RICERCA SCIENTIFICA E PROTEZIONE DEI DATI PERSONALI
Principi generali e raccomandazioni

QUADERNI DELL'OSSERVATORIO ▪ Approfondimenti 46

Fondazione CARIPLO
TUTE SERVARE MUNIFICE DONARE · 1816

RICERCA SCIENTIFICA E PROTEZIONE DEI DATI PERSONALI
Principi generali e raccomandazioni

A cura di
Paolo Guarda, Università di Trento
Giorgia Bincoletto, Università di Trento

Collana “Quaderni dell’Osservatorio” n. 46 ▪ Anno 2023

Fondazione Cariplo
Via Daniele Manin 23 ▪ 20121 Milano ▪ www.fondazionecariplo.it

Fondazione CARIPLO

INDICE

Abbreviazioni e acronimi

CAD	D.Lgs. 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale"
Codice Privacy	D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"
CGUE	Corte di Giustizia dell'Unione Europea
CNIL	Commission nationale de l'informatique et des libertés
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
D.L.	Decreto Legge
D.Lgs.	Decreto Legislativo
DPIA	Data protection impact assessment - valutazione d'impatto sui dati personali
DPbD	Data Protection by Design
Direttiva Privacy	Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"
Fondazione	Fondazione CARIPLO
Garante Privacy	Garante per la protezione dei dati personali
GDPR	Regolamento UE 2016/679 "Regolamento Generale sulla Protezione dei Dati" (RGPD - General Data Protection Regulation (GDPR))
G.U.	Gazzetta Ufficiale della Repubblica Italiana
IA	Intelligenza Artificiale
IoT	Internet of Things
OA	Open Access
OD	Open Data
OGD	Open Government Data
PNRR	Piano Nazionale di Ripresa e Resilienza
UE	Unione Europea
WP29	Gruppo Articolo 29, Data protection Working Party

Abstract

Il Quaderno è finalizzato alla descrizione dei profili giuridici relativi alla disciplina in materia di protezione dei dati personali nel contesto della ricerca scientifica, con particolare attenzione agli interventi del Garante per la protezione dei dati personali e delle autorità europee. Vengono, inoltre, introdotte le principali coordinate sul tema del c.d. Open Government Data e sul rapporto tra distribuzione open data e disciplina in materia di protezione dei dati personali. L'approccio metodologico è basato sulla "data protection by design", che viene debitamente approfondita. Il Quaderno presenta, infine, diverse tabelle esplicative con raccomandazioni schematiche e buone prassi, volte a fornire indicazioni applicative. Il lavoro è stato concluso a giugno 2022.

EXECUTIVE SUMMARY

Il lavoro presentato in questo Quaderno è finalizzato alla descrizione e all'analisi dei profili giuridici inerenti alla disciplina in materia di protezione dei dati personali nel contesto della ricerca scientifica. L'approfondimento è organizzato in cinque capitoli.

Nel primo capitolo il Quaderno inquadra il regime giuridico europeo e italiano che regola il trattamento dei dati personali nell'ambito della ricerca scientifica, con particolare attenzione alle regole del Regolamento Generale sulla protezione dei dati (GDPR), al Codice Privacy e agli interventi del Garante per la protezione dei dati personali, delle autorità europee e considerando alcune prassi applicative. Un progetto di ricerca potrebbe richiedere l'utilizzo di dati, e in particolare il trattamento di dati personali. Se da un lato è necessario proteggere il diritto alla protezione dei dati personali, dall'altro la ricerca deve sicuramente essere incentivata e la (più libera possibile) circolazione dei

dati rappresenta uno strumento imprescindibile per realizzarla. L'equilibrio tra queste due tensioni è regolato da una serie di principi e obblighi ai quali i ricercatori responsabili di un progetto di ricerca devono sottostare per l'intera durata del ciclo di vita della ricerca stessa.

Nel medesimo capitolo si presenta e analizza l'approccio basato sulla c.d. *data protection by design*, quale principio centrale da adottare in materia di protezione dei dati personali per implementare politiche interne e attuare misure tecniche che soddisfino tutti i principi previsti dalla normativa e che proteggano efficacemente i diritti degli interessati. Vista la complessità di tale approccio, il Quaderno fornirà chiare coordinate generali per la sua adozione, che andranno poi specificate ulteriormente nel concreto scenario applicativo.

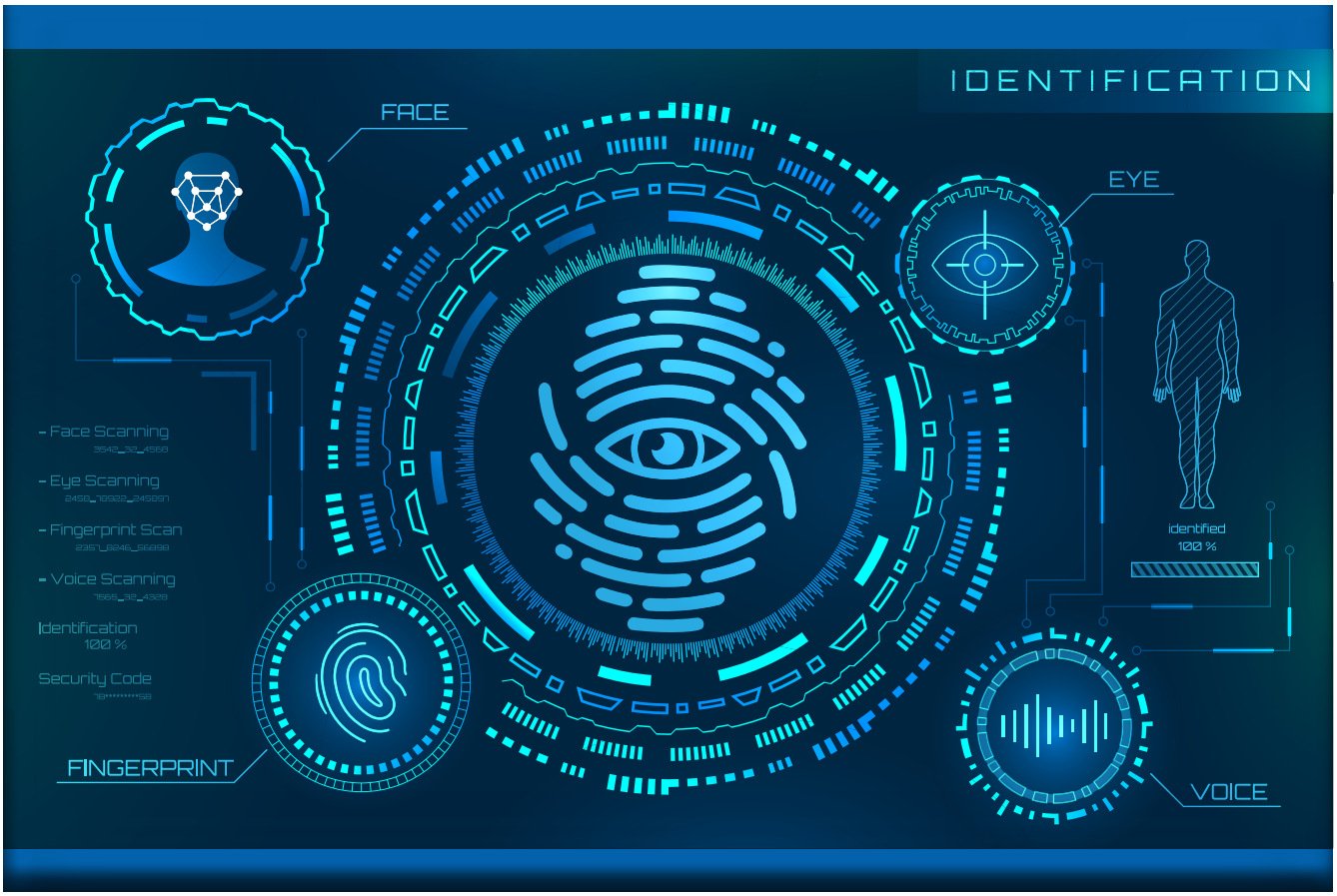
Il secondo capitolo è dedicato al tema della valorizzazione di una banca dati in modalità aperta (*Open Data*) e del c.d. *Open Government Data*. Dopo un'analisi della normativa, modificata di recente nel 2021, e per lo più riguardante il riutilizzo di documenti e dati pubblici, il capitolo affronta le questioni problematiche del rapporto tra distribuzione *Open Data* e disciplina in materia di protezione dei dati personali, strettamente connesse alla condivisione per l'uso e riuso dei dati. L'apertura potrebbe riguardare sia i dati generati come risultati della ricerca, sia quelli già conservati in database gestiti da soggetti pubblici o privati. Oltre a ciò, il Quaderno propone delle buone prassi per gli *Open Data* e per richiedere l'accesso a dati.

Nel terzo capitolo una breve descrizione di esperienze nazionali e internazionali di successo mostra soluzioni che hanno efficacemente bilanciato tra necessaria tutela dei dati personali e prospettive di riuso di dati per finalità di ricerca scientifica.

Una breve presentazione della normativa relativa al Piano Nazionale di Ripresa e Resilienza (PNRR) nel quarto capitolo tratteggia alcune indicazioni sui prossimi sviluppi che potrebbero riguardare l'utilizzo dei dati nella ricerca scientifica.

Il Quaderno offre, infine, nel quinto capitolo, diverse tabelle esplicative con raccomandazioni schematiche e buone prassi, volte a fornire indicazioni applicative. Ogni scenario applicativo presenta peculiarità che potrebbero obbligare il titolare del trattamento ad approfondire specifiche tematiche ed eventualmente a tenere in considerazione anche ulteriori discipline di dettaglio e adottare altre misure tecniche e organizzative. Tuttavia, le raccomandazioni e buone prassi seguono l'approccio di *data protection by design* e forniscono indicazioni organizzate per attività (analisi del trattamento, predisposizione documentale, basi giuridiche, predisposizione degli strumenti informatici, buone prassi del trattamento), tenendo conto delle diverse fasi temporali del progetto (fase preliminare, svolgimento dell'attività di ricerca, chiusura).

1. DATI PERSONALI E RICERCA IN EUROPA E IN ITALIA



Questa sezione descrive e analizza il regime giuridico che regola il trattamento dei dati personali nell'ambito della ricerca scientifica a livello italiano ed europeo. Oltre alla normativa applicabile vengono considerati gli interventi del Garante per la protezione dei dati e delle autorità europee ed eventuali prassi applicative sviluppate a livello istituzionale. Il regime giuridico che regola il trattamento dei dati personali nell'ambito della ricerca scientifica a livello europeo è espressione dell'articolo 8 della Carta dei diritti fondamentali dell'UE, che riconosce la protezione dei dati personali come diritto fondamentale e autonomo rispetto alla protezione della vita privata (Art. 7) e agli altri diritti fondamentali, e dell'articolo 16 del TFUE (Trattato sul funzionamento dell'Unione europea), che consente all'Unione di legiferare in materia.

Il quadro giuridico europeo sulla protezione dei dati personali è stato per più di vent'anni basato sulla

Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 ed è oggi fondato sul Regolamento 679/2016 (GDPR), il quale ha aggiornato la normativa con impatto diretto in tutti gli Stati membri dell'Unione, essendo concepito per uniformare la regole operative superando le contraddizioni o le possibili incongruenze emerse dai diversi recepimenti nazionali della precedente direttiva. Questo regolamento è di grande importanza perché rivede gli strumenti volti a tutelare i dati personali di fronte alle nuove sfide tecnologiche, creando un modello di protezione che si sta dimostrando una sorta di *benchmark* globale, con un "effetto domino" (*Brussel effect)* su altri ordinamenti giuridici, anche oltreoceano (Bradford, 2020).

In Italia, il principale riferimento in materia, che ha prima recepito la Direttiva 95/46/CE, e che è poi stato adeguato al GDPR, è il D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (o Codice Privacy), che prevede specifiche regole in materia di ricerca. La ricerca scientifica è protetta a livello costituzionale dall'Art. 9, che ne promuove lo sviluppo e dall'Art. 33, che ne sancisce la libertà. Il diritto alla protezione dei dati personali è riconosciuto in modo implicito nel catalogo dei diritti della personalità dell'Art. 2 della carta costituzionale.

Un progetto di ricerca potrebbe coinvolgere l'utilizzo di dati e, in particolare, il trattamento di quelli personali. Se da un lato è necessario proteggere i diritti fondamentali degli individui coinvolti in un progetto di ricerca, incluso il loro diritto alla protezione dei dati personali, una ricerca necessita di dati e ne vorrebbe la libera circolazione. L'equilibrio tra queste due tensioni è regolato da una serie di principi e obblighi ai quali i ricercatori responsabili di un progetto di ricerca devono sottostare per l'intera durata del ciclo di vita della ricerca stessa.

1.1. Definizioni

Per poter analizzare le regole previste dalla normativa applicabile in materia di protezione dei dati personali è preliminarmente necessario fornire alcune definizioni che si rivelano fondamentali. Queste definizioni sono state approfondite e contestualizzate nell'ambito della ricerca scientifica.

Dato personale: "qualsiasi informazione riguardante una persona fisica identificata o identificabile" (Art. 4, n. 1) GDPR). Il nucleo del dato è, pertanto, l'informazione (Guarda, 2021). La nozione ampia, flessibile e dinamica di dato personale impone un'attenta verifica durante la redazione del progetto di ricerca poiché il framework normativo si applica solamente ai dati personali e alla loro circolazione (Art. 1 GDPR). Oltre a informazioni pacificamente riconosciute come dati personali (nome, cognome, e-mail, fotografia, età), esempi di informazioni considerate tali dalla giurisprudenza della Corte di Giustizia dell'Unione Europea sono: numero di telefono; informazioni su condizioni di lavoro e *hobbies*; dati relativi al guadagno lavorativo; dettagli del passaporto; immagini della persona registrate da una videocamera; esami scritti degli studenti e commento dei docenti sugli stessi; indirizzo IP. In contesti di ricerca con partner statunitensi è possibile ritrovare l'utilizzo della dicitura "*personal information*", che è da considerarsi non pienamente sovrapponibile alla nozione di dato personale (Solove e Schwartz, 2018). Dovrà quindi essere compiuta dal gruppo una *gap analysis* di tipo normativo per definire un approccio comune durante il progetto che possa garantire la conformità alla disciplina prevista.

Dato non personale o dato anonimo: informazione che non identifica o non può identificare una persona fisica (Considerando 26 GDPR). In ambito statistico e di ricerca possono essere sviluppati i cosiddetti "dati sintetici", informazioni generate *ex novo* da algoritmi di intelligenza artificiale (IA) a partire da dataset reali di dati personali, ma successivamente scollegate dagli stessi e non riferibili a persone fisiche (Floridi, 2020). Ai dati non personali si applicano le regole del Regolamento UE 2018/1807, che mira a garantire la libera circolazione di tali dati in un'economia digitale sempre più competitiva e che definisce dato non personale il dato diverso "dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679" (Art. 3 Reg. 2018/1807). Questo Regolamento fornisce alcuni esempi specifici di dati non personali: "insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati"; "dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua"; "dati sulle esigenze

di manutenzione delle macchine industriali" (Considerando 9 Reg. 2018/1807).

Dato anonimizzato: dato privo di elementi identificativi, che si sottrae alla disciplina a seguito di un trattamento di "de-identificazione irreversibile" compiuta sul dato personale (WP 29, Parere 05/2014). La scelta della tecnica di anonimizzazione deve essere ponderata essendo l'eventuale reidentificazione, da cui conseguirebbe l'applicazione della normativa, molto rischiosa alla luce della rapida evoluzione tecnologica; all'uopo si compie una scelta in ottica di *accountability* o responsabilizzazione nel definire il dato come anonimizzato e non più personale. Al dato anonimizzato si applica il Regolamento 2018/1807; tuttavia, come specificato dallo stesso regolamento "se i progressi tecnologici consentono di trasformare dati anonimizzati in dati personali, tali dati sono trattati come dati personali e si applica di conseguenza" il GDPR (Considerando 9 Reg. 2018/1807).

Dato pseudonimizzato: dato personale a cui è stata applicata una tecnica di "pseudonimizzazione", ossia un «trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» (Art. 4, n. 5) GDPR). La pseudonimizzazione è considerata anche una misura di sicurezza e una soluzione appropriata in ottica di *data protection by design*. Al dato pseudonimizzato si applicano le regole del quadro normativo perché può identificare la persona fisica, se ricombinato con l'informazione aggiuntiva. Un progetto di ricerca che utilizza dati pseudonimizzati deve perciò rispettare la normativa in materia di dati personali.

Dataset misto: insieme strutturato di dati personali e non, molto comuni in contesti di ricerca che utilizzano strumenti di Intelligenza Artificiale (IA), *Internet of Things* (IoT) e *Big Data Analytics*. Se i dati personali e quelli anonimi sono separabili, si applicherà il GDPR ai primi e il Regolamento 2018/1807 ai secondi (Art. 2 Reg. 2018/1807); se la separazione non è possibile, o si ritiene sia economicamente inefficiente o non tecnicamente praticabile, si applicheranno le norme in materia di protezione dei dati personali all'intero dataset. Perciò, il progetto di ricerca dovrà considerare di trattare dati personali.

Categorie particolari di dati personali (o dati sensibili): dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale della persona fisica, nonché i dati genetici, i dati biometrici che identificano in modo univoco una persona fisica, i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona fisica (Art. 9, par. 1, GDPR). Il trattamento di dati sensibili in un progetto di ricerca richiede particolare attenzione poiché sono previste specifiche regole relative alla base giuridica e l'implementazione di ulteriori garanzie. A questi particolari dati potrebbero infatti applicarsi regole deontologiche definite dal Garante per una maggior protezione degli stessi (Art. 2-*quater* Codice Privacy).

Dati genetici: categoria particolare di dati personali relativi «alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica» e che possono risultare anche «dall'analisi di un campione biologico della persona fisica in questione» (Art. 4, n. 13) GDPR). Dati relativi al fenotipo, come il colore degli occhi, non sono considerati dati genetici, mentre lo sono quelli relativi al genotipo (Bygrave e Tosoni, 2020). I dati genetici non possono essere diffusi (Art. 2-*septies*, co. 8, Codice Privacy). In questo ambito, è opportuno segnalare che il trattamento dei dati deve coordinarsi con le regole dell'Art. 2-*septies* Codice Privacy e con le Prescrizioni relative al trattamento dei dati genetici del Garante (Aut. Gen. n. 8/2016). Frequentemente le informazioni genetiche rivelano caratteristiche non solo della persona fisica dalla quale sono raccolte, ma anche di membri della sua famiglia. Perciò, un progetto di ricerca dovrà attentamente valutare se più soggetti siano da considerarsi interessati al trattamento.

Dati biometrici: categoria particolare di dati personali «ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'im-

magine facciale o i dati dattiloscopici» (Art. 4, n. 14) GDPR). Ad esempio, i dati biometrici sono ricavati da impronte digitali, analisi del DNA e fotografie scattate da videocamere. I dati biometrici vengono utilizzati per identificare l'interessato e consentirne l'autorizzazione per un servizio. I dati biometrici non possono essere diffusi (Art. 2-*septies*, co. 8, Codice Privacy). In questo ambito, è opportuno segnalare che il trattamento dei dati biometrici deve coordinarsi con le regole dell'Art. 2-*septies* Codice Privacy. Se un progetto di ricerca utilizza *facial recognition systems* o sistemi di videosorveglianza quali droni che utilizzano algoritmi di IA, con alta probabilità starà raccogliendo dati biometrici.

Dati relativi alla salute: categoria particolare di dati personali relativi «alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» (Art. 4, n. 15) GDPR). La nozione è molto ampia (Guarda, 2019). La salute mentale e fisica è da intendersi infatti come passata, presente o futura (Considerando 35). Sono ricompresi in questa categoria: le informazioni riguardanti malattie, disabilità, rischio di malattie, anamnesi medica, trattamenti clinici, stato fisiologico e stato biomedico indipendentemente dalla fonte; le informazioni sulla persona fisica raccolte nel corso dell'assistenza sanitaria e della registrazione al servizio, anche transfrontaliero (Direttiva 2011/24/UE); numeri, simboli o elementi specifici attribuiti per identificare la persona in modo univoco ai fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo umano o una sostanza organica, compresi i dati genetici e i campioni biologici. Potrebbero essere ricompresi, se atti a rivelare stati di salute, anche a seguito di deduzione (WP 29, 2015): dati relativi alle abitudini di fumo e di consumo alcolico; dati sulle allergie; l'appartenenza a un gruppo di sostegno per pazienti; informazioni sulla malattia in un contesto lavorativo; dati utilizzati in un contesto sanitario amministrativo; dati sull'acquisto di prodotti medici, dispositivi e servizi quando lo stato di salute può essere dedotto da queste informazioni. I semplici dati sullo stile di vita, come il numero di passi durante una passeggiata quotidiana, sono dati meramente "grezzi".

Deve essere sottolineato che può rimanere una zona grigia di qualificazione poiché le "informazioni" grezze possono essere spesso combinate, e quindi le conclusioni sul rischio medico dell'individuo possono essere da esse dedotte, indipendentemente dal fatto che siano accurate (ad esempio utilizzando la pressione sanguigna e il sesso, l'età, ecc.). I dati relativi alla salute non possono essere diffusi (Art. 2-*septies*, co. 8, Codice Privacy) e sono previste particolari modalità di trattamento nel Codice Privacy (Artt. 2-*septies*, 75, 77-80, 81, 86-*bis*, 92-93 Codice Privacy). Un progetto di ricerca deve attentamente valutare se informazioni su stili di vita e comportamenti alimentari o quotidiani possano rientrare nella nozione di dato sanitario in base ad alcune circostanze concrete, poiché, se fosse, si dovrebbero applicare le regole relative al trattamento di dati sensibili. In ambito di dati sanitari e ricerca è opportuno tener conto anche delle discipline in materia di dispositivi medici (Reg. UE 2017/745 e 746) e di indagini cliniche (Reg. UE 536/2014).

Dati giudiziari: categoria di dati personali relativi «alle condanne penali e ai reati o a connesse misure di sicurezza» (Art. 10, GDPR). Questi dati non sono ricompresi nella categoria di dati particolari dell'Art. 9 GDPR, ma richiedono comunque particolari misure di salvaguardia e protezione e che il trattamento venga realizzato sotto il controllo dell'autorità pubblica.

Big Data: grandi aggregazioni di dati digitali caratterizzati dalle cosiddette "V": "volume, varietà, velocità, veridicità, valore, variabilità, validità, volatilità, visualizzazione, vulnerabilità" (Guarda, 2021). Un progetto di ricerca che utilizza *Big Data* deve correttamente valutare l'applicabilità della normativa in materia di protezione dei dati personali.

Trattamento di dati: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali" (Art. 4, n. 2) GDPR). Tra queste è possibile ricomprendere: «la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione,

la cancellazione o la distruzione» di dati personali (Art. 4, n. 2) GDPR). Le operazioni di trattamento sono indipendenti dalla tecnologia utilizzata, visto che la normativa è neutrale da un punto di vista tecnologico (Considerando 15). La normativa si applica sia al trattamento interamente o parzialmente automatizzato di dati personali, sia al trattamento non automatizzato di dati personali contenuti in un archivio o ad esso destinati (Art. 2, par. 1, GDPR). Esempi di operazioni considerate "trattamenti" dalla giurisprudenza della CGUE sono: caricamento di dati personali in una pagina web; raccolta di dati personali da documenti pubblici; pubblicazione di dati su carta stampata; invio di messaggi contenenti dati personali; cattura di immagini e suoni riferiti a persone fisiche; conservazione di dati personali per future richieste di accesso di un'autorità pubblica; conservazione di video interviste o pubblicazione di registrazioni di convegni; il trasferimento di dati personali al di fuori dei confini dello Spazio Economico Europeo (c.d. "trasferimento transfrontaliero di dati"). Questo Spazio comprende l'Unione Europea, l'Islanda, la Norvegia e il Liechtenstein. Si sottolinea che il processo di anonimizzazione, fino alla de-identificazione dei dati, è considerato un trattamento. Un progetto conterrà plurime attività di trattamento e dovrà, perciò, per ciascuna operazione definire la base giuridica che ne consenta l'effettuazione e informare l'interessato nell'informativa. Durante l'elaborazione e l'esecuzione del progetto di ricerca ogni attività dovrà essere considerata distintamente per la definizione delle misure di *accountability* (Art. 24 GDPR), di *data protection by design* e *by default* (Art. 25 GDPR), per la predisposizione del registro delle attività di trattamento (Art. 30 GDPR), per l'implementazione delle misure di sicurezza del trattamento (Art. 32 GDPR), e per la redazione della valutazione di impatto sulla protezione di dati - DPIA (Art. 35 GDPR).

Comunicazione di dati: particolare attività di trattamento che consiste nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi da chi ha ruoli nel trattamento dei dati (Art. 2-*ter,* par. 4, lett. a) Codice Privacy), quali, ad esempio, il responsabile del trattamento o le persone autorizzate ai sensi dell'Art. 2-*quaterdecies* Codice Privacy). Le autorità pubbliche potrebbero richiedere che alcuni dati di progetto siano ad essi comunicati per motivi di interesse pubblico o obbligo di legge.

Diffusione di dati: particolare attività di trattamento che consiste nel «dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione» (Art. 2-*ter,* par. 4, lett. b) Codice Privacy). Come anticipato, i dati genetici, biometrici e sanitari non possono in alcun modo essere diffusi (Art. 2-*septies*, co. 8, Codice Privacy), anche in ambito di ricerca.

Profilazione: particolare attività di trattamento automatizzato che consiste «nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (Art. 4, n. 4) GDPR). La profilazione è caratterizzata da due processi: l'inferenza di caratteristiche della persona fisica da alcune informazioni (creazione del profilo) e l'utilizzo di tali caratteristiche nei confronti dell'interessato durante l'attività di trattamento (applicazione del profilo). Alcuni progetti di ricerca che creano profili delle persone fisiche, ad esempio in ambito di medicina per predizione su future implicazioni, devono tener conto degli obblighi informativi ulteriori in presenza di profilazione (Art. 14, par. 2, lett. g), 15, par. 1, lett. h) GDPR).

Trasferimento transfrontaliero di dati: particolare attività di trattamento che consiste nell'invio di dati personali al di fuori dello Spazio Economico Europeo (SEE). Il progetto di ricerca scientifica dovrà prestare attenzione all'eventuale trasferimento di dati che può avvenire solo in presenza di determinate condizioni e garanzie (Artt. 44-50 GDPR).

Principi del trattamento dei dati: ogni trattamento di dati personali deve seguire i seguenti principi: liceità, correttezza, trasparenza; adeguatezza; pertinenza; minimizzazione; esattezza; limitazione della conservazione; integrità e riservatezza, responsabilizzazione (*accountability*) (Art. 5 GDPR).

Interessato: persona fisica identificata, o identificabile dal dato personale «direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (Art. 4, n. 1) GDPR). Il framework normativo non si applica ai dati riferibili a persone giuridiche. Per quanto concerne le persone decedute, il GDPR non si applica ai loro dati personali, ma alcuni Stati Membri hanno adottato diverse soluzioni prevedendo articolate discipline per la "morte digitale" (Alpa e Resta, 2020). In Italia è prevista la possibilità che congiunti, eredi o altri soggetti possano esercitare i diritti dell'interessato dopo la sua morte (Art. 2-*terdecies* Codice Privacy). Perciò, progetti di ricerca su persone decedute devono comunque preliminarmente valutare l'eventuale applicazione di alcune regole in materia di protezione dei dati personali, soprattutto se coinvolgono partner di altri Stati membri dell'Unione Europea. Il Garante ha definito poi alcuni interessati che si devono considerare "soggetti vulnerabili": minori, disabili, anziani, infermi di mente, pazienti e richiedenti asilo (Provv. n. 467 del 2018); nei trattamenti che li coinvolgono si raccomanda una valutazione d'impatto sulla protezione dei dati.

Titolare del trattamento: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua desi-

gnazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri» (Art. 4, n. 7) GDPR). Il titolare è soggetto alla normativa europea e nazionale se il suo stabilimento è nel territorio nell'Unione Europa (Art. 4, n. 16) GDPR) o se tratta dati personali di interessati che si trovano nell'UE in presenza di alcune condizioni (Art. 3 GDPR). Il titolare (*controller*) assume un ruolo chiave per le attività di trattamento perché, appunto, ne definisce finalità (perchè) e i mezzi, ossia le modalità e le misure con cui viene realizzato (come). In un progetto di ricerca è necessario definire chiaramente il titolare poiché sarà il soggetto ad assumere la regia del trattamento dei dati, con conseguenti obblighi e responsabilità, e a delegare concrete attività di trattamento a un eventuale responsabile o a soggetti incaricati. In presenza di più partner di progetto potrebbero esserci più titolari, uniti da un accordo di contitolarità (Art. 26 GDPR).

Responsabile del trattamento: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento» (Art. 4, n. 8) GDPR). Il titolare deve designare il responsabile con apposito contratto o accordo che definisca istruzioni e misure da applicare (Art. 28 GDPR). In questa categoria di soggetti non rientrano i dipendenti del titolare, ma soggetti esterni e "legalmente separati", come *service provider*. In un progetto di ricerca, alcune attività di trattamento potrebbero essere svolte dal fornitore di un *cloud* per conservare i dati, da una società esterna che sviluppa parte del software o fa analisi sui dati per conto del titolare, anche statistiche, o che raccoglie dati per questionari di soddisfazione del progetto, sempre per conto del titolare. Si sottolinea che il titolare deve monitorare le attività del responsabile, che è tenuto a precisi obblighi. In caso di responsabilità per violazione della normativa in materia di protezione dei dati personali un responsabile risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi assegnati al suo ruolo dalla normativa o ha agito in modo difforme o contrario rispetto alle istruzioni del titolare (Art. 82 GDPR). Nel documento del progetto di ricerca deve essere designato il responsabile del trattamento (Art. 3, Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (Aut. Gen. n. 9/2016)).

Responsabile della protezione dei dati - DPO: persona fisica o giuridica esperta nella materia di protezione dei dati e della gestione di dati più in generale, designata dal titolare del trattamento o dal responsabile del trattamento per supportare nel valutare e organizzare tutte le attività di trattamento (Artt. 37-39 GDPR). Il DPO deve assumere una posizione di indipendenza rispetto al titolare e al responsabile e fornire una consulenza e sorveglianza attiva e costante per tutte le operazioni svolte, come ad esempio sulla valutazione di impatto, e anche per cooperare con le autorità, tra cui il Garante. In un progetto di ricerca un DPO potrebbe assumere un ruolo chiave nel definire in concreto gli obblighi del titolare e del responsabile e suggerire le prassi applicative più conformi alla normativa.

Consenso privacy: «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento» (Art. 4, n. 11) GDPR). Il consenso è una delle possibili basi giuridiche del trattamento e può essere scritto o orale. Tuttavia, il titolare deve dimostrare di averlo raccolto. Il consenso privacy è sempre revocabile (Art. 7 GDPR). Il consenso deve essere informato; perciò, l'interessato deve poter ricevere idonea informativa. Esso deve essere distinto dal consenso a partecipare al progetto di ricerca inteso come obbligo deontologico e procedurale di un progetto di ricerca. In caso di minori partecipanti a un progetto, il consenso dovrà essere prestato da chi detiene la responsabilità genitoriale. Qualora fosse necessario raccogliere il consenso per finalità di ricerca, ma non fosse possibile individuare pienamente la finalità del trattamento al momento della raccolta dei dati, gli interessati potranno prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca, essendo valido soltanto un consenso specifico. Sebbene, quindi, ci possa essere una certa flessibilità e granularità in ambito di consenso e ricerca scientifica, il consenso dell'interessato deve rimanere specifico. Un progetto di ricerca che richiede il consenso dovrebbe trattare dati personali sulla base del

consenso soltanto con una "finalità ben descritta" (EDPB, Linee guida sul consenso 05/2020). Se la finalità non fosse possibile da definire puntualmente in via preliminare, allora essa potrebbe essere descritta più in generale. Un consenso "in bianco" per progetti di ricerca non è considerabile valido perché il principio di specificazione della finalità è chiave in ambito di dati personali. Se il progetto vorrà trattare dati particolari, il consenso dell'interessato dovrà essere esplicito (Art. 9 GDPR).

Base giuridica del trattamento: una delle basi legittime per trattare i dati personali in modo lecito. Le basi giuridiche sono elencate nell'Art. 6 per i dati personali "comuni" e nell'Art. 9, par. 2, per i dati particolari. Per ogni attività di trattamento è necessaria apposita base giuridica. Un progetto di ricerca deve valutare con attenzione la base poiché, oltre alla possibilità del consenso, potrebbe esserci un obbligo legale o un interesse pubblico ai fini di ricerca.

Informativa privacy: lista di informazioni sul trattamento dei dati che deve essere comunicata all'interessato (Art. 12-14 GDPR). Un progetto di ricerca può trattare i dati solo per le finalità indicate nell'informativa.

Diritti dell'interessato: diritti previsti dal GDPR agli Artt. 13-22, come ulteriori diritti connessi al diritto di protezione dei dati personali, ossia il diritto di ricevere informazioni (Artt. 13 e 14), il diritto di accesso (Art. 15), il diritto di rettifica (Art. 16), il diritto di cancellazione (Art. 17, spesso richiamato come "diritto all'oblio"), il diritto di limitazione del trattamento (Art. 18), il diritto di portabilità dei dati (Art. 20), il diritto di opposizione (Art. 21), il diritto a non essere sottoposto a una decisione interamente automatizzata (Art. 22, spesso richiamato in connessione a dibattiti sul diritto di spiegazione della logica dell'algoritmo). Questi diritti operano secondo particolari circostanze definite dai già menzionati articoli, non sono quindi sempre applicabili e possono essere limitati in presenza di alcune condizioni. Dovrà, pertanto, essere valutato di volta in volta l'operatività del diritto esercitabile dall'interessato. In ambito di ricerca rivestono una particolare importanza il diritto di accesso ai dati, che consente anche di richiedere informazioni sulla logica del trattamento (e quindi degli strumenti automatici utilizzati), il diritto alla cancellazione dei dati (che potrebbe impattare una ricerca) e il diritto a non essere sottoposto a una decisione interamente automatizzata (che opera in presenza di effetti significativi sulla sfera giuridica dell'interessato e potrebbe essere esercitato in presenza di algoritmi di intelligenza artificiale).

Valutazione d'impatto sulla protezione dei dati - DPIA: valutazione dell'impatto che il particolare trattamento ha sui dati personali degli interessati, tenendo conto degli eventuali rischi (Art. 35 GDPR). Una valutazione deve quantomeno contenere: «una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento»; «una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità»; «una valutazione dei rischi per i diritti e le libertà degli interessati»; e «le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità» al GDPR, «tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione» (Art. 35, par. 7, GDPR). Si consigliano a questo scopo i tool dell'European Union Agency for Cybersecurity (www.enisa.europa.eu) o dell'Autorità Garante Francese CNIL (www.cnil.fr), quest'ultimo consigliato dal Garante italiano stesso. La DPIA va sicuramente realizzata nei casi previsti nell'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 (e da EDPB, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adottate il 4 Aprile 2017). Progetti di ricerca che effettuano tipologie di trattamento che rientrano in quelle previste da tale Provvedimento dovranno effettuare la valutazione di impatto. Si possono, infine, aggiungere i progetti di ricerca e le sperimentazioni cliniche che riguardano l'archiviazione di dati particolari pseudonimizzati che riguardano soggetti vulnerabili (WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679).

1.2. Trattamento dei dati personali e ricerca negli ordinamenti europeo e italiano

1.2.1. Il contesto dell'Unione Europea

La Direttiva 95/46/CE prevedeva un *favor* per i trattamenti di dati personali con finalità di ricerca. A partire dall'entrata in vigore e dall'effettiva applicazione del GDPR (25 maggio 2018) un acceso dibattito ha affrontato la questione circa l'impatto che le nuove regole avrebbero avuto sulla ricerca scientifica quale presupposto ineludibile per assicurare lo sviluppo della conoscenza e del progresso. Sul punto è possibile affermare che il GDPR non ha cambiato il generale approccio di favore, ma ha sicuramente modificato e ampliato la regolamentazione. Come indicato nel Considerando 113, in ambito di trasferimento transfrontaliero dei dati, per quanto concerne le finalità di ricerca scientifica, storica o statistica è "opportuno tener conto delle legittime aspettative della società nei confronti di un miglioramento delle conoscenze". Il GDPR, infatti, facilita la ricerca creando un regime di deroghe ad alcune regole generali in presenza di adeguate garanzie.

Un progetto potrebbe trattare dati personali per finalità di ricerca in via principale, ossia la raccolta del dato avviene sin da subito per la ricerca, o in via secondaria, nel caso in cui il trattamento per la ricerca avviene dopo un trattamento con diversa finalità, se con esso compatibile (Guarda, 2021).

All'interno del GDPR la norma di riferimento è l'art. 89, il quale prevede che:

1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.
2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.
3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.
4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

In generale, per poter trattare i dati personali il titolare del trattamento del progetto di ricerca deve adottare adeguate garanzie e misure sia tecniche che organizzative che devono essere valutate e scelte sulla base di un'analisi dei concreti rischi e della specificità del contesto applicativo. Aspetti chiave sono la protezione della sicurezza dei dati ai sensi dell'art. 32 GDPR e l'osservanza del principio di minimizzazione, che richiede che i dati personali siano "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (Art. 5, par. 1, lett. c), GDPR).

Le misure di minimizzazione si estrinsecano in concreto in tecniche di anonimizzazione o pseudonimizzazione che limitano i dati personali utilizzabili durante le operazioni di trattamento. Tuttavia, l'utilizzo di informazioni anonime potrebbe impoverire la por-

tata informativa dei dati, fondamentale invece per la ricerca (WP29, Parere 5/2014). Si potrebbe persino sostenere che sussista un'apparente antinomia tra la finalità di ricerca e il principio di minimizzazione dei dati. Progetti di ricerca in tema di "*genome wide*" e di *Big Data* necessitano di una grandissima mole di dati, essendo votati per loro natura alla massimizzazione e accumulazione di informazioni con cui testare e addestrare gli algoritmi. Peraltro, non sempre è possibile definire anticipatamente la necessità di un dato personale per la ricerca; da qui, si delineerebbe un profilo di incompatibilità, per così dire, strutturale della ricerca scientifica con il principio di minimizzazione (Ducato, 2020). La pseudonimizzazione apparirebbe, invece, una misura da valutare se adeguata al concreto progetto di ricerca perché non priva il dato degli elementi identificativi, ma li separa dall'informazione ai fini di maggior sicurezza. In ogni caso, le soluzioni tecniche e organizzative adottate in ambito di ricerca ai sensi dell'Art. 89 avranno un intrinseco carattere dinamico e saranno volte a prevenire rischi di tipo giuridico, etico e sociale.

Come emerge dal testo dell'Art. 89 del GDPR, il regolamento ha lasciato ampio spazio e libertà agli Stati membri di derogare i principi e prevedere nuove e specifiche garanzie (Cons. 156; TIPIK, 2021). Tale possibilità a livello nazionale rappresenta, in qualche modo, un limite rispetto all'intento di uniformare il diritto della disciplina dei dati personali europei. Il settore della ricerca scientifica potrebbe, quindi, essere regolato difformemente negli Stati membri, con piccole e grandi differenze. Ciò potrebbe ricreare quella serie di ostacoli e barriere che si riteneva di voler superare con il nuovo intervento normativo rispetto all'implementazione della direttiva.

L'Art. 89 non definisce le finalità di ricerca storica, archiviazione nel pubblico interesse e ricerca scientifica e statistica. I considerando del GDPR offrono tuttavia alcune indicazioni utili.

Con riferimento alla prima categoria, il Considerando 160 del GDPR menziona la ricerca storica e la ricerca a fini genealogici, ribadendo che la normativa non dovrebbe, di regola, applicarsi alle persone decedute. Come anticipato nelle definizioni, ciò potrebbe in realtà non essere escluso in alcuni ordinamenti europei: in Italia, ad esempio, vi è una previsione che consente l'esercizio dei diritti degli interessati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione (Art. 2-*terdecies* Codice Privacy).

Separata dalla ricerca storica, vi è la finalità di archiviazione dei dati nel pubblico interesse, quale attività culturale da parte di autorità pubbliche o altri organismi che, anche in fase prodromica alla finalità di ricerca (Ducato, 2020), acquisiscono, conservano, valutano, organizzano, descrivono, comunicano, promuovono, diffondono e forniscono accesso "a registri con un valore a lungo termine per l'interesse generale" sulla base di un loro obbligo giuridico (Cons. 158 GDPR). In questa finalità rientrano ad esempio, le attività archivistiche per gli archivi di stato, gli archivi storici degli enti pubblici, e quelle effettuate da altri organismi culturali cui il diritto nazionale o dell'unione attribuisca tale specifica funzione istituzionale (European Archives Group, 2018).

La terza categoria richiamata dall'Art. 89 è la ricerca scientifica, che deve essere considerata in modo ampio come qualsiasi attività atta a generare nuova conoscenza e avanzare lo stato dell'arte in un settore scientifico (Guarda, 2021). La ricerca scientifica comprende, tra gli altri, lo "sviluppo tecnologico e dimostrazione", "la ricerca fondamentale", "la ricerca applicata", la "ricerca finanziata dai privati" e gli "studi svolti nell'interesse pubblico nel settore della sanità pubblica" (Cons. 159 GDPR). La ricerca, peraltro, riguarda sia le c.d. STEM ("*Science, Technology, Engineering and Mathematics*"), sia le scienze sociali e umanistiche (Cons. 157 GDPR). La ricerca può essere pubblica, ma anche privata e, perciò, anche con scopo di lucro, come nel caso di ricerche realizzate da società private al fine di sviluppare nuovi beni o servizi (Art. 179, par. 1, TFEU).

L'ultima tipologia prevista dall'Art. 89 GDPR è la ricerca statistica, quale «qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici» (Considerando 162). A questo settore si applicano le discipline in tema di confidenzialità sancite all'Art.

338, par. 2, TFEU e il Regolamento CE n. 223/2009 relativo alle statistiche europee. I dati in campo statistico sono generalmente aggregati e potrebbero non essere riferibili a soggetti in particolare. La differenza tra ricerca statistica e ricerca scientifica non è sempre chiara; tuttavia, è possibile individuare due caratteristiche peculiari del trattamento per fini statistici: la finalità di creare una base di conoscenza per future ricerche, anche in ambito scientifico, e l'esclusione di una ricaduta personalizzata sugli individui della ricerca (Ducato, 2020).

In presenza delle garanzie richieste dall'Art. 89, par. 1, GDPR si applica un regime che consente la deroga ad alcuni principi del trattamento dei dati personali (Artt. 5, par. 1, lett. b) limitazione delle finalità, ed e) limitazione alla conservazione, e 9, par. 2, lett. j) GDPR sulla ricerca con dati particolari) e all'esercizio di una serie di diritti dell'interessato (Artt. 14, 15, 16, 18, 21 GDPR: diritto di ricevere informazioni, diritto di accesso, diritto di rettifica, diritto di limitazione e diritto di opposizione al trattamento).

In primo luogo, in presenza di scopi di ricerca è consentita una deroga al principio di limitazione delle finalità, che prevede che i dati personali possano essere utilizzati esclusivamente per le finalità specifiche, esplicite e legittime per cui sono stati raccolti, non potendo essere ulteriormente trattati per finalità incompatibili con lo scopo originario per cui sono stati ottenuti (Art. 5, par. 1, lett. b) GDPR; WP29, Opinion 3/2013). Per ricerche scientifiche, storiche e statistiche o per archiviazioni nel pubblico interesse sarebbe consentito un ulteriore trattamento dei dati rispetto all'originaria e diversa finalità perseguita dal titolare del trattamento perché considerate ad essa compatibili da una regola generale del medesimo principio (Art. 5, par. 1, lett. b) GDPR). Il trattamento secondario ai fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile, quando il trattamento originario è lecito e tenendo conto del "contesto in cui i dati personali sono stati raccolti", delle "ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo", "della natura dei dati personali", "delle conseguenze dell'ulteriore trattamento previsto per gli interessati", e "dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto (Cons. 50 GDPR).

La deroga al principio di limitazione della finalità per i trattamenti secondari di ricerca e archiviazione semplifica chiaramente le regole per gli scopi di ricerca e permette il riuso di dati personali che siano già stati legittimamente raccolti per altre finalità. Tuttavia, l'*European Data Protection Supervisor* (EDPS), nella sua opinione preliminare sulla protezione dei dati e ricerca scientifica del 2020, propende per un'interpretazione più restrittiva: non sarebbe possibile considerare di per sé compatibile il riuso dei dati per scopi di ricerca, ma si dovrebbe effettuare in ogni caso il test di compatibilità di cui all'Art. 6, par. 4, GDPR, in quanto non sarebbe possibile assimilare le condizioni di legittimità dell'ulteriore trattamento con la determinazione della prima finalità (EDPS, 2020)[1]. Tale presunzione di compatibilità dipenderebbe, pertanto, dalla valutazione di alcuni aspetti specifici, quali: 1) la natura dei dati personali, in particolare nel caso in cui siano trattate categorie particolari di dati (Art. 6, par. 4, c) GDPR); 2) il collegamento fra lo scopo originario e gli scopi secondari (Art. 6, par. 4, lett. a) GDPR); 3) le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo (Art. 6, par. 4, lett. d) GDPR); 4) le conseguenze che l'ulteriore trattamento possa produrre (Considerando 50); 5) il contesto nel quale i dati sono stati raccolti (art. 6, par. 4, b) GDPR) (Casonato e Tomasi, 2019). Evidentemente, tale test non è di immediata eseguibilità, ma richiede un'attenta analisi.

La seconda possibile deroga è al principio di limitazione della conservazione dei dati (Art. 5, par. 1, lett.

1 Opzione auspicabile, tra l'altro, soprattutto nel caso in cui le informazioni vengano utilizzate a fini di ricerca medica. Sul punto, è atteso un chiarimento da parte dell'EDPB nelle future linee guida sul trattamento dei dati relativi alla salute per finalità di ricerca scientifica (come annunciato in EDPB, Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak).

e) GDPR), che rappresenta uno dei punti più importanti e più rilevanti per chi fa ricerca scientifica. I dati trattati per le finalità di archiviazione e ricerca possono, così, essere conservati in una forma che consenta l'identificazione degli interessati anche oltre il periodo strettamente necessario per il conseguimento dello scopo per cui sono stati originariamente raccolti, previe misure tecniche e organizzative a loro protezione (EDPS, 2020). I dati, perciò, non dovranno essere necessariamente anonimizzati oltre tale periodo, potranno essere trattati con gli elementi identificativi se implementate adeguate garanzie.

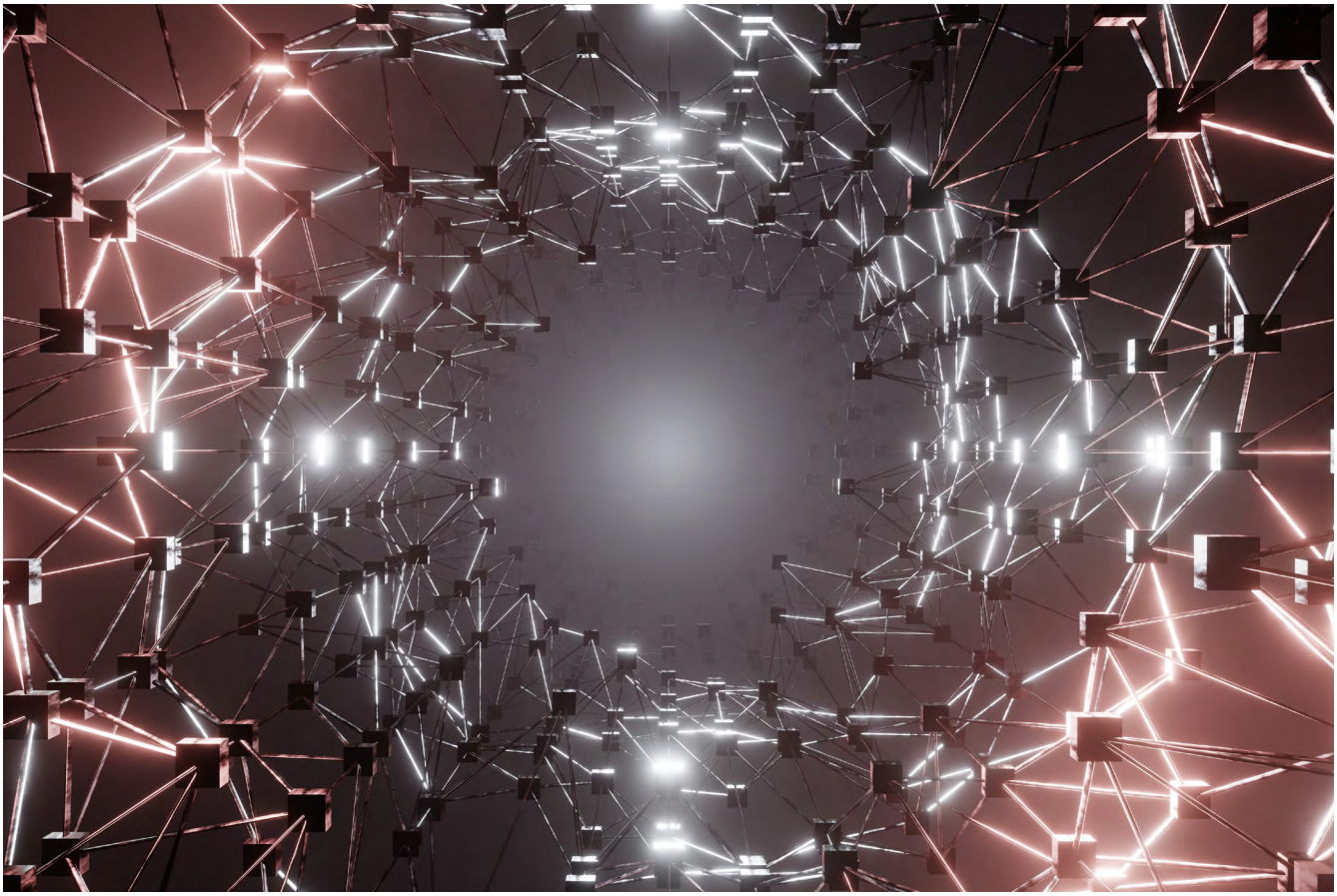
Con riferimento alle deroghe ai diritti degli interessati, un trattamento per finalità di ricerca o archiviazione nel pubblico interesse potrebbe parzialmente limitare gli obblighi informativi dell'Art. 14 GDPR. Come anticipato nelle definizioni, l'interessato ha diritto a ricevere una specifica, trasparente e accurata informativa sul trattamento dei suoi dati. Infatti, nel caso in cui la comunicazione delle informazioni richieste prevista dall'Art. 14, par. 1 e 2, risulti impossibile, o richieda uno sforzo sproporzionato, o rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di archiviazione, ricerca scientifica o statistica il titolare del trattamento può essere sollevato dall'obbligo di fornire le informazioni (Art. 14, par. 5, lett. b) GDPR). Occorre sottolineare che tale eccezione è stabilita esclusivamente per la lunga lista di informazioni dell'Art. 14, e quindi soltanto quando i dati non sono raccolti direttamente dall'interessato (come disciplinato invece dall'Art. 13). Se, in caso di dati raccolti presso l'interessato, il titolare scegliesse di non informare, o di farlo solo successivamente, perché una trasparenza sulle finalità del trattamento comprometterebbe il raggiungimento degli scopi che la ricerca si prefigge[2], si potrebbe rilevare che tale pratica risulterebbe controversa da un punto di vista etico e anche giuridico poiché l'interpretazione letterale dell'Art. 13 parrebbe non lasciare spazio a possibili eccezioni, come invece già stabilisce l'Art. 14 (EDPS, 2020).

2 Un caso pratico, ad esempio, è quello di una ricerca di carattere psicologico o sociologico volta a determinare il perché del comportamento degli individui o dei gruppi in determinate circostanze. Se ci fosse l'informazione, la validità della ricerca potrebbe essere viziata.

Il titolare del trattamento potrebbe, poi, limitare il diritto alla cancellazione dei dati qualora il suo esercizio da parte dell'interessato renda impossibile o possa pregiudicare gli obiettivi del trattamento a fini di archiviazione, ricerca o statistica (art. 17, par. 3, lett. d), GDPR). La cancellazione di tutti o parte dei dati utilizzati per uno studio, qualora tecnicamente possibile, potrebbe inficiare la validità scientifica e impedire la successiva riproducibilità dei dati a fini sperimentali. A questo proposito, è discusso se la limitazione alla cancellazione sia applicabile soltanto per gli studi già effettuati. La richiesta di cancellazione, invece, sembrerebbe perfettamente esercitabile nei confronti di eventuali dati conservati per un periodo ulteriore in attesa di riuso a fini di ricerca (art. 5, par. 1, lett. e) GDPR), in quanto l'esercizio del diritto alla cancellazione non dovrebbe pregiudicare il conseguimento degli obiettivi di una ricerca che non è ancora iniziata (Pormeister, 2017). Il diritto alla cancellazione, se applicato in modo rigido ed estremizzato, potrebbe presentare evidenti criticità nel caso di trattamenti effettuati per finalità di ricerca storica.

Circa il diritto di opposizione, esso può essere esercitato in generale dall'interessato contro il trattamento avente finalità di ricerca "per motivi connessi alla sua situazione particolare", tranne che nell'ipotesi in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico (Art. 21, par. 6, GDPR). Di fronte all'interesse superiore di rilevanza collettiva, le ragioni del singolo vengono, pertanto, limitate e il trattamento può proseguire senza alcuna limitazione.

In aggiunta a questi diritti, uno Stato membro potrebbe prevedere regole per la limitazione del diritto di accesso (Art. 15), diritto di rettifica (Art. 16), diritto di limitazione del trattamento (Art. 18) e diritto di opposizione (Art. 21), come previsto dall'Art. 89, par. 2 GDPR. Queste deroghe sono lasciate alla discrezionalità nel rispetto di tre condizioni, ovvero quando: 1) l'esercizio dei diritti in questione rischi di rendere impossibile o pregiudicare gravemente il conseguimento delle finalità specifiche del trattamento; 2) le deroghe siano necessarie al conseguimento di dette finalità; 3) siano adottate adeguate garanzie per i diritti e le libertà dell'interessato (Cons. 73 GDPR; Staunton *et al*., 2019).



Con riferimento alla base legittima per il trattamento, si possono presentare tre principali casistiche previste dall'Art 6 GDPR (dati personali non particolari). La prima base giuridica è il consenso dell'interessato, che viene confermato quale strumento per autorizzare il titolare a trattare informazioni di carattere personale (Art. 6, par. 1, lett. a) GDPR). Un comune fraintendimento, anticipato anche nelle definizioni, è quello che opera a livello pratico tra il consenso al trattamento dei dati personali, oggetto della presente analisi, e il consenso, invece, alla partecipazione al progetto che è di regola richiesto da principi di carattere etico. Sebbene da un punto di vista informativo alcuni elementi tendano a sovrapporsi, è opportuno ribadire che questi sono concettualmente, e giuridicamente, molto diversi (Quinn e Quinn, 2018; Dove, 2018; EDPB, Linee guida 5/2020). Il consenso privacy deve essere "inequivocabile" e "specifico" per l'operazione di trattamento che si intende realizzare; ciò potrebbe perciò rappresentare una sfida per l'attività di un progetto di ricerca, in quanto spesso non è agevole individuare correttamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati.

A questo proposito, e come anticipato nelle definizioni, qualora fosse necessario raccogliere il consenso per finalità di ricerca, ma il titolare non possa individuare pienamente la finalità del trattamento al momento della raccolta dei dati, egli potrà richiedere agli interessati di prestare il consenso a taluni settori della ricerca scientifica, dovendo però rispettare le norme deontologiche in materia di ricerca scientifica (Considerando 33 GDPR). Gli interessati potranno

prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca, essendo valido soltanto un consenso specifico. Sebbene, quindi, ci possa essere una certa flessibilità e granularità in ambito di consenso e ricerca scientifica, il consenso dell'interessato deve rimanere specifico. Non si potrà, quindi, praticare una sorta di "broad consent" in quanto il GDPR non può essere interpretato in modo tale da permettere a un titolare del trattamento di aggirare uno dei concetti chiave della disciplina relativo alla finalità specifica per la quale il consenso dell'interessato è richiesto. Pertanto, quando le finalità di ricerca non possono essere completamente specificate, il titolare dovrà cercare altri modi per garantire che l'essenza dei requisiti del consenso sia realizzata, individuando lo scopo della ricerca anche in termini generali, ma pur sempre circoscritti all'ambito scientifico-disciplinare interessato (EDPB, 2021; EDPB, Linee Guida 5/2020). Si ricorda, inoltre, che il consenso è sempre revocabile dall'interessato (Art. 7 GDPR).

La seconda casistica riguarda i progetti di ricerca che si possono fondare sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. c) ed e) GDPR). Si pensi alle ricerche compiute dalle università (ricerca base o applicata) e dai centri di ricerca.

La terza base giuridica, infine, è l'interesse legittimo del titolare del trattamento o di terzi, «a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore» (Art. 6, par. 1, lett. f) e Cons. 47 GDPR; WP29, Parere 6/2014). Questa possibilità è indirettamente prevista dal Considerando 47 e dal Considerando 113 che consente di tener conto delle "legittime aspettative della società nei confronti di un miglioramento delle conoscenze" in caso di finalità di ricerca scientifica o storica o a fini statistici. Dovrà, quindi, essere compiuto un test comparativo tra gli interessi del titolare, di terzi e degli interessati ("*three step test*"). Le autorità pubbliche nell'esecuzione dei loro compiti non possono fondare un trattamento sull'interesse legittimo e pertanto esso sarà una base soltanto per enti privati (art. 6, par. 1, lett. f) GDPR).

Se nel progetto di ricerca il titolare tratta dati particolari, è opportuno ricordare che il regime generale vieta di trattare queste categorie di dati, a meno che non sia applicabile una specifica eccezione elencata nell'Art. 9 GDPR. Se si dovesse richiedere il consenso, esso dovrà essere "esplicito" (Art. 9, par. 2, lett. a) GDPR). L'Art. 9, par. 2, lett. j) GDPR consente, inoltre, il trattamento qualora «necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato». Perciò, una legge nazionale o europea può autorizzare il trattamento di categorie particolari di dati per le finalità già descritte dell'Art. 89 qualora la previsione normativa sia proporzionata allo scopo perseguito e rispetti l'essenza del diritto alla protezione dei dati, ossia il principio dell'art. 8, par. 2 e 52 della Carta fondamentale dei diritti dell'Unione europea, e i principi dell'art. 5 del GDPR. Oltre alle misure adeguate già richiamate nell'analisi dell'Art. 89 per un progetto di ricerca con dati sensibili dovranno essere adottate misure "appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (Comandé e Malgieri, 2018).

Gli Stati membri possono adottare particolari previsioni in materia di trattamenti per finalità di ricerca o archiviazione. Nella prossima sezione verranno analizzate le regole italiane.

1.2.2. La disciplina in ambito italiano

Nel contesto italiano la disciplina di riferimento è inserita al Titolo VII, Artt. 97-110-*bis* del Codice Privacy, adeguato al GDPR dal D.Lgs. 10 agosto 2018, n. 101. La normativa è in larga parte conforme a quella previgente, con l'eccezione di alcune modifiche riguardanti l'adozione di regole deontologiche. Il Garante può, infatti, adottare regole deontologiche per specifici trattamenti, inclusi quelli per scopi di ricerca (Art. 2-*quater*).

In generale, l'Art. 2-*quinquies*, co. 2, lett. cc) del Codice Privacy inserisce all'interno dei trattamenti di dati particolari per motivi di interesse pubblico rilevante i trattamenti effettuati a fini di archiviazione o ricerca storica «concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato, negli archivi storici di enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante», e i trattamenti per fini di ricerca scientifica e a fini statistici da parte di soggetti del Sistan (Sistema statistico nazionale). Come anticipato, i dati genetici, biometrici e relativi alla salute non possono essere diffusi per espressa previsione legislativa (Art. 2-*septies*), nemmeno se in ambito di ricerca. L'Art. 99 del Codice recepisce poi la possibilità di derogare al principio di limitazione della conservazione per scopi di archiviazione e ricerca e prevede che tali trattamenti possano essere effettuati oltre il periodo di tempo prefissato per conseguire quelle finalità.

Per quanto concerne la disciplina in tema di ricerca storica in Italia, è poi necessario richiamare anche il Capo II del Codice Privacy agli Artt. 101-103, le Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del D.Lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 del Garante; e il D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio", con particolare attenzione al Titolo II, Capo III "Consultabilità dei documenti degli archivi e tutela della riservatezza", Artt. 122-127.

I trattamenti a fini statistici o di ricerca scientifica sono regolati dal Capo III, Artt. 104-109 del Codice Privacy. Queste norme richiedono che i trattamenti con questi fini non utilizzino i dati per prendere decisioni o provvedimenti sugli interessati e che siano rese le necessarie informazioni come richiesto dagli Artt. 13 e 14 GDPR (Art. 105 Codice Privacy). L'informativa non è dovuta soltanto quando richiederebbe uno sforzo sproporzionato rispetto al diritto dell'interessato a essere informato e vengano poste in essere forme di pubblicità idonee, come previsto dal Garante nelle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" (Regole deontologiche ricerca scientifica) e nelle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale", entrambe pubblicate ai sensi dell'art. 20, comma 4, del D.Lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018. Le prime Regole si applicano ai trattamenti effettuati da università enti o istituti di ricerca, società scientifiche e loro ricercatori per scopi statistici e scientifici, con l'esclusione di quelli connessi all'attività di tutela della salute svolte da esercenti delle professioni sanitarie o organismi sanitari e di quei trattamenti che hanno comparabile ricaduta personalizzata sugli interessati (Art. 1). Le seconde Regole deontologiche, invece, riguardano a) "enti e uffici di statistica che fanno parte o partecipano al Sistema statistico nazionale"; b) strutture diverse da questi uffici, ma «appartenenti alla medesima amministrazione o ente, qualora i relativi trattamenti siano previsti dal programma statistico nazionale e gli uffici di statistica attestino le metodologie adottate», osservando le disposizioni contenute nel D.lgs 6 settembre 1989, n. 322, nel GDPR, nel Codice Privacy nelle stesse regole deontologiche (Art. 1). In entrambi i casi il trattamento dei dati deve essere descritto nei progetti di ricerca.

Con specifico riferimento alla ricerca in ambito medico, biomedico ed epidemiologico rileva l'Art. 110 del Codice Privacy. Oltre a tale previsione rimangono applicabili alcune autorizzazioni generali al trattamento pubblicate dal Garante prima del GDPR nel 2016 (Provv. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016). In particolare l'Allegato 1, punto 5 del Provvedimento del 13 dicembre 2018 contiene le "Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016)" (Prescrizioni ricerca scientifica), le quali riguardano il trattamento effettuato da: a) università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e ai soci di dette società scientifiche; b) esercenti le professioni sanitarie e gli organismi sanitari; c) persone fisiche o giuridiche, enti, associazioni e organismi privati, nonché soggetti specificatamente preposti al trattamento quali designati o responsabili del trattamento (ricercatori, monitor, commissioni di esperti, organizzazioni

di ricerca a contratto, laboratori di analisi, ecc.) (Artt. 2-*quaterdecies* Codice Privacy e 28 GDPR) (punto 5.1). Tali prescrizioni concernono il trattamento di dati personali per finalità di ricerca medica, biomedica ed epidemiologica effettuati quando: il trattamento è necessario per la conduzione di studi effettuati con dati raccolti in precedenza a fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca ovvero ricavati da campioni biologici prelevati in precedenza per finalità di tutela della salute o per l'esecuzione di precedenti progetti di ricerca; oppure quando il trattamento è necessario per la conduzione di studi effettuati con dati riferiti a persone che, in ragione della gravità del loro stato clinico, non sono in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso (5.2). Il punto 4 dell'Allegato 1 del suddetto Provvedimento prevede, invece, le "Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016)".

Nelle Prescrizioni ricerca scientifica si prevede che la ricerca medica, biomedica ed epidemiologica deve essere svolta «nel rispetto degli orientamenti e delle disposizioni internazionali e comunitarie in materia, quali la Convenzione sui diritti dell'uomo e sulla biomedicina del 4 aprile 1997, ratificata con legge 28 marzo 2001, n. 145, la Raccomandazione del Consiglio d'Europa R(97)5 adottata il 13 febbraio 1997 relativa alla protezione dei dati sanitari e la dichiarazione di Helsinki dell'Associazione medica mondiale sui princìpi per la ricerca che coinvolge soggetti umani» (Art. 8).

Con riferimento ai requisiti di legittimità del trattamento, sia le Prescrizioni ricerca scientifica, sia le Regole deontologiche ricerca scientifica richiamano il consenso degli interessati come base giuridica del trattamento. L'art. 110 del Codice Privacy, quindi, sul presupposto che tale consenso sia richiesto per condurre una ricerca scientifica in campo medico, biomedico ed epidemiologico, disciplina al primo comma i casi in cui questo non risulta, invece, necessario. Il primo tra questi riguarda la fattispecie relativa al trattamento effettuato in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea. La previsione normativa richiama come base legittima direttamente l'Art. 9, par. 2, lett. j) GDPR e menziona espressamente, come esempio paradigmatico, la ricerca rientrante in un programma previsto ai sensi dell'Art. 12-bis D.Lgs. 502/1992 ("Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421"). Una ricerca rientrante in questo ambito potrà essere condotta senza il consenso degli interessati, a condizione che sia realizzata e resa pubblica una DPIA. Il secondo caso di esenzione del consenso è previsto dalla seconda parte del primo comma dell'art. 110 e ricorre qualora «a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca». In queste ipotesi, il punto 5.3 delle Prescrizioni ricerca scientifica stabilisce che il titolare del trattamento debba documentare nel progetto di ricerca la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. Queste ragioni rimandano principalmente a tre tipologie:

- motivi di carattere etico, riconducibili alla circostanza che l'interessato ignori la propria condizione: l'informativa sul trattamento dei dati da rendere agli interessati potrebbe comportare la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi[3];
- motivi di impossibilità organizzativa, riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati. A tal proposito, occorre considerare in particolare, i criteri di inclusione previsti dallo studio, le modalità di arruolamento, la nume-

3 Si pensi, ad esempio, agli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento curativo.

rosità statistica del campione prescelto, nonché il periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti[4]; infine, in tale contesto occorre ricomprendere anche il trattamento dei dati di coloro i quali – a fronte di ogni ragionevole sforzo compiuto per contattarli, anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente – risultino essere, al momento dell'arruolamento nello studio, deceduti o non contattabili;

- motivi di salute, riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso. Occorrerà allora che lo studio sia volto al miglioramento dello stesso stato clinico in cui versa l'interessato e che sia comprovato che la sua finalità non possa essere conseguita mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di ricerca.

Nelle ipotesi della seconda parte del primo comma dell'Art. 110 Codice Privacy il titolare del trattamento è obbligato ad adottare le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, dovrà redigere un programma di ricerca oggetto di motivato parere favorevole da parte del competente comitato etico a livello territoriale e dovrà compiere una DPIA, la quale dovrà essere necessariamente sottoposta in consultazione preventiva al Garante ai sensi dell'Art. 36 GDPR.

In tutte le ipotesi appena richiamate del primo comma dell'Art. 110 del Codice Privacy i diritti degli interessati a rettificare i dati personali senza ingiustificato ritardo possono essere limitati dal titolare. Infatti, il secondo comma di questa previsione stabilisce che nel caso in cui l'interessato al trattamento intenda esercitare i diritti di cui all'art. 16 GDPR, l'aggiornamento, la rettificazione e l'integrazione dei dati avvenga senza la modifica dei dati stessi ma con una semplice annotazione, sempre che il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca. Le Regole deontologiche ricerca riprendono questa previsione consentendo, qualora siano necessarie modifiche ai dati che riguardano l'interessato in caso di esercizio dei diritti dell'interessato cui agli Art. 15 e ss. del GDPR, al titolare del trattamento di annotare, in appositi spazi o registri, le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio (Art. 12).

A chiusura del Titolo VII del Codice Privacy è stato inserito un articolo dedicato al trattamento ulteriore (secondario) di dati personali da parte di terzi per finalità di ricerca scientifica o a fini statistici, che si inserisce nella previsione dell'Art. 89 GDPR. Questa tipologia di trattamento può essere direttamente autorizzata dal Garante, anche in caso di utilizzo di dati particolari, per soggetti terzi che svolgono "principalmente" tali attività di ricerca[5] quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 GDPR, incluse forme preventive di minimizzazione e di anonimizzazione dei dati (Art. 110-*bis*, co. 1, Codice Privacy). Questa autorizzazione può essere rilasciata su richiesta entro quarantacinque giorni, decorsi i quali la mancata pronuncia del Garante equivale a un rigetto; con tale autorizzazione o anche successivamente, se compiute ulteriori verifiche, l'autorità stabilirà le condizioni e le misure, anche di sicurezza, che sono necessarie ad assicurare adeguate garanzie (Art. 110-*bis*, co. 2, Codice Privacy). Il Garante, peraltro, può autorizzare queste tipologie di trattamenti anche

4 Si pensi, ad esempio, i casi in cui lo studio riguardi interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute.

5 Una lettura sistematica delle norme consiglierebbe di individuare i destinatari dell'articolo tra quelli indicati nell'Allegato 5 al Codice privacy Regole deontologiche ricerca.

mediante provvedimenti generali adottati d'ufficio e pubblicati in Gazzetta Ufficiale. Tali autorizzazioni generali potranno riferirsi a determinate categorie di titolari e di trattamenti, stabilire le condizioni del trattamento secondario e prescrivere le misure necessarie per assicurare adeguate garanzie a tutela degli interessati (Art. 110-*bis*, co. 3, Codice Privacy). Dalla previsione dell'Art. 110-*bis* devono ritenersi esclusi i trattamenti per l'attività clinica a fini di ricerca, effettuati da istituti di ricovero e cura a carattere scientifico, pubblici e privati, dal momento che la loro attività è strumentale all'assistenza sanitaria (Art. 110-*bis*, co. 4, Codice Privacy).

Qualunque progetto di riutilizzo dei dati per finalità di ricerca per essere sottoposto al vaglio del Garante dovrà perciò dimostrare preventivamente di aver predisposto tutte le misure adeguate a protezione dei dati. L'adozione di questi idonei accorgimenti dovrà, inoltre, essere comprovata e documentata. Tutto ciò in piena conformità al principio della responsabilizzazione, come sancito dagli articoli 5, par. 2, e 24, par. 1, GDPR).

La disciplina a protezione dei dati personali richiede l'adozione di varie misure a protezione dei dati. Durante l'elaborazione e l'esecuzione di un progetto di ricerca ogni attività dovrà essere considerata distintamente per la definizione delle misure di *accountability* (Art. 24 GDPR), di *data protection by design* e *by default* (Art. 25 GDPR), per la predisposizione del registro delle attività di trattamento (Art. 30 GDPR), per l'implementazione delle misure di sicurezza del trattamento (Art. 32 GDPR), e per la redazione della valutazione di impatto sulla protezione di dati - DPIA (Art. 35 GDPR). Come verrà approfondito nella prossima sessione, il nuovo paradigma di *data protection by design* impone di occuparsi dell'adozione di misure tecniche e organizzative adeguate rispetto all'intera architettura di ricerca: questo approccio non è mai standardizzato, richiedendo un'analisi dinamica, caso per caso, della strategia da adottare.

1.3. L'approccio di Data Protection by design

Affinché un progetto di ricerca possa fin dalla sua elaborazione considerare le regole in materia di protezione dei dati personali, evitando successive violazioni e affrontando i rischi per gli interessati fin dalla loro origine, è necessario adottare l'approccio di *data protection by design*. Questa sezione illustra tale approccio alla luce dell'Art. 25 del GDPR, che è inserito negli obblighi generali in materia di protezione dei dati, ed è sanzionabile, se non rispettato, ai sensi degli articoli 82 e 83 del GDPR.

La *privacy by design* nasce come concetto dottrinale canadese (Cavoukian, 2010) e si è affermata a livello internazionale fino alla sua codificazione, appunto, nel diritto europeo come *data protection by design* e *by default* - protezione dei dati fin dalla progettazione e per impostazione predefinita (Bincoletto, 2019). Il concetto di *privacy by design* richiede un ripensamento globale del modo di trattare i dati personali: da un approccio statico a un approccio proattivo e dinamico che implementa fin dal *design* della tecnologia e delle pratiche organizzative e commerciali sia misure tecniche che organizzative protettive dei dati; il principio richiede, infatti, l'incorporazione delle regole e dei valori della *privacy* fin dalla progettazione dei prodotti e dei servizi (Bincoletto, 2021). Da ciò deriverebbe una maggiore sicurezza dei dati personali e un miglior sviluppo delle soluzioni tecniche che terrebbero conto fin dalla loro origine delle regole giuridiche applicabili in un dato ordinamento (Bincoletto, 2020). La *privacy by design* è da intendersi come un approccio che pone l'utente e i dati personali al centro del sistema, e che consente concrete scelte di bilanciamento dei vari interessi in gioco. Quando si utilizza l'espressione *privacy by design* si fa riferimento a questo concetto che include anche una dimensione etica (EDPB, Guidelines 4/2019). L'espressione *data protection by design*, invece, è riferibile a un obbligo generale del GDPR che richiede sempre misure tecniche e organizzative, ma considerando alcuni criteri e specifici principi del GDPR.

L'Art. 25, par. 1, del GDPR (*data protection by design* - DPbD) stabilisce che considerando la natura, l'ambito, il contesto e le finalità del trattamento dei dati, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché dei diversi livelli di rischio per i diritti e le libertà delle persone posti dal trattamento, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate ed essere in grado di dimostrare che i dati personali siano trattati ai sensi del regolamento per tutta la durata delle operazioni. La *data protection by design* impone, perciò, di

recepire i principi e le regole in materia di protezione dei dati personali a partire dalla progettazione del trattamento, sia a livello di pratiche e processi, che, e soprattutto, a livello di soluzioni informatiche. La DPbD deve essere adottata sia *ex ante*, sia a trattamento pendente, fino alla sua conclusione (in caso di cancellazione dei dati o di effettiva anonimizzazione).

Il titolare del trattamento deve adottare politiche interne e attuare misure tecniche che soddisfano tutti i principi di protezione dei dati: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati, esattezza; limitazione alla conservazione; integrità e riservatezza; *accountability* o responsabilizzazione (Art. 5 GDPR). Ad esempio, il titolare dovrebbe ridurre al minimo il trattamento dei dati personali, pseudonimizzando i dati personali il prima possibile e offrendo effettiva trasparenza per quanto riguarda le funzioni delle operazioni di trattamento a livello di informativa. La tutela del dato, così, diventa parte integrante del suo trattamento. Nelle *Guidelines on Article 25 Data Protection by Design and by Default* l'EDPB fornisce esempi di implementazione per ciascun principio (EDPB, Guidelines 4/2019).

Per quanto riguarda l'attuazione concreta della DPbD, non è pensabile definire una soluzione di *data protection by design* applicabile a qualsiasi progetto di ricerca. In altri termini, quando ci si riferisce alla DPbD una ricetta "*one-size-fits-all*" non sarà conforme alla normativa (Bincoletto, 2021). Tuttavia, grazie all'approfondimento svolto, saranno qui fornite alcune coordinate generali, e poi, altre raccomandazioni schematiche e buone prassi nella Sezione 5, che possano fornire indicazioni volte al lato applicativo delle soluzioni in ottica di *data protection by design* e *by default*.

Ebbene, si può segnalare in via generale quanto segue. In primo luogo, il titolare dovrà valutare le regole applicabili al trattamento dei dati che intende compiere. È necessario raccogliere il quadro completo dei requisiti legali e delle linee guida delle autorità rilevanti per lo sviluppo dello specifico progetto con la particolare finalità di ricerca (es. scientifica o storica).

Successivamente, il titolare del trattamento deve mappare tutte le attività e le operazioni che intende porre in atto, tutte le concrete caratteristiche del prossimo trattamento (con attenzione sulla tipologia di dati e alle finalità) e il completo flusso dei dati personali a seconda del loro stato a livello tecnico (*data at rest*, *data in use, data in transit*) in quanto le misure andranno applicate a tutto e durante tutto il *data management lifecycle*.

Una volta mappato il trattamento da un punto di vista dei dati, è fondamentale definire i vari ruoli privacy (es. titolari e co-titolari, responsabili, incaricati, DPO, ecc.). Il Considerando 78 del GDPR incoraggia i produttori dei beni e servizi, che molto frequentemente non coincidono con il titolare del trattamento, a tenere conto dell'approccio di *data protection by design*; tuttavia, solo il titolare del trattamento è tenuto ad adottare la DPbD. I ricercatori che si appoggiano a soggetti esterni come fornitori di servizi e prodotti per la loro ricerca dovranno verificare che questi responsabili del trattamento adeguino le operazioni e proteggano fin dalla loro progettazione i dati trattati. Anche se non direttamente coinvolti dall'Art. 25 GDPR, i responsabili, infatti, dovrebbero garantire di adottare misure tecniche e organizzative adeguate affinché il trattamento sia conforme alla normativa (Art. 28, par. 1, GDPR). Queste garanzie potrebbero essere inserite nel contratto che delega le operazioni di trattamento. Il DPO potrà assumere un ruolo fondamentale per definire le misure di DPbD, se coinvolto fin dal principio della progettazione del trattamento.

Per scegliere le misure che implementino i principi del trattamento dei dati il titolare dovrà tenere conto di criteri oggettivi e soggettivi. Innanzitutto, le misure possono essere sia tecniche che organizzative e sono una sottocategoria di quelle che devono essere adottate dal titolare per conformità al GDPR (oltre, quindi, alle misure richieste per l'*accountability* dell'Art. 24, alle misure per limitare la conservazione dei dati, alle misure di sicurezza dell'Art. 32 GDPR e alle misure per il trasferimento transfrontaliero dei dati). Con il termine "misura" si intende qualsiasi metodo o mezzo per proteggere i dati durante il trattamento, che sia appropriato, effettivo e specifico. Sulle misure si consiglia la consultazione delle circolari dell'Agenzia per l'Italia digitale – AGID (www.agid.gov.it) e delle linee

guida dell'European Union Agency for Cybersecurity (www.enisa.europa.eu). In ambito organizzativo, è opportuno sottolineare l'importanza della formazione dei soggetti che in concreto trattano i dati personali all'interno dell'organizzazione del titolare. La formazione continua in materia di protezione dei dati personali può essere considerata una misura di sicurezza del trattamento (Art. 32 GDPR). Una maggiore sensibilità relativa alla sicurezza e ai principi privacy dei ricercatori coinvolti in un progetto di ricerca e dello staff amministrativo che lo supporta potrà contribuire alla prevenzione di eventuali violazioni dei dati.

Il criterio dello stato dell'arte richiede di prendere in considerazione ciò che è attualmente disponibile sul mercato per le misure tecniche e organizzative al fine di raggiungere più efficacemente possibile l'attuazione dei principi. Codici di condotta, certificazioni e standard possono fornire elementi dello stato dell'arte in un particolare contesto tecnico o procedurale. La valutazione dello stato dell'arte dovrebbe essere aggiornata durante lo svolgimento del trattamento dei dati.

Il criterio dei costi, invece, consente di tener conto di spese e oneri nello scegliere misure il cui costo è proporzionato alle risorse di cui il titolare dispone in concreto ("*economic feasibility*"). Nei costi possono essere considerati sia spese monetarie che risorse umane. L'inabilità di sostenere costi per la privacy non evita eventuali responsabilità in caso di violazioni, perchè le misure sono sempre proporzionate alla sostenibilità delle operazioni, a condizione che vengano fornite le adeguate garanzie per la protezione dei dati.

Considerare la natura, l'ambito di applicazione, il contesto e le finalità del trattamento significa tenere conto delle caratteristiche intrinseche del concreto trattamento, tra cui la tipologia dei dati, la quantità degli stessi, le categorie degli interessati (es. minori), la dimensione dell'organizzazione del titolare, gli elementi delle operazioni (es. mezzi automatici, utilizzo di IA), dove si svolgono queste operazioni, le circostanze che possano influire sulle aspettative degli interessati, e gli scopi di ciascuna operazione sui dati personali.

Le attività sui dati sono rischiose di per sé e il rischio (basso, medio, alto) non può essere del tutto azzerato. Pertanto, prima di scegliere le misure di DPbD è necessario valutare i rischi di queste attività, misurandoli in termini di possibilità/probabilità che un evento dannoso si verifichi (es. accesso illegittimo al dato) e impatto che tale evento potrebbe avere sulla sfera dell'interessato (significativo in caso di dati particolari). Un progetto di ricerca che tratta dati particolari è considerato ad alto grado di rischio da parte delle autorità, anche se i dati sono pseudonimizzati, da cui la necessità di adottare misure maggiormente protettive di DPbD e anche di compiere una preliminare DPIA (EDPB, 2017). Le misure prescelte e implementate dovranno essere proporzionate ai rischi individuati.

La DPbD richiedebbe, quindi, un *design project* del trattamento dei dati e un aggiornamento delle misure implementate durante il trattamento. L'attività di documentazione relativa alla DPbD è opportuna in ottica di *accountability*. Standard, codici di condotta e certificazioni, quest'ultime richiamate direttamente nel par. 3 dell'Art. 25 GDPR, sono riconosciuti come validi strumenti a supporto di tale approccio. Il GDPR prevede delle regole in materia di certificazione (Artt. 42 e 43). In Italia la certificazione può essere rilasciata tramite un percorso di riconoscimento compiuto da Accredia, Ente Italiano di Accreditamento (www.accredia.it).

L'approccio di *data protection by design* deve essere adottato assieme all'altro principio generale di *data protection by default*, che richiede l'adozione di misure tecniche e organizzative adeguate a garantire che solo i dati personali necessari per ogni specifica finalità del trattamento vengano elaborati (Art. 25, par. 2, GDPR). Questo obbligo impone l'adozione di misure tecniche che impediscano che il trattamento avvenga per finalità diverse da quelle previste e che prevengano un accesso illimitato ed eccessivo ai dati personali, minimizzandolo il più possibile (Bincoletto, 2021). I c.d. *default settings* delle soluzioni devono essere impostati in modo predefinito per limitare il numero, la tipologia e la granularità di dati raccolti, le attività compiute su tali dati, incluse il tempo di conservazione e l'accessibilità, che devono essere confinate alle finalità. Un progetto di ricerca dovrà, quindi, preliminarmente valutare la mole di dati, le categorie e la specificità richiesta per perseguire la finalità scientifica, ma non oltre il necessario.

Le esigenze di protezione dei dati personali, volte innanzitutto a limitarne, se non a impedirne l'accessibilità, possono tuttavia contrastare con principi e obblighi previsti in materia di *open government data*. La prossima sezione affronterà la questione, anche alla luce dei recenti sviluppi legislativi.

2. OPEN GOVERNMENT DATA E BANCHE DATI APERTE

Fin dagli inizi degli anni 2000, il movimento c.d. *Open Data* (OD) aspira a ridurre le barriere che ostacolano l'accesso alle informazioni (Guarda, 2021). Queste barriere – che possono essere di natura economica, tecnologica e giuridica – impediscono un accesso democratico, inclusivo e trasparente alla conoscenza generata dalla ricerca. La libera condivisione e il gratuito riuso dovrebbero coinvolgere sia le pubblicazioni sia i dati generati dalla ricerca. L'apertura può riguardare sia i dati generati come risultati della ricerca che quelli già conservati in database gestiti da soggetti pubblici o privati[1].

I principi che ispirano l'apertura dei dati in accesso aperto propongono la libera condivisione dei risultati della ricerca attraverso licenze aperte, quali, ad esempio,

1 Con riferimento alle pubblicazioni si rileva che la Fondazione adotta un approccio di "accesso aperto" nei criteri generali di concessione dei contributi. Si v. ad esempio i criteri del 2020 in Rete: www.fondazionecariplo.it.

le licenze Creative Commons (si veda il sito dell'organizzazione: creativecommons.org). In particolare, nel caso di progetti di ricerca finanziati dal programma europeo Horizon 2020 e, ora, Horizon Europe, l'OD è diventato un requisito obbligatorio: la gestione con approccio aperto dei dati deve essere pianificata sin dal principio e gestita attraverso un dettagliato Data Management Plan (si vedano le istruzioni sul sito ufficiale del programma: ec.europa.eu/research). Per quanto concerne invece l'apertura di banche dati già costituite, diversità di obblighi e strategie può sussistere a seconda della natura privata o pubblica del soggetto gestore.

Nel primo caso, consentire il libero accesso ai dati, ed eventualmente con quali modalità, rappresenta una scelta di opportunità del tutto libera. Il soggetto privato potrebbe, infatti, sposare tale approccio alla valorizzazione del proprio dataset convinto degli effetti (di rete) positivi che una condivisione di dati e informazioni apporta all'intera comunità in termini di spinta all'innovazione e alla ricerca. Potrebbe, poi, darsi il caso che la creazione della banca dati stessa sia avvenuta a seguito di un finanziamento (magari di carattere pubblico) che vincolava le scelte di valorizzazione, portando di fatto all'apertura. Non è, pertanto, possibile prevedere in questa sede le possibili modalità e le eventuali limitazioni che potranno essere imposte dai privati all'accesso ai dati. Tali questioni riguardano anche la presenza di diritti di proprietà intellettuale che possono condizionare lo scenario applicativo (come il diritto d'autore, il diritto *sui generis* sulla banca dati, la presenza di segreti commerciali, ecc.).

Nel caso dei soggetti pubblici entra invece in gioco la disciplina in materia di *Open Government Data* (OGD), la quale rappresenta una sfida volta a rendere i dati delle pubbliche amministrazioni disponibili ai cittadini in ottica di trasparenza e di promozione dell'uso e del riuso anche per la creazione di nuove imprese e servizi innovativi (Faini, 2019). La normativa che promuove tale approccio è di derivazione sia europea che nazionale.

2.1. Framework normativo europeo e italiano per gli Open Government Data

A livello europeo, con particolare riferimento ai dati relativi alla ricerca, la Commissione Europea nella Dichiarazione sull'Open Science Cloud europeo del 2017 e nel suo *Implementation Plan* del 2019 ha sottolineato che questi dati dovrebbero essere aperti per impostazione predefinita e chiusi soltanto quanto necessario. Risulta, infatti, necessario bilanciare l'apertura con la protezione dell'informazione scientifica, la commercializzazione e i diritti di proprietà intellettuale, le questioni di privacy, di protezione dei dati personali e sicurezza, seguendo il generale principio "*open by default – closed where necessary*".

Nel 2019 l'Unione Europea ha emanato la Direttiva 2019/1024 sui dati aperti e il riutilizzo delle informazioni del settore pubblico, nota anche come "Direttiva Open Data", che ha sostituito la precedente regolazione di settore per fornire un quadro giuridico comune al mercato europeo dei dati posseduti dalle pubbliche amministrazioni. La recente disciplina è costruita attorno a due pilastri fondamentali del mercato interno, ossia la trasparenza e la concorrenza leale. Ricade nell'applicazione della direttiva il materiale conservato e gestito dagli enti del settore pubblico a livello nazionale, regionale e locale, come ministeri, agenzie statali e comuni, nonché organizzazioni finanziate principalmente da o sotto il controllo di autorità pubbliche. Questa normativa europea è volta a:

- stimolare la pubblicazione di dati dinamici e all'adozione di API (*Application Program Interface*);
- limitare le eccezioni che attualmente consentono agli enti pubblici di addebitare agli utenti importi superiori ai costi marginali di diffusione per il riutilizzo dei propri dati;
- rafforzare i requisiti di trasparenza per gli accordi pubblico-privato che coinvolgono l'informazione del settore pubblico, evitando accordi di esclusiva.

A questi fini sono state introdotte alcune importanti novità che implicano un significativo impatto anche sulle norme relative ad altri settori, come la tutela della proprietà intellettuale e, soprattutto, la protezione dei dati personali.

Innanzitutto, la Direttiva Open Data stabilisce una serie di norme minime in materia di riutilizzo e modalità pratiche (Art. 1, par. 1) per agevolare il riutilizzo dei:

- documenti esistenti in possesso degli enti pubblici degli Stati membri;
- documenti esistenti in possesso delle imprese pubbliche;
- dati della ricerca (Art. 10);
- dati di elevato valore (Art. 14).

A differenza delle precedenti previsioni, i dati degli istituti di ricerca rientrano quindi nell'ambito applicativo dell'OD (Art. 1, par. 1, lett. c) Direttiva OD), così come i dati detenuti da imprese pubbliche e i dati di ricerca derivanti da finanziamenti pubblici. Secondo questa direttiva i dati della ricerca sono i «documenti in formato digitale, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca» (Art. 3, n. 9, Direttiva OD). Sono, invece, esclusi dalle previsioni della Direttiva OD i (Art. 1, par. 2):

- documenti «la cui fornitura è un'attività che esula dall'ambito dei compiti di servizio pubblico degli enti pubblici», come definiti da norme vincolanti o prassi amministrative;
- documenti in possesso di imprese pubbliche, in presenza di alcune condizioni;
- documenti su cui terzi detengono diritti di proprietà intellettuale;
- documenti, come quelli contenenti dati sensibili, che sono esclusi dall'accesso a livello nazionale per vari motivi, compresi la tutela della sicurezza dello stato, la difesa o sicurezza pubblica, la riservatezza statistica, la riservatezza commerciale, la protezione delle informazioni sensibili relative alle infrastrutture critiche (Direttiva 2008/114/CE), in virtù dei regimi di accesso vigenti sempre a livello nazionale;
- logotipi, stemmi e distintivi;
- documenti «il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali», e «parti di documenti accessibili in virtù di tali regimi che contengano dati personali il cui riutilizzo è stato definito per legge incompatibile con la normativa» in materia di privacy e protezione dei dati personali o pregiudizievole per questi diritti;
- documenti in possesso di emittenti di servizio pubblico e loro società controllate (per l'adempimento di un compito di radiodiffusione di servizio pubblico), di enti culturali diversi dalle biblioteche (comprese biblioteche universitarie, musei e archivi), di istituti di istruzione secondaria e inferiore (con alcune condizioni per tutti gli altri istituti), di organizzazioni che svolgono attività di ricerca e di organizzazioni che finanziano la ricerca, comprese le organizzazioni preposte al trasferimento dei risultati della ricerca (quando sono diversi da quelli coperti da diritti di proprietà intellettuale).

La Direttiva OD ha previsto i due principi di "*openness by design*" e "*openness by default*". In base a questi, e in (apparente) antitesi rispetto ai principi di protezione stabiliti dal GDPR, la normativa impone agli Stati membri di favorire la messa a disposizione, ove possibile per via elettronica, di dati in formato aperto per agevolare il loro libero utilizzo, il riutilizzo e la condivisione da parte di chiunque e per qualunque finalità dei dati (Art. 5 e Considerando 16).

Con riferimento alle condizioni e alle modalità del riutilizzo, un soggetto interessato può richiedere all'ente pubblico di riutilizzare particolari documenti e dati; l'ente risponderà entro un termine (20 giorni prorogabili), motivando eventuali risposte negative o concedendo l'accesso, ove possibile in forma elettronica (Art. 4, Direttiva OD). I contenuti relativi ai soggetti pubblici devono essere resi disponibili gratuitamente, salva la possibilità di recuperare i costi marginali sostenuti per la produzione, messa a disposizione e la divulgazione dei documenti, nonché per l'anonimizzazione dei dati personali e la protezione di informazioni commerciali (Art. 6, Direttiva OD)[2]. Soltanto in casi eccezionali gli enti e le imprese pubbliche potranno imporre tariffe superiori ai costi marginali per il riutilizzo dei loro dati, dovendo al contempo stabilire le somme nel rispetto di criteri oggettivi, trasparenti

2 Ai sensi dell'art. 6, par. 2, lett. b), ciò non si applica a "biblioteche, comprese le biblioteche universitarie, musei e archivi".

e verificabili[3]. Il riutilizzo dei dati può avvenire sulla base di licenze standard (Art. 8, Direttiva OD) e non può essere soggetto a condizioni, salvo che queste siano proporzionate, non discriminatorie e comunque giustificate in virtù di scopi di interesse pubblico. La possibilità di riutilizzare i dati non comporta, invece, alcun diritto di esclusiva a favore dell'utilizzatore (Art. 12, Direttiva OD).

Inoltre, la direttiva richiede l'adozione da parte della Commissione Europea di un elenco di dataset da fornire gratuitamente, da identificarsi all'interno di una gamma tematica descritta in un apposito allegato, i quali presentano un elevato potenziale commerciale e possono accelerare l'emergere di prodotti informativi a valore aggiunto in ambito europeo; con ciò si introduce, difatti, il concetto di "dataset di alto valore", definito come insieme di documenti il cui riutilizzo è associato a importanti benefici per la società e l'economia (Art. 2, par. 10, e Artt. 13-14, Direttiva OD).

Per quanto riguarda la disciplina dei dati della ricerca, la direttiva stabilisce che gli Stati membri dovranno promuovere la loro disponibilità se derivanti da ricerca finanziata con fondi pubblici e con politiche di accesso aperto, seguendo il principio di apertura per impostazione predefinita e in modo compatibile con i principi FAIR, ovvero rendendo i dati della ricerca reperibili, accessibili, interoperabili e riutilizzabili (Art. 10, Direttiva OD). Il riferimento che ciò che viene finanziato con il denaro dei contribuenti dovrebbe "appartenere" a tutti o "rientrare" nella disponibilità della comunità è la vera logica comune che caratterizza le iniziative di *open access* e quelle relative al settore delle informazioni pubbliche.

La Direttiva Open Data è stata recepita nell'ordinamento italiano con il D.Lgs. 8 novembre 2021, n. 200, entrato in vigore il 15 dicembre 2021. Questo atto ha modificato il D.Lgs. 24 gennaio 2006, n. 36, che, recependo la previgente Direttiva 2003/98/CE (Direttiva PSI, come poi modificata dalla Direttiva 2013/37/UE e abrogata dalla recente direttiva), aveva avviato un importante processo di promozione del riutilizzo dei dati della Pubblica Amministrazione (PA), in linea con le politiche legislative dell'UE relative alla trasparenza, cooperazione e unione del mercato digitale europeo, nel quadro della Digital Single Market Strategy.

Il D.Lgs. 36/2006, come modificato dal decreto di recepimento italiano, è da ritenersi la disciplina attualmente di riferimento volta a regolare le modalità di riutilizzo dei documenti contenenti *Open Data* nella disponibilità delle pubbliche amministrazioni e degli organismi di diritto pubblico. Dato pubblico è il dato "conoscibile da chiunque" (Art. 1, co. 1, lett. d) D.Lgs. 36/2006). Il decreto prevede alcuni punti principali che possono essere brevemente riassunti. Il riutilizzo dei dati può essere effettuato a fini commerciali e non. I soggetti destinatari degli obblighi in materia di OGD sono, oltre alle PA e gli organismi di diritto pubblico, anche le imprese pubbliche attive nei settori come gas, energia e le imprese private di trasporto che sono soggette a obblighi di servizio pubblico (Art. 1, co. 2, lettera d) D.Lgs. 36/2006). Il concetto di riutilizzo, ossia l'uso da parte di persone fisiche o giuridiche dei documenti detenuti dalle PA e dalle imprese sopra menzionate, non comprende lo scambio di documenti tra diverse PA (Art. 1, co. 3 D.Lgs. 36/2006).

Nel medesimo decreto trovano nuova definizione concetti quali:

- anonimizzazione, ossia «la procedura mirante a rendere anonimi documenti, rendendoli non riconducibili a una persona fisica identificata o identificabile, ovvero la procedura mirante a rendere anonimi dati personali in modo da impedire o da non consentire più l'identificazione dell'interessato» (Art. 2, co. 1, lett. c-*quinquies*), D.Lgs. 36/2006);
- dati dinamici, i «documenti informatici, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilità o rapida obsolescenza» (Art. 2, co. 1, lett. c-*sexies*), D.Lgs. 36/2006);
- dati della ricerca, i «documenti informatici, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come

3 A titolo di esempio, gli enti pubblici potranno imporre un costo maggiore se devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico.

necessari per convalidare le conclusioni e i risultati della ricerca» (Art. 2, co. 1, lett. c-*septies*), D.Lgs. 36/2006);

- serie di dati di elevato valore, i «documenti il cui riutilizzo è associato a importanti benefici per la società, l'ambiente e l'economia, in considerazione della loro idoneità per la creazione di servizi, applicazioni a valore aggiunto e nuovi posti di lavoro, nonché del numero dei potenziali beneficiari dei servizi e delle applicazioni a valore aggiunto basati su tali serie di dati» (Art. 2, co. 1, lett. c-*octies*), D.Lgs. 36/2006);
- interfaccia tra programmi applicativi API, ossia «insieme di funzioni, procedure, operazioni disponibili al programmatore, di solito raggruppate a formare un insieme di strumenti specifici per l'espletamento di un determinato compito» (Art. 2, co. 1, lett. i-*bis*), D.Lgs. 36/2006).

Come previsto dalla Direttiva OD, la normativa sul riutilizzo esclude alcune tipologie di documenti detenuti dai soggetti pubblici, compresi i documenti il cui accesso è escluso in forza della disciplina a protezione della privacy e della protezione dei dati personali, o che potrebbe pregiudicare tali diritti (Art. 3, co. h-*quater*, D.Lgs. 36/2006). Nelle clausole di salvaguardia, è fatto salvo il Codice Privacy, ma anche la disciplina sul diritto d'autore (L. 633/1941 e trattati internazionali sulla proprietà intellettuale), la disciplina sull'accesso ai documenti amministrativi (L. 241/1990, Capo V) e in materia di proprietà industriale (D.Lgs. 30/2005).

Un soggetto terzo in Italia può fare richiesta di riutilizzo di documenti alle PA e agli organismi di diritto pubblico. Le Pubbliche Amministrazioni sono obbligate a esaminare ed evadere le richieste di accesso ai dati entro un lasso di tempo ragionevole. Qualora tali limiti di tempo non siano stati fissati, viene stabilito un termine di trenta giorni lavorativi dalla comunicazione della richiesta stessa, al massimo prorogabile per ulteriori venti nel caso di richieste cospicue o complesse. In caso di assenso della PA, il richiedente riceverà i documenti, possibilmente in formato elettronico, se necessario corredati da una eventuale licenza, con un'offerta valutabile dal richiedente in un lasso di tempo ragionevole (Art. 5 D.Lgs. 36/2006). In caso, invece, di decisione negativa, la PA è sempre tenuta a motivare al richiedente il perché del diniego. Contro tale decisione sarà possibile opporre ricorso.

I dati devono essere di regola resi disponibili gratuitamente, salva la possibilità di recuperare i costi marginali, i costi per l'anonimizzazione dei dati personali o per la protezione delle informazioni commerciali a carattere riservato (Art. 7 D.Lgs. 36/2006). Sono comunque stati introdotti nuovi criteri di tariffazione, pur rimanendo fermo il principio base della gratuità. Come già parzialmente previsto dalla precedente disciplina, i soggetti pubblici vengono incoraggiati a utilizzare licenze standard (come, ad esempio, le licenze cd. *Creative Commons*), disponibili in formato digitale ed elaborate elettronicamente, provvedendo affinché i diritti conseguenti di proprietà intellettuale sui documenti, eventualmente detenuti da biblioteche o da imprese pubbliche, permettano l'utilizzo a fini commerciali e non commerciali (Art. 8 D.Lgs. 36/2006).

Per quanto riguarda i dati della ricerca, se derivanti da attività finanziata con fondi pubblici, o quando siano Open Data di una banca dati pubblica, essi sono riutilizzabili a fini commerciali previo il rispetto della disciplina in materia di protezione dei dati personali e della proprietà intellettuale e industriale (Art. 9-bis D.Lgs. 36/2006). Questi dati devono rispettare i principi FAIR: reperibilità, accessibilità, interoperabilità e riutilizzabilità (si veda: www.force11.org).

Infine, il decreto di recepimento ha modificato le regole per accordi di esclusiva (Art. 11 D.Lgs. 36/2006) e creato le condizioni per la determinazione delle sopra menzionate serie specifiche di dati di elevato valore (Art. 12-*bis* D.Lgs. 36/2006).

Con riferimento agli *Open Data*, altra disposizione normativa centrale in Italia è il D.Lgs. 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (CAD), il quale è particolarmente attento al principio della disponibilità dei dati pubblici in formato digitale. La disciplina attuale deriva dalle numerose modifiche e integrazioni che si sono succedute negli anni e che hanno seguito l'evoluzione del principio di trasparenza in senso attivo.

Agli Artt. 1, 52 e 53 si ritrovano così la definizione di "dato aperto", modificata dal decreto di recepimento della Direttiva OD, e una serie di disposizioni generali volte a razionalizzare il processo di valorizzazione del patrimonio informativo pubblico. Dati di tipo aperto sono i dati che assumono tre caratteristiche (Art. 1, co. 1-*bis* e 1-*ter* CAD):

1. sono disponibili tramite licenza o previsione normativa che consenta l'utilizzo da parte di chiunque in formato aggregato, anche a fini commerciali;
2. sono accessibili grazie alle tecnologie digitali, comprese le reti telematiche pubbliche e private, in formato aperto, ossia "reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti necessari per la fruizione dei dati stessi", sono adatti all'uso automatico dei computer e sono provvisti di metadati;
3. sono resi disponibili gratuitamente o a costi marginali come previsto dal D.Lgs. 36/2006.

Anche per questa normativa i dati dovrebbero essere aperti per impostazione predefinita (Minazzi, 2013). Il principio di "*open data by default*" prevede che i dati e i documenti pubblicati con qualsiasi modalità dalle PA, dai gestori di servizi pubblici, e dalle società a controllo pubblico, senza l'esplicita adozione di una licenza standard per il riutilizzo, si intendono rilasciati come dati di tipo aperto, ad eccezione dei casi in cui la pubblicazione riguardi dati personali (Art. 52, co. 2, CAD). Di norma si presuppone, quindi, l'applicazione automatica di una licenza aperta sui dati con la sola clausola di attribuzione della paternità, quale ad esempio la "*Creative Commons Attribution*" (CC BY) versione 4.0 come indicato dalle linee guida AgID per l'anno 2017 (reperibili in docs.italia.it).

Il CAD non fornisce la definizione della nozione di titolarità del dato, che è presupposto al riconoscimento di obblighi di pubblicazione e riutilizzo. Sul punto è opportuno richiamare l'Art. 2, n. 1, del D.Lgs. 36/2006, che la individua nella «pubblica amministrazione o l'organismo di diritto pubblico che ha originariamente formato per uso proprio o commissionato ad altro soggetto pubblico o privato il documento che rappresenta il dato o che ne ha la disponibilità». Elementi distintivi sono, quindi, la formazione del dato per opera diretta della pubblica amministrazione o dell'organismo di diritto pubblico; ovvero la detenzione indiretta, per averlo commissionato ad altro soggetto, pubblico o privato; oppure, infine, la sua concreta disponibilità.

Vista la clausola di salvaguardia della disciplina *Open Data* in materia di protezione dei dati personali, il Garante è da tempo intervenuto per fornire alcune linee guida, atte in prima battuta a supportare le pubbliche amministrazioni nella corretta applicazione degli obblighi imposti dal D.Lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" (c.d. Decreto Trasparenza). In particolare, nelle "Linee Guida in materia di trattamento dei dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" del 2014 si è stabilito che tutti gli atti oggetto di obbligo di pubblicazione in siti istituzionali delle PA debbano essere fruibili in formato di tipo aperto, riutilizzabili liberamente e senza necessità di autenticazione e indicizzabili nei motori di ricerca, con l'unico limite della citazione della fonte e dell'integrità. Di conseguenza ai cittadini viene riconosciuto un diritto di conoscibilità dei dati. Tuttavia, il Garante indica una serie di opportune cautele che i soggetti destinatari degli obblighi di pubblicazione devono applicare per evitare che l'adempimento di tali obblighi di trasparenza avvenga in violazione dei diritti tutelati dalla disciplina in materia di protezione dei dati personali e, più in generale, della Costituzione italiana.

A chiusura di questa disamina è necessario menzionare la proposta di Regolamento europeo del Parlamento e del Consiglio sulla governance europea dei dati ("*Data Governance Act*") depositata il 25 novembre 2020, che vorrebbe integrare la Direttiva OD. Questo nuovo strumento mira a promuovere la disponibilità di dati da utilizzare aumentando la fiducia negli intermediari e rafforzando i meccanismi di condivisione in tutta l'UE, rappresentando la prima di una serie di misure annunciate nella Strategia europea per i dati 2020. L'intento dichiarato è quello di offrire un modello europeo alternativo alla pratica di trattamento dei dati delle principali piattaforme tecnologiche. Il Regolamento dovrebbe incentivare la messa a disposizione dei dati del settore pubblico per il riutilizzo qualora tali dati siano oggetto di diritti di terzi (come di proprietà intellettuale) e la condivisione dei dati tra le imprese, dietro compenso. La Commissione europea vorrebbe inoltre affrontare la questione del consenso all'utilizzo di dati personali, anche per scopi c.d. "altruistici". La proposta, infatti, sviluppa la possibilità di un più ampio consenso al trattamento dei dati personali per finalità di interesse generale, come a fini di ricerca scientifica o il miglioramento di servizi pubblici (Art. 2 proposta). Il riutilizzo di dati gestiti da enti pubblici e di dati personali subirà, perciò, nuove modifiche nei prossimi anni.

La condivisione e il riutilizzo di dati in modalità aperta sono, pertanto, limitati dalla necessità di bilanciare questa peculiare modalità di valorizzazione dei dati con i principi e le tutele stabilite dalla disciplina in materia di protezione dei dati personali e dall'eventuale sussistenza di altri diritti in capo alle banche dati in oggetto, quali soprattutto i diritti di proprietà intellettuale.

2.2. Open Data e disciplina in materia di protezione dei dati personali

Valorizzare attraverso una strategia di disseminazione e distribuzione una banca dati contenente dati personali solleva diverse criticità (Jaatinen, 2016). Si possono identificare anzitutto tre criticità (Borgesius *et al*., 2016):

1. prima di tutto, una sorta di "*chilling effect*" collegato al possibile timore da parte degli individui a veder archiviate e rese pubbliche le loro informazioni. L'incertezza riguardo al corretto trattamento

dei dati personali può, infatti, avere un impatto negativo sulla qualità dei servizi offerti (sia a livello privato che pubblico);

2. in secondo luogo, è chiaro che se le informazioni vengono distribuite e condivise, i soggetti cui queste si riferiscono perdono il controllo sui propri dati personali. L'aumento di database (pubblici o privati) rilasciati in accesso aperto aumenta la possibilità di re-identificazione delle informazioni considerate anonime. Ciò porta a un incremento esponenziale dei rischi per la privacy dei cittadini e a una riduzione del controllo sulle loro informazioni personali;
3. infine, forme di distribuzione in Open Data potrebbero per assurdo portare a pratiche discriminatorie, favorendo così l'abuso di informazioni personali e potenziali invasioni della privacy dei cittadini (si veda l'uso di pacchetti di dati per finalità di marketing, lo screening delle domande di lavoro, e così via).

Ebbene, la diffusione di un database in modalità aperta contenente informazioni a carattere personale non è operazione di poco momento (Sanna, 2019; Guarda, 2021). Di seguito proviamo, in modo schematico, ad elencare le principali sfide da affrontare:

- "principio della limitazione della finalità": questo rappresenta, come descritto nella prima sezione del Quaderno, una pietra angolare nella disciplina sulla protezione dei dati personali e un ostacolo per gli *Open Data*. Mentre nel primo contesto l'attenzione al principio della "finalità specifica" del trattamento costituisce il fulcro dell'intero sistema di protezione, nell'approccio aperto si sottolinea esplicitamente l'importanza di garantire la possibilità di riutilizzare i dati "per qualsiasi scopo", commerciale o non. La disciplina prevista in materia di *Open Government Data*, come stabilito dalla Direttiva Open Data e dal decreto legislativo di recepimento italiano, prevedono che il riutilizzo dei dati personali è ammissibile soltanto se è rispettato il principio della limitazione della finalità;
- "principio di minimizzazione dei dati": i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati e protetti per impostazione predefinita (Artt. 5, par. 1, lett. c) e 25, par. 2, GDPR). Il principio di minimizzazione, nelle sue varie accezioni e istanze, contrasta con le logiche di fondo dei processi che spingono all'apertura dei dati ispirati a un presupposto totalmente diverso, secondo il quale la disponibilità di questi dev'essere la più ampia possibile (WP29, 2013);
- "sicurezza e responsabilizzazione": il titolare del trattamento deve adottare misure di sicurezza tecniche e organizzative volte a garantire che nessuno possa accedere ai dati personali se non autorizzato (Artt. 24, 25, par. 1, e 32 GDPR). Deve anche essere in grado di dimostrare che è stato fatto tutto quanto in suo potere per garantire tale sicurezza. È evidente che attraverso la diffusione di *Open Data* sia il titolare del trattamento che l'interessato perdano il controllo delle informazioni. Ciò rende impossibile affrontare adeguatamente questi obblighi della disciplina in materia di dati personali;
- "principio di trasparenza": il trattamento dei dati personali deve essere completamente chiaro e trasparente, soprattutto nei confronti dell'interessato cui i dati si riferiscono (Artt. 5, par. 1, lett. a) e 12 GDPR). Questo per prevenire possibili abusi da parte del titolare in virtù dell'asimmetria informativa tipica di questo contesto. Il riutilizzo di dati in modalità aperte cozza con questo dovere informativo perché è impossibile prevedere tutti i riutilizzi e informare via via l'interessato una volta rilasciati i dati in modalità aperta.

Nella normativa sugli *Open Data* vengono quindi fatte salve le regole in materia di dati personali e si richiama il concetto di anonimizzazione. La definizione, come sopra ricordato, è stata inserita nel quadro normativo sui dati aperti dal decreto di recepimento della Direttiva OD e si prevede in aggiunta la possibilità di riconoscimento di eventuali costi di anonimizzazione che i soggetti pubblici e privati potrebbero dover sostenere nel contesto di riutilizzo. Questo riferimento è fondamentale perché ribadisce l'essenzialità dei processi di anonimizzazione per garantire il riutilizzo sicuro delle informazioni.

In materia di anonimizzazione restano, tuttavia, le perplessità inerenti ai limiti applicativi delle tecniche utilizzabili e all'assunzione di responsabilità nell'effi-

cacia delle stesse a rendere irreversibile la de-identificazione. Il Working Party 29, nel Parere 05/2014 ha chiarito quanto sia difficile creare insiemi di dati effettivamente anonimi, mantenendo al contempo tutte le informazioni necessarie per espletare un'attività, anche perché l'anonimizzazione costituisce in sé un trattamento successivo di dati personali. L'autorità ha altresì espresso importanti raccomandazioni per l'impiego di tali tecniche al fine di poter garantire agli individui – e alla società stessa in senso lato – di fruire dei vantaggi degli *Open Data*, attenuando al contempo i rischi per gli interessati in termini di protezione dei dati personali.

I soggetti che dovranno o vorranno, quindi, costruire dataset di dati aperti dovranno utilizzare avanzate tecniche di anonimizzazione (D'Acquisto, Naldi, 2017) ed essere consapevoli che il trattamento di dati resi anonimi potrebbe comunque presentare rischi residui. L'anonimizzazione dovrebbe essere oggetto di un riesame periodico da parte del titolare del trattamento (WP29, 2014).

Per riuscire veramente a "liberare i dati" è, pertanto, necessario analizzare le varie criticità, valutare gli obiettivi perseguiti e garantire i principi e diritti sanciti dalla disciplina in materia di protezione dei dati personali.

Per iniziare, deve essere condotta un'analisi rischi-benefici. Non esiste una soluzione "*one-size-fits-all*" valida per ogni set di dati: il loro rilascio comporta vantaggi per il pubblico e potenziali rischi per la privacy individuale.

In secondo luogo, tradizionalmente l'attenzione è sempre stata posta sul momento (finale) della condivisione. Ma una gestione efficace richiede di tenere conto di tutte le fasi del ciclo di vita del dato (Green *et al*., 2017): raccolta, manutenzione, rilascio ed eliminazione. In aggiunta, è fondamentale creare strutture e processi operativi che codifichino adeguatamente la gestione della privacy nell'ambito dell'intera organizzazione che tratta i dati personali (conformemente al principio della *data protection by design*).

Università e centri di ricerca dovrebbero allora sviluppare processi di gestione dei dati chiari e coerenti atti a valutare con regolarità i rischi e i benefici connessi alla loro attività.

Infine, è essenziale investire nel tentativo di includere la società civile nei processi relativi alla gestione dei dati e alla loro distribuzione attraverso modelli aperti: per riferirsi a questi fenomeni si parla anche di "*citizen science*" (Guarda, 2021).

Vi è un evidente contrasto concettuale tra il fenomeno OD, che sottolinea l'importanza della più ampia apertura, condivisione e riutilizzo possibile, eliminando ogni tipo di barriera (tecnica, giuridica, economica) da una parte, e la normativa sulla protezione dei dati, che circoscrive e limita il trattamento dei dati alle sole finalità debitamente individuate, specificate e rese note *ex ante* all'interessato, dall'altra. Il rispetto dei principi della privacy non può essere totalmente garantito quando un database viene rilasciato seguendo un approccio OD, in quanto ciò determina la perdita totale del controllo sulle informazioni così rilasciate e sui possibili ulteriori utilizzi dei dati. L'unica soluzione applicativa ad oggi veramente affidante risiede nell'utilizzo di tecniche di anonimizzazione efficaci che rendano le informazioni rilasciate non più collegabili a una persona fisica identificata o identificabile. È necessario essere consapevoli del fatto che questo è un processo di carattere "relativo", poiché l'anonimizzazione assoluta sembra essere oramai impossibile, vista l'emersione del fenomeno dei Big Data, e intrinsecamente "dinamico", in quanto le tecnologie si evolvono assieme ai rischi di re-identificazione (Stalla-Bourdillon, Knight, 2017; Guarda, 2021).

2.3. Buone prassi

Domande preliminari da porsi prima della condivisione e apertura di dati:

- qual è la fonte dei dati?
- chi ha raccolto i dati?
- chi sta utilizzando i dati?
- con quali risorse/finanziamento sono stati raccolti i dati?
- per quali finalità sono stati raccolti i dati?
- per quali finalità sono stati conservati i dati?
- sono presenti contratti che regolano l'attività di raccolta dei dati?

- sono presenti contratti che regolano l'uso o il riutilizzo dei dati?
- cosa stabilisce la licenza sui dati?
- i dati sono qualificabili come dati personali? Rientrano in categorie particolari di dati?
- se sono presenti dati personali, si dispone di tecniche di anonimizzazione adeguate a renderli de-identificati in modo irreversibile?
- sono presenti diritti di proprietà intellettuale di terzi o segreti industriali?
- se sono presenti diritti di proprietà intellettuale, diritti di proprietà industriale, diritti al segreto (industriale, statistico, commerciale), si dispone dei diritti e/o delle autorizzazioni per valorizzare i dati secondo la strategia prescelta?

Tabella 2.1 Buone prassi *Open Data*

Fase	Raccomandazione	Descrizione	Normativa principale
Gestione del dataset e dei documenti	Verificare la sussistenza di eventuali vincoli generali insistenti sulla banca dati o sul documento	Verifica di eventuali vincoli giuridici che: ▪ impongono l'apertura della banca dati (disciplina OGD, o regole relative al finanziamento per la costituzione, ecc.), o ▪ prevedono la non condivisione in modalità aperta della stessa (obblighi giuridici cogenti, regole relative al finanziamento per la costituzione, limiti di sicurezza o difesa nazionale, vincoli di riservatezza fissati dalla legge, ecc.). Se sussistono tali vincoli, i dati sono riservati	Open data, Open Government Data D.Lgs. 36/2006, Direttiva OD CAD Normativa europea
Gestione del dataset e dei documenti	Verificare la sussistenza di eventuali vincoli di proprietà intellettuale insistenti sulla banca dati o sul documento	Analisi e verifica dei diritti di proprietà intellettuale (diritto d'autore e diritto sui generis sulle banche dati), di proprietà industriale, diritti al segreto (industriale, statistico, commerciale), eventualmente sussistenti su: ▪ la banca dati, o ▪ i documenti e dati in essa contenuti Se sussistono tali vincoli, i dati sono vincolati	Direttiva 96/9/CE (tutela giuridica delle banche dati) L. 633/1941 e trattati internazionali sulla proprietà intellettuale L. 241/1990 D.Lgs. 30/2005
Gestione del dataset e dei documenti	Verificare la presenza di eventuali dati personali nella banca dati o nel documento	Analisi dei dati e verifica della presenza di dati personali, della finalità e caratteristiche del loro trattamento	D.Lgs. 36/2003 fa salva la disciplina del GDPR e Codice Privacy
Apertura del dataset e dei documenti	Valutare la licenza da applicare al dataset per la condivisione tra gestore e utilizzatore	Analisi e scelta della licenza attraverso la quale valorizzare in modalità aperta i dati	D.Lgs. 36/2006
Apertura del dataset e dei documenti	Valutare eventuali costi per la condivisione	Analisi e fissazione di un eventuale costo per l'utilizzatore Tenendo conto della regola generale di gratuità, apposizione di un costo marginale o costo per l'adozione di misure a protezione del dataset	D.Lgs. 36/2006
Apertura del dataset e dei documenti	Anonimizzare i dati personali e condividere i dati anonimizzati	Se sono presenti dati personali, analizzare e suddividere la banca dati individuando: ▪ gli eventuali *subset* di dati considerati critici per i quali non è possibile procedere in modo sicuro e affidante all'anonimizzazione dei dati stessi: questo *subset* non potrà esser oggetto di "apertura" ▪ i *subset* di dati personali per i quali invece è possibile procedere ad anonimizzazione in vista della loro apertura ▪ Anonimizzazione con tecniche che garantiscono la de-identificazione irreversibile ▪ Condivisione dei dati anonimizzati	D.Lgs. 36/2006 GDPR e Codice Privacy
Apertura dei dati limitata all'utilizzatore (comunicazione e trattamento secondario di dati personali) Non si tratta di *Open Data*, ma di condivisione di dati	Valutare la costruzione di un trattamento ulteriore (secondario) di dati personali (es. fini di ricerca) con la creazione di ruoli privacy e l'applicazione delle regole in materia di protezione dei dati personali	Analisi e verifica del trattamento dei dati personali Valutare di limitare la condivisione (apertura limitata) del dataset solo per l'utilizzatore, che potrà assumere il ruolo di responsabile del trattamento o contitolare del trattamento V. Sez. Raccomandazioni e Prassi sul trattamento di dati personali	GDPR e Codice Privacy

Tabella 2.2 Buone prassi per richiedere l'accesso a dati nella disponibilità altrui

Fase	Raccomandazione	Descrizione	Normativa principale
Richiesta dataset o documenti nella disponibilità di una pubblica amministrazione o di un organismo di diritto pubblico	Richiedere il riutilizzo di documenti per fini commerciali, o non, a una pubblica amministrazione o a un organismo di diritto pubblico soggetto alla disciplina *Open Data*	Richiesta alla pubblica amministrazione o organismo di diritto pubblico, che dovrà rispondere entro 30 giorni (prorogabili di 20 giorni) e valuterà sull'opportunità del riutilizzo. In caso di diniego, che dovrà essere motivato, è possibile opporre ricorso amministrativo. In caso di accoglimento, i documenti verranno forniti tramite licenza standard per il riutilizzo, gratuitamente (a meno che non vengano applicati costi marginali) e, ove possibile, in formato elettronico	*Open Data*, *Open Government Data* D.Lgs. 36/2006 e Direttiva OD Art. 2 esclude una lista di documenti di cui non è possibile richiedere il riutilizzo
Richiesta di un dataset o documenti contenenti dati non personali e pubblicati come *Open Data* da parte di un privato	Richiedere il riutilizzo di dati a chi è nella loro disponibilità e li ha pubblicati come *Open Data* in un portale, sito web o piattaforma	Richiesta dei dati pubblicati e accessibili a chi ne ha la disponibilità e ottenimento degli stessi tramite licenza, gratuitamente o previo pagamento di un costo. Chi ha pubblicato i dati avrà primariamente verificato la sussistenza di limiti derivanti dalla disciplina in materia di dati personali o in materia di proprietà intellettuale o in virtù di altri diritti o obblighi. Se necessario, i dati saranno stati anonimizzati con adeguate tecniche che impediscano la re-identificazione	
Richiesta di un dataset o documenti contenenti dati personali, come trattamento secondario di dati Non si tratta di *Open Data*, ma di condivisione di dati personali in un ambito di trattamento	Richiedere i dati per costruire un trattamento ulteriore (secondario) di dati personali (es. fini di ricerca) con la creazione di ruoli privacy e l'applicazione delle regole in materia di protezione dei dati personali	Analisi e verifica del trattamento principale dei dati personali rispetto all'eventuale trattamento secondario, se compatibile con la finalità Costruzione del ruolo privacy dell'utilizzatore, che potrà assumere il ruolo di responsabile del trattamento o contitolare del trattamento Progettazione del trattamento secondario di dati personali in ottica di *data protection by design* e *by default* V. Sez. Raccomandazioni e Prassi sul trattamento di dati personali	

(*continua...*)

(*segue...*)

Fase	Raccomandazione	Descrizione	Normativa principale
Richiesta dataset o documenti con dati personali, anche particolari, per un progetto di ricerca scientifica o statistica	Soggetti terzi diversi dal titolare del trattamento che ha raccolto i dati (per una finalità in via principale) che intendono realizzare un trattamento ulteriore di dati (in via secondaria) per finalità di ricerca, e che svolgono principalmente ricerche scientifiche o statistiche, possono richiedere di trattare i dati al Garante per la protezione dei dati personali Ciò è possibile qualora per particolari ragioni informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità della ricerca	Richiesta di autorizzazione preventiva e vincolante al Garante per la protezione dei dati personali, che risponderà entro 45 giorni (meccanismo del silenzio-dissenso) e indicherà misure e condizioni, anche di sicurezza per il trattamento Adozione di misure appropriate a protezione dei dati, come preventiva minimizzazione, pseudonimizzazione o anonimizzazione Il Garante può aver pubblicato in G.U. un'autorizzazione generale d'ufficio in relazione a determinate categorie di titolari e di trattamenti e con l'indicazione di misure e garanzie. In questo caso, il soggetto può trattare i dati seguendo le indicazioni dell'autorità	GDPR e Art. 110-*bis* Codice Privacy

3. ESPERIENZE DI SUCCESSO E SCENARI APPLICATIVI

In questo capitolo si presentano alcuni scenari applicativi finalizzati a bilanciare l'attività di ricerca e la corretta tutela dei dati personali, all'esito di processi organizzativi o progetti di ricerca, per rendere accessibili i dati.

3.1. Montreal Neurological Institute and Hospital

Una prima esperienza a livello internazionale in cui i dati della ricerca sono stati gestiti con successo è il Montreal Neurological Institute and Hospital (MNI) o "Neuro" in Canada. Questo istituto di ricerca e di insegnamento è stato fondato nel 1934 dal noto neurochirurgo W. Penfield e fa parte della missione neuroscientifica del McGill University Health Center (MUCH). Il Neuro è attualmente uno dei punti di riferimento a livello mondiale per la ricerca in materia di neuroscienza, per la cura avanzata dei pazienti e per il trattamento dei disturbi del sistema nervoso (Risdale, 2016).

Il MNI è considerato il primo istituto accademico del suo genere ad adottare pienamente i principi della Scienza Aperta. Ciò è dimostrato anche da un recente progetto. Nel 2016, infatti, grazie a una cospicua donazione da parte della famiglia Tanenbaum, il Neuro ha dato inizio a un esperimento di durata quinquennale garantendo libero accesso ai dati e pubblicando le soluzioni tecnologiche in licenza aperta attraverso la creazione del "Tanenbaum Open Science Institute" (TOSI). L'obiettivo del TOSI è di accelerare i progressi della ricerca, reinventare il suo ruolo nella comunità e facilitare la diffusione delle scoperte neuroscientifiche in tutto il mondo (Gold, 2016; Owens, 2016). Questa apertura e condivisione ha interessato, pertanto, i dati sperimentali, i campioni biologici, i materiali da laboratorio, le tecniche e i modelli di business. Il progetto intende perciò favorire il contatto tra esperti provenienti da tutto il mondo e accelerare la scoperta di nuove e moderne terapie per il trattamento e la cura di pazienti affetti da malattie neurologiche. Questa esperienza si inserisce nella c.d. "terza missione" dell'università, che richiederebbe di diffondere la conoscenza in modo libero per apportare benefici allo sviluppo, anche di carattere economico e sociale, della comunità (Paparella, 2014).

Questa scelta di apertura del TOSI segue cinque principi fondamentali che sono stati adottati dall'intera comunità scientifica nel 2017 con il diretto supporto della McGill University (Poupon *et al*., 2017):

1. "*Public release of scientific data and resources*": il MNI e i suoi ricercatori renderanno liberamente disponibili tutti i dati positivi e negativi, i modelli utilizzati, le fonti di dati, i reagenti, gli algoritmi, il software e le altre risorse scientifiche, non più tardi della data di pubblicazione del primo articolo relativo a questi dati o risorse;
2. "*External research partnerships*": tutti i dati e le risorse scientifiche generate attraverso i partenariati di ricerca, che possono coinvolgere sia soggetti commerciali che di carattere filantropico o provenienti dal settore pubblico, dovranno essere rilasciati pubblicamente nel rispetto del primo principio;
3. "*Access to the Clinical Biological Imaging and Genetic repository (C-BIGr)*": il C-BIGr supporterà la creazione di conoscenza e innovazione massimizzando il valore a lungo termine dei contributi dei partecipanti alla ricerca e delle risorse scientifiche create dai ricercatori MNI e dai loro collaboratori. Il Neuro riconosce al contempo il primato della salvaguardia della dignità degli individui e della privacy dei pazienti partecipanti ai progetti di ricerca, e del rispetto dei diritti e degli obblighi nei loro confronti attraverso il processo di consenso informato;
4. "*Unique position on intellectual property rights*": il MNI e i suoi ricercatori nella qualità di dipendenti o consulenti non potranno mai ottenere la tutela brevettuale per quanto scoperto o far valere alcun tipo di diritto di protezione sui dati in relazione alle ricerche svolte. Ciò rappresenta una decisione innovativa e audace che rompe una delle barriere di carattere legale che possono limitare la diffusione della conoscenza;
5. "*Autonomy*": l'istituto di ricerca sosterrà e garantirà l'autonomia di tutti i soggetti coinvolti in un progetto (ricercatori, personale amministrativo, tirocinanti e pazienti), a condizione che ciò non comprometta i principi fondamentali dell'intero sistema.

Il TOSI, infine, oltre a creare un'infrastruttura di ricerca per la condivisione dei dati, ha sviluppato numerosi programmi, collaborazioni e forme di incentivo per i ricercatori e i loro partner commerciali con l'obiettivo di attivare delle relazioni stabili anche all'esterno degli enti di ricerca, determinando maggiori ricadute positive nella comunità in termini di progresso e di stimolo a nuove scoperte.

3.2. Health Data Hub

Nel contesto francese troviamo uno scenario che è pensato per favorire un trattamento di dati personali relativi alla salute raccolti primariamente ai fini di cura dei pazienti, e utilizzabili secondariamente per finalità di ricerca (Bincoletto, Guarda, 2021).

In Francia il sistema sanitario ha una forma amministrativa centralizzata ed è misto tra servizi pubblici e privati, entrambi regolati dal *Code de la santé publique*. Questo codice ha istituito il c.d. *Dossier pharmaceutique* (Artt. R1111-20-10 – R1111-20-13), che può essere considerato l'equivalente francese del Fascicolo

Sanitario Elettronico italiano (FSE). Il *Dossier* raccoglie i dati dei pazienti per finalità di cura; tuttavia, in caso di anonimizzazione, tali dati possono essere usati per finalità di ricerca. Dal sistema nazionale sanitario possono, quindi, essere creati database di dati aggregati e anonimizzati per la ricerca, lo studio e per la valutazione (Art. R1461-5).

Il *système national des données de santé* (SNDS), per le cui caratteristiche si considera un'esperienza unica in Europa, è gestito dalla *Caisse nationale de l'assurance maladie* e consente il collegamento tra vari database, tra cui quelli gestiti dagli ospedali pubblici, dalle assicurazioni sanitarie, e, in futuro, anche quelli delle organizzazioni esterne che offrono servizi sanitari, e il database sulle cause mediche dei decessi (si veda www.snds.gouv.fr). Lo scopo del SNDS è di rendere questi dati disponibili per studi, ricerche o trattamenti di interesse pubblico che contribuiscono a uno dei seguenti scopi: fornire informazioni sulla salute pubblica e privata; attuare politiche sanitarie; conoscere la spesa sanitaria; informare i professionisti e le istituzioni sulle loro attività; creare innovazione nei campi della salute e dell'assistenza medico-sociale; attuare politiche di sorveglianza, monitoraggio e sicurezza sanitaria. A partire dal 2017 qualsiasi soggetto pubblico o privato, con o senza scopo di lucro, può chiedere di accedere a questi dati, previa autorizzazione del CNIL, per effettuare studi o ricerche.

La Loi n. 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé ha modificato il Code de la santé publique, ampliando l'utilizzo dei dati relativi alla salute per varie finalità e modificando anche la normativa francese in materia di protezione dei dati personali (Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés e la Loi n. 2018-493 du 20 juin 2018 relative à la protection des données personnelles). Nello stesso anno è stato creato l'Health Data Hub (*Plateforme des données de santé*) (si veda: www.cnil.fr), piattaforma che utilizza meccanismi di IA e che aspira a promuovere e facilitare la condivisione di dati relativi alla salute provenienti da una vasta gamma di fonti per essere riutilizzati per finalità di ricerca. Questa piattaforma è riferita sia a una soluzione tecnologica che conserva e rende disponibili i dati per progetti che abbiano un interesse pubblico, sia a un gruppo d'interesse incaricato di amministrare la gestione dei processi.

L'Health Data Hub è operativo dall'aprile 2020 ed è stato utilizzato per finalità di interesse pubblico in materia di emergenza sanitaria e per qualche progetto pilota di ricerca[1]. L'Art. L.1462-1 del *Code de la santé publique* indica le finalità perseguite dalla piattaforma:

- raccogliere, organizzare e rendere disponibili i dati relativi alla salute, in particolare i dati conservati dal SNDS, e promuovere l'innovazione nell'uso di tali dati;
- informare i pazienti, promuovere e facilitare l'esercizio dei loro diritti attraverso il portale collegato all'Hub;
- contribuire allo sviluppo delle metodologie di riferimento sviluppate dal CNIL per consentire l'accesso ai dati da parte dei terzi;
- facilitare la disponibilità di dataset con un basso rischio di impatto del trattamento dei dati, tramite la disponibilità di un valido e sicuro supporto tecnologico;
- contribuire alla diffusione di standard per lo scambio e l'utilizzo di dati relativi alla salute;
- sostenere, in particolare finanziariamente, i responsabili dei progetti selezionati nell'ambito dei bandi di gara e i produttori di dati associati ai progetti selezionati.

In materia di protezione dei dati viene indicato che i dati personali devono essere pseudonimizzati, che non saranno accessibili liberamente, ma soltanto tramite scenari che includano: "*specific project spaces*" validati dalla CNIL; l'implementazione di adeguate misure di sicurezza; l'effettuazione di *audit* interni ed esterni; la conclusione di contratti che vincolino gli utilizzatori della piattaforma. I progetti di ricerca dovranno conformarsi a una metodologia di riferimento definita dalla CNIL (*Méthodologies de référence* MR-001-006) e in alcuni casi richiede-

1 Si v. l'Arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire e in Rete: www.legifrance.gouv.fr e www.health-data-hub.fr.

ranno l'autorizzazione dell'autorità. In caso di utilizzo dell'Hub la base giuridica del trattamento è di tipo legale (*Code de la santè publique*) e non sarà necessario il consenso dell'interessato.

L'Health Data Hub rappresenta un'interessante soluzione istituzionalizzata e procedimentalizzata per utilizzare dati personali già presenti nel sistema sanitario nazionale per ulteriori finalità di ricerca in presenza di appropriate garanzie e misure di sicurezza e con il coinvolgimento dell'autorità garante in materia di protezione dei dati personali.

3.3. KRAKEN

Il progetto Horizon 2020 "KRAKEN" (*BroKeRage and MArKet platform for pErsoNal data)* si propone di sviluppare una piattaforma che possa consentire lo scambio sicuro e affidabile di dati personali, applicando le regole del GDPR e creando una sorta di *marketplace* dei dataset (www.krakenh2020.eu). Questa piattaforma intende restituire il controllo dei dati agli utenti, considerati "fornitori di dati", durante l'intero ciclo di vita dei dati. Allo stesso tempo, gli "utilizzatori", ossia soggetti pubblici o privati, potranno ottenere i dati su richiesta per specifiche finalità, con o senza scopo di lucro, a seconda delle condizioni previste dal fornitore.

Nell'*Ethical and legal management report* del progetto vengono indicati tre principi fondamentali che la piattaforma rispetta:

1. l'adozione dell'approccio di *data protection by design*, mercé l'implementazione di specifiche misure a protezione dei dati, inclusa la crittografia;
2. il consenso specifico, tramite l'utilizzo di "*improved informed consent tools*", che permettano al fornitore dei dati di acconsentire e controllare l'accesso agli stessi una dettagliata interfaccia *mobile* e *web-based*; il fornitore predefinisce, infatti, le condizioni di utilizzo dei dati, regolando il tempo di condivisione, le finalità consentite, la tipologia di soggetti (pubblici o privati), l'eventuale accesso ai dati da parte di terze parti;
3. minimizzazione e limitazione della finalità, poiché solo i dati direttamente rilevanti e necessari per la finalità di ricerca verranno concessi all'utilizzatore.

KRAKEN utilizza un'infrastruttura basata sulla tecnologia blockchain e su un *Self-Sovereign Identity (SSI) system*. Il progetto combina, interopera ed estende i migliori risultati di due piattaforme informatiche svilup-

pate nell'ambito di altri due progetti europei: CREDENTIAL (che ha creato un *cloud* sicuro per dati personali) e MyHealthMyData (che ha creato un sistema decentralizzato per caricare e scambiare dati relativi alla salute tra individui, ospedali e ricercatori). Un progetto pilota di KRAKEN è dedicato allo scambio di dati sanitari tra pazienti o strutture sanitarie come fornitori, e utilizzatori come enti di ricerca o enti pubblici. Questa esperienza adotta aspetti chiave in materia di protezione dei dati personali bilanciando esigenze di tutela e sicurezza con la possibilità di condividere i dati in assenza di obblighi e a vantaggio di un loro utilizzo anche per finalità di ricerca.

3.4. European Open Science Cloud (EOSC)

L'ultimo contesto applicativo di interesse che si ritiene utile riportare è quello rappresentato dallo European Open Science Cloud (EOSC) (Guarda, 2021). Questo si propone di creare un contesto atto a ospitare ed elaborare i dati della ricerca e aspira a sostenere e incentivare le scienze nell'ambito dell'UE. La Commissione europea ha avviato il progetto nel 2015 con lo scopo di sviluppare un ambiente fidato, virtuale e federato in grado di valicare i confini disciplinari e geografici e di archiviare, condividere, elaborare e riutilizzare oggetti digitali della ricerca, incluse pubblicazioni, dati e soluzioni tecnologiche. Con EOSC sono stati riuniti stakeholder istituzionali, nazionali ed europei, con iniziative e infrastrutture di dati per sviluppare un ecosistema scientifico aperto e inclusivo e per ogni disciplina (COM (2016)178). Sono, a titolo di esempio, incluse la scienza medica, le scienze sociali, le scienze agroalimentari e le scienze naturali.

EOSC consente, quindi, la creazione di un ambiente digitale in cui i ricercatori possano accedere a dati correttamente gestiti, impiegare servizi e strumenti avanzati e conoscere le migliori pratiche a livello internazionale basate su di essi. Questo progetto cambia il paradigma in cui la scienza viene condotta, promuovendo fin dal principio l'adozione dei principi FAIR (reperibilità, accessibilità, interoperabilità e riutilizzabilità dei dati della ricerca) nel costruire un'importante infrastruttura scientifica di base per la scienza europea, che dovrà guidare e condizionare lo sviluppo futuro di tutte le infrastrutture utilizzate in tale contesto. Esso riunisce iniziative istituzionali, nazionali ed europee, i fornitori di dati e servizi, e le infrastrutture di ricerca e tutte le parti interessate per co-progettare e implementare un "*European Research Data Commons*".

L'adozione di EOSC è stata intrapresa dal 2018 con l'istituzione di una struttura di governance a più livelli che ne guida e supervisiona l'attuazione e con l'approvazione della Dichiarazione di Vienna da parte di numerose comunità di ricerca, come università, istituti di ricerca, organizzazioni intergovernative, laboratori, biblioteche e associazioni scientifiche che chiarisce i principi dell'iniziativa. Nel 2020 è iniziato lo sviluppo del portale di EOSC, inserito dalla "*European Data Strategy*" come il nucleo di uno spazio dedicato ai dati della scienza, della ricerca e dell'innovazione che si articolerà in nove settori. Dal 2024 questo portale verrà aperto al settore pubblico e privato ed entro il 2025 sarà attivo il servizio per i ricercatori dell'UE.

EOSC segue le politiche di scienza e ricerca aperta e i principi di riutilizzo degli OD. Il portale dovrà essere conforme alle regole del GDPR, della Direttiva (EU) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Network and information security – NIS), e della Direttiva Open Data. Il corpus legislativo a livello dell'UE che influisce direttamente sull'interoperabilità giuridica e sull'adozione dei principi FAIR nel contesto dell'EOSC include infatti la disciplina in materia di protezione dei dati personali e, più in generale, le varie discipline volte a proteggere le informazioni ritenute sensibili o confidenziali, ma anche i diritti di proprietà intellettuale (in particolare diritto d'autore e diritto sui generis sulle banche dati).

Con particolare attenzione alla disciplina in materia di protezione dei dati personali, la sfida per EOSC è rappresentata dalla necessità di integrare la conformità alle regole stabilite dal GDPR senza compromettere l'interoperabilità giuridica e, quindi, la possibilità di utilizzare i dati nel modo più ampio al fine di sfruttare tutti i vantaggi che la loro condivisione può apportare allo sviluppo della conoscenza scientifica. Del *favor* che contraddistingue la disciplina europea si è già detto, in special modo con riferimento ai possibili usi secondari dei dati per finalità di archiviazione nel pubblico inte-

resse, di ricerca scientifica o storica o a fini statistici e all'essenziale adozione degli approcci *data protection by design* e *by default*. L'architettura di EOSC dovrà inoltre, ove possibile, favorire i processi di anonimizzazione dei dati personali, in modo che, come sopra specificato, le informazioni possano essere liberamente condivise secondo il concetto OD e per scopi secondari, senza che ciò presenti rischi per gli individui.

4. CENNI SULL'UTILIZZO DEI DATI PER LA RICERCA NELL'AMBITO DEL PNRR

Il Piano Nazionale di Ripresa e Resilienza (PNRR) italiano si inserisce all'interno del programma dell'Unione Europea Next Generation EU. Esso avrà una durata di sei anni (2021-2026) e prevedrà ingenti investimenti in ambito di ricerca e, a giugno 2022, è ancora in via di completamento. Le misure e le azioni che concretamente verranno adottate non sono ancora state del tutto determinate. Senza alcuna pretesa di completezza ed esaustività, di seguito si fornirà, comunque, una schematica descrizione della nuova disciplina sull'utilizzo dei dati.

Il PNRR si compone di diverse missioni. In particolare, la missione 4 è esplicitamente dedicata a "Istruzione e Ricerca" ed è volta a "rafforzare il sistema educativo, le competenze digitali e tecnico-scientifiche, la ricerca e il trasferimento tecnologico". Anche altre missioni potranno coinvolgere direttamente l'attività di ricerca, come ad esempio la missione "Salute" (si veda www.mef.gov.it). La guida "Italia Domani" illustra, invece, il cronoprogramma, i modelli organizzativi e le strutture delle missioni e le modalità attuative del PNRR (si veda

italiadomani.gov.it). Le misure incentiveranno la creazione di progetti di ricerca interdisciplinari con ricadute nazionali e con una forte connessione tra università e imprese.

Nelle linee guida per le iniziative di sistema della missione 4, sulla componente "Dalla ricerca all'impresa", i dati, personali o non personali, rappresentano elementi chiave sia delle infrastrutture di ricerca che di innovazione (si veda www.mur.gov.it). I Partenariati e i Centri Nazionali che verranno creati per questa missione processeranno grandi moli di dati. L'approccio sui dati è descritto come aperto e competitivo, basato sulla "innovazione aperta" e sui "dati aperti". Allo stesso tempo, dovranno essere considerati eventuali diritti di proprietà intellettuale e le esigenze di riservatezza. Essendo, tuttavia, favorita la transizione verso "un'economia basata sulla conoscenza", e avendo l'obiettivo di ottenere risultati "duraturi e sostenibili", si può immaginare che i progetti di ricerca tenderanno verso i paradigmi *open* sopra descritti. I bandi per i progetti verranno pubblicati nel primo trimestre del 2022.

Il Programma Nazionale per la Ricerca 2021 - 2027, pubblicato il 23 gennaio 2021, fa espresso riferimento all'accesso aperto ai risultati della ricerca in modalità FAIR come "trampolino di lancio per maggiori opportunità di innovazione" (si veda www.mur.gov.it). All'interno del Programma viene annunciato il Piano nazionale per la scienza aperta, che proporrà delle linee strategiche in allineamento con l'iniziativa EOSC. Tale piano non è stato ad oggi ancora pubblicato.

Con riferimento alla recente normativa, in attesa di ulteriori decreti relativi alla missione 4, si segnala il D.L. 31 maggio 2021, n. 77, Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure, convertito con la L. 29 luglio 2021, n. 108, il quale presenta delle "disposizioni in materia di produzione di basi di dati mediante informazioni provenienti da archivi amministrativi ai fini dell'attuazione del PNRR". Nell'art. 11-*bis* si prevede che l'ISTAT e gli altri enti del Sistema statistico nazionale possano produrre le informazioni statistiche necessarie alla gestione della ripresa a partire da archivi amministrativi, escludendone alcuni (es. banca dati nazionale unica della documentazione antimafia). Ai sensi del co. 5 della medesima disposizione e dell'Art. 5 *ter* del D.Lgs. 14 marzo 2013, n. 33 – Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, questi dati, se anonimizzati, potranno essere comunicati per finalità di ricerca agli enti che partecipano al Sistema statistico nazionale e a ricercatori appartenenti a università, enti di ricerca e istituzioni pubbliche o private e loro strutture di ricerca, soggetti che sono inseriti nell'elenco dell'Autorità Statistica dell'UE (Eurostat) o che risultano in possesso di particolari requisiti verificati dal Sistan.

Il D.L. 8 ottobre 2021, n. 139, coordinato con la legge di conversione del 3 dicembre 2021, n. 205 recante "Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali", pubblicata in G.U. n. 291 del 7 dicembre 2021, ha introdotto alcune misure e modifiche relative al trattamento di dati personali per finalità di ricerca. Tuttavia, ad oggi, tali disposizioni si riferiscono a enti e organizzazioni pubbliche titolari del trattamento che potranno utilizzare i dati raccolti anche per finalità di ricerca, se privati di elementi identificativi diretti, e compatibilmente con le loro principali finalità di interesse pubblico. Non vengono previste novità per enti di ricerca privati o soggetti privati che intendono effettuare delle ricerche.

Il D.L. 30 aprile 2022, n. 36, entrato in vigore il 1 maggio 2022, contiene ulteriori misure anche per l'ambito di ricerca. L'attuazione del PNRR è in costante evoluzione. La disciplina di dettaglio che verrà fornita dovrà quindi essere oggetto di nuovi approfondimenti. I principi e le regole generali analizzati in questo Quaderno rappresentano comunque il punto di riferimento per qualsiasi attività di ricerca che riguardi il trattamento di dati personali.

5. RACCOMANDAZIONI SCHEMATICHE E BUONE PRASSI

Questo capitolo si propone di fornire alcune raccomandazioni e buone prassi utili per impostare correttamente la gestione di un progetto di ricerca che preveda il trattamento di dati personali. La loro esposizione è volutamente schematica al fine di risultare più facilmente fruibile. Evidentemente ogni scenario applicativo potrà presentare peculiarità proprie che potrebbero obbligare il titolare del trattamento ad approfondire specifiche tematiche ed eventualmente a dover tenere in considerazione anche ulteriori discipline di dettaglio e ad adottare altre misure tecniche e organizzative.

Le raccomandazioni e buone prassi seguono l'approccio di *data protection by design* sopra illustrato e indicano il principio applicabile al trattamento dei dati personali (Art. 5 GDPR) al quale si conformano ed eventuali norme chiave da consultare.

Le indicazioni sono organizzate per attività:

- analisi del trattamento;
- predisposizione documentale;
- basi giuridiche;
- predisposizione degli strumenti informatici;
- buone prassi del trattamento.

Le raccomandazioni sono poi ulteriormente articolate nelle singole fasi progettuali:

- fase preliminare alla ricerca (al momento di determinare le finalità e i mezzi del trattamento);
- fase relativa allo svolgersi dell'attività di ricerca (all'atto del trattamento, dalla raccolta dei dati alle successive operazioni);
- fase di chiusura del progetto di ricerca (alla conclusione del trattamento).

Per la compilazione di progetti di ricerca in ambito europeo si consiglia la consultazione anche delle Linee Guida dell'Agenzia per la Promozione della Ricerca Europea per l'Italia (APRE) per il trattamento dei dati personali nei progetti Horizon 2020, "Progettazione e Consortium Agreement", "Implementazione, Sfruttamento dei risultati, Disseminazione e Comunicazione", "Project Management e Rendicontazione".

Tabella 5.1 – Analisi del trattamento dei dati

Fase	Raccomandazione	Descrizione	Principio e norme rilevanti
Prima dell'inizio	Chiarire se il progetto di ricerca rientrerà nello scopo territoriale e materiale della normativa in materia di protezione di dati personali	Valutazione dell'applicazione della disciplina a protezione dei dati personali o sua non applicazione Chiarire se si tratteranno dati personali o dati anonimi Chiarire se si tratterà un dataset misto Chiarire se il trattamento sarà effettuato all'interno dello Spazio Economico Europeo In caso di progetti che riguardano anche ordinamenti giuridici terzi (es. USA), effettuazione di una *gap analysis* di tipo normativo per definire un approccio comune durante il progetto che possa garantire la conformità alla normativa interna e esterna	Liceità Artt. 1-3 GDPR
Prima dell'inizio	Definire le finalità dello specifico progetto di ricerca	Individuazione della finalità di ricerca: ricerca scientifica, storica, fini statistici, archiviazione nel pubblico interesse La finalità deve essere esplicita, lecita e il più possibile specifica Il trattamento dei dati personali deve essere effettuato per la realizzazione delle finalità scientifiche del progetto di ricerca	Limitazione della finalità Art. 89 GDPR
Prima dell'inizio	Chiarire se il progetto di ricerca rientra in una particolare categoria di ricerca (storica, scientifica, statistica, o di archiviazione nel pubblico interesse)	Valutazione dell'applicazione delle norme di ricerca storica, scientifica, statistica, o di archiviazione nel pubblico interesse	Liceità Artt. 101 – 103 Codice Privacy per ricerca storica, con Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica e "Codice dei beni culturali e del paesaggio" (Artt. 122 – 127) Artt. 104 – 109 Codice Privacy per ricerca scientifica o a fini statistici, con Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, e Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica
Prima dell'inizio	Chiarire se si tratta di una ricerca con trattamento in via principale o come trattamento secondario compatibile di dati raccolti per altre precedenti finalità	Individuare se i dati che verranno trattati dovranno essere raccolti *ex novo* o se sono già stati trattati per altre finalità Nel secondo caso, valutazione della compatibilità della finalità di ricerca perseguibile con la finalità principale	Limitazione della finalità e accountability Art. 5, par. 1, lett. B) GDPR

(*continua...*)

(*segue..*) **Tabella 5.1 – Analisi del trattamento dei dati**

Fase	Raccomandazione	Descrizione	Principio e norme rilevanti
Prima dell'inizio	Mappare le caratteristiche del trattamento, ossia natura, ambito e contesto del trattamento	Limitazione dei dati da raccogliere a quanto necessario per il conseguimento delle finalità Individuazione della quantità di dati necessaria per la finalità Individuazione di categorie di dati personali: comuni o particolari, e quali tipologie di dati particolari (con attenzione a dati biometrici, genetici, relativi alla salute) Individuazione delle categorie di interessati: minori d'età e/o maggiori d'età Chiarire se i dati personali si riferiscono a persone in vita o decedute Chiarire se i dati si riferiscono a soggetti vulnerabili: minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo Limitazione dell'ambito territoriale (entro e/o fuori lo SEE) Chiarire la modalità di raccolta dei dati: presso o non presso l'interessato	Liceità, minimizzazione e accountability Art. 9 GDPR Artt. 2-*quater*, 2-*septies* Codice Privacy Regole deontologiche del Garante in materia di dati particolari
Prima dell'inizio	Mappare il flusso dei dati personali che verranno raccolti e delle operazioni	Individuazione delle separate tipologie di operazioni di trattamento, come raccolta, conservazione, comunicazioni (anche in banche dati in open access), diffusioni, trasferimenti transfrontalieri, profilazione, pseudonimizzazione Particolare attenzione alle modalità di raccolta dei dati personali (es. registrazioni, *trial* clinici, etc.) Particolare attenzione in caso di processi automatici di decisione e profilazione, per l'individuazione di rischi per i diritti e le libertà Definire le modalità di comunicazione e diffusione dei dati nel progetto di ricerca Il flusso dei dati personali potrebbe essere descritto attraverso diagrammi	Accountability, minimizzazione I dati genetici, biometrici e relativi alla salute non possono essere diffusi, Art. 2-*septies* Codice Privacy Art. 22 GDPR
Prima dell'inizio	Definire e mappare i mezzi del trattamento	Individuazione dei mezzi (automatizzati o non) del trattamento e degli strumenti informatici e delle infrastrutture con cui verranno svolte le operazioni	Accountability
Prima dell'inizio	Definire le basi giuridiche	Individuare una base giuridica per ogni attività di trattamento. Si v. tabella apposita	Liceità Artt. 6-10, 89 GDPR
Prima dell'inizio	Definire il periodo di conservazione dei dati e le modalità	Individuazione del tempo di termine di conservazione dei dati personali o criteri necessari per poterlo determinare I dati per finalità di ricerca potranno essere conservati anche oltre il tempo di conservazione originario previa l'adozione di misure tecniche e organizzative adeguate Definizione delle modalità di conservazione del dato (es. database)	Limitazione della conservazione Art. 5, par. 1, lett. E) GDPR Art. 99 Codice Privacy

(*continua...*)

(*segue…*)

Fase	Raccomandazione	Descrizione	Principio e norme rilevanti
Prima dell'inizio	Mappare i ruoli privacy	Individuazione dei ruoli di titolare del trattamento, responsabile del trattamento, responsabile della protezione dei dati – DPO, incaricati e autorizzati all'interno del progetto di ricerca Individuazione di eventuali co-titolari del trattamento all'interno del progetto di ricerca	Accountability Artt. 26, 28 GDPR
Prima dell'inizio	Assegnare le responsabilità privacy all'interno e all'esterno dell'organizzazione del titolare	Allocazione dei compiti relativi alla protezione dei dati personali all'interno e all'esterno dell'organizzazione del titolare	Accountability
Prima dell'inizio	Effettuare la valutazione d'impatto del trattamento – DPIA, quando necessario	Individuazione dei rischi e valutazione del loro impatto, con scelta delle misure appropriate per affrontarli In generale, i rischi sono maggiori in caso di progetti di ricerca che trattano categorie particolari di dati personali, di categorie vulnerabili di soggetti (come i minori), di trattamenti su larga scala di dati, di utilizzo di tecniche automatizzate che impattino i diritti e le libertà degli interessati Valutazione se il trattamento rientra nella categoria di attività che sempre richiedono la DPIA secondo le autorità europee e il Garante La valutazione deve essere compiuta per tutte le attività di trattamento del progetto	Accountability Art. 35 GDPR
Prima dell'inizio	Individuare le misure di DPbD, valutando stato dell'arte e costi di attuazione, predisponendo un *budget* privacy	Individuazione dei rischi del trattamento per le libertà e i diritti degli interessati, con scelta delle misure appropriate per affrontarli in ottica di protezione by design	Accountability Art. 25 GDPR
Prima dell'inizio	Individuare le misure di sicurezza, valutando stato dell'arte e costi di attuazione, predisponendo un *budget* per la sicurezza	Individuazione dei rischi di sicurezza e valutazione del loro impatto, con scelta delle misure appropriate per affrontarli Differenziare a seconda dei database utilizzati, categorie di dati, standard e protocolli applicabili	Integrazione e riservatezza Art. 32 GDPR
Prima dell'inizio	Individuare i diritti che operativamente potranno essere esercitati dagli interessati Chiarire le modalità di esercizio dei diritti	Individuazione di quali tra i diritti riconosciuti in materia di protezione dei dati personali sono applicabili, tenuto conto delle deroghe presenti in ambito di ricerca Individuazione delle misure necessarie perché questi diritti possano essere operativi (es. diritto di accesso, anche alle informazioni sulla logica dell'algoritmo)	Artt. 13-22 GDPR

Tabella 5.2 – Basi giuridiche del trattamento. Alcune esemplificazioni

Tipologia di progetto di ricerca	Base giuridica	Riferimento normativo
Progetto di ricerca con dati personali comuni	Consenso sulla base di adeguata informativa che descriva la finalità di ricerca (no *broad consent*) La finalità deve essere il più possibile specifica. Se non fosse possibile, sarebbe necessario quantomeno definire il settore scientifico-disciplinare della ricerca scientifica o la parte del progetto di ricerca a cui prestare consenso Obbligo legale previsto da una specifica normativa Esecuzione di un interesse pubblico (es. ricerca base dell'università o di un centro di ricerca) Legittimo interesse di enti privati per la ricerca, ma non in caso di autorità pubbliche. Dovrà essere compiuto un test comparativo tra gli interessi del titolare e degli interessati, perché gli ultimi non prevalgono	Art. 6 GDPR Art. 2-*quinquies*, co. 2, lett. cc) Codice Privacy: interesse pubblico rilevante per i trattamenti effettuati a fini di archiviazione o ricerca storica "concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato, negli archivi storici di enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante", e per i trattamenti per fini di ricerca scientifica e a fini statistici da parte di soggetti del Sistan
Progetto di ricerca con categorie particolari di dati personali	Consenso esplicito sulla base di adeguata informativa che descriva la finalità di ricerca con maggior dettaglio possibile e si riferisca alle tipologie di dati particolari trattati Legge nazionale o europea che autorizzi il trattamento di particolari categorie di dati per finalità di ricerca e preveda misure adeguate	Art. 9, par. 2, lett. a) GDPR per consenso Art. 9, par. 2, lett. j) e 89 GDPR esplicitamente dedicati a trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. La legge nazionale o dell'UE dovrà essere proporzionata alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato
Progetto di ricerca in ambito medico, biomedico ed epidemiologico	Consenso, a meno che: Ricerca rientri in un programma finalizzato ai sensi dell'art. 12-bis D.Lgs. 502/1992 e venga condotta e resa pubblica una DPIA Ricerca in relazione alla quale, per particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure informarli rischia di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità della ricerca stessa. La ricerca dovrà, tuttavia, essere approvata dal comitato etico e dovrà essere compiuta una DPIA sottoposta a preventiva consultazione del Garante	Art. 110 Codice Privacy Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, e Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica

(*continua...*)

(*segue…*)

Tipologia di progetto di ricerca	Base giuridica	Riferimento normativo
Progetto di ricerca scientifica o statistica da parte di soggetti terzi che svolgono principalmente ricerche scientifiche o statistiche, anche su dati particolari Sono esclusi i trattamenti per l'attività clinica a fini di ricerca, effettuati da istituti di ricovero e cura a carattere scientifico, pubblici e privati	Art. 89 GDPR e su richiesta, autorizzazione preventiva del Garante se informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità della ricerca, e vengano adottate misure appropriate a tutela dei dati come minimizzazione e anonimizzazione Art. 89 GDPR e autorizzazione generale del Garante per categorie di titolari del trattamento con particolari misure da applicare	Art. 110-*bis* Codice Privacy
Progetto di ricerca su dati personali pubblicamente accessibili	Se i dati sono stati resi manifestamente pubblici dall'interessato, il consenso non è necessario e i dati, anche se particolari, potranno essere trattati dal titolare senza altra base giuridica, ma verificando la possibilità di trattarli da chi gestisce la banca dati	Art. 9, par. 2, lett. e) GDPR

Tabella 5.3 – Focus esemplificativo: trattamento di dati personali in ambito medico, biomedico ed epidemiologico, Art. 110 Codice Privacy

Contesto	Soggetti	Passi applicativi e misure
Ricerca in ambito medico, biomedico ed epidemiologico ▪ che tratterà dati personali, anche dati particolari (Art. 9 GDPR) ▪ effettuata in base a disposizioni di legge nazionali o europee o nel contesto di un programma nazionale di ricerca biomedica e sanitaria (Art. 12 *bis* D.Lgs. 502/1992)	Soggetti privati e pubblici senza raccogliere il consenso degli interessati	Conduzione e pubblicazione di una DPIA (Artt. 35 e 36 GDPR)
Ricerca in ambito medico, biomedico ed epidemiologico ▪ che tratterà dati personali, anche dati particolari (Art. 9 GDPR) ▪ in cui per particolari ragioni informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità della ricerca	Soggetti privati e pubblici senza raccogliere il consenso	Motivato parere favorevole del comitato etico territorialmente competente sul programma di ricerca Adozione di misure appropriate a protezione dei dati Consultazione preventiva del Garante sulla DPIA (Art. 36 GDPR)

Tabella 5.4 – Focus esemplificativo: trattamento ulteriore da parte di terzi di dati personali ai fini di ricerca scientifica o a fini statistici, Art. 110-bis Codice Privacy

Contesto	Soggetti	Passi applicativi e misure
Ricerca scientifica o statistica ▪ che tratterà dati personali, anche dati particolari (Art. 9 GDPR) ▪ in cui per particolari ragioni informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità della ricerca	Soggetti terzi ▪ diversi dal titolare che ha raccolto i dati per una finalità in via principale; ▪ che intendono realizzare un trattamento ulteriore di dati (in via secondaria) per finalità di ricerca; ▪ che svolgono come attività principalmente ricerche scientifiche o statistiche; ▪ diversi da istituti di ricovero e cura a carattere scientifico, pubblici e privati che raccolgono dati per l'attività clinica e li trattano anche a fini di ricerca	Autorizzazione preventiva e vincolante del Garante per la protezione dei dati personali ▪ entro 45 giorni dalla richiesta; ▪ meccanismo del silenzio-dissenso; ▪ indicazione di misure e condizioni, anche di sicurezza Adozione di misure appropriate a protezione dei dati, come preventiva minimizzazione, pseudonimizzazione o anonimizzazione
Ricerca scientifica o statistica ▪ che tratterà dati personali, anche dati particolari (Art. 9 GDPR) ▪ in cui per particolari ragioni informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento della finalità della ricerca	Soggetti terzi ▪ diversi dal titolare che ha raccolto i dati per una finalità in via principale; ▪ che intendono realizzare un trattamento ulteriore di dati (in via secondaria) per finalità di ricerca; ▪ che svolgono principalmente ricerche scientifiche o statistiche; ▪ diversi da istituti di ricovero e cura a carattere scientifico, pubblici e privati che raccolgono dati per l'attività clinica e li trattano anche a fini di ricerca; ▪ che rientrano in una delle categorie di soggetti prevista da una autorizzazione generale del Garante o che effettueranno un trattamento specifico previsto da una autorizzazione	Autorizzazione generale del Garante per la protezione dei dati personali adottata d'ufficio ▪ in relazione a determinate categorie di titolari e di trattamenti; ▪ indicazione di misure e garanzie; ▪ pubblicazione in Gazzetta Ufficiale

Tabella 5.5 Predisposizione documentale del trattamento dei dati

Fase	Raccomandazione	Descrizione	Principio
Prima dell'inizio	Inserire gli aspetti privacy nel progetto di ricerca (*data management plan*)	Predisposizione documentale relativa al trattamento dei dati nel progetto di ricerca	Accountability
Prima dell'inizio	Ricevere l'approvazione del comitato etico territorialmente competente Richiesta obbligatoria per ricerche in ambito medico, biomedico ed epidemiologico	Qualora sia necessario, richiesta e approvazione del comitato etico sul progetto di ricerca Tenere conto anche degli aspetti etici e dell'integrità della ricerca (*ethics self assessment)*	Accountability Art. 110 Codice Privacy
Prima dell'inizio	Redigere l'informativa privacy	Predisposizione delle informative privacy: ▪ informativa per dati raccolti presso l'interessato ▪ informativa per dati raccolti presso soggetti terzi diversi dall'interessato ▪ informativa per interessati minorenni Le informative dovrebbero essere chiare, comprensibili e modulari	Trasparenza Artt. 12-14 GDPR
Prima dell'inizio	Preparare (eventuale) modulo consenso	Predisposizione del modulo per il consenso dell'interessato (adulto o minore) Il modulo deve essere separato rispetto al modulo di assenso alla partecipazione al progetto di ricerca	Liceità Artt. 6 o 9 GDPR
Prima dell'inizio	Predisporre i contratti e le "deleghe" relative al trattamento dei dati	Predisposizione di: ▪ contratto con il responsabile del trattamento; ▪ accordo con eventuali contitolari del trattamento; ▪ deleghe interne agli autorizzati e agli incaricati; ▪ contratto con DPO	Accountability Artt. 26, 28 GDPR
Prima dell'inizio	Se applicabile, predisporre il registro del trattamento dei dati	Predisposizione del registro del trattamento sulla base delle valutazioni prima effettuate sulle caratteristiche	Accountability Art. 30 GDPR
Prima dell'inizio	Predisporre schede privacy di istruzione per incaricati al trattamento	Predisposizione di documenti in tema di buone prassi all'interno dell'organizzazione del titolare	Accountability
Prima dell'inizio	Predisporre policy del progetto sulla disseminazione dei risultati della ricerca e di *open access* e *open data*	Predisposizione delle policy affinché le pubblicazioni siano in *open access* e l'accesso ai dati relativi alla ricerca sia aperto, secondo particolari garanzie	Accountability Disciplina Open Access
Durante e dopo	Conservazione della documentazione privacy anche oltre la conclusione del programma di ricerca	Conservazione in forma riservata della documentazione privacy per un tempo definito dopo la conclusione del progetto di ricerca	Accountability

Tabella 5.6 – Punti chiave informativa privacy

Elemento chiave	Principali riferimenti (Artt. 12-14 GDPR)
Identità e contatti del titolare del trattamento	Art. 4, n. 7) GDPR
Identità e contatti del responsabile di protezione dati (DPO)	Art. 4, n. 8) GDPR
Categoria di dati personali trattati e fonti	Art. 4, n. 1), 13), 14), 15)
Basi giuridiche del trattamento per ciascuna operazione di trattamento e finalità	Artt. 6-11 GDPR
Finalità del trattamento, se non fosse possibile individuare pienamente la finalità al momento della raccolta dei dati è necessario definire settore scientifico-disciplinare o finalità di parte del progetto	Art. 5, par. 1, lett. b) GDPR
Modalità di trattamento dei dati personali, incluse elaborazioni, diffusioni e conservazioni, ed esistenza di processi decisionali automatizzati; in caso di profilazione specificazione della logica utilizzata l'importanza per il trattamento e le conseguenze per l'interessato	Art. 4, n. 2) GDPR
Destinatari dei dati personali, o categorie di destinatari, e interazione con soggetti coinvolti nel progetto	Art. 4, n. 9), 10) GDPR
Eventuale trasferimento dei dati all'estero	Art. 4, n. 23) GDPR
Definizione del periodo di conservazione dei dati	Art. 5, par. 1, lett. e) GDPR
Definizione dei diritti dell'interessato e modalità di loro esercizio	Artt. 12-22 GDPR
Definizione delle misure di sicurezza	Artt. 5, par. 1, lett. f), 32 GDPR

Tabella 5.7 Predisposizione strumenti informatici

Fase del trattamento	Raccomandazione	Descrizione	Principio
Prima dell'inizio del trattamento	Mappare il flusso dei dati personali dal punto di vista tecnico e gli strumenti per trattarli	Mappatura dei dati secondo gli stati: *at rest, in use, in transit* Mappatura degli strumenti informatici (database, software, cloud, ecc.)	Accountability e sicurezza
Prima dell'inizio del trattamento e durante il trattamento	Valutare i rischi per la sicurezza dei dati e implementare le misure di sicurezza relative a conservazione, utilizzo e trasmissione di dati	Implementazione delle misure adeguate per mitigare i rischi di sicurezza, quali: ▪ per conservazione: pseudonimizzazione, crittografia, separazione dei database, *backup* e *recovery systems*, *intrusion control systems*, *audit* e *log systems* ▪ per utilizzo e accesso: *access control system*, *identity control system*, *authentication system* ▪ per trasmissione e comunicazione: *Secure transmission network*	Riservatezza, integrità, confidenzialità Art. 32 GDPR
Prima dell'inizio del trattamento e durante il trattamento	Valutare di utilizzare standard, certificazioni o codici di condotta	Eventualmente applicare standard e richiedere all'organismo di accreditamento di ottenere una certificazione	Accountability Artt. 25, par. 3, 42-45 GDPR
Durante il trattamento - ricerca	Mantenere le misure tecniche e aggiornarle se necessario	Aggiornamento delle misure tecniche, effettuando anche test di monitoraggio della sicurezza	Accountability e sicurezza Art. 32 GDPR

Tabella 5.8 – Buone prassi del trattamento

Fase	Raccomandazione	Descrizione	Principio
All'inizio del trattamento	Consegnare l'informativa del trattamento	Consegna dell'informativa all'interessato Se la comunicazione dell'informativa per dati raccolti presso soggetti terzi diversi dall'interessato risulti impossibile o pregiudichi gravemente il conseguimento delle finalità di archiviazione, ricerca scientifica o statistica, il titolare del trattamento può essere sollevato dall'obbligo di fornire le informazioni, ma dovranno essere adottate altre forme di pubblicità (es. pubblicazione su un quotidiano di larga diffusione di un annuncio sul progetto di ricerca)	Accountability
All'inizio del trattamento	Consegnare i moduli relativi al consenso dell'interessato	Raccolta del consenso dell'interessato	Accountability
Durante il trattamento – ricerca	Verifica dell'impostazione sui ruoli privacy	Monitoraggio degli incarichi e dei ruoli privacy	Accountability
Durante il trattamento – ricerca	Organizzazione di corsi di formazione per incaricati e soggetti con ruoli privacy	Formare in ambito di protezione dei dati personali e sicurezza i soggetti coinvolti nel trattamento	Accountability
Durante il trattamento – ricerca	Aggiornamento della documentazione privacy	Monitoraggio e aggiornamento di informative, moduli consenso, autorizzazioni interne ed esterne all'organizzazione del titolare, documenti sulle buone prassi, registro del trattamento	Accountability
Durante il trattamento – ricerca	Valutazione di chi può avere legittimo accesso ai dati personali all'interno del progetto di ricerca (*data sharing agreement*)	Restrizione dell'accesso a eventuali banche dati del progetto soltanto a chi è specificatamente autorizzato dal responsabile del progetto e per determinati dati personali	Riservatezza Art. 29 GDPR
Durante il trattamento – ricerca	Comunicare i dati personali a partner di progetto solo quando necessario e in presenza di adeguate garanzie	Comunicazione di dati personali soltanto qualora sia necessario per la finalità del progetto di ricerca e per le attività dello stesso Comunicazione sicura dei dati, valutando l'applicazione di misure tecniche quali cifratura o pseudonimizzazione	Riservatezza
Durante il trattamento – ricerca	Comunicare i dati personali a pubbliche amministrazioni e altri soggetti pubblici o privati solo quando necessario e in presenza di adeguate garanzie	Comunicazione di dati personali soltanto qualora si necessario per la finalità del progetto di ricerca e per le attività dello stesso Comunicazione sicura dei dati, valutando l'applicazione di misure tecniche quali cifratura o pseudonimizzazione	Riservatezza

(*continua...*)

(*segue…*) **Tabella 5.8 – Buone prassi del trattamento**

Fase	Raccomandazione	Descrizione	Principio
Durante il trattamento – ricerca e dopo il trattamento	Diffondere i dati personali e i risultati della ricerca solo in forma aggregata e anonimizzata con tecniche che assicurino la non identificazione degli interessati Diffondere i dati sui risultati della ricerca in banche dati ad accesso aperto per replicare e verificare le analisi sui dati, in presenza di adeguate garanzie	I dati genetici, biometrici e relativi alla salute non possono essere in alcun modo diffusi, e gli altri dati personali non dovrebbero essere diffusi a meno che non si applichino tecniche di anonimizzazione efficaci o non sia richiesto da un obbligo legale Diffusione dei dati relativi ai risultati della ricerca in forma aggregata e anonimizzata in banche dati ad accesso aperto	Riservatezza
Durante il trattamento – ricerca	Trasferire i dati all'esterno dello Spazio Economico Europeo soltanto in applicazione di adeguate garanzie previste dalla normativa e per le finalità del progetto di ricerca	Se possibile, evitare di trasferire dati personali all'esterno dello Spazio Economico Europeo Se necessario trasferire i dati all'estero, scegliere la base giuridica per il trasferimento, effettuare una valutazione dei rischi del trasferimento e implementare adeguate misure tecniche e organizzative a protezione dei dati affinché all'estero siano trattati con un livello adeguato di protezione	Liceità, Accountability
Durante il trattamento – ricerca	Comunicare eventuali casi di violazione di dati personali	Comunicazione degli incaricati e autorizzati al trattamento di eventuali violazioni di dati personali durante il progetto (es. *data breach*) Eventuale comunicazione della violazione al Garante	Integrità e riservatezza Art. 34 GDPR
Alla conclusione del trattamento – ricerca	Cancellare, anonimizzare o conservare i dati personali per una durata massima di tempo e per una precisa finalità	Al termine del progetto di ricerca i dati personali dovranno essere cancellati, anonimizzati o conservati per un tempo massimo per una specifica finalità e in presenza di particolari garanzie a loro protezione	Liceità, Limitazione delle finalità, Integrità e Riservatezza

BIBLIOGRAFIA

Alpa A., Resta G. (2020), *Le persone e la famiglia 1. Le persone fisiche e i diritti della personalità, seconda edizione*. Milano: Wolters Kluwer.

Angiolini C. (2020), *Lo Statuto dei dati personali. Uno studio a partire dalla nozione di bene*. Torino: Giappichelli.

Bianca C.M., Busnelli F.D. (a cura di) (2007), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*. Padova: CEDAM.

Bincoletto G. (2019), *La privacy by design. Un'analisi comparata nell'era digitale*. Roma: Aracne Editrice.

Bincoletto G. (2020), European Union EDPB Guidelines 4/2019 on Data Protection by Design and by Default. *EDPL*, 6, 4: 574-579 – Doi: 10.21552/edpl/2020/4/14.

Bincoletto G. (2021), *Data protection by design in the e-health care context: theoretical and applied perspectives*. Baden-Baden: Nomos – Doi: 10.5771/9783748929895

Bincoletto G., Guarda P. (2021), A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data. *Opinio Juris in Comparatione*, 1, 1: 43-76.

Borgesius F.Z., Gray J., van Eechoud M. (2016), Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework. *Berkeley Technology Law Journal*, 30, 2: 2079.

Bradford A. (2020), *The Brussels effect: How the European Union rules the world*. Oxford: Oxford University Press – Doi: 10.1093/oso/9780190088583.001.0001.

Bygrave L., Tosoni L. (2020), Art. 4 (13) Genetic data. In: Kuner C*., Bygrave L.A., Docksey C., Drechsler L.* (eds.), *The EU General Data Protection Regulation (GDPR). A Commentary*. Oxford: Oxford University Press. 197-206 – Doi: 10.1093/oso/9780198826491.003.0019.

Cardarelli F., Sica S., Zeno-Zencovich V. (a cura di) (2004), *Il codice dei dati personali. Temi e problemi*. Milano: Giuffrè.

Casonato C., Tomasi M. (2019), Diritti e ricerca biomedica: una proposta verso nuove conoscenze. *BioLaw Journal – Rivista di Biodiritto*, 1: 343-358 – Doi: 10.15168/2284-4503-368.

Cavoukian A. (2010), Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society*, 3, 2: 247-251 – Doi: 10.1007/s12394-010-0062-y.

Comandé G. (2019), Ricerca in sanità e data protection… un puzzle risolvibile. *Rivista Italiana di Medicina Legale*, XLI, 1: 187-207 – http://hdl.handle.net/11382/528989.

Comandé G., Malgieri G. (2018), *Guida al trattamento ed alla sicurezza dei dati personali. Le opportunità e le sfide del Regolamento UE e del codice italiano riformato*. Milano: Il Sole 24 Ore.

Cuffaro V., D'Orazio R., Ricciuto V. (a cura di) (2019), *I dati personali nel diritto europeo*. Bologna: Giappichelli.

D'Acquisto G., Naldi M. (2017), *Big Data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*. Torino: Giappichelli Editore.

D'Orazio R., Finocchiaro G., Pollicino O., Resta G. (a cura di) (2021), *Codice della privacy e data protection*. Milano: Giuffré.

Dos Santos C. (2012), On Privacy and Personal Data Protection as Regards Re-use of Public Sector Information (PSI). *Masaryk University Journal of Law and Technology,* 6, 3: 337.

Dove E.S. (2018), The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *The Journal of Law, Medicine &* Ethics, 46, 4: 1013-1030 – Doi: 10.1177/1073110518822003.

Ducato R. (2020), Data protection, scientific research and the role of information. *Computer Law and Security Review*, 37. Doi: 10.1016/j.clsr.2020.105412.

Faini F. (2019), *Data society. Governo dei dati e tutela dei diritti nell'era digitale.* Milano: Giuffrè.

Finck M., Pallas. F. (2020), They who must not be identified – Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10: 1, 11-36 – Doi: 10.1093/idpl/ipz026.

Finocchiaro G. (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*. Bologna: Zanichelli.

Finocchiaro G. (2019), Il principio di accountability. *Giurisprudenza Italiana*, 171, 12: 2778-2782.

Floridi L. (2020), What the Near Future of Artificial Intelligence Could Be. In: Burr C., Milano S. (eds.), *The 2019 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook*. Cham: Springer Publishing – Doi: 10.1007/978-3-030-29145-7_9.

Galetta D.U. (2019), "Open Government", "Open Data" e azione amministrativa. *Istituzioni del Federalismo*, 3: 663-683.

Gold E.R. (2016), Accelerating Translational Research through Open Science: The Neu Experiment. *PLoS Biology*, 14, 12: e2001259. Doi: 10.1371/journal.pbio.2001259.

Granieri M. (2017), Il trattamento di categorie particolari di dati personali nel Regolamento UE 2016/679. *Le Nuove leggi civili commentate*, 1: 165-190.

Green B., Cunningham G., Ekblaw A., Kominers P., Linzer A., Crawford S.P (2017), Open Data Privacy. Berkman Klein Center for Internet & Society Research. Berkman Klein Center Research, *Harvard Public Law Working Paper* n. 17-07 – Doi: 10.2139/ssrn.2924751.

Guarda P. (2017), Privacy e protezione dei dati personali. In: Benacchio G.A., Casucci F. (a cura di), *Temi e Istituti di Diritto Privato dell'Unione Europea*. Torino: Giappichelli. 133-152.

Guarda P. (2019), I dati sanitari. In: Cuffaro V., D'Orazio R., Ricciuto V. (a cura di), *I dati personali nel diritto europeo*. Torino: Giappichelli. 591-626.

Guarda P. (2020), "Free data?" Open science in the age of personal data protection. In: Rooksby J.H. (ed.), *Research Handbook on Intellectual Property and Technology Transfer*. Cheltenham: Edward Elgar Publisher. 391-410 – Doi: 10.4337/9781788116633.00028.

Guarda P. (2021), *Il regime giuridico dei dati della ricerca scientifica*. Trento: Editoriale Scientifica.

Hoffman S. (2015), Citizen Science: The Law and Ethics of Public Access to Medical Big Data. *Berkeley Technology Law Journal*, 30, 3: 1741-1805 – Doi: http://dx.doi.org/10.15779/Z385Z78.

Kuner C., Bygrave L.A., Docksey C., Drechsler L. (eds.) (2020), *The EU General Data Protection Regulation: a Commentary*. Oxford: Oxford University Press – Doi: 10.1093/oso/9780198826491.001.0001.

Minazzi F. (2013), Il principio dell'Open Data by Default nel Codice dell'Amministrazione digitale: profili interpretativi e questioni metodologiche – www.federalismi.it.

Owens B. (2016), Montreal Institute going "open" to accelerate science. *Science*, 351: 6271 – science.sciencemag.org – Doi: 10.1126/science.351.6271.329.

Paparella N. (2014), *A proposito della Terza missione. Una nuova versione del modello della tripla elica*. Napoli: Giapeto.

Pormeister K. (2017), Genetic data and the research exemption: Is the GDPR going to far? *International Data Privacy Law*, 7, 2: 137-146 – Doi: 10.1093/idpl/ipx006.

Poupon V., Seyller A., Rouleau G. A. (2017), The Tanenbaum Open Science Institute: leading a paradigm shift at the Montreal Neurological Institute. *Neuron*, 95, 5: 1002-1006 – Doi: 10.1016/j.neuron.2017.07.026.

Quinn P., Quinn L. (2018), Big genetic data and its big data protection challenges. *Computer Law & Security Review*, 34, 5: 1000-1018 – Doi: 10.1016/j.clsr.2018.05.028.

Risdale C. (2016), Open Science, Open Data: Lessons from the Montreal Neurological Institute. Research Data Canada – www.rdc-drc.ca.

Sanna R. (2019), *Dalla trasparenza amministativa ai dati aperti. Opportunità e rischi delle autostrade informatiche*. Torino: Giappichelli Editore.

Solove D.J., Schwartz P.M. (2018), *Information Privacy Law*. Aspen: Wolters Kluwer.

Stalla-Bourdillon S., Knight A. (2017), Anonymous data v. personal data, a false debate: an EU perspective on anonymization, pseudonymization and personal data. *Wisconsin International Law Journal*, 34, 2: 284-322.

Staunton C., Slokenberga S., Mascalzoni D. (2019), The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics*, 27: 1159-1167 – Doi: 10.1038/s41431-019-0386-5.

Strowel A. (2018), Big data and data appropriation in the EU. In: Aplin T. (ed.), *Research handbook on Intellectual Property and Digital Technologies*. Camberley: Edward Elgar. 107-134 – Doi: 10.4337/9781785368349.00013.

van Eechoud M., van Velze S., Caspers M., Eskens S.J., Leerssen P., Austere L. (2014), *LAPSI Position Paper on Access to Data*, in Rete: lib.uva.nl/discovery.

Normativa e documenti in ambito europeo

Article29 Working Party (2015), A*NNEX – health data in apps and devices. Annex to the letter of 5.2.2015*.

Article29 Working Party (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, adottate il 13 ottobre 2017.

Article29 Working Party (2013), *Opinion 3/2013 on purpose limitation*, adottata il 2 aprile 2013 – ec.europa.eu/justice/article-29.

Article29 Working Party (2014), *Parere 5/2014 del Gruppo di lavoro Articolo 29 sulle tecniche di anonimizzazione, adottato il 10 aprile 2014* – ronchilegal.eu/wp-content/.

Article29 Working Party (2014), *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9 aprile 2014 – ec.europa.eu/justice/article-29/.

Commissione Europea (2019), *Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM/2019/250 final – eur-lex.europa.eu/legal-content/.

Commissione Europea (2019), *Directorate-General for Research and Innovation, European Open Science Cloud (EOSC) strategic implementation plan* – Doi: 10.2777/202370.

Commissione Europea (2017), *EOSC Declaration*, 26 ottobre 2017 – ec.europa.eu/research/openscience/pdf.

Commissione Europea (2020), *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)*, COM/2020/767 – eur-lex.europa.eu/legal-content.

UE – Unione Europea (2019), *Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico*. PE/28/2019/REV/1. GU L 172 del 26.6.2019 – ELI: data.europa.eu/eli/dir/2019/1024/oj.

UE – Unione Europea (1996), *Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati*. GU L 172 del 27.03.1996 – eur-lex.europa.eu/legal-content/.

EDPB – European Data Protection Board (2021), *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adottate il 2 Febbraio 2021 – edpb.europa.eu.

EDPB – European Data Protection Board (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, adottate il 4 April 2017 – ec.europa.eu/newsroom/article29/.

EDPB – European Data Protection Board (2020), *Linee guida 04/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, Versione 2.0, adottate il 20 ottobre 2020 – edpb.europa.eu.

EDPB – European Data Protection Board (2020), *Linee guida 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 4 maggio 2020 – edpb.europa.eu.

EDPB – European Data Protection Board (2020), *Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19*, adottate il 21 aprile 2020 – edpb.europa.eu.

EDPB – European Data Protection Board (2020), *Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE*, adottate il 10 novembre 2020 – edpb.europa.eu.

EDPS – European Data Protection Supervisor (2017), *Opinion 10/2017 on safeguards and derogations under Article 89 GDPR in the context of a proposal for a Regulation on integrated farm statistics*, adottate il 20 Novembre 2017 – edpb.europa.eu.

EDPS – European Data Protection Supervisor (2020), *Preliminary opinion on data protection and scientific research*, adottate il 6 gennaio 2020 – edps.europa.eu/data-protection/.

Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio, dell'11 marzo 2009, *relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il Regolamento (CE) n. 322/97 del Consiglio, relativo alle statistiche comunitarie, e la decisione 89/382/CEE, Euratom del Consiglio, che istituisce un comitato del programma statistico delle Comunità europee*. GU L 87 del 31.3.2009 – ELI: http://data.europa.eu/eli/reg/2009/223/oj.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*. GU L 119 del 4.5.2016 – ELI: http://data.europa.eu/eli/reg/2016/679/oj.

Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, r*elativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio*. GU L 117 del 5.5.2017 – ELI: http://data.europa.eu/eli/reg/2017/745/oj.

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.* PE/53/2018/REV/1, GU L 303 del 28.11.2018 – ELI: http://data.europa.eu/eli/reg/2018/1807/oj.

Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, *sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE*. GU L 158 del 27.5.2014. GU L 158 del 27.5.2014 – ELI: http://data.europa.eu/eli/reg/2014/536/oj.

Trattato sull'Unione Europea (2020), (versione consolidata), C202/1 – ELI: http://data.europa.eu/eli/treaty/teu_2016/oj.

Normativa e documenti in ambito italiano

Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, pubblicato sulla G.U. n. 134 del 12 giugno 2014.

Garante per la protezione dei dati personali, Provvedimento n. 467 dell'11 ottobre 2018, doc. web n. 9058979, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*, pubblicato in G.U. n. 269 del 19 novembre 2018.

Garante per la protezione dei dati personali, *Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali n. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il D.Lgs. n. 101/2018 di adeguamento del Codice – 13 dicembre 2018: 4. Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016); 5. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica* (aut. gen. n. 9/2016)

Garante per la protezione dei dati personali, *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del D.Lgs. 10 agosto 2018, n. 101* – 19 dicembre 2018.

Garante per la protezione dei dati personali, *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale pubblicate ai sensi dell'art. 20, comma 4, del D.Lgs. 10 agosto 2018, n. 101* – 19 dicembre 2018.

D.Lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali. In particolare: Titolo V "Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici"*, artt. 97 – 110-*bis* .

D.Lgs. 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale*.

D.Lgs. 24 gennaio 2006, n. 36, *Attuazione della direttiva (UE) 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che ha abrogato la direttiva 2003/98/CE*.

D.Lgs. 14 marzo 2013, n. 33, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni note*.

D.L. 31 maggio 2021, n. 77, *Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure, convertito con modificazioni dalla L. 29 luglio 2021, n. 108*.

D.Lgs. 8 novembre 2021, n. 200, *Attuazione della direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico*.

L. 3 dicembre 2021, n. 205, *Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali*.

Altri contratti e documenti

European Archives Group (2018), *Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector*.

European Union Agency for Cybersecurity (2018), *Handbook on Security of Personal Data Processing*.

Gruppo di lavoro CODAU (2017), *Linee guida in materia di privacy e protezione dei dati personali in ambito universitario*, Versione 1.1 – novembre 2017.

APRE – Agenzia per la Promozione della Ricerca Europea (2021), *Linee Guida dell'APRE per l'Italia, per il trattamento dei dati personali nei progetti Horizon 2020*, "Progettazione e Consortium Agreement", "Implementazione, Sfruttamento dei risultati, Disseminazione e Comunicazione", "Project Management e Rendicontazione".

TIPIK Legal (2021), *Report on the implementation of specific provisions of the Regulation (EU) 2016/679*. Directorate – General for Justice and Consumers, Unit C.3 Data Protection.

I QUADERNI DELL'OSSERVATORIO

Nella Collana QUADERNI DELL'OSSERVATORIO sono stati pubblicati i seguenti titoli, scaricabili sul sito www.fondazionecariplo.it/osservatorio.

Quaderno N.1 Periferie, cultura e inclusione sociale

Quaderno N.2 Il valore potenziale dei lasciti alle istituzioni di beneficenza

Quaderno N.3 Stranieri si nasce...e si rimane?

Quaderno N.4 Oltre la famiglia: strumenti per l'autonomia dei disabili

Quaderno N.5 L'educazione finanziaria per i giovani

Quaderno N.6 Ricerca scientifica in ambito biomedico

Quaderno N.7 Servizi per l'infanzia

Quaderno N.8 Assicurazione per persone con disabilità e loro famiglie

Quaderno N.9 Progetti e politiche per la mobilità urbana sostenibile

Quaderno N.10 Le organizzazioni culturali di fronte alla crisi

Quaderno N.11 I Social Impact Bond

Quaderno N.12 Lavoro e Psiche. Un progetto sperimentale per l'integrazione lavorativa di persone con gravi disturbi psichiatrici

Quaderno N.13 Il bando "Audit energetico degli edifici di proprietà dei comuni piccoli e medi"

Quaderno N.14 Infrastrutture di ricerca in Italia

Quaderno N.15 Performance economica e sociale delle istituzioni di microfinanza: alcune evidenze empiriche

Quaderno N.16 Cessione della nuda proprietà da parte di soggetti fragili: il possibile ruolo di un soggetto dedicato

Quaderno N.17 Abitare leggero. Verso una nuova generazione di servizi per anziani

Quaderno N.18 Progetti culturali e sviluppo urbano. Visioni, criticità e opportunità per nuove politiche nell'area metropolitana di Milano

Quaderno N.19 Sperimentare politiche sociali innovative. Manuale introduttivo

Quaderno N.20 #BICIttadini. Interventi a favore della mobilità ciclistica

Quaderno N.21 Resilienza tra territorio e comunità. Approcci, strategie, temi e casi

Quaderno N.22 Favorire la coesione sociale con le biblioteche. Valutazione del bando

Quaderno N.23 Il “mercato” dei lasciti testamentari. Nuove stime per Italia e Lombardia (2014-2030)

Quaderno N.24 Il bando abitare sociale temporaneo. Mappatura e analisi dei progetti finanziati (2000-2013)

Quaderno N.25 Lo sviluppo dei Green Jobs. Uno scenario di evoluzione quantitativa e qualitativa e alcune ipotesi di adeguamento dei percorsi formativi

Quaderno N.26 House rich, cash poor. Come rendere liquida la ricchezza rappresentata dalla casa di abitazione

Quaderno N.27 Bando materiali avanzati 2003-2013. Progetti e risultati

Quaderno N.28 Sperimenta, impara, adatta. Sviluppare politiche pubbliche con gli esperimenti randomizzati controllati

Quaderno N.29 Conoscere per conservare. 10 anni per la Conservazione Programmata

Quaderno N.30 Il collocamento mirato e le convenzioni ex-art.14. Evidenze e riflessioni

Quaderno N.31 Fondazioni di comunità. L’esperienza di Fondazione Cariplo

Quaderno N.32 Prendiamoci un caffè. I luoghi del welfare nel Bando Welfare in azione

Quaderno N.33 Ricerca scientifica in ambito biomedico. Progetti e risultati del Bando 2001-2013

Quaderno N.34 Tecniche di *nudging* in ambito ambientale. Una rassegna di esperienze e risultati

Quaderno N.35 L’impatto del Covid-19 sugli enti di terzo settore – Prime stime sui dati delle candidature al Bando LETS GO!

Quaderno N.36 Responsabilità sociale per la rigenerazione delle periferie – Imprese ed esperienze sul campo

Quaderno N.37 Tecnologie digitali e didattica laboratoriale nell’educazione STEM – Evidenze scientifiche e raccomandazioni pratiche

Quaderno N.38 Beni naturali e servizi ecosistemici – Riflessioni ed esperienze dalla comunità di pratica del bando Capitale Naturale

Quaderno N.39 L’invecchiamento in Lombardia – Tendenze demografiche e politiche pubbliche regionali per gli anziani non autosufficienti: quali lezioni per il futuro?

Quaderno N.40 La denatalità a Milano, Italia, Europa – Fatti, politiche, opzioni sperimentali

Quaderno N.41 Il valore della natura. Esperienze dalle comunità di pratica del bando Capitale Naturale

Quaderno N.42 Ricerca scientifica e protezione dei dati personali – Principi generali e raccomandazioni

Questo quaderno é scaricabile dal sito – *This document can be downloaded from*
www.fondazionecariplo.it/osservatorio

Può essere citato – Quote as:
Guarda P., Bincoletto G. (2023), RICERCA SCIENTIFICA E PROTEZIONE DEI DATI PERSONALI – Principi generali e raccomandazioni. Milano: Fondazione Cariplo.

ISBN: 979-12-80051-13-4

Fondazione
CARIPLO
TUTE SERVARE MUNIFICE DONARE • 1816

Fondazione Cariplo
Via Daniele Manin, 23
20121 Milano
www.fondazionecariplo.it
ISBN: 979-12-80051-13-4