analisi ricevuta, possano «ritenere più prudente non opporsi alle risultanze dei sistemi algoritmici» (cfr. provv. n. 276 del 30 luglio 2022, cit.), così da vanificare il meccanismo (sancito anche dall'art. 22 del GDPR) del contributo dell'agente umano (secondo l'approccio dello *human-in-the-loop*); in dottrina, tuttavia, si sottolinea che anche la stessa generazione delle liste di contribuenti "a rischio" è da attribuirsi a procedure non integralmente automatizzate, ma che vedono il contributo di funzionari specificamente formati per interagire con l'insieme di applicativi da cui è costituito il sistema Ve.R.A.; cfr. Didimo W., Grilli L., Liotta G., e Montecchiani F. (2022), "Processi decisionali efficienti e affidabili tramite analisi visuale con metodologia human-in-the-loop: un caso di studio sulla valutazione del rischio fiscale". in *Rivista Italiana Di Informatica E Diritto*, 4(2), 15-21; disponibile all'indirizzo: https://doi.org/10.32091/RIID0092 (01.3.2023).

[46] Come si legge nella circolare n. 21/e del 20 giugno 2022, "l'analisi del rischio di evasione basata sui dati dell'Archivio dei rapporti (…) sarà potenziata mediante l'elaborazione, a cura del Settore Analisi del rischio e ricerche per la *tax compliance* della Divisione Contribuenti, di nuove liste selettive per l'attività di controllo, che saranno rese disponibili mediante

quella operativa vera e propria maturi successivamente all'introduzione delle modifiche al Codice che hanno "allentato" la *strict legality rule*, nella direzione di dotare le amministrazioni di margini di autonoma iniziativa nell'implementare sistemi di trattamento dei dati personali strumentali all'esercizio delle funzioni istituzionali. La tempistica delle interlocuzioni intrattenute con il Garante lo conferma. Lo schema di decreto attuativo dell'art. 1, comma 683 della l. n. 160/2019 è sottoposto al parere del Garante il giorno 15 novembre 2021, cioè dopo l'adozione del decreto «capienze», mentre il parere del Garante è del 22 dicembre, data successiva alla conversione in legge di tale decreto. Il provvedimento è chiamato a definire aspetti cruciali del trattamento, ovvero: a) le specifiche limitazioni e le modalità di esercizio dei diritti di cui agli articoli 14, 15, 17, 18 e 21 del regolamento (UE) 2016/679, in modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto all'obiettivo di interesse pubblico; b) le disposizioni specifiche relative al contenuto minimo essenziale di cui all'articolo 23, paragrafo 2, del regolamento (UE) 2016/679; c) le misure adeguate a tutela dei diritti e delle libertà degli interessati. Anche in questo caso, il Garante adotta un parere favorevole, condizionato tuttavia al rispetto di una serie significativa di indicazioni[47]. Tuttavia, nel nuovo quadro giuridico, tale interlocuzione non attiva (come sarebbe stato necessario, in precedenza) la necessità di "passare" anche per il legislatore, così adeguare il parametro normativo[48]. L'accento è ora posto sull'autonoma iniziativa dell'amministrazione titolare del trattamento, e sulla sua capacità di *rendere conto* (*accountability*) del rispetto dei principi del regolamento (strumentalità necessaria, limitazione

l'applicativo Ve.R.A. Gli elenchi elaborati a livello centrale, mediante specifici criteri di rischio basati sull'utilizzo integrato delle informazioni comunicate dagli operatori finanziari all'Archivio dei rapporti finanziari e degli altri elementi presenti in Anagrafe tributaria, permetteranno a ciascuna Direzione regionale e provinciale di indirizzare l'ordinaria attività di controllo nei confronti delle posizioni a più elevato rischio di evasione, previa autonoma valutazione della proficuità comparata", 25; cfr. Francioso C. (2023)., "Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela", cit., e Conigliaro M. (2022), "Lotta all'evasione con l'intelligenza artificiale 'Ve.R.A.'", in *Fisco (Il)*, 32/33, 3107 ss.

[47] Cfr. il parere n. 453 del 22 dicembre 2021, [doc. web n. 9738520]: le condizioni *ivi* indicate attengono sostanzialmente a tutti i punti disciplinati dal decreto, ovvero: l'individuazione delle categorie di trattamenti e di dati personali oggetto delle limitazioni; la trasparenza del trattamento e gli obblighi informativi nei confronti degli interessati; il diritto di accesso; il diritto di limitazione di trattamento; le misure a tutela dei diritti e delle libertà degli interessati.

[48] Per una analoga ricostruzione dell'impatto prodotto dalle modifiche del Codice privacy e sul conseguente "via libera" sistema di analisi del rischio di evasione Ve.R.A., cfr. Francioso C. (2023)., "Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela", cit. "Con il provvedimento del 22 dicembre 2021 e la valutazione d'impatto del 30 luglio 2022, il Garante *ha finalmente autorizzato il trattamento dei dati personali con il nuovo strumento algoritmico di analisi del rischio fiscale*, seppur fra varie riserve e raccomandazioni" (*ivi*, par. 1, corsivo aggiunto).

della finalità del trattamento, minimizzazione, trasparenza, etc.) in un rapporto diretto con l'autorità di garanzia; quest'ultima opera in funzione di verifica, *in itinere* ed *ex post*, ma non anche in funzione di autorizzazione (*ex ante*). Una prima conferma significativa di questo mutato rapporto l'abbiamo già osservata: i criteri di selezione (elaborati mediante soluzioni di *machine learning*) non devono essere espressi, notificati e conosciuti in via preventiva (anche quando questo risulti impossibile da realizzarsi), ma piuttosto verificati ed eventualmente corretti (nella loro efficacia e negli eventuali effetti pregiudizievoli) sulla base di un *assessment* continuo. Il mutamento nella dinamica dei rapporti è anche ben rappresentato dal successivo passaggio procedurale (anche questo, già previsto dall'art. 1, comma 684 della l. n. 160/2020), ovvero la realizzazione da parte del titolare del trattamento di una "valutazione unitaria di impatto sulla protezione del dati", sentito il Garante. La valutazione è stata presentata al Garante il 18 maggio 2022, e successivamente integrata – sulla base delle interlocuzioni intercorse – in data 14 e 27 luglio 2022. Il parere del Garante è stato poi adottato il 30 luglio, sulla base di una procedura d'urgenza[49]. I tempi, dunque, sono dettati dall'amministrazione (in base alla più forte autonomia di iniziativa acquisita nel nuovo quadro giuridico disegnata dal decreto «capienze»), ed il Garante è interessato a intervenire tempestivamente nel procedimento, così da assicurare che la valutazione di impatto possa essere adottata, in ossequio al principio di responsabilizzazione (con tutte le conseguenze del caso).

Anche con riferimento a questo secondo caso di studio, è stato possibile osservare alcuni effetti determinati dal quadro normativo che regge i criteri di legittimazione al trattamento dei dati personali per l'esercizio di compiti di interesse pubblico. Le indicazioni emerse dall'analisi sono di sicuro rilievo, con particolare (ma non esclusivo) riferimento alle relazioni che legano i diversi attori (legislatore, amministrazione titolare del trattamento, autorità di controllo) dei processi di elaborazione ed implementazione di soluzioni di trattamento dei dati personali. Nel capitolo conclusivo, cerchiamo di trarre (anche) da queste osservazioni alcune indicazioni di ordine più generale.

[49] Cfr. il provvedimento n. 276 del 30 luglio 2022, *cit*.

3. Gestione delle visite medico-fiscali e trattamento dei dati personali: il caso del modello predittivo SAVIO di INPS (terzo caso di studio)

3.1. Dalla sospensione del tool *SAVIO all'annullamento della sanzione irrogata dal Garante*

L'INPS gestisce le visite fiscali relative alla intera platea dei lavoratori dipendenti del settore privato (e di quelli del settore pubblico, a partire dal 2017[50]). L'Istituto riceve i certificati e/o gli attestati di malattia redatti dal medico curante e dispone i controlli, o d'ufficio o su richiesta del datore di lavoro. In una memoria presentata nel 2018 in audizione presso il Senato della Repubblica, l'Istituto ha indicato in circa 18 milioni/anno il numero di certificati medici ricevuti, mentre – sulla base delle risorse allora in essere – lo stesso istituto dichiarava di poter svolgere circa un milione di visite di controllo all'anno, ossia un percentuale di circa il 5 % rispetto al totale. Sin dal 2011 l'INPS si è dotata di un meccanismo di *machine learning* mediante il quale seleziona(va) i certificati medici presentati dai lavoratori per cui è risulta più opportuno predisporre controlli, in ragione della maggiore probabilità che certi eventi di malattia possano risolversi prima del previsto, ma anche in relazione alla possibilità che si verifichino comportamenti opportunistici. Il sistema, pertanto, ha la funzione di indirizzare e concentrare le visite sui casi maggiormente a rischio di abuso, così da ottimizzare l'uso delle risorse di controllo e l'efficacia dell'esercizio della relativa funzione. Secondo quanto dichiarato dall'Istituto, la valutazione circa la probabilità è fondata su indicazioni maturate nel corso del tempo (*machine learning* supervisionato). Ad esempio, si è notato che un maggior numero di idoneità a tornare al lavoro viene accertato nei giorni immediatamente precedenti o successivi il fine settimana. Di qui la scelta di sottoporre a particolare attenzione le assenze dal lavoro iniziate il venerdì o il lunedì. Altre informazioni rilevanti nel decidere come indirizzare le visite dei medici fiscali sono, alla luce dell'esperienza passata, quelle legate alla dimensione ed attività economica dell'azienda di appartenenza, alla durata della malattia, al tipo di rapporto di lavoro, alla qualifica e importo della retribuzione giornaliera, al numero di certificati degli ultimi due anni, al numero di precedenti visite concluse con idoneità, etc.[51]

[50] Cfr. d.lgs 75/2017, che ha inserito il comma 2-bis all'articolo 55-septies del d.lgs.165/2001.

[51] Cfr. il testo dell'Audizione del Presidente Inps, Boeri, *Visite mediche di controllo d'ufficio – metodologie di* data mining *– procedimento sanzionatorio del Garante per la protezione dei dati personali*, 6 settembre 2018, presso la XI Commissione permanente lavoro pubblico e privato, previdenza sociale del Senato.

Tale sistema di supporto istruttorio, denominato "SAVIO", è stato sospeso a seguito di una istruttoria del Garante privacy, in ragione della contrarietà rispetto al Codice; il Garante ha anche adottato nei confronti di INPS un'ordinanza di ingiunzione, per il pagamento di una sanzione amministrativa pari a 40.000 euro. Nell'atto di ingiunzione, il Garante riconosce che il trattamento risponde alle esigenze connesse alle disposizioni che affidano ad INPS i compiti di disporre le visite domiciliari di controllo dei lavoratori assenti dal servizio per malattia, e che introducono la trasmissione telematica delle certificazioni di malattia sia per il settore pubblico che privato. Tuttavia, nella normativa il trattamento in questione non è previsto, né con riferimento alle operazioni eseguibili, né con riferimento alle tipologie di dati trattati (tra cui, anche dati sensibili). Pertanto, in assenza di tale esplicita previsione, secondo il Garante il trattamento in questione appare realizzato in violazione dell'art. 20 del Codice (allora ancora vigente). Inoltre, il dispositivo SAVIO è stato ritenuto un procedimento integralmente automatizzato, che configurava una vera e propria profilazione, e quindi posto in essere in violazione sia dell'art. 14 del Codice, sia dell'art. 37 (mancata notifica al Garante). Infine, con riferimento al trattamento di dati sensibili, è stata constatata la violazione dell'obbligo di informativa di cui all'art. 22, comma 2[52]. Le contestazioni del Garante sembrano condivisibili quanto ai profili di legittimazione al trattamento di cui all'art. 20 del Codice. In effetti, la disciplina vigente (pre-d.lgs. 101/2018) era conformata sul modello della *strict legality rule*, quando ad essere trattati ci fossero anche dati sensibili (come pare il caso in questione, quantomeno con riferimento alla presentazione del certificato medico). Non del tutto persuasive risultavano, invece, le censure fondate sull'art. 14, in quanto gli atti ed i provvedimenti adottati da INPS non si basavano unicamente sul *trattamento automatizzato*: le indicazioni fornite dal sistema si inseriscono in un procedimento nel quale, a valle, l'intervento umano ricorre a più riprese (decisione su come utilizzare le indicazioni circa i certificati da verificare, effettuazione del controllo, assunzione delle decisioni conseguenti). Perplessa è anche la qualificazione dello "score" attribuito a ciascun certificato sottoposto al trattamento in termini di *profilazione*: le considerazioni fattuali formulate dal titolare del trattamento

[52] "Tale trattamento, che non risulta essere stato sottoposto a verifica preliminare ai sensi dell'art. 17 del Codice, è stato effettuato in base a norme che, nonostante riconoscano l'obbligo di disporre delle visite domiciliari di controllo dei lavoratori assenti dal servizio per malattia e introducano la trasmissione telematica delle certificazioni di malattia sia per il settore pubblico che privato, non dispongono nulla in merito ai tipi di dati e alle operazioni eseguibili nell'ambito del trattamento automatizzato in argomento, quindi in violazione di quanto statuito dagli artt. 14 e 20 del Codice in materia di protezione dei dati personali, provv. n. 492 del 29 novembre 2018 [doc. web n. 9078812].

(sia in sede di istruttoria che, successivamente, in sede di giudizio sull'ingiunzione), ed in particolare la circostanza per cui diversi certificati presentati dallo stesso lavoratore possono ricevere *score* anche molto diversi tra loro – dal momento che tali punteggi sono funzionali non a classificare il comportamento di una certa persona entro una determinata classe di comportamenti, ma piuttosto ad assegnare un valore al rischio di abuso allo specifico certificato – non appaiono del tutto prive di fondamento. In ogni caso, ciò che importa notare è che, in vigenza della *strict legality rule*, la mancata esplicitazione in legge del tipo di operazioni e del tipo di dati oggetto di trattamento ha comportato certamente la carenza di base di legittimazione a trattare dati personali sensibili.

L'impossibilità di impiegare lo strumento SAVIO ha determinato, ad avviso di INPS, ricadute significative sull'efficienza e l'efficacia nell'esercizio dei compiti di controllo sulle assenze per malattia, che l'Istituto ha anche stimato, sia in termini di perdita di efficacia del controllo, sia in termini di valore delle giornate lavoro non retribuite in esito alla conferma d'idoneità al lavoro dei pazienti visitati[53]. Anche sulla base di queste considerazioni, l'Istituto, in audizione in Senato, ha proposto di risolvere l'*impasse* determinata a seguito dei provvedimenti del Garante mediante l'adozione di una disposizione legislativa atta ad autorizzare il trattamento in questione[54].

Respinto dal Tribunale di Roma il ricorso avverso l'ordinanza-ingiunzione con sentenza del 3 marzo 2020, n. 4609, l'Istituto ha fatto ricorso per Cassazione. In tale sede, con ordinanza n. 6177/2023 la Cassazione ha ribaltato tale giudizio ed annullato l'ingiunzione[55]. I motivi che hanno indotto la Suprema Corte a ribaltare la sentenza di merito sono molto interessanti, sebbene non tutti pienamente persuasivi. In particolare, il passaggio meno convincente è quello che ritiene lecito il trattamento realizzato mediante il *tool* SAVIO in quanto tale trattamento è giudicato *necessario per adempiere a un obbligo previsto dalla legge*, e come tale inquadrabile nella fattispecie di legittimazione al trattamento di cui all'art. 24, comma 1, lett. a) del Codice. Questa interpretazione, tuttavia, non tiene conto del fatto che la disposizione in questione ha un ambito soggettivo di applicazione che si riferisce ai soggetti privati e agli enti pubblici economici, mentre (condivisibilmente) l'ingiunzione del Garante aveva considerato il trattamento come funzionale

[53] Cfr. Boscarino, R., Di Porto E., e Naticchioni P. (2018), "SAVIO Shut Down: Effetti sulle Visite Mediche di Controllo", *INPS DCSR Studi e Analisi*, Nota n. 2.

[54] A tale scopo, nella Memoria presentata alla XI Commissione permanente lavoro pubblico e privato, previdenza sociale del Senato nel settembre del 2018, il presidente dell'Istituto ha anche formulato una esplicita proposta di disposto legislativo.

[55] Cass. civ. Sez. I, Ord., 1°marzo 2023, n. 6177.

all'esercizio di compiti di interesse pubblico (posti in essere da un ente pubblico *non economico*, e quindi ente pubblico *tout court*) e pertanto, in ragione del coinvolgimento di dati sensibili, lo aveva ricondotto alla fattispecie di cui all'art. 20 del Codice. Inoltre, la (indebita) sovrapposizione/confusione effettuata tra esecuzione di compiti di interesse pubblico e adempito di obblighi previsti dalla legge, consente al giudice di ritenere *non dovuta* l'informativa agli interessati, sulla base di quanto disposto dall'art. 13, comma 5, lett. a) del Codice[56].

Più persuasivi i passaggi in cui il giudice sottolinea che il trattamento in questione non sia da valutarsi come esclusivamente automatizzato, mentre in riferimento alla connotazione di tale trattamento nei termini di una *profilazione*, la valutazione (che la esclude) appare invischiata in questioni di diritto intertemporale (dovendosi confrontare con nozioni di profilazione mutevoli, nel succedersi del regime del GDPR a quello previgente, formato da direttiva e legge nazionale di recepimento); così come persuasivo è il passaggio che individua nei compiti svolti dall'Istituto in materia di controllo delle assenze per malattia, un trattamento "necessario per adempiere a specifici obblighi o compiti previsti dalla legge (...) in materia di (...) di previdenza e assistenza", così come previsto dall'art. 68 del Codice.

In ogni caso, le considerazioni svolte dalla Cassazione sono di grande interesse, quantomeno sotto due distinti (ma connessi) profili. Per un verso, la Cassazione sottolinea il ruolo che la digitalizzazione è in condizione di svolgere per assicurare un esercizio più efficiente ed efficace dell'azione amministrativa, in linea con il canone del buon andamento e della trasparenza di cui all'art. 97 Cost., al punto da considerare il ricorso a certe modalità di trattamento (ivi compresi la *big data analytics* e il *machine learning*) come una opzione oramai necessitata, che si impone alla stessa amministrazione[57].

[56] La disposizione in questione, nel caso in cui i dati trattati non siano raccolti presso l'interessato, esclude che sia dovuta l'informativa quando "i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria"

[57] "Più in dettaglio, circa l'esigenza di ricorrere ai sistemi informatici di ausilio interno ai propri compiti istituzionali, deve evidenziarsi che essa si è imposta prepotentemente anche nel nostro ordinamento (…) Per realizzare i fini di cui alla Cost., art. 97 si esige dunque l'utilizzo delle procedure informatiche, idonee ad incrementare i "beni" della celerità, efficienza, trasparenza, imparzialità e neutralità della p.a., dunque il "buon andamento". La pubblica amministrazione deve poter sfruttare le rilevanti potenzialità della c.d. rivoluzione digitale: (..) Il punto è che un più elevato livello di digitalizzazione dell'amministrazione pubblica costituisce strumento fondamentale per migliorare la qualità dei servizi resi ed espletati, proprio nell'àmbito delle procedure seriali, implicanti l'elaborazione di ingenti quantità di istanze, dove emerge, con tutta la sua forza, l'utilità di tale modalità operativa di gestione dei pubblici interessi", Cass. n. 6177/2023, punto 8.5.

In secondo luogo, proprio il fatto che il ricorso a queste soluzioni tecnologicamente caratterizzate risponde a canoni costituzionalmente imposti (a cominciare dall'art, 97 Cost.), comporta – agli occhi del giudice – la necessità di un coordinamento e di un bilanciamento con le disposizioni a tutela dei dati personali. Solo all'esito di tale bilanciamento si dovrebbe valutare l'effettiva contrarietà degli strumenti impiegati dall'amministrazione rispetto a tali disposizioni[58]. Una lettura che sembra animata dall'intento di adeguare (per via interpretativa) un quadro normativo (quello ancora in vigore fino all'adozione delle modifiche introdotte con il d.lgs. 101/2018) giudicato non del tutto adeguato ad accogliere e integrare le tecniche e le soluzioni abilitate dalla digitalizzazione nell'ambito del settore pubblico. Si ha quasi l'impressione che il giudice abbia letto le disposizioni di ieri alla luce non solo delle esigenze di innovazione *data driven* sotto il profilo organizzativo ed operativo, ma anche nella consapevolezza dei mutamenti legislativi nel frattempo venuti a maturazione, che proprio per dare ingresso a queste esigenze hanno *allentato* i vincoli legislativi e investito sull'autonoma iniziativa delle amministrazioni, ai fini della elaborazione, sperimentazione e implementazione di soluzioni basate (anche) sul trattamento dei dati personali da porre al servizio dell'esercizio di compiti di interesse pubblico.

3.2. Il tool *SAVIO alla luce del quadro giuridico abilitato dal decreto «capienze»*

La vicenda del sistema di gestione dei controlli sui certificati di malattia è istruttiva, sotto molteplici profili. In primo luogo, ci segnala come rispetto ad alcune nozioni, che si condensano all'incrocio tra disciplina giuridica e realizzazione tecnica, si sia ancora alla ricerca di un consenso condiviso circa i relativi caratteri e ambiti applicativi. Si pensi alla nozione di trattamento *non unicamente automatizzato*, di cui il Garante e la Cassazione hanno fatto un'applicazione notevolmente diversa, nel caso di specie. O, ancora, alla nozione di *profilazione*: al di là degli aspetti connessi al mutamento del quadro

[58] "questa Corte ha già rilevato che il diritto ad esigere una corretta gestione dei propri dati personali, pur se rientrante nei diritti fondamentali di cui alla Cost., art. 2, non è un 'tiranno' o un 'totem', al quale debbano sempre sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale: al contrario, le regole sulla tutela dei dati sensibili vanno coordinate e bilanciate con le disposizioni costituzionali che tutelano altri e prevalenti diritti, per quanto ora rileva l'interesse pubblico alla celerità, trasparenza ed efficacia dell'attività amministrativa. Onde stabilire se un soggetto abbia violato le regole legali sulla gestione dei dati altrui impone di interpretare queste ultime, bilanciando gli interessi da esse tutelati con gli altri interessi costituzionalmente protetti, potenzialmente in conflitto" ivi, punto 8.3.

normativo (il giudice ha espressamente fatto riferimento alla nozione di *profilazione* desumibile dal testo dell'art. 22 del Codice, allora vigente, nella consapevolezza che essa non coincide con quella poi fatta propria dal GDPR), va sottolineato che il giudice compie un'analisi molto circostanziata sia riguardo ai caratteri della *profilazione* (come fattispecie astratta disegnata dal legislatore), sia con riferimento alla specifica soluzione oggetto dell'ingiunzione del Garante. Al di là della condivisibilità o meno delle considerazioni (anche attinenti alla ricostruzione del fatto[59]) e degli argomenti svolti dal giudice, appare evidente che non si è ancora conseguito un *ubi consistam* condiviso circa l'identificazione della nozione di profilazione (o, quantomeno, della sua corretta perimetrazione *al confine*). Ciò che può dipendere anche in misura rilevante dal fatto che si tratta di nozioni giuridicamente rilevanti[60] che implicano l'applicazione di strumenti tecnicamente complessi ed in evoluzione continua. Ma dipende anche dal fatto che l'introduzione di questi strumenti è relativamente recente nell'ambito del settore pubblico italiano, e pertanto non c'è stato ancora il tempo per il consolidarsi di prassi interpretative coerenti e condivise.

Anche questa vicenda ci consente di guardare agli effetti prodotti *dallo standard legale* sulle dinamiche di sviluppo delle soluzioni di basate sul trattamento dei dati personali in ambito pubblico, traendone indicazioni molto preziose. Infatti, la vicenda in questione ci conferma come in presenza di una *strict legality rule*, l'iniziativa dell'amministrazione (per quanto giustificata

[59] Di ciò il giudice è perfettamente consapevole, tanto da sentire il bisogno di giustificare questa (a suo avviso solo apparente) incursione nell'apprezzamento delle circostanze fattuali in sede di legittimità: "Giova premettere che l'atteggiarsi delle circostanze fattuali della vicenda concreta attiene al compito del giudice del merito ed all'accertamento al medesimo riservato; mentre appartiene al giudizio di diritto se un certo comportamento, suscettibile di essere riprodotto in una serie indefinita di casi, integri - per quanto ora interessa - la fattispecie della profilazione, ai fini delle regole sul trattamento dei dati personali: invero, il giudizio se una data vicenda concreta - la cui esistenza è rimessa in via esclusiva al giudice del merito - vada sussunta sotto l'astratto paradigma legislativo è giudizio di diritto, controllabile ai sensi dell'art. 360 c.p.c., comma 1, n. 3 (*ex multis*, Cass. 12 luglio 2019, n. 18770, in motiv.). Orbene, la descritta attività non costituiva c.d. profilazione, secondo la nozione conosciuta dall'ordinamento giuridico, all'epoca dei fatti per cui è causa", *ivi*, punto n. 9.2.

[60] Rilevanti, tra l'altro, in settori legislativi diversi e di grande impatto: la nozione di profilazione assume rilievo con riferimento alla regolamentazione di alcuni aspetti dei servizi di intermediazione sulla rete offerti dalle *very large online platforms*, quali i servizi di pubblicità veicolati dalle piattaforme online, la tutela dei minori, i sistemi di raccomandazione, ai sensi del regolamento UE 2022/2065 c.d. *Digital Services Act* (cfr. i considerando nn. 56, 68-71 e 94, nonché gli artt. 26, 28 e 38); senza contare la centralità che tale nozione assume nell'ambito della emananda disciplina europea diretta a regolamentare servizi e prodotti che incorporano soluzioni di *intelligenza artificiale* (si veda la proposta di regolamento COM(2021) 206); nonché la più recente proposta di una (controversa) regolamentazione uniforme in materia di trasparenza e *targeting* della pubblicità politica.

sotto il profilo dell'efficienza e dell'efficacia) sia destinata a restare frustrata, in assenza di un previo intervento legislativo atto ad autorizzare espressamente la finalità del trattamento, i dati da utilizzare, e le operazioni di trattamento da effettuare. Ciò che è confermato non solo dal provvedimento di sospensione del servizio e di ingiunzione della sanzione adottato dal Garante (del tutto fondato, sotto questo profilo), ma anche dalla *reazione* dell'amministrazione titolare del trattamento, che in sede di audizione (vigente il precedente assetto normativo) chiedeva appunto al legislatore di intervenire, adeguando in modo puntuale il quadro legislativo, così da renderlo conforme alla *strict legality rule*, abilitando l'adozione e l'esercizio della soluzione di trattamento.

Se guardiamo invece la medesima questione con gli occhi del regime di trattamento dei dati personali a fini di esercizio di compiti di interesse pubblico così come modificato dal decreto «capienze», i termini della questione cambiano in modo significativo. Infatti, fermo restando che il trattamento è lecito *se necessario per motivi di interesse pubblico rilevante*, l'art. 2-sexies del Codice assegna ora anche ad *atti amministrativi generali adottati alla stessa amministrazione titolare del trattamento* la facoltà di 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, sulla base del regime attualmente vigente, data l'attribuzione all'Istituto dei compiti di controllo e verifica relativamente alla certificazione di malattia (cioè, a legislazione vigente), un sistema come quello già sperimentato con la soluzione SAVIO potrebbe essere attivato in base all'iniziativa della stessa INPS, che con proprio atto generale potrebbe procedere ad esplicitare la finalità del trattamento, e ad identificare i dati da utilizzare e le operazioni da effettuare, dovendo poi assicurare – in base al principio di *responsabilizzazione* – il rispetto degli altri principi rilevanti indicati dal GDPR. Entro questa nuova cornice normativa, la *espressa e puntuale copertura legislativa* di questi aspetti non è più indispensabile, ciò che modifica evidentemente ruoli e responsabilità degli attori in gioco, così come i relativi spazi di manovra.

6. Trattamento dei dati personali e standard di legalità: due modelli a confronto

1. L'impatto dello standard legale: ruoli ed attori in gioco

La disciplina del regime di trattamento dei dati personali finalizzato all'esercizio di compiti di interesse pubblico, per come declinatasi nell'ordinamento italiano nel corso degli anni successivi all'entrata in vigore del GPDR, offre l'occasione di osservare all'opera, con particolare nitore, gli effetti derivanti dall'adozione di strategie regolatorie molto differenti. In effetti, a differenza di quanto abbiamo potuto osservare in altri ordinamenti nazionali dell'UE, il caso italiano si segnala perché ha proceduto, nel corso di un lasso di tempo tutto sommato breve, a definire (prima, nel 2018) e rivedere (poi, nel 2021) lo standard legale connesso a questo specifico presupposto di trattamento dei dati personali, conformandolo – nelle due occasioni di intervento – a due modelli tra loro molto diversi. Infatti, in altri ordinamenti, dove pure sono state compiute scelte regolatorie di carattere *trasversale*, queste hanno più spesso riguardato alcuni (a volte, uno solo) dei diversi aspetti del regime di trattamento dei dati personali che le clausole contenute nell'art. 6, parr. 2 e 3 del regolamento aprono all'intervento del legislatore domestico; più spesso, l'intervento normativo ha riguardato specifiche categorie di dati o specifici interesse pubblici o modalità di trattamento. Invece, le opzioni legislative maturate nel nostro ordinamento si sono caratterizzate per avere, in un primo momento, adottato un regime *trasversale* e *uniforme* di *stretta legalità*, applicandolo in via generale a tutti i trattamenti posti in essere per finalità di interesse pubblico. La legge (o il regolamento, se così previsto dalla legge) doveva cioè espressamente individuare le finalità del trattamento, i dati da sottoporre a trattamento, le operazioni eseguibili. In questo modo, è stato esplorato in modo particolarmente significativo lo spazio di manovra accordato dal regolamento, distanziando in modo marcato la disciplina in-

terna dallo standard legale *di base* fissato dallo stesso regolamento. Successivamente, il legislatore è ritornato su questa scelta, ed in modo altrettanto significativo ha *invertito la rotta*, adottando uno standard legale che per molti aspetti risulta *aderente* a quello fissato dal regolamento, e per alcuni altri aspetti (il regime del trattamento consistente nella comunicazione a privati e nella diffusione al pubblico) addirittura al di sotto di tale standard (per come interpretato dalla Corte di giustizia).

Queste scelte, così *nette* e *differenziate* tra loro[1], costituiscono quindi lo sfondo ed il presupposto ideale per osservarne i caratteri e l'impatto prodotti sulle soluzioni concretamente sperimentate di trattamento dei dati personali, e per metterli a confronto. L'osservazione è stata compiuta mediante l'analisi di tre casi di studio, che ci hanno consentito di verificare gli effetti determinati dal cambio di regime. Vale la pena di sottolineare che le tipologie di trattamento osservate sono accomunate dalla *ratio* che sottende a ciascuno dei trattamenti indagati. Infatti, in tutti e tre i casi abbiamo visto all'opera (a diversi stadi di sperimentazione, sviluppo e applicazione) meccanismi e strumenti finalizzati a contribuire all'efficienza e all'efficacia dello specifico compito di interesse pubblico cui il trattamento risulta servente. In particolare, nel caso dello strumento Ve.R.A. sviluppato dall'Agenzia delle Entrate, il trattamento dei dati è funzionale ad evidenziare liste di contribuenti caratterizzati da profili rischio più elevato di evasione fiscale: in questo modo, le risorse (di personale, organizzative e finanziarie) dedicate ai controlli e agli accertamenti possono essere più opportunamente indirizzate, ciò che dovrebbe avere un impatto sull'efficacia nell'azione di emersione della base imponibile e di contrasto ai comportamenti elusivi. Allo stesso modo, il *tool* SAVIO elaborato dall'INPS, nell'assegnare ai certificati medici per malattia uno *score* che quantifica il tasso di rischio di comportamenti abusivi, serve ad indirizzare le attività di accertamento e verifica, così da incrementare effettività ed efficacia delle attività di controllo assegnate all'Istituto. Anche l'attività *sperimentale* che mira a verificare la fattibilità di una mappatura degli interessi che fanno capo ad un addetto all'esercizio di una funzione pubblica, utile a verificare la veridicità delle dichiarazioni di assenza di conflitto d'interessi ha la medesima *ratio*, quella cioè di dotare le amministra-

[1] Senza presumere che la diagnosi formulata a suo tempo da Luciano Vandelli sia applicabile anche a questo caso specifico – anche perché alcuni dei fattori che hanno condotto quantomeno ad alcuni di questi cambi repentini di direzione sono ben noti, e sono evidenziati nel corso di questa analisi – non si può fare a meno di richiamare alla memoria la sua garbata ma tagliente ironia, nel vivisezionare analoghe fattispecie di schizofrenia legislativa: Vandelli L. (2006), *Psicopatologia delle riforme quotidiane. Le turbe delle istituzioni: sintomi, diagnosi e terapie*, Bologna.

zioni di strumenti di supporto istruttorio necessari per incrementare l'efficacia di tali attività di verifica. In altre parole, in tutti e tre i casi di studio indagati il trattamento dei dati personali è realizzato con lo scopo di incrementare l'efficienza e l'efficacia del compito di interesse pubblico cui sono strumentali. Una circostanza significativa, non solo perché (sul piano interno) questa esigenza corrisponde ad uno dei canoni costituzionali dell'azione amministrativa, ma anche perché (come abbiamo avuto modi di verificare più in alto), il contributo del trattamento in termini di incremento dell'efficienza e dell'efficacia nell'esercizio dei compiti di interesse pubblico costituisce uno degli elementi che – nella giurisprudenza della Corte di giustizia – inverano il requisito di *necessità del trattamento*[2].

La circostanza più evidente che abbiamo osservato è che *effettivamente* l'adozione di uno standard legale prossimo (o coincidente) con la *necessary clause* promuove il protagonismo e l'autonoma iniziativa dell'amministrazione titolare del trattamento, nel procedere ad elaborare e/o finalizzare soluzioni di trattamento strumentali all'esecuzione di compiti di intesse pubblico affidati dalla legge. Nel caso dello strumento Ve.R.A., questa circostanza è meno evidente, dal momento che per un lungo periodo la realizzazione dello strumento è stata in qualche modo guidata e stimolata anche mediante l'intervento di successive modifiche, integrazioni e ampliamenti della base giuridica inizialmente delineata dal d.l. 201 del 2011, e ulteriormente rilanciata con la legge 160/2019. D'altra parte, entro il *framework* della *strict legality rule*, il ruolo del Garante è piuttosto quello di "guardiano" della conformità delle scelte operate dal titolare del trattamento al parametro legislativo[3]: il Garante interloquisce con l'Agenzia delle Entrate (e con il Ministero competente), ma molte delle sue osservazioni, obiezioni, raccomandazioni finiscono per essere recepite o veicolate in sede legislativa. Si osserva, in altre parole, una dinamica nella quale il titolare del trattamento – nel sottoporre all'autorità di controllo gli schemi dei provvedimenti propedeutici alla sperimentazione e allo sviluppo dello strumento – stimola l'emersione progressiva di aspetti e problematiche che vengono in qualche modo affrontati

[2] Cfr. cap. 3, par. 2.4.

[3] A conferma, si noti come viene compendiato in dottrina il ruolo del Garante in vigenza della *strict legality rule* (a partire dai compiti di vaglio preventivo dei trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati, abrogati dal d.l. n. 139/2021): «non vi è dubbio che l'abrogazione di tale vaglio preventivo avrà l'effetto di modificare grandemente il quadro attuale posto che, come noto, il Garante aveva assunto negli ultimi anni un ruolo sempre più attivo quale autorità deputata a vagliare la rispondenza, specie in termini di proporzionalità, tra gli obiettivi della misura legislativa e le esigenze di tutela dei dati personali anche nel settore fiscale» (così Marcheselli A. e Ronco S.M. (2022), "Dati personali, Regolamento GDPR e indagini dell'Amministrazione finanziaria: un modello moderno di tutela dei diritti fondamentali?", cit., 98).

anche mediante il ricorso alla modifica del parametro legislativo (si pensi alle questioni relative ai limiti temporali di conservazione dei dati), mentre altre restano senza risposta (è il caso della richiesta di esplicitazione dei criteri di analisi mediante i quali individuare i contribuenti che presentino indicazioni di rischio più elevato di evasione/elusione), così impedendo di fatto che il processo possa trovare uno sbocco operativo. In questo schema, il soggetto che gioca un ruolo essenziale di iniziativa e di stimolo è necessariamente il legislatore. Questi opera certamente su impulso dell'amministrazione titolare del trattamento, ma vede il suo principale interlocutore (nella definizione del quadro normativo) nell'autorità di controllo.

Questo scenario cambia in seguito alle modifiche apportate al Codice, che altera le dinamiche che si osservano tra gli attori in gioco. Il legislatore (che aveva "rilanciato" la partita con la legge finanziaria per il 2020) esce di scena: l'Agenzia per le entrate assume l'iniziativa, e sottopone al Garante prima i decreti per la definizione delle misure di limitazione dei diritti degli interessati e di garanzia dei diritti essenziali e successivamente la valutazione d'impatto complessiva. Dal canto suo, il Garante non può più contare sulla sponda *legislativa*: il confronto con il titolare del trattamento diventa diretto e l'autorità di controllo è in qualche modo costretta ad "inseguire", come è illustrato dalle tempistiche mediante le quali viene dato il via libera alla valutazione d'impatto (cioè, mediante procedura d'urgenza). Si noti: i pareri del Garante continuano a riportare osservazioni e richieste di modifiche e di integrazione, che però non sono più in condizione di determinare un effetto di "blocco" nella *messa a regime dello strumento*. Infatti, l'allentamento della *strict legality rule* comporta anche la "riespansione" del principio di *responsabilizzazione* (art. 5, par. 2 del GDPR), che consente al titolare del trattamento (anche quando è un soggetto pubblico, come nel caso di specie) di dare avvio al trattamento, assumendosi la responsabilità quanto al rispetto dei principi del regolamento. In questa diversa dinamica, dunque, le osservazioni formulate del Garante operano – contemporaneamente – per fornire al titolare del trattamento elementi di valutazione utili a conformare il trattamento e ad attivare questa responsabilità. La *compliance* rispetto al quadro normativo a tutela dei dati personali (ma pure, contemporaneamente, di garanzia della loro libera circolazione) si sviluppa dunque in un *confronto* tra amministrazione titolare del trattamento e autorità di garanzia, senza la necessaria intermediazione del legislatore (salvo per ciò che concerne l'attribuzione dei compiti di interesse pubblico), ma piuttosto sotto il controllo *successivo* operato in sede giurisdizionale.

Anche con riferimento al caso del *tool* SAVIO possono essere constatate dinamiche e ruoli analoghi. È confermato che sotto la *strict legality rule*, il ruolo propulsivo spetta al legislatore: in assenza di suo intervento *previo* il

trattamento è privo del presupposto di liceità. Infatti, è lo stesso Istituto titolare del trattamento – dopo aver subito il provvedimento sanzionatorio del Garante (guardiano della *strict legality rule)* – che richiede l'intervento del legislatore, riconoscendo esplicitamente di non disporre di uno spazio di autonoma iniziativa. Abbiamo anche visto come, sulla base del diverso standard legale introdotto con il d.l. n. 139/2021, tale spazio di iniziativa autonoma potrebbe invece risultare oggi disponibile.

Infine, anche nel caso della sperimentazione di una mappatura dei conflitti d'interessi, l'evoluzione del quadro normativo ha inciso in modo determinante sul ruolo interpretato dal titolare del trattamento: sotto la *strict legality rule*, la finalità del progetto condotto da ANAC era quella di saggiare le potenzialità di una metodologia al fine di formulare una proposta di intervento *al legislatore*; intervenute le modifiche al quadro normativo, il titolare ha potuto assumere l'iniziativa e procedere a una prima sperimentazione diretta della mappatura (mediante la realizzazione di una *proof of concept*), mettendo in atto alcuni trattamenti dei dati personali (funzionali alla sperimentazione) che altrimenti le sarebbero stati preclusi.

Pertanto, la modifica delle regole del gioco contribuisce a modificare il ruolo e lo spazio di iniziativa dei diversi attori, il che comporta una serie ulteriore di conseguenze, su cui è opportuno soffermarsi.

2. Le dinamiche degli standard legali di trattamento dei dati

2.1. Trattamento dei dati e innovazione

Un primo elemento connesso allo spazio di iniziativa effettivamente assegnato all'amministrazione titolare del trattamento è rappresentato dalla capacità di assumere, da parte di quest'ultima, un ruolo di *guida* relativamente ai processi di innovazione organizzativa ed operativa delle funzioni e dei servizi gestiti. Poiché, infatti, larga parte dell'innovazione, nell'epoca attuale, si fonda sulla capacità di elaborazione (e rielaborazione) delle informazioni (la cd. *data economy*[4], ciò che comprende anche il trattamento di dati personali), avere a disposizione un margine (più o meno significativo, o altrimenti nullo) di autonoma iniziativa nella progettazione, sperimentazione

[4] La letteratura, sul punto, è sterminata. Sia qui sufficiente rinviare a Mayer-Schönberger V. e Ramge T. (2018), *Reinventing Capitalism in the Age of Big Data*, London, e Zuboff S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019.

e messa in opera di meccanismi che si basano sul (o includono anche il) trattamento di dati personali, significa anche (per questa stessa ragione) disporre (o meno) di spazi *per innovare*, potendo cioè contribuire a definire direzione, obiettivi ed esigenze cui indirizzare la sperimentazione di soluzioni innovative. Pertanto, il regime giuridico applicato al trattamento dei dati personali da porre al servizio del perseguimento di compiti di interesse pubblico, nella misura in cui incide sugli spazi effettivamente disponibili alle amministrazioni nell'assumere autonomamente l'iniziativa di elaborare/testare/mettere in opera strumenti che implicano il trattamento di dati personali, incide direttamente sulla capacità delle stesse amministrazioni di fare innovazione, di essere cioè protagoniste dei processi di innovazione. Il che, evidentemente, ha conseguenze di rilievo sulle soluzioni applicate all'esercizio delle funzioni pubbliche in termini di appropriatezza, adeguatezza, aggiornamento, adattabilità rispetto alle specifiche esigenze del servizio e delle funzioni cui tali strumenti sono preordinati.

Può essere utile, a questo riguardo, un parallelo con il titolo di legittimazione di cui alla lettera f) dell'art. 6 del regolamento, che è tipicamente il titolo di legittimazione in base al quale le imprese sono autorizzate a trattare i dati personali senza il consenso degli interessati. In questo caso, l'appropriatezza della soluzione di trattamento legittimata dal regolamento è in funzione del fatto che tale trattamento risulti *necessario* per il perseguimento del legittimo interesse del titolare del trattamento. Quest'ultimo quindi, nell'esercizio della propria autonomia, è libero di scegliere un interesse da perseguire, di identificarlo e – nella misura in cui questo risulti *lecito* – di realizzare il trattamento dei dati personali (comuni) che risulti necessario per la realizzazione di questo interesse. Come noto, questo presupposto di liceità è contemperato dal necessario bilanciamento da effettuarsi tra l'interesse legittimo del titolare del trattamento (da una parte) e i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Qualora le esigenze di protezione di questi secondi risultino prevalenti rispetto al legittimo interesse del titolare del trattamento, allora il trattamento risulterà privo del presupposto di legittimazione (e quindi, illecito). Nel caso in cui il trattamento sia strumentale all'esercizio di compiti di interesse pubblico, tali compiti (come anche l'eventuale assegnazione di poteri giuridici pubblicistici) sono invece (etero) assegnati dall'ordinamento. Il titolare del trattamento, cioè, non è libero di scegliere le finalità (che gli sono assegnate dall'ordinamento, cioè dagli atti normativi-basi giuridiche dell'Unione o dello Stato membro), in ragione della consustanziale dimensione *servente* dell'amministrazione pubblica (nella sua dimensione tanto soggettiva quanto in quella oggettiva): è l'ordinamento

che *seleziona gli interessi pubblici e che ne assegna la relativa cura/il perseguimento all'amministrazione* (in ossequi al principio di legalità-indirizzo, quella che nel GDPR trova concretizzazione nell'espressione contenuta nell'art. 6(1)(e)). Nello schema del GDPR, il carattere necessario del trattamento dei dati personali (comuni) rispetto al perseguimento di queste finalità/compiti di interesse pubblico costituisce criterio di liceità, individua la finalità del trattamento e costruisce la regola di bilanciamento rispetto alla tutela della sfera giuridica degli interessati (salvo quanto detto, con riferimento alla giurisprudenza della Corte di giustizia, con riguardo ai trattamenti che comportano una ingerenza particolarmente grave, quali la comunicazione al pubblico). È questa, in sostanza, la fisionomia della *necessary clause*. Sulla base di questo standard legale, e data la (*etero*) assegnazione di un compito di interesse pubblico, il titolare del trattamento dispone di uno spazio di iniziativa (che in effetti si configura nei termini della *doverosità amministrativa*, in vista del perseguimento di interessi pubblici che sono affidati alle sue cure[5]) nel quale il trattamento necessario dei dati personali si configura per ciò stesso come lecito. La clausola di necessarietà disegna lo spazio all'interno del quale il titolare del trattamento può (*deve*) predisporre i mezzi più adatti, efficienti, efficaci, *necessari* per l'esecuzione del compito di interesse pubblico, ivi compresa la predisposizione di strumenti, procedure, soluzioni che comportano il trattamento di dati personali (comuni, ma anche particolari, qualora siano integrati anche i requisiti e i presupposti di cui all'art. 9(2)(g)).

Al netto dell'*ontologicamente diverso* regime/meccanismo di selezione degli interessi cui il trattamento dei dati e funzionale[6], la relazione di *strumentalità necessaria* tra il trattamento effettuato e l'interesse perseguito, costituisce (e limita) lo spazio entro cui il titolare del trattamento è legittimato ad assumere l'iniziativa nell'elaborare strumenti, soluzioni, mezzi di trattamento dei dati personali strumentali alla realizzazione/cura di tali interessi, tanto con riferimento al presupposto di liceità di cui alla lett. e) quanto con riferimento al presupposto di liceità di cui alla lett. f)[7]. All'interno di questo

[5] Cfr. Goggiamani G. (2005), *La doverosità della pubblica amministrazione*, Torino, 2005, nonché Rossi, G. (2011), *Potere amministrativo e interessi a soddisfazione necessaria. Crisi e nuove prospettive del diritto amministrativo*, Torino

[6] Che ricalca la linea di faglia che segna la "grande dicotomia" tra pubblico e privato, in accordo con la classica definizione formulata da Bobbio N. (1980), *Pubblico/privato*, in *Enciclopedia Einaudi*, Torino, 401.

[7] Sebbene, come detto, lo spazio di iniziativa disponibile ai titolari del trattamento che fanno riferimento al presupposto di liceità di cui alla lett f) sia limitato, oltre che dalla clausola di necessarietà, anche dall'eventuale prevalere delle esigenze di tutela dei diritti e le libertà fondamentali dell'interessato, che richiedano la protezione dei dati personali, in particolare quando l'interessato sia un minore.

framework, lo spazio di iniziativa riconosciuto alle imprese (e agli altri soggetti che esercitano la propria autonomia: associazioni, enti del terzo settore, etc.) e quello riconosciuto ai soggetti cui è assegnata l'esecuzione di compiti di interesse pubblico – lo spazio, cioè, entro cui progettare, sperimentare ed elaborare strumenti che implicano il trattamento dati personali – è conformato in termini analoghi (dalla *necessary clause*)[8]. E, pertanto, entro tale spazio può esercitarsi anche una analoga capacità di guidare e sviluppare processi innovativi, aggiornati, adeguati.

Diversamente, man mano che ci si allontana dallo standard legale declinato dalla *necessary clause*, in direzione della *strict legality rule*, lo spazio disponibile all'iniziativa dell'amministrazione si riduce. Attratti nella base giuridica legislativa elementi quali la espressa definizione della finalità del trattamento, l'identificazione dei dati da sottoporre a trattamento e delle operazioni da effettuare, il margine di manovra disponibile all'amministrazione titolare del trattamento nell'elaborare strumenti innovativi che implicano il trattamento dei dati personali (sostanzialmente) si assottiglia fino (quasi) ad azzerarsi del tutto. La *strict legality rule* presuppone un livello elevato di integrazione tra momento legislativo ed esecuzione amministrativa (e di coordinamento tra i relativi attori), che mal si concilia con le esigenze di flessibilità che i (veloci) processi di sviluppo connessi agli sviluppi tecnologici. Ma, più in generale, nella misura in cui le soluzioni di trattamento dei dati personali possono essere riguardate come una componente essenziale dei processi mediante i quali l'amministrazione *organizza* l'esercizio delle rispettive funzioni, risulta evidente come un eccessivo grado di integrazione tra legge e organizzazione (e la riserva alla prima della definizione di parti troppo ampie e pervasive della seconda) appare incompatibile con le esigenze del buon andamento[9]. Riguardare, cioè, il trattamento dei dati personali – entro il dominio dell'esecuzione dei compiti di interesse pubblico – come elemento dell'organizzazione amministrativa[10], ci aiuta a considerare

[8] Analogo parallelo è proposto da Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, cit., dove si sottolinea che se nell'art. 6, par. 1, lett. e) "la valutazione del trattamento come necessario e inevitabile è rimessa alla discrezionalità della pubblica amministrazione (…) stesso discorso potrebbe essere fatto per l'art. 6, par. 1, lett. f), del GDPR, che fa riferimento al trattamento necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi" (396 e nota n. 17).

[9] Sul punto, sia sufficiente il richiamo alla stretta connessione tra *flessibilità (e disponibilità)* degli strumenti organizzativi e canone del buon andamento, nella notissima tesi di Nigro M. (1966), *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano.

[10] "la risposta organizzativa sarà fondamentale per il potere pubblico; senza di essa, non si avranno metodi efficaci di governo del fenomeno", così Carotti B. (2020), "Algoritmi e poteri pubblici: un rapporto incendiario", in *Giornale di diritto amministrativo*, 1, 5 ss. "Con il nuovo Regolamento, la privacy non è più qualcosa che sta a valle o a monte della filiera

in modo più equilibrato (e consapevole) il relativo regime giuridico. La riconduzione (o la riserva) di una quota elevata, eccessiva, sproporzionata di elementi organizzativi alla fonte legislativa *irrigidisce* la capacità di innovazione *dell'amministrazione*, non solo (e non tanto) perché la fonte legislativa sia troppo rigida in sé (le vicende recenti testimoniano invece un trend *opposto*, con la estrema disponibilità e volatilità della fonte legislativa primaria, per effetto della assoluta centralità e ordinarietà d'uso acquisita dall'atto fonte decreto-legge), ma piuttosto perché quello strumento sfugge all'iniziativa (e al controllo) della stessa amministrazione, e risponde a dinamiche, motivazioni, presupposti ulteriori.

Il confronto con la condizione dei titolari del trattamento *privati*, che facciano uso di dati personali senza il consenso degli interessati, è utile proprio per misurare quanto e come l'integrazione dello standard legale di base (quello disegnato dalla *necessary clause*) mediante uno o più elementi della *strict lagality rule* riduca i margini disponibili all'iniziativa dell'amministrazione e alla sua capacità di guidare i propri processi di innovazione organizzativa. Si tratta di un confronto da operare *con le dovute cautele* e *distinguo*, dal momento che si tratta di due situazioni tra loro *irriducibili*, e tuttavia a livello puramente schematico (su di un piano di osservazione più astratto) è utile per constatare gli effetti che derivano dall'adozione di uno standard legale che sottragga all'amministrazione (ferma restando la *necessary clause*) la disponibilità, il controllo e/o l'iniziativa riguardo alle *modalità* di trattamento dei dati personali[11].

organizzativa e produttiva di un'organizzazione, ma la sua tutela deve essere inserita tra gli obiettivi a cui tende tutta l'azione (privacy by design e privacy by default) dei soggetti pubblici e privati, poiché le attività che pongono in essere producono e utilizzano dati in continuazione, in modo diretto e indiretto. Questa visione del dato, centrale e intrinseca all'organizzazione stessa e al modo in cui si strutturano i processi, esprime pienamente il valore e l'importanza che i dati stanno assumendo per l'economia, per le scelte pubbliche e per la lettura dell'intera società. Le organizzazioni pubbliche devono, con uno sforzo culturale e di formazione, interiorizzare il nuovo modello e sfruttarne le potenzialità connesse, in termini di dati necessari per amministrare", così Fiorentino L., (2018), "Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche", cit., 694. Per una attenta disamina dei diversi profili di impatto del GDPR sull'organizzazione delle amministrazioni pubbliche, sui ruoli (a cominciare dalla specifica figura del Responsabile della Protezione dei Dati-RPD) e sulle procedure, cfr. Bombardelli M. (2022), *Dati personali (Tutela)*, cit., in part. 360-370.

[11] Analoghe approccio argomentativo è impiegato da Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, cit., 398: "Volendo guardare allo stesso fenomeno da un altro punto di vista, la novella corregge la tendenza degli ultimi anni a intendere le norme sulla privacy come in senso particolarmente limitativo quando ad essere in gioco è l'attività amministrativa il che, a ben vedere, costituiva un non senso a fronte della possibilità viceversa consentita a soggetti privati e imprese di trattare ampiamente (e legittimamente) i dati personali dietro gli schemi del consenso (spesso prestato secondo formule standardizzate neppure lette dall'interessato) o della necessità contrattuale".

Pertanto, una prima evidenza che emerge da questo studio è la stretta connessione che si instaura tra lo *standard di legalità* riservato al trattamento dei dati in esecuzione di compiti di interesse pubblico e la *capacità di iniziativa* nonché *lo spazio di innovazione* che si finisce per attribuire ai titolari di questi trattamenti (a cominciare dalle amministrazioni), in considerazione del fatto che le soluzioni di trattamento dei dati personali costituiscono ormai un elemento essenziale delle dimensione organizzativa delle funzioni pubbliche[12].

2.2. Trattamento dei dati e rapporto con i fornitori

Un altro modo per considerare la stessa questione (spazio di iniziata e capacità di guidare i processi di innovazione) è quello di verificare gli effetti del *dual legality standard* sul rapporto che i titolari dei trattamenti vengono a strutturare con l'ambiente esterno, e in particolare con i fornitori di apparati, soluzioni, software, sistemi informativi, architetture, etc. mediante i quali si effettua in concreto il trattamento dei dati. Sotto questo specifico punto di osservazione, lo spazio di iniziativa riservato (o risultante) in capo ai titolari del trattamento si traduce anche nella capacità di interloquire con questi operatori (di mercato) da una posizione più o meno caratterizzata in termini di forza contrattuale, indipendenza progettuale, autonomia di giudizio. Infatti, nella misura in cui il titolare del trattamento non disponga di margini di iniziativa, la sua capacità di interlocuzione con l'ambiente esterno risulterà più debole, per una serie concorrente di ragioni. In primo luogo, se il ruolo di iniziativa è dislocato o condiviso con il legislatore, parte delle scelte relative ai mezzi da procurarsi su mercato risulta già predeterminata (o fortemente condizionata) dalle opzioni che sono state inserite in legge; una scelta legislativa *tecnicamente non neutra*, ad esempio, potrebbe ridurre il novero delle imprese idonee a fornire una certa applicazione, con la conseguenza di vincolare l'amministrazione a scegliere un certo partner industriale, piuttosto che un altro (con conseguente indebolimento del potere contrattuale)[13]. Inoltre, la carenza di effettivi spazi autonomi di iniziativa conduce fatalmente l'amministrazione a disinvestire nelle professionalità interne (o anche rispetto agli accordi collaborazione con soggetti esterni *non di mercato*) che

[12] Cfr. Sola A. (2020), "Utilizzo di big data nelle decisioni pubbliche tra innovazione e tutela della privacy", in *MediaLaws*, 3, 1-23; Cavallo Perin R. (eds.) (2021), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino.

[13] Cfr. Carullo G. (2020), "Principio di neutralità tecnologica e progettazione dei sistemi informatici della pubblica amministrazione", in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 21/1, 33-48.

sono indispensabili per occupare in modo attivo, consapevole e propulsivo quegli spazi. In altre parole, un'amministrazione strutturalmente priva di spazi di manovra effettivi sul fronte dell'innovazione organizzativa sarà anche priva delle risorse interne utili (necessarie) a promuovere, supportare e guidare scelte organizzative innovative[14], perché avrà (convenientemente) selezionato e allocato le risorse organizzative laddove queste possono essere effettivamente impiegate[15]. Tuttavia, in questo modo l'amministrazione si trova in condizioni di strutturale *debolezza* ogni qualvolta si trovi nelle condizioni di interloquire con il mercato per procurarsi i mezzi che le servono per sviluppare o anche semplicemente per acquistare (magari "chiavi in mano") le soluzioni con le quali erogare i servizi e gestire le procedure (e, conseguentemente, trattare i dati personali). Ciò che determina una strutturale subordinazione nei confronti degli attori di mercato, con tutte le conseguenze del caso in termini di appropriatezza dei beni e servizi acquistati e dei relativi prezzi. Non costituisce certo un fenomeno nuovo o originale, anche con specifico riferimento alle vicende dell'informatica pubblica[16]. E tuttavia, sottovalutare la profonda connessione tra soluzioni di trattamento dei dati personali e funzione di organizzazione delle amministrazioni pubbliche comporta il rischio che tutta una serie di scelte finiscano per essere di fatto *appaltate a* (e *condizionate da*) soggetti esterni all'amministrazione, guidati da *legittimi interessi* che però sono diversi, diremmo estranei a quelli che devono guidare la sperimentazione, la selezione e l'implementazione dei servizi a supporto dell'esercizio delle funzioni pubbliche. Di più: comprimere in modo strutturale e duraturo gli spazi e la capacità delle amministrazioni pubbliche di sperimentare e testare strumenti, logiche e soluzioni che implicano il trattamento di dati personali, a lungo andare determina l'accumularsi di uno squilibrio rispetto al settore privato, ciò che potrebbe far sorgere seri dubbi in ordine

[14] Cfr. Carloni E. (2019), "Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni", in *Diritto* pubblico, 2, 363-392; Sgueo G. (2019), "Tre idee di design per l'amministrazione digitale", in *Giornale di diritto amministrativo*, 1, 19 ss

[15] Cfr. De Leonardis F. (2020), "Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione", in *Munus: rivista giuridica dei servizi pubblici*, 2, 367-387; nonché Merloni F. (2022), "Il d.lgs. n. 165 del 2001 e l'organizzazione delle competenze professionali dei funzionari pubblici", in *Diritto Amministrativo*, 2, 359 ss. nonché Id (2013), "Le attività conoscitive e tecniche delle amministrazioni pubbliche. Profili organizzativi", in *Diritto pubblico*, 2, 481-520.

[16] Cfr. Fiorentino L. (2009), L'esternalizzazione delle attività amministrative: l'acquisto di beni e servizi da parte delle Pubbliche Amministrazioni e il patrimonio immobiliare dello Stato", in *Economia dei Servizi*, 2, 259-272; Ambriola V., Cignoni G. A. (1999), "Qualità, informatica e pubblica amministrazione", in *Il Mulino*, 5, 917-928; Cardarelli F. (1996), *Efficienza e razionalizzazione dell'attività amministrativa. I contratti ad oggetto informatico nella pubblica amministrazione*, Camerino; D'Elia I., Ciampi C. (1987), *L'informatica nella pubblica amministrazione. Problemi, risultati, prospettive*, Roma.

alla effettiva capacità di sviluppare (o, meglio, acquisire sul mercato) soluzioni effettivamente rispondenti alle finalità specifiche e caratteristiche dell'esercizio di funzioni pubbliche, semplicemente perché il settore pubblico ha perduto la capacità di immaginare, sperimentare e realizzare questo genere di soluzioni *di propria iniziativa, a partire dalle proprie specifiche esigenze, priorità, obiettivi*, e si trova nella condizione di dover adottare (o adattare, per quanto possibile) programmi, metriche, filosofie di calcolo sviluppare per tutt'altri fini[17].

Senza contare che affidarsi in modo preponderante (o esclusivo) all'*iniziativa* e alla capacità di *innovazione* sviluppate nel solo settore privato espone a una alternativa poco attraente: tutelare i diritti di privativa ed i segreti industriali rivendicati dai fornitori privati (correndo il rischio di compromettere in modo serio i diritti alla trasparenza, all'*explainability*, di trattamento equo e non discriminatorio), ovvero rinunciare ad implementare sistemi effettivamente innovativi (in ragione della indisponibilità di quegli stessi fornitori a compromettere i vantaggi competitivi, gli investimenti e le possibilità di profitto incorporati o derivati dallo sfruttamento dei segreti industriali).

Il rilievo di tali considerazioni appare ulteriormente accentuato dall'approccio adottato dall'*elaborando* regolamento UE sull'Intelligenza Artificiale, che fa perno sull'analisi e l'*assessment* dei rischi connesso alla predisposizione di questi applicativi sul lato dei *produttori* e dei *fornitori*, come condizione di immissione di tali prodotti sul mercato; una logica *regolatoria* diversa da quella che fa capo alla tutela dei dati personali (in cui ad essere chiamata in causa è piuttosto la responsabilità del titolare del trattamento) e che quindi richiederà (anche) alle amministrazioni una capacità di interlocuzione con produttori e fornitori *consapevole* e *attrezzata*[18].

[17] Sulle specificità che caratterizzano (in termini *assiologici*) esigenze ed approcci delle organizzazioni preposte alla cura di interessi pubblici, si veda: Pioggia A. (2022), *La cura nella Costituzione. Prospettive per una amministrazione della cura*, in (eds.) Arena G., Bombardelli M., *L'amministrazione condivisa*, 43-63; Id. (2021), *La concessione e il pubblico servizio: una storia parallela*, in (eds.) Bartolini A., *Scritti in onore di Bruno Cavallo*, Torino, 253-273; nonché, cfr. Dunleavy P., Margetts H., Bastow S. e Tinkler, J. (2006), *Digital Era Governance-IT Corporations, the State and e-Government*, New York, dove è sottolineato "how public managers need to retain and develop their own IT expertise and to carefully maintain well-contested markets if they are to deliver value for money in their dealings with the very powerful global IT industry", *ivi*, 15; Nograšek J., Vintar M. (2014), "E-government and organisational transformation of government: Black box revisited?", in *Government Information Quarterly*, 31/1, 108-118.

[18] Cfr., *ex multis*, Macchia M. e Mascolo A. (2022), *Intelligenza artificiale e regolazione*, in (eds.) Pajno A., Donati F., Perrucci A., *Intelligenza artificiale e diritto: una rivoluzione? Vol. 2: Amministrazione, responsabilità, giurisdizione.*, Bologna, 97-130; Marenghi C. (2021), "La proposta di Regolamento Ue sull'intelligenza artificiale e la regolazione privata: spunti critici in tema di norme tecniche armonizzate", in *Diritto comunitario e degli scambi internazionali* 3/4, 563-583.

Dunque, anche sotto questo profilo, il *dual legality standard* rivela una serie di effetti e di ricadute di cui tenere conto.

2.3. Trattamento dei dati e principio di limitazione della finalità

Come chiarito fin dal principio di questa indagine, il principio di limitazione della finalità del trattamento costituisce il caposaldo essenziale e distintivo del regime di tutela dei dati personali, nell'economia complessiva della trama disegnata dal GDPR. La finalità del trattamento costituisce *sempre* misura della legittimazione e limite al trattamento dei dati personali. L'attenuazione del legame immanente tra le finalità originarie (quelle che hanno giustificato *ab origine* la raccolta del dato personale) è consentita in pochissimi casi e comunque soggetta a specifiche condizioni[19], fatta salva l'ipotesi che il trattamento per una finalità incompatibile con quella originaria sia basato "su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23"[20]. Si noti: anche in quest'ultimo caso la misura legislativa dovrebbe comunque esplicitare la

[19] Cfr. art. 5(1)(b): "un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali". Certamente, l'individuazione delle ragioni e degli interessi che giustificano la deroga al principio di limitazione della finalità del trattamento inducono a riflettere sulle esigenze che una simile indicazione mira a promuovere e salvaguardare. Accanto a quelle di più immediata evidenza, pare possibile scorgere il rilievo annesso a registri e archivi pubblici, e più in generale alla funzione di conservazione dei dati utili alla catalogazione, conservazione e trasmissione intertemporale della conoscenza. Un elemento di riflessione che merita di essere valorizzato ed approfondito, nella misura in cui pare offrire una sponda alla preservazione della conoscenza *per le generazioni future* difronte al rischio che – anche in ossequio a principi sanciti dallo stesso GDPR (quali in particolare «minimizzazione dei dati» e «limitazione della conservazione») o di diritti riconosciuti agli interessati (quale in particolare il diritto di cancellazione di cui all'art. 17) – le informazioni possano andare distrutte, perdute, non trasmesse. Una riflessione, quella centrata sulla specifica funzione *pubblica* di conservazione dei dati di informazione, che potrebbe muoversi entro coordinate anche diverse da quelle più note e dibattute del rapporto tra diritto all'oblio e diritto alla rievocazione/memoria storica. Alcuni elementi, sebbene non pienamente soddisfacenti, possono cogliersi in Corte di Giustizia, sentenza del 9 marzo 2017, resa nella causa C-398/15, *Manni*, su cui si vedano le analoghe riflessioni di Forti M. (2018), "Diritto all'oblio e conservazione dei dati iscritti nei pubblici registri: qualche considerazione a margine della sentenza della Corte di giustizia nel caso Manni", in *Contratto e impresa/Europa*, 565-580; più in generale, cfr. Giuva L., Vitali S., Zanni Rosiello I (2007), *Il potere degli archivi. Usi del passato e difesa dei diritti nella società contemporanea*, Milano.

[20] Cfr. art. 6(4) GDPR.

(nuova) finalità del trattamento (incompatibile con quella originaria) così autorizzata (cfr. art. 23(2)(a))[21]. Pertanto, il principio di limitazione della finalità costituisce un parametro fondamentale (ed *ineludibile*) per verificare caratteri e ricadute del due standard legali che abbiamo evidenziato.

A ben vedere, nella misura in cui (per le ragioni più volte evidenziate) la *necessary clause* si presenta come lo standard più "permissivo", è in questo contesto che il principio di limitazione della finalità ha da giocare un ruolo più pregnante. Infatti, in assenza di una disposizione *legislativa* che autorizzi (o contempli espressamente) il trattamento caratterizzato da una finalità incompatibile con quella originaria (alla stregua dei parametri di verifica della compatibilità di cui all'art. 6(4) del GDPR), i trattamenti, legittimati dall'esecuzione di un compito di interesse pubblico, e operati su dati che non siano raccolti direttamente presso l'interessato, sono in ogni caso soggetti al rispetto di tale principio. In altre parole, il titolare del trattamento si trova *sempre* – in un contesto generale (come è anche il caso delle linee di riforma che vanno informando l'ordinamento nazionale[22]) caratterizzato da un deciso investimento nella circolazione e nell'integrazione (in termini sistemici) delle banche dati pubbliche, ai fini dell'esercizio dei compiti di interesse pubblico – a dover verificare la compatibilità tra *finalità originaria* che ha giustificato la raccolta del dato e finalità rispetto alla quale il trattamento ulteriore risulta necessariamente strumentale. La finalità (originaria) del trattamento, si presenta pertanto come un *vincolo* capace di tessere una trama che avvolge ogni suo ulteriore utilizzo, e costituire il principale elemento di freno (o di condi-

[21] Circa i requisiti ed i limiti entro i quali il legislatore può muoversi a deroga del principio di limitazione della finalità, vedi la recentissima sentenza della Corte di Giustizia, *Norra Stockholm Bygg AB*, causa C-268/21, cit.

[22] Come già sottolineato, le linee di azione e gli investimenti del muovono nella specifica, esplicita direzione di una più intensa integrazione del patrimonio informativo, mediante la realizzazione di una infrastruttura idonea ad abilitare l'interoperabilità delle banche dati pubbliche (e che fa perno sul ruolo giocato dalla Piattaforma digitale nazionale dei dati): cfr. Alberti I., "La creazione di un sistema informativo unitario pubblico con la Piattaforma digitale nazionale dati", in *Le istituzioni del federalismo*, 2, 473-495, nonché Ponti B. (2022), "Le diverse declinazioni della 'Buona amministrazione' nel PNRR", cit.; Boschetti, B. (2022), *La transizione della pubblica amministrazione verso il modello Government as a platform*, cit.. Un primo banco di prova e di sperimentazione di questo approccio è certamente rappresentato dal nuovo Codice dei contratti (adottato con il d.lgs 31 marzo 2023, n. 36): il processo che dovrebbe portare alla gestione integralmente digitale del ciclo di vita dei contratti pubblici, infatti, presuppone un'opera di standardizzazione e integrazione operativa di enorme rilievo sistemico: cfr. Racca G. M. (2022), *Le innovazioni necessarie per la trasformazione digitale e sostenibile dei contratti pubblici*, in (eds.) Cavallo Perin R., Lipari M. e Racca G. M., *Contratti pubblici e innovazioni per l'attuazione della legge delega*, Napoli, 2022, 9-44; Pignatti M. (2022), "La digitalizzazione e le tecnologie informatiche per l'efficienza e l'innovazione nei contratti pubblici", in *federalismi.it*, 12, 133-175.

zionamento) rispetto al pieno dispiegamento della funzione conoscitiva *pubblica* giustificata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici. A questo proposito, appaiono utili le seguenti considerazioni. In primo luogo, in ragione della diretta applicabilità delle clausole del regolamento (per altro, esplicitamente richiamate proprio nelle formule legislative introdotte con il decreto «capienze»), si tratterà di comprendere quale effetto produrranno in concreto i criteri elencati all'art. 6, par. 4, lett. da (a) a (e), in base ai quali va effettuata la valutazione di compatibilità delle finalità ulteriori rispetto a quelle originarie. Si tenga conto, per altro, che tale *assessment* è oggi rimesso in prima battura allo stesso titolare del trattamento, per effetto della (ri)espansione del principio di responsabilizzazione, in eventuale (ma non sempre necessario) dialogo e confronto con il Garante, e sotto il controllo (successivo) dell'autorità giurisdizionale. Alcuni di questi criteri, in effetti, potrebbero risultare più permissivi di altri, soprattutto tenuto conto dei caratteri specifici del contesto in cui vengono applicati. Facciamo riferimento, in particolare, al criterio di cui alla lett. a), in base al quale va preso in considerazione "*ogni* nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto" e quello di cui alla lett. b)[23]. Altri invece sembrano avere un'attitudine più rigorosa, in particolare qualora siano coinvolti dati particolari o giudiziari[24]. Altri ancora, assegnano un ruolo attivo al titolare del trattamento, nel propiziare il giudizio di compatibilità[25]. Senza contare che i criteri così enumerati non esauriscono il novero dei parametri cui fare riferimento nel compiere la valutazione di compatibilità, dal momento che tale elencazione risulta (*expressis verbis*) di carattere solo esemplificativo[26]. In secondo luogo, come già considerato più sopra, occorre tenere conto delle modalità con le quali sono formulate ed esplicitate le finalità del trattamento *originario*, soprattutto quando questo costituisca manifestazione dell'esercizio di una funzione conoscitiva specificamente dispiegata al fine di raccogliere in modo sistematico informazioni omogenee per tipologia, con lo scopo specifico di rendere tali informazioni disponibili per l'intero sistema pubblico[27].

[23] In base al quale occorre tenere conto "del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento".

[24] Cfr. art. 6(4), lett. c) e d) del GDPR.

[25] Cfr. *ivi*, lett. f): (si tiene conto) "dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione".

[26] Infatti, nell'introdurre tale elencazione, l'art. 6, par. 4 così recita: "al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, *tra l'altro*: (…)" (corsivo aggiunto).

[27] Sembrano corrispondere a questa strategia di fondo, come detto, le *Basi di dati in interesse nazionale* di cui agli art. 60 e ss. del Codice dell'amministrazione digitale; sul punto

Sotto le condizioni della *necessary clause*, pertanto, la trama disposta dal principio di limitazione della finalità non dipenderà soltanto dal modo con il quale saranno applicati i criteri di valutazione di *compatibilità* ai trattamenti successivi (nello specifico contesto del settore pubblico, con riferimento – cioè – a trattamenti strumentali all'esecuzione di compiti di interesse pubblico); dipenderà anche (soprattutto?) da come saranno declinate (e interpretate), in termini di ampiezza e raggio d'azione, le finalità originarie che supportano e giustificano il trattamento di raccolta e sistematizzazione dei dati personali in alcune banche dati "sistemiche".

Sotto lo standard della *strict legality rule*, la presa del principio di limitazione del trattamento è, invece, molto più debole. Infatti, mediante il ricorso allo strumento legislativo (che sotto questo standard legale *è necessitato*) il GDPR autorizza a derogare al principio, e quindi a trattare dati personali per finalità ulteriori anche *incompatibili* con quella originaria. Il tipo di tutela assicurata ai dati personali (in questo caso) si sposta di livello, potendosi giocare non in termini di sindacato circa la (compatibilità della) *finalità del trattamento*, ma piuttosto come sindacato sulla disciplina legislativa che autorizza la deroga a tale principio: tale misura legislativa deve cioè essere "necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1" del regolamento, una formula che riecheggia altre formule del diritto convenzionale europeo (e non solo dell'Unione), per declinare i presupposti per la limitazione dei diritti fondamentali. Ai sensi dell'art. 23, la disposizione legislativa può "limitare la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, *nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli* da 12 a 22" (corsivo aggiunto). Dunque, quando lo standard (ispirato a una *strict legality rule*) imponga comunque che la declinazione della base giuridica possa essere effettuata *solo mediante la legge* (o con regolamento, purché però la legge lo preveda), il vincolo derivante dalla limitazione della finalità del trattamento finisce per essere assorbito nella *base legale necessariamente legislativa*, senza svolgere un autonomo, distinto rilievo in ordine alla liceità del trattamento in questione. Infatti, dato lo *schermo* offerto dalla disposizione di rango legislativo che disponga/autorizzi il trattamento *ulteriore* per una finalità *differente* ed *incompatibile* rispetto a quella originaria, tale *finalità ulteriore* cessa di essere oggetto di rilievo e di autonoma valutazione (ai fini della liceità del trattamento), salvo per il fatto che la misura legislativa in questione debba indi-

Falcone M. (2023), *Ripensare il potere conoscitivo pubblico. La conoscenza amministrativa con i big data e gli algoritmi*, cit., in part. il cap. V.

carla in modo esplicito. Ciò perché – come già sottolineato – la deroga apportata al principio di *compatibilità* tra la finalità originaria e quella ulteriore, deve essere disposta mediante una misura legislativa che indichi in modo esplicito la nuova, diversa e ulteriore finalità così autorizzata (cfr. art. 23(2)(a)). Si noti, per inciso, che la disposizione in questione (l'art. 6(4)) non appare una mera duplicazione di quanto già disposto all'art. 23(1). Infatti, questa seconda disposizione autorizza la legislazione (dell'UE o dello Stato membro) ad introdurre limitazioni alle disposizioni contenute dell'art. 5(1) (compreso quindi il principio di limitazione della finalità del trattamento) "che corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22". Ora, poiché non è dato ravvisare (tra questi) un diritto corrispondente al principio di limitazione della finalità del trattamento, la disposizione di cui all'art. 6(4) consente di operare un *quid pluris* rispetto a quanto consentito dall'art. 23(1): ovvero, proprio autorizzare introduzione di deroghe al principio di limitazione della finalità del trattamento (ciò che l'art. 23(1), per come formulato, non avrebbe consentito di fare)[28].

Alla luce di quanto detto, vale la pena di formulare un interrogativo, ovvero se le disposizioni legislative come quelle relative alle *Basi di dati di interesse nazionale* più volte richiamate – nella misura in cui *esplicitano la finalità* di raccolta e gestione digitale delle informazioni omogenee per tipologia e contenuto, *identificandola* nel rendere disponibili tali informazioni alla conoscenza della altre amministrazioni, per lo svolgimento delle rispettive funzioni istituzionali – non possano essere interpretate come momento di esercizio ed integrazione della clausola di cui all'art. 6(4) del GDPR; ossia, se non possano essere interpretate come una *deroga esplicita* al principio di limitazione della finalità del trattamento. Più in generale, *de iure condendo*, ci si chiede se tra i margini di manovra così assicurati al legislatore nazionale non vi sia anche quello di introdurre *a monte* (cioè con riferimento alle finalità di raccolta di dati personali, omogenei per tipologia e contenuto, esplicitamente posti a disposizione e al servizio dell'esecuzione di compiti di interesse pubblico) una deroga al principio di limitazione della finalità di

[28] Cfr. Corte di giustizia, *Norra Stockholm Bygg AB* causa C-281/21 "Inoltre, qualora il trattamento dei dati personali sia effettuato per un fine diverso da quello per il quale tali dati sono stati raccolti, dall'articolo 6, paragrafo 4, del RGPD, letto alla luce del considerando 50 di tale regolamento, risulta che un siffatto trattamento è consentito a condizione che esso sia basato, segnatamente, su un atto legislativo degli Stati membri e che esso costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di uno degli obiettivi di cui all'articolo 23, paragrafo 1, del RGPD. Come indicato in tale considerando, al fine di salvaguardare tali importanti obiettivi di interesse pubblico generale, il titolare del trattamento può quindi sottoporre i dati personali a ulteriore trattamento *a prescindere dalla compatibilità di tale trattamento con le finalità per cui i dati personali sono stati inizialmente raccolti*", par. n. 33 (corsivo aggiunto).

trattamento, così da svincolare la circolazione e l'uso dei dati personali così raccolti e veicolati all'interno del settore pubblico, dai vincoli derivanti dall'applicazione di tale principio. Una prospettiva suggestiva, che contribuisce anche a rileggere in modo più articolato e consapevole (vedi *infra*, il paragrafo conclusivo) caratteri e differenze dei regimi abilitati dagli standard legali che abbiamo posto a tema e sottoposto ad analisi.

3. L'impatto sul principio di legalità

Abbiamo già evidenziato come lo standard legale attivato dalla *necessary clause* possa essere utilmente letto ed interpretato alla luce dello schema dei poteri impliciti. Per effetto della *necessary clause* (ossia, lo standard legale di base delineato dal GDPR a giustificazione del trattamento dei dati personali per l'esecuzione di compiti di interesse pubblico), all'assegnazione al titolare del trattamento di un compito di interesse pubblico consegue il riconoscimento a tale soggetto della possibilità di trattare dati personali, nella misura in cui tale trattamento risulti *necessario* all'esecuzione dei compiti di interesse pubblico. Tale *possibilità* si configura in effetti come l'assegnazione di un *potere*, dal momento che ogni trattamento dei dati personali implica una qualche compressione, ingerenza, limitazione del diritto alla tutela dei dati personali (nelle sue molteplici declinazioni concrete) riconosciuto e tutelato in capo all'interessato, e che nella fattispecie in questione tale ingerenza si produce senza il consenso dell'interessato. Di qui, l'inquadramento entro la cornice teorica dei poteri impliciti, con la conseguente tensione attivata rispetto alla tenuta del principio di legalità.

Ora, quando all'assegnazione di compiti di interesse pubblico si accompagni anche l'attribuzione esplicita di un qualche *potere giuridico*, la deroga al principio di legalità connesso all'esercizio di (ulteriori) poteri impliciti è stata interpretato in dottrina (e anche da certa giurisprudenza) come meno preoccupante, dal momento che tali ulteriori poteri troverebbero una forma di giustificazione/copertura nel potere esplicitamente attribuito (e rispetto all'esercizio del quale si configurano come strumentali)[29]. Il che però non vale certo a sanare del tutto le questioni connesse al principio di tipicità che fa da corollario al (e riempie di contenuto il) principio di legalità[30]. Molto

[29] Cfr. Bassi N. (2001), *Principio di legalità e poteri amministrativi impliciti*, cit., *passim*, Morbidelli G. (2007), "Il principio di legalità e i c.d. poteri impliciti", cit., *passim*, ma, *contra*, ad esempio, Travi A. (2008), *Il principio di legalità nel diritto amministrativo che cambia*, in *Il principio di legalità nel diritto amministrativo che cambia. Atti del 53° Convegno di studi di scienza dell'amministrazione (Varenna, 20-22 settembre 2007)*, Milano, 2008, 27.

[30] Cfr., sul punto, Travi A. (1995), "Giurisprudenza amministrativa e principio di legalità",

più controversa è invece l'ammissibilità di poteri impliciti laddove invece l'ordinamento si limiti ad assegnare all'amministrazione solo *compiti* (obiettivi, finalità, interessi da tutelare), senza però dotarla esplicitamente di un potere correlato. Ciò perché il nucleo essenziale del principio di legalità – quale meccanismo di legittimazione – consiste appunto nella circostanza per cui il potere spetta solo se esplicitamente attribuito da una norma giuridica, secondo il principio di attribuzione. In questo caso, lo schema dei poteri impliciti appare in rotta di collisione insanabile con il principio di legalità, dal momento che la sua ammissibilità aprirebbe le porte all'esercizio di un potere arbitrario (perché sostanzialmente auto-attribuito), sulla base di una giustificazione insufficiente (la strumentalità del potere all'esecuzione del compito affidato dalla legge) alla luce dello standard legale implicato dal principio di legalità.

Abbiamo potuto verificare come questa chiave di lettura alternativa (potere implicito/potere esplicito) trovi corrispondenza nello *standard duale* che caratterizza il regime di disciplina dell'uso dei dati personali finalizzato all'esercizio di compiti di interesse pubblico. La *clausola di necessarietà* che caratterizza lo standard di base disegnato dal GDPR può, infatti, essere integrata (in modo più o meno significativo) per effetto dalla legislazione *eventualmente* adottata dallo Stato membro, nell'esercizio di quel margine di manovra ad esso accordato dalle clausole di cui all'art. 6, parr. 2 e 3 del GDPR. L'intervento della disciplina di *adattamento* è suscettibile di alterare lo standard di base, secondo modalità (e anche in direzioni) diverse, a seconda del tipo di scelte concrete compiute dai legislatori locali.

Il caso italiano, sotto questo specifico angolo di osservazione, è particolarmente interessante e significativo, dal momento che nel tempo (nel tempo successivo all'entrata in vigore del regolamento 679/2016) ha sperimentato – nell'esercizio del margine di manovra di cui sopra – due standard legali molto diversi tra loro. Dapprima, uno standard legale ispirato a una *strict legality rule*, tale per cui gli elementi essenziali del trattamento dei dati personali per l'esercizio compiti di interesse pubblico (finalità del trattamento, dati da trattare, operazioni da compiere) dovevano essere esplicitamente previsti e disciplinati da una norma di legge o, nei casi previsti dalla legge, di regolamento. Successivamente, per effetto delle modifiche introdotte con il d.l. n. 139/2021 (come modificato dalla l. n. 205/2021), lo standard legale è stato profondamente riorientato nella direzione della *necessary clause*, e co-

in *Diritto pubblico*, 90 ss.; cfr. anche Pantalone P. (2020), "Regolazione indipendente e anomalie sostenibili al cospetto delle matrici della legalità", cit., 446.

munque riconoscendo all'amministrazione (al titolare del trattamento) un significativo spazio di autonomia e di iniziativa al fine di integrare e completare la base giuridica che legittima il trattamento dei dati personali.

Sulla base di questa ricostruzione, è possibile affermare che la *strict legality rule* realizza certamente un assetto nel quale le preoccupazioni connesse all'ammissibilità di *poteri impliciti* da riconoscersi alle amministrazioni, nel trattamento dei dati personali, vengono risolte in modo *esplicito* ed in aderenza alle esigenze del principio di legalità[31]. Il *potere esercitato* dall'amministrazione *nel trattare i dati personali*, in vista dell'esercizio di compiti di interesse pubblico, infatti, *deve essere* formalmente attribuito (e disciplinato in alcuni aspetti essenziali) dalla fonte legislativa.

Diversamente, l'adozione di un assetto prossimo alla piena applicazione della *necessary clause* sembra porre problemi *rilevanti*, sotto questo profilo, dal momento che questa autorizza l'amministrazione ad esercitare quelle quote di potere connesse al trattamento dei dati personali anche in assenza dell'attribuzione di questi poteri *ad opera della legge*. Vale la pena sottolineare che, quantomeno con riferimento ad alcune specifiche tipologie di trattamento, l'intervento legislativo appare comunque necessario anche in vigenza della sola *necessary clause*, per effetto di quella giurisprudenza della Corte di giustizia che – in ragione della gravità dell'ingerenza sulle libertà ed diritti fondamentali degli interessati – impone che eventuali trattamenti di dati personali finalizzati al soddisfacimento di finalità di interesse pubblico che consistano nella *comunicazione al pubblico di dati personali* debbano essere previsti e disciplinati mediante atti normativi di rango legislativo. E tuttavia, anche così il numero, le classi e le tipologie di trattamenti che restano potenzialmente governati dalla *necessary clause* è rilevantissimo.

Una prima conclusione che si potrebbe trarre dalla concreta vigenza della *necessary clause* (sia per effetto della diretta applicabilità dello standard di base contenuto nel GDPR, sia – più di recente – per effetto della specifica declinazione del margine di adattamento sperimentata con le modifiche introdotte dal d.l. 139/2021), è che in questo settore assistiamo ad una concreta manifestazione di quella *crisi* della legalità che si sperimenta da tempo, sotto molteplici punti vista, per effetto di molti fattori, e che in questo caso sarebbe

[31] Cfr. in questo senso Cardarelli F. (2021), *Comm. sub. art. 2-ter Codice Privacy*, cit., 1017: "Per ciò che concerne il trattamento dei dati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri [...] appare evidente che tanto l'evocazione dell'interesse pubblico, quanto l'esercizio del pubblico potere riguardi categorie ascrivibili in massima parte all'operato delle amministrazioni pubbliche: *per le quali vale, sotto il profilo costituzionale, l'applicazione del principio di legalità* in base al comma 2 dell'art. 97 Cost." (corsivo aggiunto).

(all'evidenza) l'effetto del prevalere dei principi e dei caratteri che sono propri del diritto dell'Unione, nel cui contesto giuridico tale principio non ha esplicito riconoscimento, in particolare se interpretato quale criterio di legittimazione del potere amministrativo[32]. In questo senso, le dinamiche del *dual legality standard* opererebbero come una sorta di *valvola* a disposizione dello Stato membro, con la quale sarebbe cioè possibile regolare la quantità di *principio di legalità* (come presupposto per l'esercizio del potere amministrativo) da immettere (o mantenere) nell'ordinamento a correzione dello standard legale applicabile *by default* (per affetto della efficacia diretta delle norme del regolamento, ivi comprese quelle che disegnano la *necessary clause*). In questo senso, il legislatore locale disporrebbe dello strumento utile per conservare (e modellare) il tipo di rapporto tra legge e (potere dell') amministrazione, adeguandolo alle proprie esigenze e alla propria identità costituzionale. Sarebbe in definitiva *questo* il senso e lo scopo delle clausole di adattamento contenute nell'art, 6, parr. 2 e 3 del regolamento, nell'economia di un sistema istituzionale complessivo che continua a rimettere alle amministrazioni degli Stati membri una quota particolarmente significativa dell'esecuzione dei compiti e delle finalità fissati dall'ordinamento dell'Unione.

Tuttavia, questa lettura, così apparentemente lineare e appagante sotto il profilo ricostruttivo (sebbene problematica con riferimento alle sue ricadute

[32] "Chi, infatti, volesse cercare la legalità nell'affollato spazio giuridico europeo con la lanterna della vecchia legalità legislativa non la troverebbe. Di più: fino alla Carta dei diritti fondamentali dell'Unione (…) che, al suo art. 49, ricalca sostanzialmente la formulazione dell'art. 7 della Convenzione europea dei diritti dell'uomo, con l'aggiunta del corollario della retroattività favorevole — il principio di legalità non compariva nel diritto scritto dell'Unione europea. Esso aveva ricevuto cittadinanza, quasi esclusivamente nel settore penale, attraverso l'attività interpretativa della Corte di giustizia che l'aveva annoverato tra i principi generali del diritto comunitario, ricavandolo dalla Convenzione europea e dalle tradizioni costituzionali degli Stati" (così Vogliotti M. (2013), *Legalità*, in *Enc. Dir., Ann*. VI, 371-435, in part. 410); ribadisce che il (debole) ancoraggio del principio di legalità nell'ordinamento "comunitario" sarebbe da reperirsi (esclusivamente) nel richiamo alle *tradizioni costituzionali comuni* quali principi generali dell'ordinamento comunitario, secondo quanto previsto dall'art. 6, par. 3 del Trattato sull'Unione Europea, Adinolfi A. (2008), *Il principio di legalità nel diritto comunitario*, in *Il principio di legalità nel diritto amministrativo che cambia. Atti del 53° Convegno di studi di scienza dell'amministrazione (Varenna, 20-22 settembre 2007)*, cit., 87 ("La prima difficoltà che presenta un'analisi del principio di legalità nell'ordinamento comunitario discende dalla peculiare terminologia che in esso viene utilizzata: infatti, né il Trattato istitutivo, né il Trattato sull'Unione europea enunciano un "principio di legalità" utilizzando questa formulazione. Si può ritenere, tuttavia, che tale principio sia richiamato implicitamente dall'art. 6 par. 1 del Trattato sull'Unione europea laddove si afferma che l'Unione si fonda, tra l'altro, sui principi di democrazia e dello stato di diritto, principi che sono "comuni agli Stati membri". Secondo tale prospettiva, dunque, il principio di legalità sarebbe intrinseco all'ordinamento dell'Unione in quanto risulta dalle tradizioni costituzionali comuni degli Stati membri"; *ivi*, 87).

concrete, con particolare riferimento alla *tenuta* di un nucleo essenziale del principio di legalità), nasconde alcune insidie, nella misura in cui rischia di occultare (o sottovalutare) alcuni aspetti specifici dei *modi* con i quali si realizza la tutela dei dati personali, per effetto della interazione (ed integrazione) dei due *standard legali* posti a tema e analizzati nel corso di questo lavoro. Nel paragrafo seguente, con cui chiudiamo il nostro lavoro di analisi, indichiamo alcuni di questi *nessi*, con specifico riferimento modo con il quale viene realizzata la tutela dei dati personali (conformemente ai principi sanciti dal GDPR) – bilanciandola con le esigenze connesse al perseguimento dei compiti di interesse pubblico – in relazione alle diverse combinazioni dei due standard legali.

4. Standard legali e conformità ai principi del regolamento

4.1. La strict legality rule *e l'effetto di «schermo»*

Come si è già avuto modo di illustrare, sotto la *strict legality rule*, la disciplina di alcuni aspetti qualificanti del trattamento (funzionale all'esecuzione di compiti di interesse pubblico) è necessariamente *attratta* nella fonte legislativa: è la legge che deve prevedere quali dati possono essere trattati e quali operazioni posso essere effettuate, e che deve esplicitare le finalità del trattamento. Come detto, l'attrazione alla fonte legislativa ha come potenziale ricaduta quella di *irrigidire* la soluzione di trattamento che il titolare è autorizzato ad implementare (quantomeno con riferimento agli elementi attratti nella fonte legislativa), dal momento che, una volta fissati in legge, questi elementi si *impongono* al titolare del trattamento. Per poterli modificare, integrare, ovvero aggiornare (ove opportuno o indispensabile) sarà quindi necessario *ritornare* alla fonte legislativa. L'irrigidimento così ottenuto opera quindi anche in termini di garanzia (l'amministrazione/il titolare del trattamento deve attenersi a quanto prescritto dalla norma, che la limita nella scelta dei mezzi da applicare).

Tuttavia, l'attrazione alla fonte legislativa di questi elementi relativi alla modalità del trattamento (esplicita indicazione della finalità del trattamento, identificazione dei dati suscettibili di trattamento, operazioni di trattamento) può avere anche un altro effetto, che è quello di *schermare* questi elementi (per come codificati/attratti nella norma) rispetto ad una integrale valutazione di conformità al parametro di liceità fissato dal GDPR, all'art. 6(1)(e). Ciò in conseguenza di due fattori, che si combinano tra loro. Per un verso, sono le stesse clausole dell'art. 6 (quelle di cui ai parr. 2) e 3)) che consen-

tono alle disposizioni introdotte dallo Stato membro di *adeguare* la base giuridica (su cui il trattamento *è fondato*) e che prevedono che tali disposizioni potrebbero contenere misure di adeguamento relative (tra l'altro) a: *le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento*; *le tipologie di dati oggetto del trattamento*; (…) *le limitazioni della finalità*, (…) *le operazioni e procedure di trattamento*" (par. 3). Tali disposizioni, dunque, possono anche individuare *direttamente* quali trattamenti possano essere effettuati, su quali tipologie dati e per quali finalità. Ovviamente, anche questi elementi possono essere valutati (in astratto) in ordine all'esistenza del *nesso di strumentalità necessaria* rispetto all'esercizio dei compiti di interesse pubblico. E tuttavia, e qui entra in gioco il secondo fattore, quando tali elementi sono disciplinati direttamente da una fonte di rango legislativo, tale valutazione è necessariamente mediata e filtrata da questa circostanza. Infatti, in questo caso è lo stesso legislatore ad aver stabilito che il trattamento in questione è strumentale all'esercizio dei compiti di interesse pubblico: anzi, nel destinare *esplicitamente* un determinato trattamento all'esecuzione del complito di interesse pubblico, è *il legislatore ad istituire il nesso di strumentalità*. Si può dire, cioè, che in questo caso il nesso di strumentalità è *sussunto* nella disposizione legislativa[33]. Questo giudizio in ordine al *nesso di strumentalità* operato dal diritto dello stato membro può essere oggetto di sindacato, e tuttavia il fatto che esso sia contenuto in un *atto legislativo* (in base alla *strict legality rule* (interna)) ha delle specifiche conseguenze, perché il tipo di sindacato cui sarà assoggettabile consegue da tale circostanza. Per un verso, infatti, l'*esistenza in sé* del margine di manovra (per come declinato nell'art. 6, parr. 2 e 3 sembrerebbe riconoscere allo stato membro anche *uno spazio*, *un margine* entro il quale formulare questo giudizio (circa l'esistenza del nesso di *strumentalità necessaria*). Inoltre, all'esistenza di spazi di adeguamento disponibili al legislatore (e, in ipotesi, utilizzati per individuare *direttamente* i trattamenti da effettuare, su quali dati, con quale finalità, sulla base della *strict legality rule*) corrisponde la circostanza per cui a essere oggetto di sindacato non saranno

[33] Abbiamo osservato questo fenomeno, con riferimento alle disposizioni legislative che prevedono la raccolta delle informazioni presso l'*Anagrafe dei rapporti finanziari*, destinate (dallo stesso legislatore) ai trattamenti di interconnessione e analisi finalizzati all'emersione di profili di rischio di evasione; abbiamo pure osservato che il Garante fin da subito formula delle osservazioni critiche in ordine alla sussistenza del nesso di strumentalità necessaria (alla luce del criterio di legittimazione di cui all'art. 6(1)(e) del GDPR), senza che – tuttavia – tali valutazioni potessero tradursi in misure concrete, proprio in ragione della *natura* (legislativa) della base giuridica che aveva istituito esplicitamente tale nesso di strumentalità: cfr. *supra*, cap. 5, par. 2.1 e il parere del Garante n. 145 del 17 aprile 2012, doc. web n. 1886775, par. C. per una analoga attrazione del nesso di necessarietà strumentale entro la previsione legislativa del trattamento, cfr. il caso trattato nella recente causa C-268/21 *Norra Stockholm Bygg AB*, cit.

detti elementi del trattamento, *in quanto tali*, ma piuttosto (innanzitutto) le *misure* nelle quali tali elementi del trattamento sono espressamente previsti e disciplinati. Nel caso della *strict legality rule*, si tratterà di quelle disposizioni che avranno disciplinato (alcuni de)gli elementi di cui all'art. 6(3) GDPR, in base alla clausola di adattamento di cui all'art. 6(2).

Tuttavia, proprio in base all'art. 6(3) del GDPR tale misura così introdotta "persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito". Come si vede, nel caso in cui intervengano disposizioni dello stato membro volte a *precisare* e *adattare* la base giuridica che legittima il trattamento (effettuato per finalità di cui all'art. 6(1)(e)), il parametro di giudizio da applicare a queste disposizioni è che tali misure risultino *proporzionate* e che *perseguano un interesse pubblico*.

La lettura della giurisprudenza della Corte di giustizia fornisce significative conferme. Fermo restando che a giudizio della Corte il presupposto di liceità resta *sempre* quello indicato all'art. 6(1)(e), quando si è trattato di farne applicazione in costanza di una disciplina di adattamento adottata (o mantenuta) dallo Stato membro, possiamo constatare che le modalità di sindacato mutano a seconda delle circostanze concrete. Si è già visto che solo nel caso in cui l'ingerenza nel diritto alla tutela dei dati personali si configuri come *particolarmente grave* (nel caso cioè di trattamenti che consistono nella comunicazione al pubblico di dati personali) la Corte proceda direttamente a verificare se la *misura prevista dalla legge comporti dei limiti/delle ingerenze a questi diritti entro quanto strettamente necessario per il conseguimento del fine di interesse pubblico*[34]; ma abbiamo anche constatato come in quel caso il criterio di necessarietà applicato non serve a verificare il nesso di strumentalità tra il trattamento disposto e il compito di interesse pubblico da eseguire, quanto piuttosto a contenere la misura entro cui è lecito limitare i diritti dell'interessato. Quando invece l'ingerenza non raggiunge questa soglia di *gravità*, la Corte generalmente rimette la valutazione circa l'integrazione del requisito di *necessarietà strumentale* al giudice nazionale[35], anche in ragione dell'opportunità di valutare le disposizioni pertinenti con riferimento allo specifico contesto legislativo ed ordinamentale in cui si inseriscono. E tuttavia, in questo modo il giudice nazionale si trova nella necessità di valutare misure che possono essere state disposte o mediante disposizioni interne subordinate e/o soggette alla legge – e che quindi possono essere più agevolmente sindacate ed aggredite dal giudice stesso; oppure, misure che sono state disposte mediante atti di rango *legislativo* – come nell'ipotesi di

[34] Cfr. Corte di giustizia UE, C-184/20, punto n. 70; nonché C-439/19, punto n. 109-110.

[35] Cfr. Corte di giustizia UE, C-73/16, punto n. 112-113; C-524/06, punti n. 66-67; C-268/21, punto n. 46.

cui stiamo discutendo. In questa seconda ipotesi, esperita ed esaurita (eventualmente) la fase del rinvio pregiudiziale, il giudice potrà *sì* sindacare l'atto legislativo (al fine, eventualmente, di disapplicarlo) ma alla stregua del parametro indicato dallo stesso GDPR, ovvero in base ad una valutazione circa la *proporzionalità* della misura così disposta rispetto all'obiettivo di interesse pubblico (art. 6, par. 3). In altre parole, rimesso o posizionato il giudizio di conformità con il GDPR sul piano nazionale, in questa sede – qualora il trattamento sia disciplinato da disposizione di legge – la valutazione non potrà avere per oggetto l'*effettiva ricorrenza del nesso di strumentalità necessaria* (che è implicitamente o esplicitamente dichiarata dal legislatore), ma piuttosto la *proporzionalità* della misura legislativa che lo dispone.

Pertanto, sotto la *strict legality rule*, una volta che il legislatore abbia costituito direttamente (in modo implicito o esplicito) il nesso di strumentalità necessaria del trattamento, e nella misura in cui abbia direttamente identificato nella norma legislativa la tipologia di dati da trattare e le operazioni che possono essere effettuate, questi elementi (quantomeno, per quanto concerne gli aspetti direttamente declinati nel testo legislativo) potranno essere valutato in termini di *proporzionalità* rispetto all'obiettivo di interesse pubblico, in ragione del margine di adattamento riconosciuto allo stesso legislatore nazionale.

L'effetto complessivo che si potrebbe registrare, dunque – conseguente all'attrazione di una serie di elementi qualificanti del trattamento alla fonte legislativa primaria – sarebbe non solo quello di irrigidimento *della soluzione di trattamento*, ma anche di *un più limitato spazio di sindacabilità*, di raffrontabilità con il parametro costituito dal GDPR. In particolare, salvo che per i trattamenti caratterizzati da un tasso di ingerenza particolarmente grave sul diritto alla tutela dei dati personali, il nesso di strumentalità potrebbe venire valutato non alla stregua del requisito di necessarietà strumentale, ma in base a quello di proporzionalità rispetto all'obiettivo legittimo perseguito, un criterio di sindacato applicato per altro non *al trattamento*, ma alla disciplina legislativa che ne incorpori e ne declini alcuni elementi. Nella misura in cui tale valutazione è ricondotta (dalla stessa Corte di giustizia) alla verifica del rispetto del principio di minimizzazione[36], ciò comporta che il *focus* del giu-

[36] Nella giurisprudenza della Corte di giustizia, il riferimento per l'applicazione di questo specifico giudizio di proporzionalità è reperito nel principio di *minimizzazione* di cui all'art. 5(1)(c) del GDPR (cfr. C-268/21, punto n. 46: "la considerazione degli interessi in gioco rientra nell'ambito dell'esame della proporzionalità della misura, che sono previste all'articolo 6, paragrafi 3 e 4, del RGPD e che condizionano la liceità del trattamento di dati personali. A tal riguardo, occorre quindi tenere conto anche dell'articolo 5, paragrafo 1, di quest'ultimo, e in particolare del principio della «minimizzazione dei dati» di cui alla lettera c) di tale disposizione, che dà espressione al principio di proporzionalità"; nonché, in termini analoghi, C-439/19).

dizio si sposta in ogni caso dalla verifica del *nesso di strumentalità del trattamento*, alla valutazione del criterio di *minimizzazione dei dati* oggetto del trattamento: un "salto" nel quale la verifica del nesso di strumentalità necessaria (del trattamento) viene implicitamente assorbita (e data per acquisita)[37].

Di più, qualora questa misura legislativa risultasse/fosse valutata come effettivamente *proporzionata*, gli elementi del trattamento dei dati che si traducono poi in mera applicazione di quanto già previsto e disposto nell'atto legislativo risulterebbero sostanzialmente sottratti ad un sindacato ulteriore, quanto ai profili di necessarietà (del trattamento, in quanto già istituita dalla norma di legge), necessarietà (dei dati trattati, se ed in quanto già identificati nella norma legislativa); tipologia di operazioni eseguibili (se ed in quanto descritte dalla norma).

Insomma, lo standard della *strict legality rule*, imponendo l'attrazione nel testo della legge della disciplina di una serie di elementi del trattamento, comporterebbe non solo un irrigidimento del trattamento stesso, ma anche uno schermatura degli elementi oggetto di *legificazione* da un più approfondito esame/sindacato alla stregua del principio di necessarietà, dal momento che tali elementi resterebbero assorbiti nel sindacato riservato invece al veicolo che li dispone, sindacato articolato nei termini della proporzionalità rispetto all'obiettivo legittimo perseguito dalla disposizione legislativa.

Sotto questo profilo, il caso del *tool* Ve.R.A. è indicativo. Più volte nel corso del tempo il Garante, nei suoi pareri, ha sollevato dubbi e perplessità in ordine ai profili di necessarietà del trattamento come individuato dal legislatore, anche con riferimento alle modalità di raccolta e trattamento dei dati. E tuttavia, il fatto che tali elementi del trattamento fossero previsti nella legge ha sostanzialmente impedito che il Garante potesse richiederne la verifica/la correzione al titolare del trattamento. E anche la specifica formulazione testuale mediante la quale è stata inserita nel nostro ordinamento la *necessary clause* suggerisce che la consapevolezza per il potenziale effetto di *schermo* esercitato dalla disciplina di adattamento nazionale è stata presa in considerazione[38]. L'esercizio del margine di manovra in accordo alla *strict legality*

[37] Si consideri, poi, che l'*assessment* relativo al principio di *minimizzazione dei dati* difficilmente potrà avere a oggetto la disciplina legislativa, a meno che questa non individui in modo analitico e compiuto la tipologia di dati oggetto del trattamento; il che però non accade quasi mai, dal momento che questo genere di scelte di precisazione, selezione e individuazione de dati da fare oggetto di trattamento sono rimesse a fonti subordinate (quando non ad atti della stessa amministrazione), laddove il legislatore si limita piuttosto ad individuare la classe e la tipologia di dati oggetto di trattamento. Anche qui, il caso di studio relativo all'indicatore del rischio di evasione ci ha fornito utilissime indicazioni.

[38] In altre parole, la scelta di ribadire nel testo del comma 1-bis dell'art.2-ter, come introdotto a seguito della conversione in legge del d.l. 139/2021 la piena soggezione dei trattamenti al rispetto del GDPR (mediante espressioni quali: "*fermo restando ogni altro obbligo previsto dal*

rule, pertanto, potrebbe comportare un tasso più ridotto di aderenza ad alcuni dei principi/vincoli del GDPR, a cominciare dalla verifica del nesso di strumentalità necessaria del trattamento, nella misura in cui questo risulti direttamente disciplinato, per aspetti qualificanti, dalla norma di legge.

Più in generale, l'effetto combinato di *irrigidimento* e *schermatura* conseguente alla *strict legality rule*, pare configurare soluzioni di trattamento dei dati personali per l'esercizio dei compiti di interesse pubblico non solo poco flessibili, ma pure caratterizzate (almeno, potenzialmente) da tassi meno intensi di aderenza ai principi e ai vincoli del GDPR.

4.2. Necessary clause *e conformità al regolamento*

Analizziamo adesso, sotto i medesimi profili, gli effetti conseguenti all'adozione della *necessary clause*, con specifico riferimento alla sua declinazione nell'ordinamento nazionale a seguito delle modifiche al Codice apportate nell'autunno del 2021. Come già sottolineato, l'adozione di questo standard legale, nella misura in *alleggerisce* e *semplifica* i presupposti di liceità del trattamento dei dati personali per l'esercizio di compiti di interesse pubblico, determina un ribilanciamento delle esigenze di funzionalità, buon andamento e autonoma iniziativa delle amministrazioni (*rectius*, dei titolari di trattamento per l'esecuzione di compiti di interesse pubblico) rispetto alle esigenza di predeterminazione (in legge) della funzione amministrativa anche con riferimento agli elementi connessi al trattamento dei dati personali. Infatti, un maggiore spazio di manovra e di iniziativa in capo alle amministrazioni pubbliche comporta *di per sé* un aumento dei rischi di trattamenti scorretti, pericolosi, lesivi. Inoltre, per le ragioni già evidenziate, la *necessary clause* pone questioni specifiche in ordine alla ammissibilità della quota di potere implicito così riconosciuta alle amministrazioni.

Limitando l'analisi al trattamento dei dati personali comuni (fermo restando che *per analogia*, data la disciplina positiva vigente, molte di queste considerazioni potrebbero essere estese anche al trattamento dei dati particolari), il presupposto di liceità fissato con il decreto «capienze» consente ai titolari di ampliare lo spazio di iniziativa secondo due meccanismi: 1) specificare la base giuridica mediante l'adozione di un atto amministrativo generale (art. 2-ter, comma 1); adottare il trattamento che risulti comunque necessario al perseguimento di un compito di interesse pubblico (comma 1-

Regolamento" nonché "*in modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle liberta' degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento e dal presente codice*") andrebbe letta proprio in questo senso, a congiurare ogni eventuale effetto di *schermo*.

bis). Ciò che qui si vuole sottolineare è che entrambi questi meccanismi comportano il dovere per l'amministrazione di esplicitare il nesso di strumentalità necessaria del trattamento posto in essere, secondo modalità che comportano una piena sindacabilità di queste scelte alla luce del parametro (di legittimazione) di cui all'art. 6(1)(e) del GDPR.

Infatti, gli atti amministrativi generali – con i quali il titolare può sia specificare/precisare il compito di interesse pubblico cui il trattamento è strumentale, sia individuare ed esplicitare gli ulteriori elementi che integrano la clausola di necessarietà strumentale (*quali trattamenti*, *quali dati*, *per quali finalità*) – sono assoggettati al pieno rispetto delle disposizioni del regolamento, sia quando siano oggetto di valutazione preventiva ad opera dell'autorità di controllo nazionale (in virtù dell'art. 36 del GDPR), sia in sede di controllo: giurisdizionale, ma non solo[39]. Infatti, in questo caso l'istituzione del vincolo di *strumentalità necessaria* non appare fruire dell'effetto di *schermatura* analogo a quello prodotto (o conseguente) dalla fonte legislativa primaria. L'atto amministrativo generale (anche in quanto esplicitamente distinto da un atto di natura regolamentare) non è una fonte dell'ordinamento (interno), e come tale interloquisce con le fonti del diritto (a cominciare con quella di diretta applicazione rappresentata dal GDPR) in modo conseguente. Al di là delle peculiarità del riparto di competenza giurisdizionale in materia di tutela dei dati personali, ciò assicura una piena "presa" dei principi e delle disposizioni del regolamento. In particolare, quegli spazi di *deroga* che potrebbero essere ammissibili in ragione della fonte adoperata per introdurli (la legge) – fermi restando i limiti e le condizioni per la limitazione di tali diritti alla luce della giurisprudenza della Corte di giustizia – appaiono in effetti *preclusi* a basi legali interne che non assurgano al rango di fonti del diritto. E perciò, per questa tipologia di atti *effettivamente* l'integrazione ad opera di disposizioni interne (quella autorizzata dall'art. 6, parr. 2 e 3) non può che tradursi in una *ulteriore precisazione* dei requisiti già disposti dal GDPR[40]. In altre parole, poiché tali atti generali si configurano, tipicamente, come la modalità con la quale *predisporre* e *organizzare* una determinata ipotesi di trattamento da destinare in modo stabile al servizio dell'esecuzione di uno specifico compito di interesse pubblico (cioè, sono

[39] Come ribadito di recente dalla Corte di giustizia, infatti, "le autorità di controllo hanno come compito principale quello di sorvegliare l'applicazione del RGDP e di vigilare sul rispetto di quest'ultimo (…) Inoltre (…) ogni autorità di controllo è tenuta, nel suo territorio, a trattare i reclami che qualsiasi persona (…) ha il diritto di proporre quando considera che un trattamento di dati personali che la riguardano costituisca una violazione di tale regolamento, e ad esaminarne l'oggetto nella misura necessaria", cfr. *Schrems II*, causa C-311/18, punti 108-109.

[40] Cfr. Wagner J. e Benecke A. (2016), "National legislation within the framework of the Gdpr", cit., 354.

atti di organizzazione della *funzione*[41]), essi verranno chiamati in causa ogni qualvolta il titolare del trattamento sia chiamato (nelle sedi opportune) a dare prova e dimostrazione di aver predisposto il trattamento nel rispetto dei principi del regolamento[42].

Quanto al secondo meccanismo (il trattamento *consentito se necessario*), questo non solo incorpora già la clausola in questione, ma – come ricordato poco più alto – la disposizione che lo introduce ribadisce integralmente i vincoli conseguenti da "ogni altro obbligo previsto dal Regolamento", nonché quelli specifici previsti dall'art. 6 "in modo da assicurare che [il trattamento dei dati] non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati". Tali vincoli, quindi, *si dispiegano pienamente*. In questo caso, è la misura di trattamento specifica che deve in qualche modo indicare, rendere evidenti, gli elementi che sono indispensabili per fondarne la liceità, a cominciare dal nesso di *strumentalità necessaria* rispetto al compito di interesse pubblico cui il trattamento è servente. Come è stato chiarito efficacemente dall'avvocato generale Bobek, l'onere di giustificazione (in termini di integrazione del presupposto di liceità) che grava su un singolo trattamento operato in concreto è inversamente proporzionale a quanto già assolto in questo senso dalle basi giuridiche che disciplinano *in astratto* quella ipotesi di trattamento[43]. Pertanto, il presupposto di liceità accordato dall'art. 2-ter, comma 1-bis impone oneri variabili al titolare che vi faccia ricorso, a seconda delle circostanze concrete. Nel caso in cui la base legale sia già strutturata, la clausola opera come "norma di chiusura", in modo da consentire (se necessario) di completare il presupposto di liceità, in riferimento al caso concreto. In assenza invece di un previo quadro di riferimento (che non vada oltre l'assegnazione del compito di interesse pubblico),

[41] Per l'attrazione della nozione di funzione amministrativa entro il campo dell'*organizzazione*, in quanto predeterminazione dei complessi di attività attribuite ai soggetti pubblici in vista della cura di specifici interessi pubblici, si veda Merloni F. (2009), *Organizzazione amministrativa e garanzie dell'imparzialità. Funzioni amministrative e funzionari alla luce del principio di distinzione tra politica e amministrazione*, in *Diritto pubblico*, 2009, 1, 57 ss.

[42] Sulla base del principio di responsabilizzazione di cui all'art. 5, par. 2 del GDPR.

[43] "In altre parole, i due livelli di regolamentazione, ossia quello legislativo e quello amministrativo, che fungono da base giuridica finale del trattamento dei dati, operano congiuntamente. Almeno uno di essi deve essere sufficientemente specifico e adeguato a uno o più tipi o quantità determinati di [trattamenti]. Quanto più è dettagliato il livello legislativo e strutturale per tali [trattamenti], quanto meno è necessario che lo sia la singola [operazione] amministrativa. Il livello legislativo potrebbe anche essere così dettagliato e completo da essere del tutto autosufficiente e immediatamente esecutivo. Al contrario, quanto più generico e vago è il livello legislativo, tanto più a livello della singola [operazione] amministrativa saranno necessari dettagli, compresa l'esplicita dichiarazione delle finalità che ne delimiterà così la portata", così le conclusioni dell'Avvocato generale Bobek, C-175/20, punto n. 81.

la clausola consente di integrare tutti gli elementi necessari a fondare la liceità del trattamento. In questo caso, l'onere è molto più impegnativo: il titolare del trattamento dovrà declinare il requisito della strumentalità necessaria rispetto ad una molteplicità di elementi (essenzialmente: quali – e quanti – dati trattare, quali operazioni effettuare, per quale finalità). In ogni caso (cioè, a prescindere dalla collocazione dell'ipotesi di trattamento da fondare, entro lo spettro compreso tra questi due estremi), è sempre da assicurarsi la conformità rispetto ai requisiti di cui all'art. 6(1)(e), ai principi di cui all'art. 5, ed in generale alle pertinenti disposizioni del regolamento.

Pertanto, a fronte degli (indubbiamente) maggiori margini di manovra in termini *di disponibilità degli strumenti di trattamento* e di *autonoma iniziativa* riconosciuti dal decreto «capienze» ai titolari del trattamento cui sono affidati compiti di interesse pubblico, il loro concreto esercizio resta costantemente sottoposto ai vincoli derivanti sia dal presupposto di liceità della *strumentalità necessaria*, sia dagli altri principi ed istituti del GDPR. Nella misura in cui la rispondenza a tali principi integra (con riferimento ai trattamenti concretamente posti in opera) l'equilibrio delineato dal regolamento, nel combinare le esigenze di tutela dei dati personali e le esigenze del loro trattamento per fini di interesse pubblico, è arduo argomentare che tale *standard legale* comporti effettivamente un *depotenziamento* della tutela dei dati personali[44], sul piano delle *regole*, soprattutto se posto a confronto con quello realizzato sotto lo standard della *strict legality rule*. Piuttosto, per le ragioni argomentate più sopra, la *necessary clause* – sotto la quale acquista maggiore rilievo e pregnanza il principio di «responsabilizzazione» – pare più idonea (rispetto al regime di *strict legality rule*) a promuovere una verifica ed un adeguamento costanti dei presupposti di trattamento, proprio perché i mezzi per fare fronte a tale adeguamento sono nella disponibilità del titolare del trattamento. Ciò che risulta un aspetto per il vero *cruciale*, in un ambito operativo caratterizzato da dinamiche di sviluppo e avanzamento tecnologico formidabili.

[44] Vedi quanto argomentato in sede di audizione sulla conversione in legge del decreto 139/2021, da M. Bassini, "Giova subito sgombrare il terreno da un potenziale equivoco: non pare che, sul piano prettamente contenutistico, le norme di nuova introduzione conducano a un'effrazione rispetto alla fonte sovranazionale competente, ossia il Regolamento generale sulla protezione dei dati personali ("GDPR"). Nondimeno, il nuovo assetto che giunge a configurarsi per effetto di queste chirurgiche modifiche previste dall'art. 9 sembra realizzare un complessivo depotenziamento della posizione di tutela dell'interessato al cospetto di trattamenti di dati personali da parte soprattutto della Pubblica Amministrazione, depotenziamento cui non è estraneo il ridimensionamento dei poteri conferiti all'Autorità garante per la protezione dei dati personali proprio a questo proposito".

Ovviamente, tale assetto, proprio nella misura in cui assegna una *maggiore autonomia operativa e di iniziativa*, comporta anche maggiore *responsabilità*, ed è quindi una *sfida* per le amministrazioni che intendano approfittarne. La *strict legality rule* costituisce infatti anche un modulo regolatorio nell'ambito del quale i titolari del trattamento possono trovare maggiori sicurezze, potendo confidare nella copertura offerta dalla legge, laddove invece la *necessary clause* li pone a diretto confronto con i vincoli e le condizioni imposte dal GDPR, e con la necessità di conformarsi a essi, senza la rete di protezione costituita dalla legge. Un ambiente operativo impegnativo, dunque, che richiede amministrazioni consapevoli e convenientemente attrezzate.

5. Quale legalità per il trattamento dei dati personali

Giunti al termine di questo percorso di ricerca, vorremmo provare ad inquadrare i caratteri degli standard legali individuati ed analizzati nel corso di questo di lavoro entro coordinate concettuali idonee a inserire le dinamiche (e le opzioni) che abbiamo osservato entro percorsi e chiavi di interpretazione più generali. Per farlo, ci appoggeremo ad una disanima della nozione di *legalità* che, preso atto dello stato di profonda *crisi* in cui versa la sua declinazione moderna, piuttosto che arrendersi di fronte ai suoi "sentieri interrotti"[45] ovvero considerarla definitivamente superata (e quindi da abbandonare in favore di altre nozioni, che catturino in modo più sincero le sostanze contemporanee del giuridico[46]), propone di rinnovarne l'identità mediante un ritorno all'antico[47]. La chiave interpretativa mette a confronto la *legalità dei moderni*, fondata sul pilastro della legge, in quanto *auctoritas* posta al vertice della piramide delle fonti e fondamento di validità dell'intero ordinamento giuridico, a una legalità come espressione di un "paradigma giuridico medievale", "un tessuto di *auctoritates* e *rationes*, intimamente intrecciate: le prime, infatti, per essere valide, devono essere conformi alle *rationes* del diritto (il diritto *ex parte societatis*); le seconde, per farsi valere,

[45] Riprendendo il titolo di un noto saggio di Fabio Merusi (Merusi F. (2007), *Sentieri interrotti della legalità. La decostruzione del diritto amministrativo*, Bologna).

[46] Come propone di fare Sabino Cassese, ad esempio, mediante il ricorso alla locuzione «regola di diritto» (Cassese S. (2003), *Le basi costituzionali*, in *Trattato di diritto amministrativo*, (eds.) Cassese S., *Diritto amministrativo generale*, I, Milano, 220 ss.) o a quella di «rispetto del diritto» (Cassese S. (2006), *Il diritto amministrativo e i suoi principi*, in *Istituzioni di diritto amministrativo* (eds.), Cassese S., Milano, 8 ss.).

[47] Cfr. Vogliotti M. (2013), *Legalità*, cit., *passim*.

devono tradursi, assumendo idonee forme e seguendo corretti itinerari procedurali, in *auctoritates*"[48]. Questa chiave interpretativa, particolarmente suggestiva, sia sotto il profilo analitico-ricostruttivo, sia in ragione della capacità di (ri)leggere, *in prospettiva*, tutti i principali fattori più recenti di rottura della legalità (dei moderni), viene qui richiamata nei suoi tratti essenziali, perché essi si prestano in modo particolarmente efficace a catturare ed illustrare le opzioni che caratterizzano il *dual legality standard* che siamo andati delineando.

Secondo questa lettura, nella prospettiva moderna, la "legalità è misura della corrispondenza degli atti di esercizio del potere (sentenze o provvedimenti) alla sostanza della legge (…) Amministrazione e giurisdizione sono concepite come attività esecutive, riproduttive di sostanze normative previamente definite, nella loro interezza e nelle linee essenziali, dal rappresentante del popolo sovrano"[49]. Entro queste coordinate concettuali, la legalità è "*corrispodenza*, che individua nella legge la garanzia principale se non unica dei diritti, e [la] giustizia amministrativa come controllo dell'adeguamento dell'atto alla sostanza legislativa per la «restaurazione della legalità obiettiva»" e "in modo ancora più rigoroso, la giurisdizione (…) era concepita come una mera cinghia di trasmissione che doveva consentire alle sostanze normative disposte sui gradini della piramide delle fonti di arrivare integre al livello dei fatti"[50]. *Mutatis mutandis*, riconosciamo qui alcuni tratti dello standard che abbiamo declinato in termini di *strict legality rule*: l'idea che gli elementi essenziali del trattamento debbano essere disciplinati *dalla* e *nella* legge e che la verifica in funzione della tutela dei dati personali debba esprimersi come controllo della corrispondenza/rispondenza del trattamento concretamente organizzato e svolto al modello descritto nella legge. Anche con riferimento a questo approccio, si può constatare che "in caso di imprevisti «il meccanismo è del tutto indifeso; la sua unica salvezza consiste nell'intervento del suo costruttore»"[51].

Diversamente, la *nuova* legalità "teleologica, progettuale e paratattica" (che si contrappone a quella "correspondista, esecutiva e ipotattica"[52]) recupera la seconda dimensione del diritto, da intendersi come *conformità allo scopo*, propria del sapere giuridico (nell'ordine medioevale) in quanto *sapere pratico*. Emblematico, sotto questo profilo, il delinearsi di un nuovo ruolo dell'amministrazione, la cui funzione "non è più (prevalentemente) funzione

[48] Cfr. *ivi*, 420.
[49] Cfr. *ibidem*.
[50] Cfr. *ivi*, 421.
[51] Cfr. *ivi*, 422, dove si richiama un passo di Mayr O. (1988), *La bilancia e l'orologio. Libertà e autorità nel pensiero politico dell'Europa moderna* (1986), Bologna, 209.
[52] Cfr. Vogliotti M. (2013), *op. cit.*, 424.

(giuridica) di mantenimento e restaurazione della legalità in esecuzione e sviluppo della legge, ma è (prevalentemente) funzione di assistenza ed integrazione sociali, certo in esecuzione della legge, ma anche in adempimento diretto di esigenze di giustizia che danno senso ultimo alla legge e ne colmano le lacune"[53]. La legittimazione del potere si sposta così dalla norma alla sua idoneità a perseguire lo scopo pratico: il potere deve poter essere nel suo complesso tale da consentire la realizzazione del fine proprio per cui è stato attribuito[54]. Di qui anche l'ammissibilità di poteri impliciti, nella misura in cui la legalità vada intesa non tanto come "tipizzazione ad opera della norma del tipo di provvedimento adottabile", quanto piuttosto riferibile "allo scopo di interesse pubblico"[55]. Questo diverso modo di intendere la legalità "muta radicalmente la vecchia sceneggiatura e attribuisce all'amministrazione e alla giurisdizione un ruolo da protagonista che il copione della modernità giuridica – concepito per un legislatore onnisciente – non poteva contemplare"[56]. In tale contesto, lo spazio lasciato alla discrezionalità dell'amministrazione non è solo conformato dalle regole legislative e non (*auctoritates*) e da principi (*rationes*), in particolare quelli di ragionevolezza, buon andamento ed imparzialità, ma anche dalla necessità di dover applicare e rispettare criteri o conoscenze tecniche, o dalla natura delle cose (desumendo cioè la "regola dalla logica della materia da regolare")[57]. Come è stato sottolineato, ciò che non solo è inevitabile, ma è anche un elemento necessario "per un adeguato funzionamento della macchina statale"[58].

Non è difficile scorgere, qui, in modo sufficientemente nitido i caratteri che abbiamo individuato a proposito dello standard legale di trattamento dei dati personali che abbiamo declinato come *necessary clause*. La centralità dello *scopo* come elemento di legittimazione del potere, la conseguente ammissibilità di *poteri impliciti*, il rilievo dell'integrazione della norma nel serrato confronto con le esigenze della società, con i saperi tecnici e la natura delle cose (si pensi alle rilievo delle "sostanze" informatiche, digitali, algoritmiche nella predisposizione delle soluzioni di trattamento dei dati personali), alla luce delle *rationes* costituite dai principi sul trattamento dei dati di

[53] Cfr. *ivi*, 424: qui l'Autore cita testualmente un passo di Nigro M. (1983), "È ancora attuale una giustizia amministrativa?", in *Foro it.*, V, 254.

[54] Cfr. *ibidem*.

[55] Cfr. *ibidem*, dove sono richiamati i passi tratti da Bassi N. (2001), *Principio di legalità e poteri amministrativi impliciti*, cit., 251.

[56] Cfr. *ivi*, 426-27.

[57] Cfr. *ibidem*

[58] Cfr. *ibidem*, dove sono richiamati sia Merusi F. (2011), *Ragionevolezza e discrezionalità amministrativa*, Napoli, 13 e De Pretis D. e Marchetti B. (2007), *La discrezionalità della pubblica amministrazione*, in Della Cananea G. e Dugato M., a cura di, *Diritto amministrativo e Corte costituzionale*, Napoli, 372 e 383.

cui all'art. 5 del GDPR. Come pure il ruolo da protagonista svolto dall'amministrazione (attiva e di controllo) e dalla giurisdizione, nella *tessitura* di questa legalità. Né è casuale che sia da identificare nel diritto dell'Unione il fattore propulsivo che immette nell'ordinamento nazionale questo specifico standard legale[59]. Il regime regolatorio abilitato dalla *necessary clause* pare quindi rispondere in modo fedele ad una rilettura della legalità in termini essenzialmente dualistici[60]: mentre l'*auctoritas* seleziona e attribuisce gli obiettivi di interesse pubblico, i mezzi per il loro raggiungimento sono costruiti (intessuti) sulla base delle *rationes* individuate dal GDPR (i principi di cui all'art. 5, il nesso di strumentalità necessaria di cui all'art. 6(1)(e)), nel continuo confronto con le esigenze espresse dalla società (mediate e filtrate

[59] "È davvero epocale — segno di un vero e proprio mutamento di paradigma giuridico — la metamorfosi della legalità, quale appare chiaramente dalla prospettiva europea: alla luce della nuova legalità ibrida (sbilanciata, come si è visto, verso il lato della ratio, della legittimazione e dei modi tipici della giurisdizione), il potere non è più valutato secondo il parametro unitario, formale, indiscutibile e inflessibile, della conformità al tipo legislativo (*dura lex sed lex*), ma secondo una rete di regole e, soprattutto, di principi, che valgono per la loro sostanza valoriale e sono flessibili, sempre oggetto di discussione e necessariamente soggetti a ponderazione e a bilanciamenti (252). Alla domanda: "è quel potere legale?" non si può più rispondere, come rispondeva, ecolalicamente e deresponsabilizzandosi, il giurista moderno, indicando la legge (*ita lex*), ma si deve rispondere, tramite una complessa e prudente attività di tessitura argomentativa di *auctoritates* e *rationes*, valutando se quel potere, in quel particolare contesto, è esercitato conformemente a diritto, ossia rispettando i parametri normativi vigenti (che saranno legislativi laddove una legge vi sia) e una rete di principi tra cui, ad esempio, quelli di ragionevolezza, proporzionalità, trasparenza, imparzialità, motivazione, sussidiarietà, leale cooperazione, cui va aggiunta la costellazione dei principi procedurali racchiusi nelle formule del giusto processo e del giusto procedimento amministrativo", così Vogliotti M. (2013), *Legalità*, cit., 412.

[60] Per una ricostruzione del fenomeno amministrativo, nell'opera più matura Massimo Severo Giannini, come espressione di una concezione *dualistica*, si veda Di Gaspare G. (1992), *Il potere nel diritto pubblico*, Padova, in part. 255 ss. ("Da questa fondamentale nozione di discrezionalità amministrativa conviene cercare di porre in luce un ulteriore aspetto importante per la raffigurazione dinamica del potere. Questo è costruito dall'accennata prevalenza del profilo soggettivo. La dialettica interno-esterno, sul crinale autorità-libertà, si ricompone, infatti, nella ponderazione tra interessi, nella scelta che si attua esclusivamente nella figura soggettiva. Ed in effetti, tra la previsione legislativa di un interesse e la sua cura concreta nell'ordinamento giuridico, si interpone necessariamente la figura soggettiva. In altre parole, la norma di legge intanto canonizza un interesse in quanto lo attribuisce, in tanto prevede un potere in quanto lo configura come potestà (…) Il collegamento sempre più evidente tra discrezionalità e funzione consente, ponendosi dal punto di vista del diritto positivo, di comprendere come questo attributo intrinseco della figura soggettiva, questo «agire libero», sostanzialmente politico, emerga dall'esperienza giuridica attraverso un collegamento con la norma positiva che non lo fonda (né lo concede, né lo autorizza, per usare la terminologia di Kelsen o del Donati) ma lo rende solo giuridicamente evidente in quanto, attraverso la funzionalizzazione della potestà, la norma giuridica rende «*rilevanti per tutto il loro svolgersi*» l'esercizio delle attività autoritative da parte delle figure soggettive pubbliche", *ivi* 261-262 e 269-270).

dai diversi attori coinvolti nel processo) e con le ragioni/i vincoli imposti dal processo di sviluppo tecnologico ("la natura delle cose").

Vale la pena, a questo proposito, di trarre spunto da alcune considerazioni circa i caratteri di questa diversa legalità, al fine di individuarne alcuni presupposti che risultano critici per una sua effettiva *vitalità*. Come nota Vogliotti "questa nuova legalità teleologica, [che] non misura più la distanza tra l'atto e la norma, ma mira all'agire bene, mossa dalla causa finale della giustizia – da intendersi come equo bilanciamento, nel contesto dell'azione e nel corso di un *due process of law* di plurimi e contrastanti interessi (…) è una legalità che sposta l'accento dalla *sostanza* (il dato legislativo) alle *relazioni*. Nel consegue che il problema fondamentale della nuova legalità (e del nuovo paradigma giuridico di cui è espressione) non è più assicurare la qualità delle sostanze normative, in linea con l'ontologia oggettualistica moderna, ma garantire la qualità delle relazioni della rete del diritto e di coloro che sono chiamati a tesserle"[61]. Anche qui, la chiave interpretativa proposta illumina una serie di elementi, che assumo rilievo centrale nell'economia della *necessary clause*. In primo luogo, la *qualità di coloro che sono chiamati a tessere le reti di relazioni*, a cominciare dalle amministrazioni[62] chiamate (sotto questo paradigma) a svolgere un ruolo attivo ed impegnativo, nell'immaginare, sperimentare, strutturare e mantenere aderenti alle *rationes* le soluzioni che implicano il trattamento di dati personali, per il perseguimento di interessi pubblici. Una qualità indispensabile, come detto, proprio con riferimento alle relazioni da intrattenere (e intessere) con l'ambiente in cui i titolari dei trattamenti operano: relazioni con i cittadini (destinatari ultimi dell'esercizio della funzione, e componente ontologica del loro *scopo*); con le altre amministrazioni; con le autorità di controllo; con il mondo della ricerca (interlocutore indispensabile per svolgere quel ruolo attivo in termini di innovazione di cui si è già parlato); con le imprese, fornitrici e partner di progetto. Si pensi a come le reti di relazioni si stanno rivelando centrali nella *governance* dei dati personali, a cominciare dalla *rete delle autorità nazionali di controllo*[63]; si pensi, ancora, all'evoluzione del modello di circolazione e integrazione del patrimonio informativo pubblico, abilitato ed alimentato dalla costruzione di relazioni che si strutturano in funzione non solo

[61] Vogliotti M. (2013), *Legalità*, cit., 431.

[62] "Sebbene il Garante sia indubbiamente l'autorità protagonista del perseguimento dell'interesse pubblico alla protezione dei dati personali, anche in virtù delle sue funzioni regolatorie, non può non rilevarsi che l'attività di tutela dei dati personali condivisa con tutte le amministrazioni", così Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, cit., 390.

[63] La costruzione della rete delle autorità di controllo, dell'*hub* di riferimento (l'*European Data Protection Board*) e delle procedure di cooperazione, assistenza reciproca e di coerenza impegna tutta la parte VII del GDPR (Cooperazione e coerenza), dall'art. 60 all'art. 72.

dell'esecuzione dei compiti di interesse pubblico dei diversi attori, ma anche in ragione della stessa finalità di agevolare la circolazione dei dati. Del ruolo svolto dalle reti di *relazioni multilivello*, in sede di esercizio della funzione di tutela dei diritti è quasi appena il caso di accennare, tanto ne sono noti, evidenti e dibattuti le dinamiche e gli effetti[64].

Queste relazioni vanno opportunamente alimentate, mantenute funzionali, vitali e significative, dal momento che il loro tasso di *qualità* è presupposto e condizione di funzionamento di uno standard basato sulla *necessary clause*. Sotto questo profilo, vale la pena sottolineare che alcune scelte compiute al momento del passaggio a questo standard legale appaiono poco coerenti rispetto a questa esigenza. Facciamo riferimento, in particolare, al ruolo che l'autorità di controllo deve essere chiamata a giocare. Infatti, il superamento dello schema in cui il Garante opera quale *guardiano* della conformità del trattamento rispetto al parametro legislativo, ne esalta il (diverso) ruolo, quale nodo essenziale della rete, ai fini della costruzione, verifica ed aggiornamento della conformità dei trattamenti organizzati e realizzati dai titolari del trattamento alle *rationes* del GDPR. Un ruolo non più di controllo/*interdizione* ma piuttosto di *collaborazione*, assolutamente vitale, proprio nella prospettiva della qualità delle reti in cui si tesse la tela della legalità come *conformità rispetto allo scopo*. Sotto questo profilo, la scelta di ridimensionare il ruolo del Garante[65] (in chiave di semplificazione ed alleggerimento) rischia di privare i titolari del trattamento della possibilità di avvalersi di un supporto qualificato e dedicato[66]. Vanno invece valorizzate le occasioni e le procedure di confronto (senza però riconoscere al Garante poteri di interdizione o di blocco, che appaiono in contraddizione con il principio di responsabilizzazione di cui all'art. 5(2) del regolamento), per consentire di mantenere aperto e di alimentare il dialogo e la collaborazione tra autorità di controllo (di consiglio?) e pubbliche amministrazioni, all'interno di un contesto regolatorio profondamente mutato, nel quale tale interlocuzione risponderebbe principalmente agli interessi e alle esigenze degli stessi titolari del trattamento. In questo mutato contesto, tuttavia, tenuto conto della maggiore capacità di iniziativa in capo alle amministrazioni, andrebbe anche valutata

[64] Cfr., *ex multis*, (eds) Bilancia P. e De Marco E. (2004), *La tutela multilivello dei diritti: punti di crisi, problemi aperti, momenti di stabilizzazione*, Milano; D'Atena A. (2007), *Costituzionalismo multilivello e dinamiche istituzionali*, Torino.

[65] "I decisori politici, infatti, hanno sentito l'esigenza di ricollocare il Garante nel quadro istituzionale, rischiando però, di fatto, di far retrocedere il diritto alla riservatezza rispetto ad altri diritti costituzionalmente protetti.", così Palladini V. (2022), Il ruolo del Garante per la protezione dei dati personali nell'emergenza sanitaria, cit., 178.

[66] Suggeriscono di intervenire per "ripristinare un qualche ruolo del Garante" Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, cit., 397.

l'opportunità di adeguare l'autorità sotto il profilo *dimensionale*, quanto a risorse organizzative e professionali disponibili in ruolo, idonee ad affrontare un volume di lavoro destinato con tutta probabilità ad aumentare.

Lo standard legale condensato nella *necessary clause* appare, in definitiva, più adeguato – sotto molteplici aspetti – ad assecondare un rinnovato protagonismo del settore pubblico, anche con riferimento allo sviluppo e alla innovazione di soluzioni di trattamento dei dati personali che rispondano effettivamente alle esigenze che caratterizzano il perseguimento di interessi pubblici, generali, collettivi. Ma si tratta di uno standard *esigente* e *impegnativo*, e richiede dunque che si torni a investire in modo consistente e appropriato in amministrazioni forti, motivate, innovative e protagoniste, nel governo della società.

Riferimenti bibliografici

AA.VV. (2021), "Poteri Privati", in *Diritto Pubblico*, 3

Adinolfi A. (2008), *Il principio di legalità nel diritto comunitario*, in *Il principio di legalità nel diritto amministrativo che cambia. Atti del 53° Convegno di studi di scienza dell'amministrazione (Varenna, 20-22 settembre 2007)*, Milano, ss. 87

Alberti I. (2022), "La creazione di un sistema informativo unitario pubblico con la Piattaforma digitale nazionale dati", in *Le istituzioni del federalismo*, 2, 473-495

Allena M., Vernile S. (2022), *Intelligenza artificiale, trattamento di dati personali e pubblica amministrazione*, in (eds.) Pajno A., Donati F., Perrucci A., I*ntelligenza artificiale e diritto: una rivoluzione? Vol. 1: Diritti fondamentali, dati personali e regolazione*, Bologna, 395-96

Amato G. (1997), *Autorità semi-indipendenti ed autorità di garanzia*, in *Riv. trim. dir. pubbl.*, 1997, 645 ss.

Ambriola V., Cignoni G. A. (1999), "Qualità, informatica e pubblica amministrazione", in *Il Mulino*, 5, 917-928

Amparo Gran Ruiz M. (2022), "Fiscal Transformations due to AI and Robotization: Where Do Recent Changes in Tax Administrations, Procedures and Legal Systems Lead Us?", in *Northwestern Journal of Technology and Intellectual Property*, 19, 4, 325-363

ANAC (2014), *Analisi istruttoria per l'individuazione di indicatori di rischio corruzione e di prevenzione e contrasto nelle amministrazioni pubbliche*, disponibile al sito https://shorturl.at/otST8 (consultato il 4.5.2023)

Andersson S., Heywood P. M. (2009), "The Politics of Perception: Use and Abuse of Transparency International's Approach to Measuring Corruption", in *Political Studies*, 57, pp. 746-767

Angiolini V. (1999), *Legalità dell'amministrazione interna e comunitaria*, in (eds) C. Pinelli, *Amministrazione e legalità. Fonti normative e ordinamenti. Atti del Convegno, Macerata, 21 e 22 maggio 1999*, Milano

Avanzini G. (2019), *Decisioni amministrative ed algoritmi informatici. Predominazione, analisi predittiva e nuove forme di intellegibilità*, Napoli

Azzena L. M. (2021), "L'algoritmo nella formazione della decisione amministrativa: l'esperienza italiana", in *Revista brasileira de estudos políticos*, 123, 503

Bajpai R. e Myers B. (2020), *Enhancing Government Effectiveness and Transparency the Fight Against Corruption*, Word Bank, 235

Balducci Romano, F. (2015), "La protezione dei dati personali nell'Unione Europea tra libertà di circolazione e diritti fondamentali dell'uomo", *Rivista italiana di diritto pubblico comunitario*, 2016, 1619-1660
Barnett R. E. (2003), "The Original Meaning of the Necessary and Proper Clause", in *University of Pennsylvania Journal of Constitutional Law*, 2, 183 ss.
Barone A. (2016), *Territorio e politiche anticorruzione*, in Scoca F.G. e Di Sciascio A. (eds.), *Le proprietà pubbliche: tutela, valorizzazione e gestione*, Napoli, 113-134
Bassi N. (2001), *Principio di legalità e poteri amministrativi impliciti*, Milano, in spec. 220 ss.
Berrettini, A. (2020) "Conflitto di interessi e contratti pubblici: un difficile equilibrio tra (in)certezza del diritto e tassatività delle situazioni conflittuali", in *Federalismi.it*, 7, 1-30
Bianca C. M., Busnelli F. D. (2007), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (codice della privacy)*, Padova, 456-540
Bilancia P. e De Marco E. (2004), *La tutela multilivello dei diritti: punti di crisi, problemi aperti, momenti di stabilizzazione*, Milano
Black G., Stevens L. (2013), *Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest*, in *SCRIPTed*, 10:1, disponibile in http://script-ed.org/?p=835
Bobbio N. (1980), *Pubblico/privato*, in *Enciclopedia Einaudi*, Torino, 401
Boeri T. (2018), *Visite mediche di controllo d'ufficio – metodologie di* data mining *– procedimento sanzionatorio del Garante per la protezione dei dati personali*, 6 settembre 2018, presso la XI Commissione permanente lavoro pubblico e privato, previdenza sociale del Senato
Bombardelli M. (2022), *Dati personali (Tutela)*, in Mattarella B.G. e Ramajoli M., *Funzioni amministrative* - Enciclopedia del diritto-I tematici, Milano, III, 351-381
Boscarino, R., Di Porto E., e Naticchioni P. (2018), "SAVIO Shut Down: Effetti sulle Visite Mediche di Controllo", *INPS DCSR Studi e Analisi*, Nota n. 2
Boschetti, B. (2022), *La transizione della pubblica amministrazione verso il modello Government as a platform*, in Lalli A. (ed.), *L'amministrazione pubblica nell'era digitale*, Torino, 1- 44)
Braibant G. (1971), "La protection des droits individuels au regard du développement", in *Revue internationale de droit comparé*, 23-4, 793-817
Brouwer, E. R. (2011), *Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation*, in Besselink L. F. M., Prechal S., & Pennings F. (eds.), *The Eclipse of the Legality Principle in the European Union*, 273-294
Buttarelli G. (1997), *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Milano
Buttarelli G. (2022), *L'interoperabilità dei dati nella Pubblica Amministrazione*, in Bontempi V. (eds.), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, Roma, 140 ss.
Bygrave, L. (2002), *Data Protection Law—Approaching Its Rationale, Logic and Limits*, The Hague

Bygrave, L. (2014), *Data Privacy Law—An International Perspective*, Oxford
Calvano R. (2006), *I poteri impliciti comunitari. L'art. 308 TCE come base giuridica per l'espansione dell'azione comunitaria*, in Mangiameli S. (eds.), *L'ordinamento europeo. L'esercizio delle competenze*, Milano, 100 ss.
Cantone R. (2020), *Il sistema della prevenzione della corruzione*, Torino
Cantone R. e Merloni F. (2019), "Conflitti di interesse: una diversa prospettiva", in *Diritto pubblico*, 886 ss.
Cantone R., Merloni F. (2015), *La nuova Autorità nazionale anticorruzione*, Torino
Cardarelli F. (1996), *Efficienza e razionalizzazione dell'attività amministrativa. I contratti ad oggetto informatico nella pubblica amministrazione*, Camerino
Cardarelli F. (2021), *Comm. sub. art. 2-ter Codice Privacy*, in D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (eds.), *Codice della privacy e data protection*, Milano, 1011 ss.
Cardarelli F., Sica S., Zeno-Zencovich V. (2004), *Il codice dei dati personali: temi e problemi*, Milano.
Carinci A. (2019), "Fisco e privacy: storia infinita di un apparente ossimoro", in *Fisco (Il)*, 46, 4407 ss.
Carloni E. (2009), "La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata", in *Rivista trimestrale di diritto pubblico*, 1, 155-186
Carloni E. (2019), "Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni", in *Diritto pubblico*, 2, 363-392
Carloni E. (2020), "I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo", in *Diritto amministrativo*, n. 2, 273-304
Carloni E. (2023), *L'anticorruzione. Politiche, regole, modelli*, Bologna
Carotti B. (2020), "Algoritmi e poteri pubblici: un rapporto incendiario", in *Giornale di diritto amministrativo*, 1, 5 ss.
Carullo G. (2020), "Principio di neutralità tecnologica e progettazione dei sistemi informatici della pubblica amministrazione", in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 21/1, 33-48
Carullo G. (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*, 1, 131 ss.
Carullo G. (2021), "Decisione amministrativa e intelligenza artificiale", in *Diritto dell'Informazione e dell'Informatica*, 3, 431
Casavola F. P. (1997), *Quale 'statuto' per le Autorità indipendenti*, in Amato G. (eds.), *Regolazione e garanzia del pluralismo*, Milano, 18 ss.
Cassese S. (1996), "Poteri indipendenti, Stati, relazioni ultrastatali", in *Foro it.*, V, 7 ss.
Cassese S. (2003), *Le basi costituzionali*, in *Trattato di diritto amministrativo*, (eds.) Cassese S., *Diritto amministrativo generale*, I, Milano, 220 ss.
Cassese S. (2006), *Il diritto amministrativo e i suoi principi*, (eds.) Cassese S., *Istituzioni di diritto amministrativo*, Milano, 8 ss.
Cassese S. (2009), *Il diritto globale. Giustizia e democrazia oltre lo Stato*, Torino.
Cassese S. (2017), "Verso un diritto europeo italiano", in *Riv. trim. dir. pubbl.*, 303

Cate F.H., e Mayer-Schönberger V. (2013), "Notice and consent in a world of Big Data", in *International Data Privacy Law*, 3, 67-73
Cavallo Perin R. (eds.) (2021), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino
Cavallo Perin R. e Alberti I. (2020), *Atti e procedimenti digitali*, in Cavallo Perin R., e Galetta D.-U. (eds.), *Diritto dell'Amministrazione pubblica digitale*, Torino,119-158
Cecili M. e Cardone M. (2020), "Osservazioni sulla disciplina in materia di tutela dei dati personali in tempi di Covid-19. L'Italia e i modelli sudcoreano, israeliano e cinese: opzioni a confronto", *Nomos*, 1, 47 ss.
Cerulli Irelli V. (1993), *Premesse problematiche allo studio delle 'amministrazioni indipendenti'*, in *Mercati e amministrazioni indipendenti*, (eds.) Bassi F. e Merusi F., Milano, 3 ss.
Charron N. (2015), "Do corruption measures have a perception problem? Assessing the relationship between experiences and perceptions of corruption among citizens and experts", in *European Political Science Review*, 1-25
Chiti M. P. e Natalini A. (eds.) (2012), *Lo spazio amministrativo europeo: le pubbliche amministrazioni dopo il Trattato di Lisbona*, Bologna
Choroszewicz M., Mäihäniemi B. (2020), "Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries", *Global Perspectives* 1(1): 12910. doi: https://doi.org/10.1525/gp.2020.12910
Cinque A. (2021), "'Privacy', 'big-data' e 'contact tracing': il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute", *La Nuova Giurisprudenza Civile Commentata*, 4, 957-968
Civitarese Matteucci S. (2019), "«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità", in *Diritto pubblico*, 1, 5-42
Clarich M. (2001), *Un approccio 'madinsoniano'*, in Grassini F. A. (eds.), *L'indipendenza delle autorità*, il Mulino, 92 ss.
Colapietro C., Iannuzzi A. (2020), "'App' di 'contact tracing' e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali", in *dirittifondamentali.it*, 2, 772-803
Conigliaro M. (2020), "RecoveryFund: verso la riforma fiscale con innovazione digitale, big data, tracciabilità e tassazione per cassa", in *Fisco*, 40, 4850 ss.
Conigliaro M. (2022), "Lotta all'evasione con l'intelligenza artificiale 'Ve.R.A.'", in *Fisco (Il)*, 32/33, 3107 ss.
Contessa, C. (2017), "Circa la nozione in senso funzionale del conflitto d'interessi nel codice dei contratti", in *Urbanistica e appalti*, 6, 824
Cortese F. (2021), *Comm. sub. art. 2-sexies Codice Privacy*, in D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (eds.), *Codice della privacy e data protection*, Milano, 1043 ss
Costantini F., Franco G. (2019), "Decisione automatizzata, dati personali e pubblica amministrazione in Europa: verso un 'Social credit system'?", in *Istituzioni del Federalismo*, 3, 715-738
Craig P. e de Burca G. (2015), *EU Law: Text, Cases, and Materials*, Oxford, 106 e ss.

Crespi S. (2020), "Applicazioni di tracciamento a tutela della salute e protezione dei dati personali nell'era Covid-19: quale (nuovo) bilanciamento tra diritti?", *Eurojus*, 3, 218-255
D'Alberti M. (1995), *Autorità indipendenti (dir. amm.)*, in *Enc. giur.*, IV, Roma
D'Alberti M. (2017), *Corruzione e pubblica amministrazione*, Napoli
D'Ancona S. (2018), "Scambio di dati tra le pubbliche amministrazioni e principio di buona amministrazione nel diritto comunitario e nazionale. Interferenze colle norme sulla privacy. Reg UE n. 679/2016", in *Rivista italiana di diritto pubblico comunitario*, 3/4, 587-627
D'Atena A. (2007), *Costituzionalismo multilivello e dinamiche istituzionali*, Torino
D'Elia I. Ciampi C. (1987), *L'informatica nella pubblica amministrazione. Problemi, risultati, prospettive*, Roma.
D'Ippolito G. (2018), "Il principio di limitazione delle finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data", in *Il diritto dell'informazione e dell'informatica*, n. 6, 943-987
Daniele L. (2015), *Atti dell'Unione europea*, in Enciclopedia del diritto - Annali VIII
D'Arcangelo L. (2020), "'Contact tracing' e protezione dei dati nella fase 2 dell'epidemia da Covid-19 (anche nel rapporto di lavoro)", in *giustiziacivile.com*, 5, 1 ss.
Davies S. (2016), "The Data Protection Regulation: A Triumph of Pragmatism over Principle", in *Eur. Data. Prot. L. Rev.* 290 ss.
de la Feria R. e Grau Ruiz M.A. (2022), "The Robotisation of Tax Administration", in M.A. Grau Ruiz (eds.), *Interactive Robotics: Legal, Ethical, Social and Economic Aspects*, Cham, § III
De Leonardis F. (2020), "Big data, decisioni amministrative e 'povertà' di risorse della pubblica amministrazione", in *Munus: rivista giuridica dei servizi pubblici*, 2, 367-387
De Pretis D. e Marchetti B. (2007), *La discrezionalità della pubblica amministrazione*, in Della Cananea G. e Dugato M., a cura di, *Diritto amministrativo e Corte costituzionale*, Napoli, 341-387
Degrave E. (2014), *L'e-Gouvernement et la protection de la vie privée: Légalité, transparence et contrôle*, Bruxelles.
Degrave E. (2017), *L'administration belge organisée en réseaux: réutilisation des données à caractère personnel et protection de la vie privée*, in Auby J. B. e De Gregorio V., a cura di, *Données urbaines et smart cities*, Berger-Levrault, 184-187
Del Gatto, S. (2020), "Potere algoritmico, digital welfare state e garanzie per gli amministrati. I nodi ancora da sciogliere", in *Rivista italiana di diritto pubblico comunitario*, 6, 829-855
Della Cananea G. (2011), *Diritto amministrativo europeo. Principi e istituti*, Milano
Di Gaspare G. (1992), *Il potere nel diritto pubblico*, Padova
Didimo W., Grilli L., Liotta G., e Montecchiani F. (2022), "Processi decisionali efficienti e affidabili tramite analisi visuale con metodologia human-in-the-loop: un caso di studio sulla valutazione del rischio fiscale". in *Rivista Italiana Di Informatica E Diritto*, 4(2), 15-21 disponibile all'indirizzo: https://doi.org/10.32091/RIID0092 (01.3.2023)

Drechsler, L. C. (2023). "What purpose is left for purpose limitation as a guiding principle of the General Data Protection Regulation after Case C- 268/21, Norra Stockholm Bygg AB v Per Nycander AB?", in *https://eulawlive.com*, 15 marzo 2023 (accesso 15 maggio 2023)
Dunleavy P., Margetts H., Bastow S. e Tinkler, J. (2006), *Digital Era Governance-IT Corporations, the State and e-Government*, New York
Durst L. (2019), *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in Rocco P. (eds.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 41-63
EDPS (2016), *Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights. Background paper*
Etteldorf C. (2019), "Germany revisited: the second data protection adaption and implementation act", *European Data Protection Law Review (EDPL)*, 5(3), 397-403, in part. 397
Falcone M. (2023), *Ripensare il potere conoscitivo pubblico. La conoscenza amministrativa con i big data e gli algoritmi*, Napoli
Faraguna P. (2015), *L'identità nazionale nell'Unione europea come problema e come soluzione*, il Mulino
Farri F. (2020), "Digitalizzazione dell'amministrazione finanziaria e diritti dei contribuenti", in *Rivista di diritto tributario*, 6, 115-139
Faúndez-Ugalde A., Mellado-Silva R., Aldunate-Lizana E. (2020), "Use of artificial intelligence by tax administrations: An analysis regarding taxpayers' rights in Latin American countries", in *Computer Law & Security Review*, 38
Federico G. (2018), Il conflitto di interessi nell'esercizio del potere amministrativo, Torino
Ferrara R. (2019), "Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale", in *Diritto Amministrativo*, 4, 774
Finocchiaro G. (2018), "Italy: the legislative procedure for national harmonisation with the gdpr", *European Data Protection Law Review (EDPL)*, 4(4), 496-499
Fiorentino L. (2009), L'esternalizzazione delle attività amministrative: l'acquisto di beni e servizi da parte delle Pubbliche Amministrazioni e il patrimonio immobiliare dello Stato", in *Economia dei Servizi*, 2, 259-272
Fiorentino L., (2018), "Il trattamento dei dati personali: l'impatto sulle amministrazioni pubbliche", in *Giornale Dir. Amm.*, 6, 690 ss.
Fonderico G. (2018), "La regolazione amministrativa del trattamento dei dati personali", in *Giorn. Dir. Amm.*, 4, 415-422
Forti M. (2018), "Diritto all'oblio e conservazione dei dati iscritti nei pubblici registri: qualche considerazione a margine della sentenza della Corte di giustizia nel caso Manni", in *Contratto e impresa/Europa*, 565-580
Francario F. (2021), "Protezione dei dati personali e pubblica amministrazione", in *giustiziainsieme.it*, disponibile al sito https://shorturl.at/jmL29 (1.5.2023)
Franchini C. (1988), "Le autorità amministrative indipendenti" in *Rivista trimestrale di diritto pubblico*, 3, 539 ss.

Francioso C. (2023), "Intelligenza artificiale nell'istruttoria tributaria e nuove esigenze di tutela", in *Rassegna tributaria*, 1, 47-94
Fransoni G. (2020), *Le indagini tributarie. Attività e poteri conoscitivi nel diritto tributario,* Torino
Frego Luppi S. A. (2013), "L'obbligo di astensione nella disciplina del procedimento dopo la legge n. 190 del 2012", in *Dir. amm.*, 694 ss.
Frenzel E.M. (2018), *Rechtmäßigkeit der Verarbeitung*, in Paal B.P., Pauly D.A., *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, C.H. Beck, Munich, 86
Froomkin A. M. (2019), "Big Data: Destroyer of Informed Consent", in *Yale Journal of Health Policy, Law, and Ethics*, https://ssrn.com/abstract=3405482 (01.04.2023)
Galetta D.-U. (2020), "Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia", in *Rivista italiana di diritto pubblico comunitario*, 3/4, 501
Gantchev V. (2019), "Data protection in the age of welfare conditionality: Respect for basic rights or a race to the bottom?" *European Journal of Social Security*, 21(1), 3–22 https://doi.org/10.1177/1388262719838109
Gemmi A. (2021), "Il principio di legalità tra "authorities" e "golden power": quale spazio per i poteri impliciti", in *Rivista Italiana di Diritto Pubblico Comunitario*, 2, 365-397
Giannantonio E. (1999), *Dati personali (tutela dei)*, in *Enciclopedia del diritto*, agg. III, par. 1
Giardina A. (1975), T*he rule of law and implied powers in the European communities*, in *The Italian Yearbook of International Law*, 99-111
Giuva L., Vitali S., Zanni Rosiello I (2007), *Il potere degli archivi. Usi del passato e difesa dei diritti nella società contemporanea*, Milano
Goggiamani G. (2005), *La doverosità della pubblica amministrazione*, Torino, 2005
González Fuster G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, New York
Guerra M.P. (1996), *Funzione conoscitiva e pubblici poteri*, Milano
Guerra M.P. (2005), "Circolazione dell'informazione e sistema informativo pubblico: profili giuridici dell'accesso interamministrativo telematico. Tra Testo Unico sulla documentazione amministrativa e codice dell'amministrazione digitale", *Diritto Pubblico*, 2, 525-571
Guidara A. (2023), "Accertamento dei tributi e intelligenza artificiale: prime riflessioni per una visione di sistema", in *Dir. e Prat. Trib.*, 2, 384
Hadwick D. e Lan S. (2021), "Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany", in *World Tax J.*, 609 ss.
Hahn I. (2021), "Purpose Limitation in the Time of Data Power: Is There a Way Forward?", in *European Data Protection Law Review*, 7, 1, 31-44
Hert P., Papakonstantinou V. (2016), "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", in *Computer Law & Security Review*, 32/2, 179-194

Hildebrandt M. (2013), "Slaves to Big Data. Or Are We?", in *IDP: revista d'Internet, dret i política*, 17, 27-44
Iannotta L. (2001), *Principio di legalità e amministrazione di risultato*, in *Scritti in onore di Elio Casetta*, vol. II, Napoli
ISS (2020), *Rapporto ISS COVID-19. Protezione dei dati personali nell'emergenza COVID-19*, n. 42
Iudica, G. (2016), *Il conflitto di interessi nel diritto amministrativo*, Torino
Knockaert M. (2019), "La loi du 30 juillet 2018: l'échange de données à caractère personnel au sein du secteur public", *Revue du droit des technologies de l'information*, 74, 5-24
Lagioia F., Sartor G. (2020), "Profilazione e decisione algoritmica: dal mercato alla sfera pubblica", in *federalismi.it*, 11, 85-110
Lalli, A., Moreschini, A., Ricci, M. (2019), *L'ANAC e la disciplina dei conflitti di interessi*, Napoli
Lalli, A., Moreschini, A., Ricci, M. (2019), *La prassi dell'Anac in materia di conflitto di interessi*, Napoli
Lambsdorff J. (2006), *Measuring corruption – the validity and precision of subjective indicators (Cpi)*, in (eds.) C. Sampford, A. Shacklock, C. Connors, F. Galtung, *Measuring Corruption*, Aldershot, Ashgate, 81-99
Latte S. (2020), "Immuni: framing and first considerations one month from the start", *European Journal of Privacy Law & Technologies*, 2, 362-373
Lazzaro F. (2011), "Coordinamento informativo e pubbliche amministrazioni", in *Istituzioni del federalismo*, 3, 659-681
Leissler G., Reisinger P., Böszörmenyi J. (2019), *National Adaptations of the GDPR in Austria*, in Mc Cullagh K., Tambou O., Bourton S. (eds.), *National Adaptations of the GDPR*, Collection Open Access Book, Blogdroiteuropeen, Luxembourg, February, 37
Levi F. (1967), *L'attività conoscitiva della pubblica amministrazione*, Torino
Liu T., Juang W., Yu C. (2023), "Understanding Corruption with Perceived Corruption: The Understudied Effect of Corruption Tolerance", in *Public Integrity*, 25/2, 207-219
Longobardi N. (1991), *Le 'amministrazioni indipendenti': profili introduttivi*, in *Scritti per Mario Nigro*, II, 73 ss.
Lorenzmeier S. (2017), *Europarecht – schnell erfasst*, Berlin, Heidelberg, 147
Lubrano E. (2018), *Il conflitto di interessi nell'esercizio dell'attività amministrativa*, Torino
Lynskey O. (2015), *The foundations of EU data protection law*, Oxford
Macchia M. (2022), "Pubblica amministrazione e tecniche algoritmiche", in *DPCE Online*, 1, 51
Macchia M. e Mascolo A. (2022), *Intelligenza artificiale e regolazione*, in (eds.) Pajno A., Donati F., Perrucci A., *Intelligenza artificiale e diritto: una rivoluzione? Vol. 2: Amministrazione, responsabilità, giurisdizione.*, Bologna, 97-130
Malgieri G., Comandé G. (2017), "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", in *International Data Privacy Law*, 7/4, 262

Manetti M. (1994), *Poteri neutrali e Costituzione*, Milano
Manfredi G. (2021), *Legalità procedurale*, in *Diritto amministrativo*, 4,749 ss.
Marcheselli A., Ronco S. (2022), "Dati personali, Regolamento GDPR e indagini dell'Amministrazione finanziaria: un modello moderno di tutela dei diritti fondamentali?", in *Rivista di diritto tributario*, I, 97 ss.
Marchianò G. (2020), "La legalità algoritmica nella giurisprudenza amministrativa", in *Il diritto dell'economia*, 3, 229-258
Marenghi C. (2021), "La proposta di Regolamento Ue sull'intelligenza artificiale e la regolazione privata: spunti critici in tema di norme tecniche armonizzate", in *Diritto comunitario e degli scambi internazionali* 3/4, 563-583.
Marongiu D. (2008), "I dati delle pubbliche amministrazioni come patrimonio economico nella società dell'informazione", in *Informatica e diritto*, 1-2, 355-368
Marzuoli C. (1982), *Principio di legalità e attività di diritto privato della pubblica amministrazione*, Milano.
Massera A. (1988), *'Autonomia' e 'indipendenza' nell'amministrazione dello Stato*, in *Studi in onore di M. S. Giannini*, III, Milano, 449 ss.
Massera A., *I principi generali dell'azione amministrativa tra ordinamento nazionale e ordinamento comunitario*, in *Diritto Amministrativo*, 4, 707
Masucci A. (2020) "L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri"*,* in *Diritto Pubblico,* 3, 943-979
Mattarella B. G. (2006), "Il Rapporto autorità-libertà e il diritto amministrativo europeo", in *Riv. Trim. Dir. Pubbl.*, 909- 928
Mattarella B. G. e Pelissero M. (eds.) (2013), *La legge anticorruzione. Prevenzione e repressione della corruzione*, Torino.
Mayer-Schönberger V. e Ramge T. (2018), *Reinventing Capitalism in the Age of Big Data*, London
Mayr O. (1988), *La bilancia e l'orologio. Libertà e autorità nel pensiero politico dell'Europa moderna* (1986), Bologna, 209
Mazzoni M., Stanziano A., Recchi L. (2017), "Rappresentazione e percezione della corruzione in Italia. Verso una strumentalizzazione del fenomeno", in *Comunicazione politica*, 1, 99-118
Mc Cullagh K., Tambou O., Bourton S. (2019), *National adaptations of the GDPR*, Blogdroiteuropéen, disponibile all'indirizzo https://hal.science/hal-03521416
Merloni F. (1997), "Fortuna e limiti delle cosiddette autorità amministrative indipendenti", in *Pol. Dir.*, 639 ss. Nissolai S. (1996), *I poteri garanti della Costituzione e le autorità indipendenti*, Pisa
Merloni F. (2009), *Organizzazione amministrativa e garanzie dell'imparzialità. Funzioni amministrative e funzionari alla luce del principio di distinzione tra politica e amministrazione*, in *Diritto pubblico*, 2009, 1, 57 ss.
Merloni F. (2022), "Il d.lgs. n. 165 del 2001 e l'organizzazione delle competenze professionali dei funzionari pubblici", in *Diritto Amministrativo*, 2, 359 ss.
Merloni F. (2013), "Le attività conoscitive e tecniche delle amministrazioni pubbliche. Profili organizzativi", in *Diritto pubblico*, 2, 481-520
Merusi F. (2000), *Democrazia e autorità indipendenti. Un romanzo 'quasi' giallo*, Bologna

Merusi F. (2007), "Il principio di legalità nel diritto amministrativo che cambia", in *Diritto pubblico*, 2, 427-444
Merusi F. (2007), *Sentieri interrotti della legalità. La decostruzione del diritto amministrativo*, Bologna
Merusi F. (2011), *Ragionevolezza e discrezionalità amministrativa*, Napoli
Miscenic E. e Hoffmann A.-L. (2020), "The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)", in *EU and comparative law issues and challenges series (ECLIC)*, 44-61
Miscenic E. e Hoffmann A.-L. (2020), *The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)*, cit., 47
Moore M. e Tambini D. (eds.) (2018), *Digital dominance: The power of Google, Amazon, Facebook and Apple*. New York
Morbidelli G. (2007), "Il principio di legalità e i c.d. poteri impliciti", in *Diritto amministrativo,* 4, 723 ss.
Nicola F. G. e Pollicino O. (2020), "The balkanization of data privacy regulation", in *West Virginia Law Review*, 123(1), 61-116
Nicotra I. A. (2016), *L'Autorità Nazionale Anticorruzione: tra prevenzione e attività regolatoria*, Torino
Nigro M. (1966), *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano.
Nigro M. (1983), "È ancora attuale una giustizia amministrativa?", in *Foro it.*, V, 254
Nograšek J. e Vintar M. (2014), "E-government and organisational transformation of government: Black box revisited?", in *Government Information Quarterly*, 31/1, 108-118
Nunziata M. (2017), *Riflessioni in tema di lotta alla corruzione: rimedi preventivi e repressivi*, Roma
Pajno A. (2017), "*Diritto europeo e trasformazioni del diritto amministrativo*. *Alcune provvisorie osservazioni*, in *Rivista italiana di diritto pubblico comunitario*, 27/2, 467-478
Palladini V. (2022), "Il ruolo del Garante per la protezione dei dati personali nell'emergenza sanitaria", in *Osservatorio costituzionale*, 2/153-178
Pantalone P. (2018), *Autorità indipendenti e matrici di legalità*, Napoli
Pantalone P. (2020), "Regolazione indipendente e anomalie sostenibili al cospetto delle matrici della legalità", in *P.A. Persona e Amministrazione*, I, 446 ss.
Paolantonio N. (2021), "Il potere discrezionale della pubblica automazione. Sconcerto e stilemi (sul controllo giudiziario delle "decisioni algoritmiche")", in *Diritto Amministrativo*, 4, 813
Passaro M. (1996), *Le amministrazioni indipendenti*, Torino
Patsalia T. e Kalogiannis V. (2021), "Greek Implementation of the GDPR", in *Thompson Reuters Practical Law*, giugno, testo disponibile al sito: https://uk.practicallaw.thomsonreuters.com/w-026-6627?transitionType=Default&contextData=(sc.Default)

Pelino E. (2019), *Sub art. 2-ter d.lgs. 196/2003*, in (eds.) Bolognini L., Pelino E., *Codice della disciplina privacy*, Milano, 97, ss.
Perez R. (1996), "Autorità indipendenti e tutela dei diritti", in *Riv. trim. dir. pubbl.*, 115 ss.
Pericu G. (1996), "Brevi riflessioni sul ruolo istituzionale delle autorità amministrative indipendenti", in *Diritto amministrativo*, 1 ss
Perongini S. (2004), *Principio di legalità e risultato amministrativo*, in Immordino M. e Police A. (eds.) *Principio di legalità e amministrazione di risultati*, Atti Convegno di Palermo 27-28 febbraio 2003, Torino, 39-50
Pertot T. (2020), "*Immuni* e tracciamento digitale: fra protezione dei dati personali, problemi di efficacia e qualche prospettiva futura", *Le Nuove leggi civili commentate*, 5, 1131-1165
Picozza E. (1997), *Attività amministrativa e diritto comunitario*, in *Enc. giur.*, Roma, Agg. III, 23
Piga F. (1987), "Modernizzazione dello Stato: le istituzioni della funzione di controllo", in *Foro amm.*, I, 809 ss.
Pignatti M. (2022), "La digitalizzazione e le tecnologie informatiche per l'efficienza e l'innovazione nei contratti pubblici", in *federalismi.it*, 12, 133-175
Pioggia A. (2021), *La concessione e il pubblico servizio: una storia parallela*, in (eds.) Bartolini A., *Scritti in onore di Bruno Cavallo*, Torino, 253-273
Pioggia A. (2022), *La cura nella Costituzione. Prospettive per una amministrazione della cura*, in (eds.) Arena G., Bombardelli M., *L'amministrazione condivisa*, 43-63
Pitruzzella G. (2022), "Dati fiscali e diritti fondamentali", in *Diritto e politica tributaria internazionale*, 2, 666 ss.
Piraino F. (2017), "Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", in *Nuove leggi civ. comm.*, 2, par. 3.
Pizzetti F. (2021), *La parte I del Codice novellato*, in Pizzetti F. (eds.), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino
Pizzetti F. (2020), "Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti", in *MediaLaws*, 2, 11-33
Pizzetti F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. II, Torino
Poletti D. (2020), "Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza", *Persona e Mercato*, 2, 65-76
Pollicino O. (2023), *Potere digitale*, in Ruotolo M. e Cartabia M. (eds), *Potere e Costituzione – Enciclopedia del diritto-I tematici*, Milano, V
Pollicino O. e Repetto G. (2019), "Not to be Pushed Aside: the Italian Constitutional Court and the European Court of Justice", in *VerfBlog*, 2/27, disponibile in https://verfassungsblog.de/not-to-be-pushed-aside-the-italian-constitutional-court-and-the-european-court-of-justice
Ponti B. (2008), *I dati di fonte pubblica: coordinamento, qualità e riutilizzo*, in (eds.) Merloni F., *La trasparenza amministrativa*, Milano, 405-442
Ponti B. (2008), *Titolarità e riutilizzo dei dati pubblici*, in (eds.) Id., *Il regime dei dati pubblici*, Rimini, 213-252
Ponti B. (2018), *Oltre la percezione: concretizzare le potenzialità conoscitive degli*

indicatori basati sull'elaborazione degli hard data di fonte amministrativa, in (eds.) Ponti B. e Gnaldi M., *Misurare la corruzione oggi. Obiettivi, metodi, esperienze*, Milano 47-58
Ponti B. (2019), *Il luogo adatto dove bilanciare. Il "posizionamento" del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019*, in *Istituzioni del Federalismo*, 2, 529 ss.
Ponti B. (2021), *Informazione pubblica, trasparenza e potere conoscitivo: come proseguendo sui percorsi indicati da Francesco Merloni*, in Pioggia A., Carloni E., Ponti B. (eds.), *Studi in onore di Francesco Merloni*, Torino, 207-222
Ponti B. (2022), "Le diverse declinazioni della 'Buona amministrazione' nel PNRR", in *Istituzioni del federalismo*, 2, 401-418
Ponti B. (eds.) (2022), "Gli algoritmi pubblici tra legalità e partecipazione", Sezione monografica in *Rivista italiana di informatica e diritto*, 4, 2
Ponti B. (2007), "Il patrimonio informativo pubblico come risorsa: i limiti del regime italiano di riutilizzo dei dati delle pubbliche amministrazioni", *Diritto pubblico*, n. 3, 991-1014
Ponti B. (2019), "La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi", *Diritto dell'informazione e dell'informatica*, 2, 383-422
Portinaro P.P. (1996), *Il principio di legalità*, in Enciclopedia delle scienze sociali, Roma, 216 ss.
Predieri A. (1997), *L'erompere delle autorità amministrative indipendenti*, Firenze, 1997
Presutti, L. (2018), "Il conflitto di interessi come causa di esclusione nel nuovo codice", in *Urbanistica e appalti*, 4, 548
Racca G. M. (2022), *Le innovazioni necessarie per la trasformazione digitale e sostenibile dei contratti pubblici*, in (eds.) Cavallo Perin R., Lipari M. e Racca G. M., *Contratti pubblici e innovazioni per l'attuazione della legge delega*, Napoli, 2022, 9-44
Ragucci G. (2019), "L'analisi del rischio di evasione in base ai dati dell'archivio dei rapporti con gli intermediari finanziari: prove generali dell'accertamento "algoritmico"?", in *Riv. tel. dir. trib.*, disponibile al sito https://shorturl.at/vFOQ4 (5.5.2023)
Ramajoli M. (2018), "Consolidamento e metabolizzazione del modello delle Autorità di regolazione nell'età delle incertezze", in *Rivista della regolazione dei mercati*, 2, 17 ss. Pantalone P. (2018), *Autorità indipendenti e matrici di legalità*, Napoli
Ribes Ribes A. (2020), "La inteligencia artificial al servicio del «compliance tributario», in *Revista española de derecho financiero*, 2020, 125 ss.
Richards N. M. (2015), "Why Data Privacy Law Is (Mostly) Constitutional/ The Contemporary First Amendment: Freedom of Speech, Press, and Assembly Symposium", in *William & Mary Law Review*, 56, 1501-1532
Rizzuto I. (2018), "Le nuove frontiere del 'digital marketing': dalla profilazione alla manipolazione 'online' nell'ambito politico alla luce del GDPR", in *Ciberspazio e Diritto*, 1-2, 99-120
Rodotà S. (1973), *Elaboratori elettronici e controllo sociale*, Bologna

Rodotà S. (1991), ""Privacy" e costruzione della sfera privata. Ipotesi e prospettive", in *Politica del diritto*, 4, 521-546
Rodotà S. (2004), "Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy", in *Europa e diritto privato*, 1-10
Rodotà S. (2009), *Data Protection as a Fundamental Right*, in Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds), *Reinventing Data Protection?*, Springer
Rossi, G. (2011), *Potere amministrativo e interessi a soddisfazione necessaria. Crisi e nuove prospettive del diritto amministrativo*, Torino
Roßnagel A. (2017), "Gesetzgebung im Rahmen der Datenschutz-Grundverordnung", in *Datenschutz Datensich*, 41, 277
Roßnagel, A., Nebel, M., & Richter, P. (2015), *Was bleibt vom Europäischen Datenschutzrecht. Überlegungen zum Ratsentwurf der DS-GVO*, ZD, 455
Rotenberg M. (2020), "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection", in *European Law Journal*, 1 ss.
Rovati A. M. (2011), "Prime note su proprietà intellettuale e riutilizzo dei dati pubblici", in *Informatica e diritto*, 1-2, 153-184
Santoro A. (2019), *Nuove frontiere per l'efficienza dell'amministrazione fiscale: tra analisi del rischio e problemi di privacy*, in Arachi G. e Baldini M. (eds.), *La finanza pubblica italiana. Rapporto 2019*, Bologna, 66 ss.
Santoro A. (2019), "Più che i pagamenti elettronici serve il profilo dell'evasore", in lavo-ce.info, 24.09.2019, disponibile al sito: https://lavoce.info consultata il 5 maggio 2023
Sappa C. (2011), "Diritti di proprietà intellettuale e dati pubblici nell'ordinamento italiano", in *Informatica e diritto*, 1-2, 185-197
Sartoretti C. (2021), "Le authorities al tempo del covid-19. Riflessioni sul ruolo delle autorità indipendenti: modello in declino o consolidato?", in *DPCE Online*, 47/2, disponibile al sito: https://www.dpceonline.it/index.php/dpceonline/article/view/1347 (15.5.2023)
Sattler, A. (2018), *From Personality to Property?*, in Bakhoum, M., Conde Gallego, B., Mackenrodt, MO., Surblytė-Namavičienė, G. (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law, vol 28. Berlin, Heidelberg
Scagliarini S. (2013), *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Roma, 2013, 108
Scholtz R., Pitschas R. (1984), *Informationelle Selbstbestimmung und staatliche Informationsverantwortung*, Berlin
Schwartz P. M. e Karl-Nikolaus P. (2018), "Transatlantic Data Privacy Law", Georgetown Law Journal, 115-180
Sgueo G. (2019), "Tre idee di design per l'amministrazione digitale", in *Giornale di diritto amministrativo*, 1, 19 ss.
Sgueo G. (2022), *I servizi pubblici digitali*, in (eds.) Bontempi V., *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, 119-126
Shakil M. H., Tasnia M. (2022), *Artificial Intelligence and Tax Administration in Asia and the Pacific*, in (eds.) Hendriyetty N., Evans C., Kim C. J., Taghizadeh-Hesary F., *Taxation in the Digital Economy New Models in Asia and the Pacific*, 45-55

Simoncini A (2019), "Profili costituzionali dell'amministrazione algoritmica", in *Riv. Trim. Diritto Pubbl.*, 2019, 4, 1145
Simoncini M. (2021), "Lo Stato digitale. L'agire provvedimentale dell'amministrazione e le sfide dell'innovazione tecnologica", in *Riv. Trim. Dir. Pubbl.*, 2, 529
Skunbiszewski K. (1989), *Implied powers of International Organizations*, in *International Law at a time of Perplexity, Essays in Honour of S. Rosenne*, Dordrecht-Boston-Londra.
Sola A. (2020), "Utilizzo di big data nelle decisioni pubbliche tra innovazione e tutela della privacy", in *MediaLaws*, 3, 1-23
Spangaro A. (2022), "Il concetto di profilazione tra 'direttiva madre' e GDPR, in *Giurisprudenza italiana*, 7, 1579-1587
Spuntarelli S. (2023), *Poteri impliciti*, in Ruotolo M. e Cartabia M. (eds), *Potere e Costituzione* – Enciclopedia del diritto-I tematici, Milano, V
Strinati C. (2020), "Algoritmi e decisioni amministrative", in *Foro Amm.*, 7, 1591, fasc. 7
Tambou O. (2018), "France: the french approach to the gdpr implementation", in *European Data Protection Law Review (EDPL)*, 4(1), 88-94, in part. 89-90
Tambou O. (2019), *The French Adaptation of the GDPR*, in Mc Cullagh K., Tambou O., Bourton S. (eds.), *National Adaptations of the GDPR*, Collection Open Access Book, in *Blogdroiteuropeen*, Luxembourg, 52 ss.
Tartaglia Polcini G. (2018), *La corruzione tra realtà e rappresentazione. Ovvero: come si può alterare la reputazione di un paese*, Bologna
Tavani, H. (2008). *Informational Privacy: Concepts, Theories, and Controversies*, in Himma K. e Tavani H. (eds.), *The Handbook of Information and Computer Ethics*, Indianapolis, 131-164
Thouvenin, F. (2021), "Informational Self-Determination: A Convincing Rationale for Data Protection Law?" in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 4/246-257
Tigano F. (2022), "Protezione dei dati e pubblica amministrazione: alcuni spunti di riflessione", in *Diritto e società*, 2, 413-432
Torchia L. (2006), *Il governo delle differenze. Il principio di equivalenza nell'ordinamento europeo*, Bologna
Touffait A. (1973), "Libertés publiques et Informatique", in *Exposé Académie Science morale et politique*, G.P. II
Travi A. (1995), "Giurisprudenza amministrativa e principio di legalità", in *Diritto pubblico*, 90 ss.
Travi A. (2008), *Il principio di legalità nel diritto amministrativo che cambia*, in *Il principio di legalità nel diritto amministrativo che cambia. Atti del 53° Convegno di studi di scienza dell'amministrazione (Varenna, 20-22 settembre 2007)*, Milano, 2008, 27
Uricchio A. (2019), "Robot tax: modelli di prelievo e prospettive di riforma", in *Giur. It.*, 7, 1657 ss.
Vandelli L. (2006), *Psicopatologia delle riforme quotidiane. Le turbe delle istituzioni: sintomi, diagnosi e terapie*, Bologna
Vari F. e Piergentili F. (2021), "'To no other end, but the... Safety, and publick good

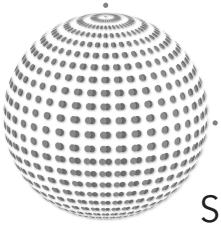
of the People': le limitazioni alla protezione dei dati personali per contenere la pandemia di Covid-19", *Rivista AIC*, 1, 328-342
Vecchio F. (2012), *Primazia del diritto europeo e salvaguardia delle identità costituzionali: effetti asimmetrici dell'europeizzazione dei controlimiti*, Torino
Vitalis, A. (1981), *Informatique, pouvoir et libertés*, Paris
Vogliotti M. (2013), *Legalità*, in *Enc. Dir., Ann*. VI, 371-435
von Grafenstein M. (2018), *The Principle of Purpose Limitation in Data Protection Laws*. *The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Baden-Baden.
Wachter S., Mittelstadt B., Floridi L. (2017), "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", in *International Data Privacy Law*, 7/2, 76–99
Wagner J. and Benecke A. (2016), "National legislation within the framework of the gdpr", in *European Data Protection Law Review (EDPL)*, 2(3), 353-361
Wieringa M. (2023), "Hey SyRI, tell me about algorithmic accountability: Lessons from a landmark case", in *Data & Policy*, 5, E2
Yu X., Zhao Y. (2019), "Dualism in data protection: Balancing the right to personal data and the data property right", in *Computer Law & Security Review*, 35/5
Zarsky T. (2017), "Incompatible: The GDPR in the Age of Big Data", in *Seton Hall Law Review*, 47, 4(2), https://ssrn.com/abstract=3022646 (01.04.2023)
Zhang K. (2019), "Incomplete Data Protection Law", in *German Law Journal*, 15(6), 1071-1104
Zopf, F. (2022), "Two worlds colliding the gdpr in between public and private law", in *European Data Protection Law Review* (EDPL), 8(2), 210-220
Zuboff S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York

FrancoAngeli:

a strong international commitment

Our rich catalogue of publications includes hundreds of English-language monographs, as well as many journals that are published, partially or in whole, in English.

The **FrancoAngeli**, **FrancoAngeli Journals** and **FrancoAngeli Series** websites now offer a completely dual language interface, in Italian and English.



Since 2006, we have been making our content available in digital format, as one of the first partners and contributors to the **Torrossa** platform for the distribution of digital content to Italian and foreign academic institutions. **Torrossa** is a pan-European platform which currently provides access to nearly 400,000 e-books and more than 1,000 e-journals in many languages from academic publishers in Italy and Spain, and, more recently, French, German, Swiss, Belgian, Dutch, and English publishers. It regularly serves more than 3,000 libraries worldwide.

Ensuring international visibility and discoverability for our authors is of crucial importance to us.

FrancoAngeli

torrossa
Online Digital Library

Questo LIBRO ti è piaciuto?

Comunicaci il tuo giudizio su:
www.francoangeli.it/opinione

VUOI RICEVERE GLI AGGIORNAMENTI
SULLE NOSTRE NOVITÀ
NELLE AREE CHE TI INTERESSANO?

ISCRIVITI ALLE NOSTRE NEWSLETTER SEGUICI SU:

FrancoAngeli
La passione per le conoscenze

Vi aspettiamo su:

www.francoangeli.it

per scaricare (gratuitamente) i cataloghi delle nostre pubblicazioni

DIVISI PER ARGOMENTI E CENTINAIA DI VOCI: PER FACILITARE LE VOSTRE RICERCHE.

Management, finanza, marketing, operations, HR
Psicologia e psicoterapia: teorie e tecniche
Didattica, scienze della formazione
Economia, economia aziendale
Sociologia
Antropologia
Comunicazione e media
Medicina, sanità

Architettura, design, arte, territorio
Informatica, ingegneria
Scienze
Filosofia, letteratura, linguistica, storia
Politica, diritto
Psicologia, benessere, autoaiuto
Efficacia personale
Politiche e servizi sociali

FrancoAngeli

La passione per le conoscenze

Attività amministrativa e trattamento dei dati personali

I dati personali costituiscono una materia prima tradizionale e necessaria per l'esercizio delle funzioni pubbliche. Le capacità di conservazione, gestione ed elaborazione dei dati, connesse all'incessante sviluppo delle tecnologie dell'informazione, pongono questioni centrali, all'incrocio tra l'opportunità di mettere tali potenzialità al servizio di interessi generali (a cominciare da un più efficiente ed efficace esercizio dell'attività amministrativa) e l'esigenza di assicurare ai consociati la tutela dei diritti fondamentali dai rischi cui sono esposti, proprio in ragione della disponibilità e dell'uso di queste tecnologie. Il saggio propone una chiave di lettura che muove dal margine di manovra che il GDPR accorda agli Stati membri nel declinare la disciplina del trattamento dei dati personali finalizzato all'esecuzione di compiti di interesse pubblico. L'indagine mette a tema il duplice standard legale che ne risulta, ne inquadra le possibili opzioni (in un ventaglio di possibilità comprese tra la *necessary clause* posta dal regolamento europeo e la *strict legality rule*) e ne registra gli effetti, anche attraverso l'analisi approfondita di alcuni casi di studio, caratterizzati dall'impiego di innovativi sistemi di trattamento dei dati personali a supporto dell'attività amministrativa. Il saggio offre così una lettura articolata degli impatti conseguenti allo standard di legalità concretamente applicato dal legislatore nazionale, anche per effetto delle più recenti oscillazioni del quadro positivo, e perviene ad alcune conclusioni non scontate in ordine al rapporto tra fonti di regolazione, tutela dei dati e promozione dell'autonomia di iniziativa e dell'innovazione delle amministrazioni pubbliche, anche alla luce di una rilettura del canone della legalità.

Benedetto Ponti è professore associato di Diritto amministrativo nel Dipartimento di Scienze Politiche dell'Università degli studi di Perugia, dove insegna Diritto amministrativo e Diritto dei media digitali. Nel medesimo Ateneo è Direttore del Master universitario di secondo livello per "Esperti in progettazione e gestione dell'anticorruzione e della trasparenza-EXPACT". Docente di Diritto dell'informazione presso la Scuola di Giornalismo Radiotelevisivo di Perugia, è stato consulente dell'Autorità nazionale anticorruzione in materia di trasparenza amministrativa e nella formulazione di indicatori per la misurazione del rischio di corruzione a livello territoriale. I suoi interessi di ricerca riguardano, in particolare, il regime dei dati pubblici, l'organizzazione e l'imparzialità dell'amministrazione, gli istituti di prevenzione della corruzione, la trasparenza amministrativa e il diritto dei media digitali.

FrancoAngeli
La passione per le conoscenze