Sommario

Premessa

Si propone con il presente documento un primo adeguamento delle istruzioni a suo tempo indirizzate agli incaricati del trattamento dei dati personali (adesso “persone autorizzate al trattamento”) con Provvedimento del Direttore Generale n. 187 del 30 marzo 2017.

Esso condivide con quel Provvedimento la convinzione che non una schematica serie di prescrizioni, quanto piuttosto solo una argomentata illustrazione dei principi posti a tutela del diritto alla protezione dei dati personali consenta una loro effettiva e consapevole attuazione, perseguendo insomma, come si auspicava un tempo, lo sviluppo di una cosiddetta “cultura della privacy”; una cognizione insomma che consenta un approccio verso le problematiche privacy sistematico e razionale, non integralista (o, all’opposto, di rifiuto), sostenuto dal principio della tutela dei diritti (complessivamente intesi) della persona e del bilanciamento degli interessi.

Indicazioni di carattere generale

1. Il quadro normativo

Le disposizioni in materia di diritto alla protezione delle persone fisiche rispetto al trattamento dei dati personali, attualmente vigenti sono le seguenti:

- il *Regolamento 2016/679/UE del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati* (di seguito: Regolamento Generale o Regolamento)[1];
- il D.Lgs. 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e 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* (di seguito: D.Lgs. 196/2003 o Codice).

Il Codice è stato adeguato al Regolamento Generale, a far data dal 19 settembre 2018, a mezzo del D.Lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205).

Si precisa che, ai sensi dell'art. 22 comma 4 del D.Lgs. 101/2018:

> A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto.

Inoltre, ai sensi dell'art. 22 comma 11 del D.Lgs. 196/2003:

> Le disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, relative al trattamento di dati genetici, biometrici o relativi alla salute continuano a trovare applicazione, in quanto compatibili con il Regolamento (UE) 2016/679, sino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2 -septies del citato codice, introdotto dall'articolo 2, comma 1, lett. e) del presente decreto.

L'art. 2-septies del Codice prevede che l'Autorità Garante adotti un provvedimento recante misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute.

Inutile dire che l'espressione "in quanto compatibili con il Regolamento" determina ampia incertezza sui possibili perduranti effetti di articoli formalmente già abrogati; si comprende lo scopo di voler fare salvi i

[1] Il Regolamento Generale è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è entrato in vigore il 24 maggio 2016 ed è divenuto definitivamente applicabile in via obbligatoria dal 25 maggio 2018.

provvedimenti già approvati dall'Autorità in base a tali articoli, ma la modalità scelta dal legislatore per raggiungere tale obiettivo – una sorta di abrogazione imperfetta, tipo "così è se vi pare" - sembra perlomeno bizzarra; e comunque, nell'ottica della responsabilizzazione, tali provvedimenti avrebbero potuto ben essere ancora utilmente presi in considerazione dai Titolari come esplicazione ed attuazione di quei principi che il nuovo Regolamento condivide con la Direttiva 95/46 (della cui abrogazione, questo sì, almeno siamo certi)[2].

2. Il diritto alla protezione dei dati personali

Tanto il Regolamento che il Codice, come d'altronde le disposizioni nazionali precedenti, inquadrano e sostengono il "diritto alla protezione dei dati personali" (il termine anglosassone *privacy* non è utilizzato dal legislatore europeo o nazionale) attraverso una difesa - una *protezione*, appunto - più estesa rispetto alla tutela della riservatezza, ovvero alla mera salvaguardia di un ambito di segretezza o comunque di un contesto "privato" e domestico (la privacy come "*right to let be alone*", come diritto *ad essere lasciati in pace*[3]).

Dalla constatazione obiettiva che la nostra rappresentazione sociale appare sempre più affidata ad informazioni sparse in una molteplicità di banche dati ed ai profili che su questa base sono costruiti, e che l'individuo tende ad essere risolto in un pacchetto di informazioni, ad essere proiettato in una sorta di "corpo elettronico" che offre un'immagine più o meno parziale della sua identità, di fatto affidata al modo in cui queste informazioni vengono trattate, collegate, fatte circolare, deriva l'esigenza di ampliare l'oggetto di una possibile tutela, rivendicando, quale indispensabile sviluppo di quell'*habeas corpus* dal quale si è storicamente sviluppata la libertà personale, una sorta di *habeas data*, e qualificando la tutela della persona rispetto al trattamento dei dati come un suo diritto fondamentale, una componente essenziale della nuova cittadinanza.

Nata come diritto dell'individuo ad escludere gli altri da ogni forma di invasione della propria sfera privata, la tutela della privacy si è dunque sempre più strutturata come diritto di chiunque ad un controllo sui dati che lo riguardino, ovunque essi si trovino.

Per l'ambito in cui intende affermarsi, e per i soggetti con (o contro) cui deve confrontarsi, la rivendicazione di un siffatto diritto è oggi realisticamente possibile solo se esercitata e perseguita non *uti singuli*, in una prospettiva solipsistica o idiosincratica, ma solo da parte di una persona intesa come "individuo sociale", nell'accezione dell'art. 2 Cost.. La normativa privacy, già a partire dalla Direttiva 95/46, garantisce d'altronde all'interessato

[2]Si tratta della *Direttiva del Parlamento Europeo e del Consiglio 95/46* del 24 ottobre 1995 relativa *alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati* (e delle sue conseguenti espressioni a livello nazionale, la L. 31 dicembre 1996 n. 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali,* e poi il Codice stesso nelle sue versioni precedenti al D.Lgs. 10 agosto 2018, n. 101).

[3] E' questa la notissima definizione proposta in *The Right to Privacy*, l'articolo – definito come il più influente della storia del diritto – pubblicato nel 1890 a firma di S. Warren e L. Brandeis sulla Harward Law Review. Il termine *alone* è da tradursi con "in pace", "indisturbati", piuttosto che, come spesso avviene, con "soli". *The Right to Privacy* identificava il nucleo fondamentale della privacy nella pretesa dell'individuo di essere lasciato libero da ingerenze non autorizzate, da parte tanto di soggetti privati come dello Stato, nella propria sfera intima/familiare, e nella facoltà di vietare la diffusione di notizie di carattere personale, riproducendo lo schema e gli strumenti di difesa della proprietà privata, la cui tutela si realizza appunto, in primo luogo, attraverso un diritto di esclusione (lat. *excludere*, con il significato di *proibire*, *impedire*). Si trattava dunque di un diritto declinato in una accezione sostanzialmente negativa (molto prossima alla attuale nozione di *diritto alla riservatezza*, pur se con essa non coincidente), anche se l'impostarlo comunque, già in quelle prime formulazioni, come diritto non sulle cose ma della persona consentì immediatamente di svilupparlo, più ampiamente, nella direzione dei diritti della personalità (passando, come è stato scritto, dalla cd. *privacy property* alla cd. *privacy dignity*).

una protezione che può prevalere su una sua opposta scelta: la nozione individualistica del diritto alla privacy è dunque oramai superata, e si prevede una tutela che si realizza non più soltanto attraverso strumenti di carattere contrattualistico (il consenso, appunto, che ha un ruolo sempre più residuale) ma in particolare attraverso una disciplina regolata, che un'autorità pubblica di controllo – il Garante per la protezione dei dati personali - implementa e sorveglia.

Pur se spesso si parla di *data protection*, di protezione dei dati personali, occorre non dimenticare che la tutela non è diretta ai dati, ma alla persona fisica cui i dati si riferiscono rispetto ad un loro (non lecito o scorretto) trattamento. Al centro dell'attenzione è posta dunque la persona, non i dati. E in effetti, il titolo completo del Regolamento Generale, pur se spesso riassunto in Regolamento sulla protezione dei dati, è infatti *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* …[4].

Diciamo, meglio, che la tutela può riguardare i dati solo nella misura in cui la loro protezione è strumentale alla tutela della persona cui essi si riferiscono (la qual cosa comporta anche il bilanciamento di tale tutela con quella di altri diritti della stessa persona, o anche di altri individui con i quali la persona si trova socialmente unita).

Inoltre, la centralità, nella disciplina, del *trattamento* ("protezione delle persone fisiche rispetto al *trattamento* dei dati personali) piuttosto che dei *dati personali* staticamente considerati, riflette il fatto che le normative sulla privacy muovono dall'assunto che nelle società (appunto) dell'informazione non è possibile isolare i dati personali e mantenerli intangibili (non è possibile, richiamando la risalente nozione sopra citata, essere "lasciati in pace"); di conseguenza, esse non nascono per proibire che i dati vengano trattati, ma perché possano essere utilizzati e circolare come è loro essenziale; ciò dovrà farsi, però, solo secondo principi e regole finalizzati alla tutela delle persone fisiche cui essi si riferiscono.

3. Dalla Direttiva al Regolamento

Gli sviluppi della rivoluzione tecnologica dell'ultimo decennio, che hanno portato in primo piano le problematiche legate ai caratteri (prima eccezionali) della delocalizzazione e della virtualizzazione (si pensi alle problematiche legate al *cloud computing*, alla geolocalizzazione, alla biometria, all'*e-Health*, al *m-Health*), hanno spinto la Commissione Europea verso un superamento della *Direttiva 95/46*, all'origine delle prime disposizioni

[4] Così era per la Direttiva UE 46/95, abrogata dal Regolamento (ed entrambi richiamano la *Convenzione di Strasburgo del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*). Alla Direttiva 46/95 si rifacevano tanto la L. 675/96 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* che il Codice; in questo, effettivamente, tale indicazione è in effetti andata perduta; è stata però in qualche modo recuperata dopo l'aggiornamento al Regolamento Generale effettuato con il D.Lgs. 101/2018, che ha ricompreso nella rubrica il richiamo integrale al Regolamento Generale. Tra l'altro, nella prima stesura della L. 675/96 l'espressione "protezione dei dati personali" non era presente, introdotta dall'art. 3, comma 1, D.Lgs. 9 maggio 1997, n. 123 (la L. 675/96 è entrata in vigore l'8 maggio 1997) in riferimento alla denominazione dell'Autorità, modificata da "Garante per la protezione delle persone e altri soggetti rispetto al trattamento dei dati personali" (in effetti un po' eccedente) a "Garante per la protezione dei dati personali".

nazionali in materia di protezione dei dati personali, a favore di un atto applicabile in via diretta in tutti i Paesi UE. Il Regolamento Generale ha dunque abrogato la Direttiva 95/46, ma con essa comunque condivide molti tratti, particolari e generali, e tra questi ultimi:

- la previsione di diverse modalità di legittimazione di un soggetto (il cd. *Titolare*, cfr. § 14) che effettua trattamenti di dati (ovvero che raccoglie, utilizza, elabora, archivia ecc. dati personali), delle quali il consenso dell'interessato ne rappresenta soltanto una, e non la più rilevante, in particolare relativamente agli enti pubblici;
- la tutela accordata alle sole persone fisiche (non agli enti collettivi);
- il riconoscimento di poteri di controllo direttamente al soggetto al quale i dati trattati si riferiscono (attraverso gli strumenti dell'informativa, del diritto d'accesso ai dati e, ove previsto, del consenso);
- l'istituzione di una autorità indipendente di controllo (nel nostro ordinamento, il *Garante per la protezione dei dati personali)*;
- uno specifico apparato sanzionatorio, ulteriore rispetto alle sanzioni civilistiche.

Si è preferita l'adozione di un Regolamento piuttosto che di una Direttiva in quanto un Regolamento entra direttamente in vigore nei paesi aderenti all'Unione (una Direttiva solo in casi particolari e residuali). E' ad ogni modo fatta salva la possibilità, per alcune materie di integrazioni da parte dei legislatori nazionali. Tale prerogativa è prevista all'art. 9 par. 4 del Regolamento, per il quale

> Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Si è visto sopra che il legislatore ha direttamente previsto, all'art. 2-septies del Codice, che il Garante predisponga le misure di garanzia (propriamente, il comma 1 dell'articolo perla di "misure di garanzia *disposte* dal Garante") in conformità delle quali devono eseguirsi i trattamenti di dati genetici, biometrici e relativi alla salute.

Un Regolamento Europeo (così come una Direttiva, peraltro) si struttura su una serie di Considerando e su un successivo articolato. Il § 2.2 del *Manuale interistituzionale di convenzioni redazionali dell'Unione Europea*, precisa che i considerando di un atto normativo indicano la motivazione dell'articolato dell'atto stesso. Nei Considerando si troverà dunque una contestualizzazione ed una esplicazione delle disposizioni dettate negli articoli veri e propri, e devono essere analizzati assieme all'articolo o agli articoli cui si riferiscono, per poter individuare correttamente la norma da essi complessivamente posta.

4. Garante per la protezione dei dati personali

Un punto qualificante della Direttiva 95/46/CE era la previsione di un apposito organismo di garanzia e tutela dei diritti, posto in condizione di poter agire in modo indipendente; tale organismo è tutt'oggi rappresentato, nel nostro ordinamento, dall'*Autorità Garante per la protezione dei dati personali*, soggetto classificabile tra le cd. autorità amministrative indipendenti. Le Autorità amministrative indipendenti sono enti che svolgono funzioni di regolazione e protezione di interessi collettivi in alcuni settori socialmente rilevanti, funzioni che devono essere esercitate senza condizionamenti da parte del potere politico, amministrativo, economico. Quelle attualmente attive – a parte la *Banca d'Italia*, da qualche commentatore qualificata come tale – sono la *Commissione nazionale per le società e la borsa,* l'*Autorità garante della concorrenza e del mercato,* la *Commissione di garanzia sullo sciopero nei servizi pubblici essenziali,* l'*Autorità per l'energia elettrica, il gas e il servizio idrico,* l'*Autorità per le garanzie nelle comunicazioni,* l'*Autorità garante dell'infanzia e dell'adolescenza,* l'*Autorità di regolazione dei trasporti,* l'*Istituto per la vigilanza sulle assicurazioni,* l'*Autorità nazionale anticorruzione e per la valutazione e la trasparenza delle amministrazioni pubbliche*. Più precisamente il *Garante,* per la peculiarità dei fini perseguiti – la tutela dei diritti fondamentali della persona – è classificabile non tra le *autorità di regolazione e controllo* di un dato settore di attività economica, quanto piuttosto tra le *autorità di garanzia* la cui istituzione è direttamente collegata all'attuazione di principi costituzionali (nel senso che le funzioni ad esso attribuite sono connesse a diritti e libertà tutelati direttamente dalla Costituzione, in particolare dall'art. 13 Cost).

Il Garante per la protezione dei dati personali è un organismo collegiale (e non una persona fisica, quando i media "intervistano il Garante" in realtà fanno di solito riferimento al presidente dell'Autorità). Ai sensi dell'art. 153 comma 1 del Codice

> Il Garante è composto dal Collegio, che ne costituisce il vertice, e dall'Ufficio.
> Il Collegio è costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato.

Il Garante per la protezione dei dati personali assume vari compiti, tra i quali i seguenti

- sorveglia e assicura l'applicazione del Regolamento;
- promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento
- fornisce consulenza, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
- promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;
- su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal Regolamento
- tratta i reclami e svolge le indagini opportune sull'oggetto del reclamo;
- svolge indagini sull'applicazione del Regolamento.

L'autorità ha poteri di indagine, correttivi, autorizzativi e consultivi, specificati all'art. 58 del Regolamento.

5. Responsabilizzazione/Accountability

Nel parere 3/2010 il Gruppo dei Garanti ex art 29[5], richiamando un proprio precedente documento del dicembre 2009, aveva evidenziato come il quadro giuridico derivato dalla Direttiva 95/46/UE non fosse riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducessero in meccanismi efficaci atti a fornire una protezione reale degli interessati; proponeva pertanto alla Commissione di introdurre meccanismi basati sulla *responsabilità*, con la possibilità anzi di formalizzare, nella versione riveduta della Direttiva (allora non si era ancora pensato alla adozione di un Regolamento), un *principio di responsabilità* in base al quale i titolari del trattamento fossero tenuti ad adottare le misure necessarie per garantire concretamente il rispetto degli obblighi e dei principi fondamentali sulla protezione dei dati; proponeva quindi una architettura giuridica dei meccanismi di responsabilità basata su due livelli: il primo livello sarebbe costituito da un obbligo di base vincolante per tutti i responsabili del trattamento (comprensivo di due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove), ed un secondo livello che avrebbe incluso sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure.

Il Nuovo Regolamento UE ha adesso esplicitamente introdotto un principio di *responsabilizzazione* (termine che traduce quello inglese di *accountability*) del Titolare del trattamento (ovvero del soggetto che determina le finalità e i mezzi del trattamento di dati personali, cfr. § 14).

L'art. 5 (*Principi applicabili al trattamento di dati personali*) par. 1 del Regolamento prescrive analiticamente alcuni principi che assicurano l'adeguatezza del trattamento; la *responsabilizzazione* del Titolare (art. 5 par. 2) consiste nel rispettare tali principi e nell'essere in grado di dimostrare ("comprovare") di averli rispettati:

> 1. I dati personali sono:
> a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
> b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
> c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
> d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

[5] Si tratta di un coordinamento, principalmente, di rappresentanti delle Autorità di controllo nazionali previsto dall'art. 29 della Direttiva 46/95 e sostituito dal 25 maggio 2018 dall'EDPB, l'European Data Protection Board.

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)[6].

[6] L'articolo citato ripropone, modificato, l'art. 6 *Qualità dei dati* (*Principles relating to data quality*) della Direttiva 46/95, che recitava:

1. Gli Stati membri dispongono che i dati personali devono essere:
a) trattati lealmente e lecitamente;
b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;
d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati;
e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.
2. Il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1.

Nella Direttiva, il *controller*, quello che per noi è il *Titolare* (cfr. § 14), è appunto tradotto con *Responsabile*. Diciamo che nel Regolamento i medesimi principi sono chiaramente individuati e definiti, ed in tal modo maggiormente enfatizzati. Tali principi erano stati anche inseriti, con la consueta estrema chiarezza, nell'oggi abrogato art. 11 *Modalità del trattamento e requisiti dei dati* del D.Lgs. 196/2003, che ci può essere utile per una loro più diretta comprensione (posto che, di quei principi, offre una declinazione diversa ma non contrastante, ed è questo uno dei casi in cui l'abrogazione è avvenuta non perché la disposizione contraddice al Regolamento, ma perché la norma che se ne trae è da questo già espressa):

1. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

In passato si parlava di un *principio di finalità*, adesso, esplicitamente, di *limitazione* della finalità; si parla analogamente di *limitazione della conservazione*, e si traduce il principio di necessità in quello della *minimizzazione dei dati*: il trattamento adeguato è evidentemente quello che, su presupposti leciti, raggiunge lo scopo prefissato riducendo al minimo il trattamento dei dati ad esso necessari; il Regolamento, possiamo dire, è informato ad un generale *principio di necessità*.

Si evidenzia inoltre che il Titolare si responsabilizza anche rispetto alla possibilità di "comprovare" l'applicazione di quei principi. Tale assunto viene ribadito all'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, *ed essere in grado di dimostrare*, che il trattamento è effettuato conformemente al presente Regolamento." *Comprovare, dimostrare*: coniugato alla nozione di privacy by default e by design (cfr. § 7) e soprattutto alla Valutazione d'impatto (cfr. § 8) quale strumento (e documento) per valutare l'adeguatezza del trattamento, ciò si traduce senz'altro in un obbligo di documentazione preventiva.

Da un principio di maggior responsabilizzazione del Titolare consegue anche che con il Regolamento Generale l'intervento delle autorità di controllo sarà principalmente "ex post", successivo alle determinazioni assunte autonomamente dal Titolare; da qui l'abolizione di alcuni istituti previsti dalla direttiva 46/95 e dal Codice pre adeguamento, come la notifica preventiva dei trattamenti all'autorità di controllo ed il cosiddetto prior checking (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e di effettuazione delle valutazioni di impatto in piena autonomia (e, dunque, responsabilità).

Riassumendo, il Regolamento pone una serie di regole di carattere generale, che definiscono un perimetro, molto ampio, entro il quale il Titolare deve trovare una propria "adeguata" misura, con un considerevole ambito di autonomia; ferme restando ovviamente le ulteriori determinazioni – queste sì ordinariamente puntuali e analitiche – poste dal legislatore nazionale e dalla Autorità Garante, che per lo più continua ad impostare i propri interventi sulla falsariga di quelli definiti nella vigenza del precedente quadro normativo.

In riferimento a quest'ultimo punto, è evidente come per l'Autorità si stabilisca, per gli enti pubblici, una precaria dialettica tra le basi giuridiche che li riguardano direttamente – e segnatamente quelle relative agli obblighi legali o ai compiti di interesse pubblico (art. 6 par. 1 lettere c) e) o di interesse pubblico rilevante (art. 9 par. 2 g) – e le altre pur invocabili in riferimento ai loro diversi ambiti di competenza istituzionale; ciò in particolare allorquando il Codice post adeguamento ribadisce in via prioritaria che tali basi giuridiche debbano tradursi senz'altro in una norma di legge o, nei casi previsti dalla legge, di regolamento (per quanto riguarda il rapporto con le finalità di cura cfr. il § 20.4.2), con la conseguenza di attrarre irresistibilmente verso tali atti normativi tutte le attività di trattamento, da qualunque eventuale ulteriore base giuridica di carattere più generale legittimati, effettuate da enti pubblici.

Vero è che alcune recentissime modifiche apportate dal D.L. 8 ottobre 2021 n. 139 al dettato del *Codice* hanno molto limitato gli effetti di tale impostazione. Ci si riferisce in particolare alle integrazioni all'art. 2-ter e all'art. 2-sexies.

Si ricorda che il Regolamento non distingue, relativamente alla liceità e legittimità, tra le varie operazioni di trattamento – per cui il trattamento è complessivamente lecito in riferimento ad una certa base giuridica, ivi compresa la comunicazione e diffusione dei dati – laddove il comma 4 dell'art. 2-ter integra la definizione di trattamento di dati offerta dall'art. 4 2) del Regolamento specificando cosa debba intendersi per "comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione" ("disclosure by transmission, dissemination or otherwise making available"):

> 4. Si intende per:
>
> a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
> b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dunque; l'attuale redazione dei primi 4 commi dell'art. 2-ter del Codice è la seguente:

> 1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali.
> 1-bis. Fermo restando ogni altro obbligo previsto dal Regolamento e dal presente codice, il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, … è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri …. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle liberta' degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento.
> 2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis.
> 3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-bis. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

Riassumendo: qualora il trattamento dei dati comuni abbia per scopo l'adempimento di un obbligo legale o l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, la base giuridica è rappresentata:

- da una norma di legge o di regolamento (quest'ultima non deve essere più, a sua volta, prevista da una norma di legge, come nella redazione precedente al D.L. 139/2021) o da atti amministrativi generali[7]; tale base giuridica è valida per ogni operazione di trattamento, ivi comprese comunicazione e diffusione;
- dall'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri, senza che una puntuale disposizione lo preveda; tale base giuridica è valida per ogni operazione di trattamento, ivi compresa la comunicazione a soggetti che trattano i dati per le medesime finalità (compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri), ma non, immediatamente, per la comunicazione a soggetti che trattano i dati per uno scopo diverso o per la diffusione dei dati, essendo in tali casi necessario che ne venga data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

Di fatto, l'avere tra le proprie finalità istituzionali l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri, consente di compiere ogni operazione di trattamento, indipendentemente che ciò sia prescritto in una puntuale previsione normativa, tranne la comunicazione a soggetti che trattano quei dati per uno scopo diverso o la diffusione dei dati. Tale limitazione non sussiste qualora quel trattamento sia previsto in un atto amministrativo generale.

6. Principi di Responsabilizzazione/Accountability

Comunque, la *responsabilizzazione* del Titolare deve valutarsi in riferimento ai seguenti principi, che andiamo adesso ad esaminare analiticamente:

- limitazione della finalità del trattamento;
- liceità del trattamento;
- correttezza del trattamento;
- trasparenza del trattamento;
- minimizzazione dei dati;
- esattezza e aggiornamento dei dati;
- limitazione della conservazione dei dati,
- sicurezza dei dati (integrità e riservatezza).

6.1. Finalità e limitazione della finalità

Tra i principi generali ai quali il titolare del trattamento dei dati personali deve conformarsi, il Regolamento prevede tra gli altri quello di *limitazione della finalità del trattamento* (art. 5 par. 1 lettera b), in riferimento al quale i dati devono essere

> raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con

[7] Si tratta di atti con i quali, pur se risultano privi di forza precettiva, una amministrazione ha il potere di determinare effetti giuridici in relazione a rapporti che abbiano le medesime caratteristiche. Ne è un esempio il bando di concorso. In tali casi la legge non produce direttamente l'effetto, attribuendo il relativo potere alla amministrazione. Sono atti sottratti alla partecipazione procedimentale.

> tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»)[8]

Limitazione della finalità, dunque: andiamo a verificare il senso di tale nozione.

Anzitutto, leggendo la disposizione citata, vere e proprie limitazioni non se ne scorgono. Più che di *limitazioni* qui parrebbe parlarsi piuttosto di *permessi*: si possono trattare dati precedentemente raccolti con modalità non incompatibili con le finalità della raccolta, poi si elencano alcune finalità la compatibilità delle quali è data per acquisita.

Al solito, quando nel testo del Regolamento si avverte una qualche asimmetria logica, è opportuno esaminarne il testo in inglese, lingua nella quale è stato originariamente redatto[9].

Si nota immediatamente che la traduzione italiana, posponendo il "not" ("non") nel primo periodo, fa venir meno il senso appunto della *limitazione* del testo inglese poiché volge la prescrizione - da negativa che era (un divieto, sostanzialmente) - in positiva: meglio sarebbe stato tradurre, appunto,

> raccolti per finalità determinate, esplicite e legittime, e non ulteriormente trattati in un modo che sia incompatibile con tali finalità

Ovvero, i dati raccolti – dati (l'art. 5 del Regolamento di focalizza sui dati) di cui il titolare ha già la disponibilità - possono essere trattati per le finalità lecite originarie, ma non ulteriormente, se non a seguito di una valutazione di compatibilità non solo della nuova finalità (che diremo "finalità secondaria") rispetto alla precedente (che diremo "finalità primaria"), ma, più ampiamente, delle modalità con cui questa complessivamente si realizza ed attua.

L'art. 5 par. 1 lettera b) del Regolamento Generale 2016/679 prescrive ai titolari del trattamento il rispetto, tra gli altri, del principio di *limitazione della finalità,* secondo cui il Titolare non può immediatamente disporre dei dati già raccolti per una specifica finalità (ad

[8] Circa la preventiva valutazione positiva di compatibilità posta dal richiamato art. 89 del Regolamento, relativamente ad un "ulteriore trattamento … a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici", corre subito la necessità di anticipare che, in quanto norme speciali, che pongono una specifica limitazione al trattamento ai sensi dell'art. 9 par. 4 del Regolamento, le disposizioni in materia di ricerca in campo medico, biomedico ed epidemiologico che sono poste dal Codice, non si avvantaggiano di tale ampia valutazione di compatibilità in riferimento alla ricerca scientifica.

[9] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89, not be considered to be incompatible with the initial purposes ('purpose limitation')

es. quella di cura) *ad libitum*, per finalità ulteriori, avendone invece un possesso *condizionato,* e appunto *limitato*; potrà infatti trattare quei dati *limitatamente* alla finalità lecita per cui li ha raccolti, mentre ogni eventuale finalità ulteriore dovrà essere oggetto di una specifica valutazione di compatibilità. La originaria liceità del trattamento di quei dati non si comunica dunque a finalità, a scopi ulteriori: se la finalità muta, i presupposti di liceità del trattamento cambiano con essa, in quanto avremo un trattamento sostanzialmente diverso, pur se effettuato dallo stesso soggetto utilizzando le medesime informazioni.

Tale principio, che si focalizza sui dati già raccolti, a ben vedere, è specificazione di un principio più generale: al di là del prima e del dopo, delle finalità primarie e secondarie, ogni finalità di trattamento (e potremmo dire: ogni singolo trattamento) ha specifici presupposti - che chiameremo *condizioni di liceità* o *basi giuridiche* - e, di conseguenza, il Titolare deve sempre valutarne preventivamente la specifica liceità.

6.2. Liceità e base giuridica del trattamento

Il profilo della liceità del trattamento riguarda specifiche regole di condotta determinate a priori direttamente dal legislatore (e dal Garante).

L'art. 13 del Regolamento, relativo alle Informazioni da mettere a disposizione dell'interessato (cfr. § 9), distingue esplicitamente tra *finalità* e *base giuridica del trattamento* (il Titolare fornisce all'interessato informazioni circa "le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento").

Che rapporto sussiste tra *finalità* e *base giuridica del trattamento*?

La *finalità* è una situazione di fatto, è cioè il motivo per il quale e l'obiettivo pratico in vista del quale si trattano informazioni di carattere personale.

Ad esempio: una Azienda sanitaria deve inviare una proposta di screening a una certa categoria di cittadini, ne raccoglie pertanto nominativi ed indirizzi; tratta quei dati (nominativi ed indirizzi) allo scopo, per la finalità (pratica) di realizzare lo screening. Quello scopo pratico è anzi costitutivo della nozione stessa di Titolare: se un soggetto sceglie di trattare dati per uno scopo, e secondo certe modalità a questo funzionali, è, solo per questo, di fatto, un Titolare del trattamento (indipendentemente dalla liceità di quella attività).

Pur se la finalità, in quanto tale, è un elemento che resta esterno rispetto alla definizione di trattamento offerta dal Regolamento[10], è essa che rende ragione del trattamento stesso (non si trattano dati personali senza scopo, così, per intenti ludico-combinatori), ed è in primo luogo in riferimento ad essa che deve essere valutata - rispetto al caso concreto - tanto la liceità e l'adeguatezza del trattamento che la legittimazione del Titolare ad effettuarlo.

[10] "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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

La nozione di *finalità* ci ricorda che le operazioni applicate ai dati sono normalmente effettuate per un interesse ed uno scopo pratico: nel mondo reale, un trattamento di dati non sussiste di per sé, ma è regolarmente connesso ad una attività, quale causa finale, del quale esso rappresenta il supporto o l'esito informativo; la finalità, lo scopo, l'interesse condizionano le operazioni da effettuarsi su certi dati (riferiti a certi interessati), che devono essere tali, da un punto di vista qualitativo e quantitativo, da consentirne il raggiungimento.

Potremmo ipotizzare uno schema "finalistico" come il seguente, nel quale ogni elemento determina e condiziona il successivo:

scopo > attività > operazioni di trattamento (modalità e mezzi)

E' lo scopo, la finalità, che determina come si organizza l'attività, e questa richiede un particolare trattamento di dati personali per poter svolgersi in maniera funzionale allo scopo.

La *base giuridica* è invece una situazione di diritto, nel senso che è una condizione prevista dalla norma che, qualora soddisfatta, rende lecita quella finalità (quel trattamento), spesso in riferimento ad una certa categoria di titolari. In alcuni casi, cioè si prescrive che chi effettua un dato trattamento debba possedere certe caratteristiche: la finalità di "diagnosi assistenza o terapia sanitaria" di cui all'art. 9 par. 2 lettera h) del Regolamento, deve fare riferimento, ai sensi dell'art. 9 par. 3, alla "responsabilità di un professionista sottoposto al segreto professionale": ne segue che, ad esempio, un artigiano non può trattare dati per finalità di "diagnosi assistenza o terapia sanitaria".

La liceità di un trattamento deve anzitutto potersi recuperare nel Regolamento: un determinato scopo pratico, una finalità, sarà dunque lecita in quanto riconducibile ad una determinata disposizione del Regolamento che propone una base giuridica nella quale essa sia inquadrabile.

Le basi giuridiche del trattamento sono indicate, per quanto di nostro interesse, agli artt. 6 e 9 del Regolamento.

L'art. 6 si riferisce alla liceità del trattamento in generale:

> Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni …" (comma 1)

L'art. 9 pone ulteriori condizioni in riferimento alle categorie particolari di dati personali; anzi, questi dati, *prima facie*, non possono essere trattati ("È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"), per cui le basi giuridiche consentite dall'art. 6 vengono meno; tale divieto non si applica però se si verificano alcuni "casi", ovvero in presenza di specifiche, ulteriori basi giuridiche.

Nella tabella che segue si propone il raffronto tra quelle dell'art. 6 e quelle dell'art. 9. Come si vede, alcune basi giuridiche previste dall'art. 6 non sono utilizzabili per il trattamento di categorie di dati particolari (ad es.

il contratto non è presupposto sufficiente per trattarli, cfr. § 20.7), in altri casi sono introdotte alcune condizioni accessorie: ad es. per le finalità cd. amministrative il trattamento deve essere necessario per l'esecuzione di un compito di interesse pubblico nel caso dei dati diversi da quelli afferenti alle categorie particolari, per motivi di interesse pubblico *rilevante* per queste, oltre al fatto che nel secondo caso il trattamento deve essere "proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (una aggiunta pure pletorica, considerato che potrebbe applicarsi a qualsiasi tipologia di trattamento, ma che serve comunque, retoricamente, ad evidenziare che ci si trova di fronte a dati il cui trattamento presenta maggiori rischi per i diritti dell'interessato).

Articolo 6	Articolo 9
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso	
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica	c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato
f) il trattamento è necessario per il perseguimento del legittimo interesse 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. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti	
	b)il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato
	e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato
	f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali
	h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3
	i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale

Come evidente, gli artt. 6 e 9 ricomprendono alcune condizioni di liceità riferibili all'interessato (ha espresso il consenso al trattamento dei propri dati personali, il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato), ed altre, introdotte dalla locuzione "il trattamento è necessario per …", che sono riconducibili a macro finalità (vi sia o meno speso quel termine).

Esempio: un ente pubblico tratta i dati per soddisfare uno scopo previsto da una legge; tale scopo è riconducibile alla base giuridica rappresentata, se si tratta di dati comuni, dall'art. 6 per. 1 lettera e ("il trattamento è necessario per l'esecuzione di un compito di interesse pubblico") oppure, se si tratta di categorie particolari di dati, dall'art. 9 par. 2 lettera g (: "il trattamento è necessario per motivi di interesse pubblico rilevante") del Regolamento.

Dunque, sia prima di iniziare un ulteriore trattamento di dati che già possiede per una nuova finalità, sia che raccolga dati *ex novo* a tal fine, il Titolare deve accertare se, oltre che ad essere funzionali uno scopo pratico, magari senz'altro meritevole nonché compatibile con le proprie finalità istituzionali, esso soddisfi anche ad uno scopo lecito, individuandone la base giuridica nell'articolato del Regolamento.

Tale verifica dovrà essere ordinariamente effettuata nell'ambito di una D.P.I.A., un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli (cfr. § 8).

Occorre precisare che se una finalità di trattamento è valutata in generale lecita da una disposizione del Regolamento, questa è condizione necessaria ma non sufficiente per poter procedere senz'altro al trattamento stesso. Si tratta infatti di una liceità *prima* facie: ulteriori condizioni possono essere previste da altre disposizioni normative, a livello legislativo o regolamentare, o anche da Linee Guida delle Autorità di controllo. Vi sarà inoltre da valutare la adeguatezza del trattamento anche alla luce degli altri principi stabiliti dall'art. 5 del Regolamento: minimizzazione dei dati, esattezza, limitazione della conservazione, riservatezza e integrità ecc.. Tutto ciò sarà valutato e documentato nella D.P.I.A..

6.3. Minimizzazione dei dati

La *minimizzazione dei dati* si traduce nella garanzia che i dati siano "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" art. 5 paragrafo 1 c) del Regolamento). Si tratta di un principio che in ambito nazionale era già stato definito come principio di *pertinenza o non eccedenza*, oppure di *necessità/indispensabilità*. Ovvio che adeguatezza, pertinenza e limitazione dei dati non sono elementi assoluti, ma relativi allo scopo: sono elementi che trovano una loro misura in riferimento ad un principio di necessità non assolutizzabile. Sarà dunque lecito utilizzare, tanto da un punto di vista qualitativo che quantitativo, solo le informazioni indispensabili per la finalità perseguita.[11].

Chi valuta quali dati sono o meno necessari allo scopo? Ovviamente il Titolare, che, nell'ottica della responsabilizzazione dovrà argomentare e sostenere tale valutazione (che dovrà essere, oltre che ovviamente preventiva, preventivamente documentata). Potrà poi esservi, eventualmente, una verifica da parte dell'Autorità di controllo.

[11] La disposizione ripete, esclusa la precisazione «minimizzazione dei dati», quella a suo tempo offerta dall'art. 5 paragrafo 1 c) della Direttiva 46/95, che a sua volta era stata diversamente declinata - limitatamente ai sistemi informativi ed ai programmi informatici - dall'art. 3 del Codice pre adeguamento (adesso abrogato), rubricato appunto *Principio di necessità nel trattamento dei dati*: "i sistemi informativi e i programmi informatici devono essere configurati "riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

Il Regolamento Generale, individuando agli artt. 6 e 9, le condizioni di liceità del trattamento riferisce ad alcune di queste un criterio di necessità: "il trattamento è necessario per …". Come osserva il Provvedimento dell'Autorità Garante recante *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario* del 7 marzo 2019, i trattamenti necessari sono "quelli essenziali per il raggiungimento di una o più finalità determinate". In questo caso si parla, in generale, del trattamento nel suo complesso.

La valutazione circa la minimizzazione dei dati deve essere effettuata non rispetto al trattamento complessivamente inteso rispetto ad una finalità generalmente considerata (ad es. la finalità di cura in astratto), ma in riferimento al trattamento concreto e dunque ai dati ad esso specificamente necessari.

6.4. Correttezza del trattamento

Il profilo della *correttezza del trattamento* (nella Direttiva *95/46* si parlava di *lealtà*) richiama il più generale principio di *buona fede* (in senso oggettivo, ovvero quel principio che impone ad una parte di salvaguardare l'utilità dell'altra a prescindere da specifici obblighi, laddove la buona fede soggettiva è piuttosto la situazione psicologica di colui che ignora di ledere l'altrui diritto), che può essere variamente soddisfatto con l'individuazione, da parte del Titolare, di modalità di condotta ad esso comunque rispondenti e ricomprende anche la trasparenza nel comportamento del Titolare. I dati sono trattati *correttamente* ad es. se il trattamento rispetta le buone pratiche della sicurezza.

6.5. Trasparenza

I dati devono essere "trattati in modo … trasparente nei confronti dell'interessato". Per il Considerando n. 39:

> Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale

> trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali.

La trasparenza, in particolare, si sostanzia nella messa a disposizione degli interessati di idonee *informazioni* (prima si parlava di *informativa*). Le tipologie di informazioni da fornire sono precisate nell'art. 13 del Regolamento:

- l'identità e i dati di contatto del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo.
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'eventuale esistenza di un processo decisionale automatizzato.

6.6. Esattezza e aggiornamento dei dati (e diritto all'oblio)

I dati personali trattati devono essere esatti e, se necessario, aggiornati.

Vi sono delle situazioni nelle quali un dato, pur esatto nel momento in cui è stato raccolto, col divenire del tempo non lo è più, per cui deve essere aggiornato: il vecchio dato verrà superato e cancellato, ed in un certo senso obliato. Vi saranno invece situazioni nelle quali l'esattezza storica del dato dovrà essere salvaguardata ed il dato conservato. E' questione, spesso, più di attualità o inattualità, che di esattezza o inesattezza, del dato.

Qualora però l'informazione sia senz'altro riferita all'oggi, il dato inattuale può assumere profili di inesattezza: ero celibe, poi mi sono coniugato, ma adesso sono coniugato e basta. Ma se devo documentare un percorso diagnostico, le ipotesi diagnostiche che non

si sono rivelate esatte non perdono il loro valore e significato, anche attuale, e possono (anzi devono) essere legittimamente conservate.

In alcune circostanze sarà privilegiato il dato attuale e cancellato quello che non lo è più, in altre quest'ultimo manterrà una sua dignità informativa e dovrà essere conservato, magari in collegamento con il nuovo dato.

La questione della attualità/inattualità delle informazioni viene in causa nel caso del diritto all'oblio. Il diritto all'oblio si confronta in particolare, proprio attraverso il problema della pretesa inesattezza del dato intesa come sua inattualità, con quella dell'identità personale.

L'identità personale deve essere intesa come formula sintetica per distinguere il soggetto da un punto di vista globale, nella vita di relazione e sociale, nella molteplicità delle sue caratteristiche e manifestazioni (morali, sociali, politiche, intellettuali, professionali ecc.), cioè, in definitiva, come diritto a non vedere travisata la propria personalità nella vita di relazione. La questione più pregnante, in riferimento al diritto all'identità personale, è oggi se questo comprenda anche il diritto a ricostruire una propria nuova identità, coerente con un rinnovato progetto di vita, e se esiste dunque una tutela della persona rispetto alla diffusione di informazioni veritiere ma risalenti e *non più attuali*, riconducibile ad un cd. diritto all'oblio.

Dal nostro punto di vista, è lecito chiederci se dati sostanzialmente esatti ma non più attuali, nel senso che sono riferibili ad una fase della vita di una persona adesso superata, possano ancora essere considerati tali. Il diritto all'oblio, quando riconosciuto, sottende una risposta positiva a tale quesito. Non è però un diritto assoluto, e deve dunque confrontarsi con alcuni presupposti e condizioni.

Assumiamo il caso tipico di chi sia stato coinvolto in un fatto che ha avuto un rilievo mediatico, e che le moderne tecnologie della conoscenza e dell'informazione sono in grado di rendere indefinitamente accessibile. Il dibattito sul diritto all'oblio è stato sollecitato in primo luogo da trattamenti di dati effettuati su internet, a loro volta originati in ambito giornalistico; è stato osservato che adesso il problema non è più quello della *damnatio memoriae*: al contrario, la nuova *damnatio* è piuttosto quella della conservazione del ricordo: come diceva Rodotà, "Google non dimentica mai".

La giurisprudenza tende a riconoscere un tale diritto, ma attraverso un bilanciamento con il diritto all'informazione (tutelato dall'art. 21 Cost.), e dunque solo laddove non si riscontri più un interesse pubblico alla diffusione di quelle informazioni; insomma, il diritto all'oblio, nel suo rapporto dialettico con il diritto di cronaca, si fonda sul presupposto che l'interesse pubblico alla conoscenza di un fatto è racchiuso in un limitato spazio temporale, e che con il trascorrere del tempo si affievolisce fino a scomparire; in tal senso si collega anche al diritto alla riservatezza, rispetto a fatti che, venuto meno l'interesse pubblico, tornano ad essere privati (ancorché veri). Laddove un interesse pubblico persista, si tratterà semplicemente di pretendere un trattamento di dati corretti, nel senso appunto dell'esattezza e dell'aggiornamento: se sono stato imputato e poi prosciolto, l'informazione relativa alla imputazione sarà vera in senso proprio soltanto se sarà accompagnata da quella dell'assoluzione.
Il diritto all'oblio, quindi, è riconosciuto nella misura in cui salvaguarda l'interessato dalla pubblicazione di informazioni potenzialmente lesive in ragione della perdita di attualità delle stesse a causa del lasso di tempo intercorso dall'accadimento del fatto; viene invece meno laddove l'interesse pubblico alla divulgazione della notizia rinasca o semplicemente permanga (anche per esigenze storiche, didattiche,

culturali o sociali, preso atto che un fatto di cronaca può successivamente assumere rilevanza quale fatto storico così modificandosi le finalità del trattamento originario). Dunque, se i fatti risalenti nel tempo sono in stretta correlazione con nuovi fatti di cronaca di interesse pubblico sulla base del principio di pertinenza, essi possono essere riproposti.

Stabilito tale principio, ne segue però anche che lo spostamento della notizia in un archivio storico memorizzato nella rete internet deve essere realizzato con modalità tali da consentire alla medesima di garantire caratteri di verità ed esattezza, e conseguentemente di liceità e correttezza, mediante i relativi aggiornamento e contestualizzazione. Quindi, un dato personale raccolto e diffuso lecitamente per finalità di cronaca diventa incompleto, e quindi inesatto o non vero, se mantenuto per finalità storiche così com'è, non integrato con il collegamento della notizia ad altre informazioni successivamente pubblicate concernenti l'evoluzione della vicenda.

Rispetto a tale impostazione, che bilancia diritto alla identità personale ed alla riservatezza da un lato e diritto di cronaca dall'altro, problematiche diverse pone oggi la questione del diritto all'oblio degli accessi effettuati in Rete, non trattandosi qui del diritto di ciascuno a che altri non vengano riproposti fatti di un passato più o meno risalente, quanto del diritto di ciascuno a recuperare ed annullare le proprie tracce in rete, lasciate volontariamente ma anche non volontariamente (es. foto riprese da altri e postate su Facebook).

Il Nuovo Regolamento UE dedica adesso l'art. 17 al *Diritto all'oblio e alla cancellazione*.

Si evidenzia che, ai sensi del par. 3 dell'art. 17, il diritto all'oblio e alla cancellazione non trova spazio nel caso di trattamento svolto per l'adempimento di un obbligo giuridico cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; inoltre, più in particolare, per motivi di interesse pubblico nel settore della sanità pubblica, cioè in ambito sanitario.

6.7. Limitazione della conservazione

La conservazione del dato può essere a tempo illimitato – come ad esempio per le cartelle cliniche – o limitato; in quest'ultimo caso la limitazione della conservazione dei dati si traduce nella loro cancellazione, solitamente attraverso lo scarto dei documenti che li contengono.

I termini di conservazione devono essere esplicitati nelle informazioni all'interessato (cfr. § 6.5), l'art. 13 del Regolamento prevedendo appunto che venga declinato "il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo".

Devono essere assolutamente evitate indicazioni tautologiche quali "i dati saranno conservati per il periodo di tempo previsto dalla vigente normativa", evidente indizio della sicura ignoranza della medesima da parte di chi le ha scritte. I *criteri* possono invece essere utili nel caso si debba indicare la possibilità che il termine di conservazione indicato possa essere prorogato in ragione della possibilità di riferire ai dati una diversa finalità.

6.8. Sicurezza

Ai sensi dell'art. 5 par. 2 del Regolamento, i dati devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)".

Le politiche di sicurezza sono necessarie per evitare:

- la divulgazione di dati personali o l'accesso agli stessi non autorizzati o accidentali;
- la modifica non autorizzata o accidentale di dati personali (così che i dati sono modificati o incompleti);
- la perdita della possibilità di accesso o distruzione accidentale o non autorizzata di dati personali.

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafi 1-2; nel Regolamento Generale si parla conseguentemente solo di misure adeguate – individuate come tali dal Titolare - e non più di misure minime di sicurezza, normativamente stabilite; la nozione di misure minime di sicurezza è dunque superata, e non sussistono più obblighi generalizzati – con previsione di una sanzione penale in caso di mancato rispetto - di una loro adozione (ex art. 33 e Allegato B del Codice pre adeguamento); la valutazione sulle misure da adottare sarà invece rimessa, in riferimento a casi specifici ed effettivi, alla responsabilità del titolare in rapporto ai rischi da esso, volta per volta, individuati.

7. Privacy by default e privacy by design

Le misure e i principi sopra elencati devono essere assicurati prima di procedere al trattamento dei dati vero e proprio, attraverso un'analisi preventiva – documentata - ed un impegno applicativo da parte dei titolari, e tradursi in una "impostazione predefinita" del trattamento stesso che risponda a criteri di adeguatezza, in particolare in materia di liceità e sicurezza del trattamento: questa impostazione di verifica preventiva si traduce nel principio della *protezione dei dati fin dalla fase di progettazione e dall'inizio del trattamento (data protection by default and by design*): assicurarla non significa altro che programmare esattamente un processo (che comporta l'utilizzo di dati personali) prima di iniziarlo (come il semplice buon senso dovrebbe consigliare, più che una disposizione normativa prescrivere).

Comunque sia, possiamo ben dire che, nella protezione dei dati personali, strategie storicamente apprezzate come quella per cui "si inizia e poi si guarda" non hanno spazio alcuno.

8. Valutazione d'impatto (DPIA)

Come può il Titolare accertarsi di assolvere effettivamente agli obblighi che gli sono imputati?

Gli strumenti che il Titolare può utilizzare per responsabilizzarsi sono essenzialmente due: la cd. *Valutazione d'impatto sulla protezione dei dati* (Data Protection Impact Assessment DPIA) e le istruzioni a Responsabili e persone autorizzate al trattamento.

Con la prima, il Titolare valuta la liceità del trattamento (cfr. § 6.2) e si predefiniscono le misure, tecniche ed organizzative che ne assicurano, più ampiamente, l'adeguatezza; con le seconde comunica ai soggetti che operano per esso le regole che ha ritenuto di dover implementare per attuare tali misure in concreto, e che essi dovranno applicare senza margini di discrezionalità (cfr. § 17).

Alla DPIA il Regolamento dedica i Considerando 84, 89-93, 95 ed il Capo IV sezione III; il gruppo europeo dei Garanti ha emesso delle linee guida sulla conduzione delle DPIA (*Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679*, d'ora in avanti: *Linee guida sulla DPIA*).

La DPIA è un processo

> inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità[12].

La DPIA deve soddisfare alcuni requisiti basilari, indicate all'art. 35, paragrafo 7 e nei considerando 84 e 90 del Regolamento, mettendo a disposizione:

- una descrizione sistematica del trattamento;
- la esplicitazione delle finalità del trattamento;
- una valutazione della necessità e proporzionalità del trattamento;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure tecniche e organizzative che il titolare ritiene di dover adottare allo scopo di mitigare tali rischi.

[12] WP 248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017, pag. 4.

Una DPIA è obbligatoria allorquando il trattamento "possa presentare un rischio elevato" per i diritti dell'interessato, e dunque sempre in ambito sanitario (come si deduce dalle stesse *Linee guida sulla DPIA*, che riconducono i trattamenti in ambito sanitario a quelli "relativi ad interessati vulnerabili"); in particolare, soprattutto in tale ambito, l'espletamento di una DPIA è requisito particolarmente necessario qualora si intenda introdurre una tecnologia di trattamento innovativa, un nuovo sistema di informatica sanitaria, un nuovo processo assistenziale; è senz'altro necessaria anche in riferimento ad ogni progetto di ricerca, anche osservazionale.

La DPIA deve effettuarsi prima dell'inizio del trattamento, ma l'obbligo di condurre una DPIA vige anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi. La DPIA non può essere un'attività *una tantum*, ma un processo permanente e continuativo, soprattutto se si ha a che fare con un trattamento dinamico e soggetto a continue trasformazioni.

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento ovvero consultare l'autorità di controllo per ottenere indicazioni su come gestire il rischio residuale; l'autorità – che risponderà entro otto settimane, prorogabili di ulteriori sei settimane per trattamenti particolarmente complessi - non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 comma 2 del Regolamento (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

Spetta al titolare garantire l'effettuazione della DPIA (art. 35, paragrafo 2 del Regolamento). consultandosi con il DPO (art. 35, paragrafo 2 del Regolamento, cfr. § 19); tale consultazione e le conseguenti decisioni assunte dal titolare devono essere documentate. Il DPO è chiamato anche a monitorare lo svolgimento della DPIA (art. 39, paragrafo 1, lettera c del Regolamento). Se il trattamento è svolto, in tutto o in parte, da un responsabile (cfr. § 15), quest'ultimo deve assistere il titolare nella conduzione della DPIA fornendo ogni informazione necessaria conformemente all'art. 28, paragrafo 3, lettera f del Regolamento.

La DPIA è uno strumento importante in termini di *accountability* del titolare, in quanto è una procedura che permette di garantire e dimostrare la conformità e l'adeguatezza di un trattamento. Posto che il Regolamento prescrive che il Titolare valuti preventivamente l'adeguatezza di ogni trattamento e di tale valutazione mantenga idonea documentazione, è evidente che la DPIA appare uno strumento *ordinario*, e forse anzi il *principale* strumento a disposizione del Titolare per assolvere ai propri obblighi in materia di protezione dei dati personali.

Considerato che l'inosservanza degli obblighi concernenti la DPIA – ovvero: il mancato svolgimento della DPIA quando il trattamento debba considerarsi soggetto a tale valutazione (art. 35, paragrafi 1 e 3- 4 RGPD), lo svolgimento non corretto di una DPIA (art. 35, paragrafi 2 e 7-9 RGPD) o la mancata consultazione dell'autorità di controllo ove ciò sia necessario (art. 36, paragrafo 3, lettera e del Regolamento) - può comportare una sanzione amministrativa pecuniaria fino a 10 milioni di euro, è anche da questo punto di vista opportuno che si tratta di un processo che deve essere gestito tempestivamente e in via ordinaria.

Per l'esecuzione della DPIA l'Azienda ha predisposto il format allegato sub 1).

9. Quando un dato è personale

La definizione di dato personale offerta dall'art. 4 1) del Regolamento Generale è la seguente:

> qualsiasi informazione riguardante (*relating to*) una persona fisica identificata o identificabile («interessato» - *data subject*); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Il dato personale è un oggetto riconducibile al genere "informazione", è cioè un oggetto immateriale: è dato personale l'immagine, non la foto, l'impronta digitale, non i dermatoglifi o il dito, le informazioni genetiche, non il campione biologico.

In quanto informazione, il dato personale può modificare il proprio contenuto informativo se associato ad altri dati (una anagrafica associata, in una bolla, ad una spedizione è diversa dalla medesima anagrafica associata ad un referto di laboratorio, nel primo caso avremo un documento che reca dati comuni, nel secondo dati relativi alla salute), e potrà anche avere significati diversi per i diversi titolari che lo utilizzano (magari per finalità differenti) o per l'interessato. Saranno poi essenziali alla sua natura, come per qualsiasi informazione, la circolazione e la condivisione: e ciò confliggerà con eventuali pretese esclusive al suo utilizzo, e dunque con pretese di carattere proprietario, dominicale, non utilmente declinabili rispetto ai dati personali.

Si aggiunga che, come meglio vedremo in seguito, il dato è personale se consente non solo l'identificazione attuale e diretta dell'interessato, ma anche se ne permette una identificazione indiretta, cioè a seguito del collegamento con altri dati, non solo quelli al momento disponibili, ma anche quegli altri prospetticamente accessibili. Ne segue che un dato dovrà essere trattato (attualmente) come personale (cioè esso "è" dato personale)

nella misura in cui, per così dire, ha la ragionevole probabilità di diventarlo compiutamente solo in un momento successivo, quando sarà effettivamente ricollegabile ad un interessato, ovvero quando quella informazione, associata ad altre, consentirà una effettiva identificazione della persona fisica (interessato) cui si riferisce.

Il dato personale è dunque un oggetto che possiede caratteri di dinamicità, pluralità, probabilità, plurisignificatività, che è caratterizzato da una *vaghezza* che condivide con molti altri oggetti cosiddetti sociali, enti che, se esistono nella realtà naturale, sono ricreati e riqualificati dalla particolare prospettiva dalla quale sono osservati e trattati (nel nostro caso, si tratta di oggetti riconducibili all'ambito del diritto, creati o ricreati dal diritto). Per intenderci, consideriamo le impronte digitali, dalle quali possono essere tratte informazioni che nell'attuale sistematica dei dati personali – dunque una qualificazione di carattere giuridico - sono qualificabili come dati "biometrici". I dermatoglifi sono di per sé un oggetto fisico, fisiologico, una caratteristica anatomica, e le impronte digitali sono le informazioni (dati personali) che possono essere tratte da essi. Applicando determinate tecniche di elaborazione automatizzate, si ha una particolare tipologia di dato personale che l'attuale normativa definisce appunto dati personali *biometrici*, ed in particolare dati *dattiloscopici*; i dati biometrici sono definiti dall'all'art. 4 paragrafo 1 14 del Regolamento Generale come "i 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'immagine facciale o i dati dattiloscopici"; sono dati ricompresi tra le categorie particolari di dati di cui all'art. 9 del Regolamento. Dunque, ci troviamo di fronte al trattamento di un oggetto fisico che acquisisce specifiche connotazioni in quanto gli sono riconosciute in ambito giuridico, dando luogo ad un oggetto diverso (posto su un diverso piano della realtà), privo della consistenza degli enti materiali (allo stesso modo in cui un muro può fungere da confine, per cui esso non viene più in causa quale aggregato materiale di mattoni, ma appunto, funzionalmente, come confine, come fatto giuridico, con le prerogative e prescrizioni, socialmente riconosciute, che a ciò conseguono, così che un confine potrà essere percepito e rispettato come tale anche se quel muro è caduto o non c'è mai stato). Il dato dattilometrico si emancipa dall'eventuale supporto fisico (i dermatoglifi), che può essere visto quasi come un suo pre-testo, ed è trattato come un oggetto immateriale, appunto come *informazione*.

Preso atto che una norma qualifica la fattispecie concreta cui si riferisce non a fini teoretici, per classificare astrattamente la realtà (ed in tal caso il *deficit* conseguente ad una insoddisfacente o non concorde classificazione sarebbe meramente cognitivo o comunicativo), ma, attraverso un processo di giuridificazione funzionale di oggetti, a loro volta esito della oggettivazione di proprietà, per intervenirvi con prescrizioni (facoltà, obblighi, divieti, ecc.) e dunque orientare i comportamenti, si tratterà allora, per i nostri scopi, di chiarire come le informazioni che si possono trarre da una nota scritta, un'immagine, una registrazione vocale, l'elaborazione di una caratteristica fisica o comportamentale, una espressione in qualsiasi modo documentata, sono (sono considerate e giuridicamente qualificate) come *dati personali* e come tali devono essere trattate (nel senso che alla qualificazione, alla definizione essenziale, sono coordinati e conseguenti specifici obblighi giuridici). Sarà dunque per uno scopo eminentemente "pratico" che dobbiamo impegnarci in una analisi delle nozioni di dato personale così come di trattamento di dati, titolare, responsabile ecc., essenziali per comprendere la disciplina in materia.

Si tratta di nozioni per le quali la normativa ha preferito adottare concetti descrittivi e referenziali che, di esse, restituiscono l'aspetto contestuale e relazionale.

Così, l'interessato è "la persona fisica cui si riferiscono i dati".

Si noti come il termine *interessato* abbia una connotazione passiva/attiva: è la persona interessata dai dati, il soggetto in senso proprio, ma anche la persona interessata ai dati, cioè che ha un interesse, giuridicamente protetto, al loro corretto utilizzo ed alla relativa protezione. Soprattutto, i dati personali "si riferiscono"

all'interessato, non sono informazioni proprie dell'interessato, che non è "il proprietario dei dati": anzi spesso ne è, per così dire, l'oggetto, l'interessato subisce il dato (che normalmente è il prodotto, l'esito di una altrui attività), da cui una possibile relazione alienante e la conseguente necessità anche di affrancarsene con la soluzione del diritto all'oblio (che è una sorta di protezione dai dati personali).

Il rapporto tra l'interessato ed il dato personale è di tipo informativo e relazionale (quella data informazione riguarda una certa persona fisica), per cui i diritti che l'interessato può vantare rispetto ai dati che a lui si riferiscono non sono, normalmente, quelli di goderne e disporne in maniere esclusiva, ma sono appunto diritti di protezione e controllo, che ordinariamente non si risolvono neppure in un mero diritto di autodeterminazione (per cui, almeno a partire dalle normative privacy degli anni '90, è venuta meno la centralità dello strumento del consenso come principale fonte della liceità per l'utilizzo dei dati).

Il Titolare del trattamento non è neppur esso "il proprietario dei dati", è piuttosto, anch'esso, il soggetto che si relaziona, e stabilisce un rapporto attivo, con certe informazioni di carattere personale, utilizzandole con varie modalità da esso determinate per i propri scopi; e, normalmente, vi saranno più titolari del trattamento.

9.1. Il dato personale tra identificazione, identificabilità e riconoscibilità

Il dato personale è dunque quel dato che abbia, di per sé solo ed immediatamente, oppure successivamente ed in correlazione con altri, un contenuto informativo correlato o correlabile ad una persona fisica infine identificata.

Nella nozione di dato personale proposta dalla normativa non viene ad ogni modo offerta la definizione di identificazione o di persona identificata. Cosa significa, allora, identificare una persona fisica?

Identificare una persona fisica significa sostanzialmente individuare un soggetto tra altri, sfruttando certi elementi informativi. Tale riconoscimento esita solitamente (ma non necessariamente), in accordo con il soggiacente paradigma investigativo-giudiziario, nella individuazione dei dati anagrafici della persona fisica (il suo *nome*). L'identificazione è un processo; essa ha il carattere della (quasi) immediatezza nel caso dei dati – appunto - immediatamente identificativi, e prevede invece una serie di fasi ed un coordinamento di informazioni nel caso di dati non immediatamente identificativi, fino all'accesso all'informazione direttamente identificativa.

L'identificazione di una persona fisica è dunque principalmente assicurata dalla correlazione tra alcune informazioni che la riguardano (che possono essere, si pensi al documento di identità –caratteristiche fisiche e dati anagrafici), ed il proprio *nome giuridico* (formato, ai sensi dell'art. 6 del Codice Civile, da *prenome* e *cognome*). Il nome è sicuramente il principale strumento di individuazione ed identificazione della persona fisica - tanto che la legge configura un diritto al nome e la relativa tutela - e la nozione di persona identificata implica normalmente un riferimento al nome di quella persona. Allo scopo di accertare con sicurezza l'identità, il nome della persona, qualora non

estremamente particolare, dovrà essere però combinato con altre informazioni per evitare confusioni con eventuali omonimi.

Potremmo prendere come esempio di un set di dati sicuramente identificativi quelli non a caso confluiti nella carta di identità, immagine, nome, data e luogo di nascita. Il codice fiscale, univocamente riferito ad un cittadino, ha certamente una fortissima capacità identificativa.

Se si suppone che l'esito debba essere l'identificazione nominativa, anche l'immagine dovrebbe essere qualificata come identificativo indiretto; pure, l'immagine (si parla di immagine in questo caso in senso proprio, ai sensi della legge sul diritto d'autore) ha un rapporto tale con la persona fisica che ne è prevista una specifica tutela, essendo essa in grado, se non di identificare, almeno di individuarla chiaramente tra le altre. Secondo il Parere 4/2007 del Gruppo ex art. 29, "Le immagini registrate da un sistema di videosorveglianza possono essere dati personali nella misura in cui le persone riprese sono riconoscibili". In una videoripresa posso considerare sufficientemente individuato, quale rapinatore, il tizio che, in mezzo ai clienti di una banca, agita una pistola davanti alla cassa, e bloccarlo all'uscita; e si pensi anche alle immagini, non necessariamente taggate, postate su Facebook. Viene qui appunto in questione il problema della riconoscibilità, che è propedeutica ad una possibile, ma affatto necessaria, identificazione nominativa dell'interessato (il bullismo on line o il revenge porn funzionano benissimo senza necessità di spendere il nome delle persone riprese). Riassumendo il concetto nei termini di una sentenza della Cassazione civile (sez. III, 27.01.2014 n° 1608), "... l'individuabilità della persona ... non ne postula l'esplicita indicazione del nominativo, essendo sufficiente che essa possa venire individuata anche per esclusione in via deduttiva, tra una categoria di persone ...".

Tale assunto riguarda solo le immagini e la loro particolare tutela o è riconducibile ad un profilo più generale, sistematico?

Il fatto è che la questione della riconoscibilità, della distinguibilità di una persona rispetto alle altre, deve essere posta in riferimento alla probabilità che possano determinarsi su di essa concreti effetti attraverso tale riconoscibilità. La nozione di dato personale ricomprende anzi la riferibilità di una informazione ad un soggetto identificabile seppur non identificato non perché potrebbe trattarsi di elemento propedeutico rispetto ad una successiva possibile identificazione, ma perché gli effetti del trattamento su di essa possono già aversi a questo livello. La definizione di dato personale offerta dal Regolamento Generale ricomprende adesso anche l'identificativo on line, che certo prescinde dal nome: i dati di navigazione in internet devono considerarsi dati personali; i cookies, infatti (sui quali il Garante, in data 8 maggio 2014, ha adottato uno specifico provvedimento, Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie), se non consentono di identificare nominativamente l'utente cui si riferiscono, riescono comunque a ricostruirne un dettagliato profilo, ne esaminano il comportamento per cercare di orientarlo, con effetti tali da consigliare di

applicare appunto, anche a tali informazioni, la qualificazione di dati personali (appunto per uno scopo di protezione del soggetto cui sono riconducibili).

Sistematizzando il principio potremmo dunque sostenere che ci troviamo di fronte ad un dato personale quando il trattamento di una certa informazione pone esigenze di protezione della persona cui essa è riferibile: il dato non è personale in astratto, ma funzionalmente allo scopo di protezione che informa la materia ("protezione delle persone fisiche rispetto al trattamento dei dati personali").

Si evidenzia come il nome ed i dati anagrafici siano a loro volta dati personali. Normalmente la situazione è quella in cui si dovrà associare i dati relativi ad una certa situazione o condizione (che quando tale associazione avrà avuto buon esito si qualificheranno a loro volta come dati personali) ad una persona fisica attraverso il riferimento ai suoi dati (personali) identificativi; potrebbe essere necessario raggiungere questi dati identificativi attraverso una correlazione e confronto di informazioni, a partire da dati che, al momento, non appaiono riferibili ad una persona fisica o comunque univocamente identificativi. Comunque, il dato personale si qualifica sempre quale un sistema, un coordinamento di informazioni entro un dato contesto.

Il *quantum* di informazioni sufficiente per accedere all'identificazione è relativo al contesto di trattamento: tanto a quello attuale come anche a quelli futuri, considerato che la identificazione dell'interessato, essendo un processo, può essere raggiunta anche in un tempo successivo (come dice il Garante, "a posteriori"). A determinare se gli elementi in nostro possesso siano o meno sufficienti per raggiungere già adesso un'identificazione, è dunque il contesto della situazione specifica: al limite, anche un cognome (se molto comune) non basterà ad identificare una persona tra l'intera popolazione di un paese, ma sarà con buone probabilità sufficiente a identificare uno studente in una classe o un dipendente in Azienda. Insomma, il fatto che una persona cui si riferisce l'informazione possa o meno essere identificata dipende ordinariamente dalle circostanze e dallo specifico contesto: sono questi che possono trasformare un mero dato in un dato personale (ma sulla nozione di assolutezza del dato personale cfr. § 10).

Posto che, in astratto, qualunque soggetto è identificabile nel giusto contesto a partire da alcuni dati (dipende da quali altre informazioni riesco a reperire e ad associarvi, adesso come successivamente), ne segue forse che ogni informazione che possa in teoria essere correlata ad una persona fisica è per ciò stesso, in via d'ipotesi, dato personale?

La risposta è ovviamente negativa, anche considerando la definizione di dato personale sopra richiamata, che non dispone una identità tra dato e dato personale

Una essenzializzazione della comprensione, cioè dei tratti distintivi della nozione di dato personale, con la correlata indefinita estensione della nozione stessa non ha, giuridicamente, utilità alcuna. Se le definizioni offerte dal diritto hanno uno scopo pratico, di regolazione di rapporti (infine) tra soggetti, tale scopo, per potersi realizzare efficacemente, ha bisogno di delimitare gli oggetti o i soggetti cui si applica: questo assunto di buon senso rappresenta il pur mobile argine a qualsiasi eccessiva generalizzazione, da

qualsivoglia soggetto pretesa (anche dalle stesse Autorità Garanti, che ovviamente tendono ad ampliare il proprio campo di intervento) dei criteri di applicazione di una norma.

La personalità di un dato deve essere valutata tanto attualmente, ora e adesso, come anche, diciamo così, su di un piano (non acriticamente ma) ragionevolmente prospettico. Occorrerà cioè determinare se la possibilità di identificazione, anche in un futuro prevedibile, abbia una ragionevole probabilità di attuarsi, e per far ciò dovranno prendersi in considerazione l'insieme dei mezzi che possono essere, appunto, *ragionevolmente* utilizzati allo scopo. Come riassume il Considerando n. 26 del Regolamento Generale:

> Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica (*To ascertain whether means are reasonably likely to be used to identify the natural person*), si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

Il principio secondo il quale l'interessato può ritenersi non identificabile se il rischio di identificazione è tale da far ritenere sproporzionati i mezzi eventualmente necessari per procedere all'identificazione stessa rispetto al pericolo di lesione dei diritti degli interessati che può derivarne, è esplicitato al comma 2 dell'art. 104 del *Codice*, *Ambito applicativo e dati identificativi per scopi statistici o scientifici,* per il quale appunto:

> in relazione ai dati identificativi si tiene conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal Titolare o da altri per identificare l'interessato, anche in base alle conoscenze acquisite in relazione al progresso tecnico[13]

[13] Nelle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101,* art. 4 comma 1, più analiticamente:

> un interessato si ritiene identificabile quando, con l´impiego di mezzi ragionevoli, è possibile stabilire un´associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano;
>
> (…) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
>
> - risorse economiche;
> - risorse di tempo;
> - archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
> - archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;
> - risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
> - conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;..

Si parla di *sviluppi tecnologici* e di *progresso tecnico*.

Si evidenzia come l'ambito nel quale deve apprezzarsi la probabilità di identificazione sia relativa non solo al titolare, ma anche ad "altri" soggetti; quindi la valutazione circa la identificabilità della persona fisica cui si riferisce il dato non deve essere effettuata solo nell'ambito del titolare e delle informazioni in suo possesso (ed è ovvio che, se comunico o diffondo una informazione, aumentano esponenzialmente i soggetti che possono a loro volta detenere informazioni che, associate con quelle di partenza, determinino un effetto identificativo).

Occorrerà dunque prendere in considerazione le informazioni ulteriori che, per altra via, un soggetto potrà avere acquisito, e non solo le tecnologie al momento disponibili, ma anche i loro futuri "sviluppi" (comunque prevedibili).

Dunque, la sola attuale possibilità di identificazione non è sufficiente ad escludere la personalità del dato; ma, simmetricamente, l'ipotetica possibilità di identificazione non è sufficiente per considerare un interessato identificabile, dovendo il discorso porsi piuttosto su un piano di *probabilità*: se, tenendo conto dell'insieme delle risorse tecniche ed informative che possono essere *ragionevolmente* utilizzate per identificare detta persona, e che possono *ragionevolmente*, anche in un tempo successivo, prevedersi come disponibili, quella possibilità non esiste o è trascurabile, quella persona non dovrebbe essere considerata identificabile, e tali dati non dovrebbero essere qualificati come dati personali.

Diciamo che, in generale, occorre applicare un principio di precauzione, ma sempre con ragionevolezza, assumendosi, al solito, la responsabilità di una equilibrata valutazione.

9.2. Sulle diverse tipologie di dati personali

Il Regolamento Generale, dopo aver offerto all'art. 4 1) la nozione di dato personale, specifica poi, sempre all'art. 4, ai punti 13-15, quelle di dati genetici, dati biometrici e dati relativi alla salute. Tali tipologie di dati sono ricomprese dall'art. 9 tra le *categorie particolari di dati personali* (assieme ai dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, e ai dati relativi alla vita sessuale o all'orientamento sessuale della persona); sono categorie particolari perché, in relazione alla loro sensibilità per i diritti della persona (nel Codice pre adeguamento si chiamavano infatti dati *sensibili*, anche se nell'elenco di questi non erano presenti i dati genetici, i dati biometrici e si parlava solo di dati relativi alla vita sessuale – in binomio con quelli idonei a rivelare lo stato di salute – e non anche di dati relativi all'orientamento sessuale), hanno particolari modalità di trattamento: anzi, l'art. 9 par. 1 ne vieta *prima facie* il trattamento, salvo che per alcune finalità che sono elencate nel paragrafo successivo. Tale peculiarità di trattamento trova senz'altro ragione nel fatto che la maggior parte di essi sono stati e possono tutt'oggi essere utilizzati a fini

discriminatori. In particolare, la preoccupazione del legislatore di prendere atto di rischi storicamente accertati può evidenziarsi nel ricomprendere tra le categorie particolari di dati quelli relativi alla razza: alcuni commentatori avevano manifestato, già in passato, perplessità circa l'opportunità di inserire in un testo normativo il riferimento ad un concetto la cui scientificità è nulla. Attenzione che ribadisce il fatto che scopo della normativa non è la protezione dei dati – dati che in questo non hanno nessuna reale consistenza epistemologica, e che certo non hanno alcuna ragione di essere tutelati - e neppure della riservatezza (non c'è alcuna informazione segreta da tutelare), quanto quella delle persone fisiche che potrebbero subire le conseguenze di un loro trattamento (come è stato osservato, il fatto che le razze non esistano non significa che non esista il razzismo).

L'art. 10 è poi dedicato ai *dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza*.

In alcune informative si trova scritto che saranno trattati dati personali e sensibili (tralasciamo il fatto che dato sensibile non è espressione più in uso); è una dizione esatta?

No, in quanto il rapporto dei primi rispetto ai secondi non è paritetico, ma piuttosto da genere a specie, In generale, infatti, possono individuarsi tre macrocategorie di dati personali:

- categorie particolari di dati personali;
- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- dati personali diversi dalle tipologie sopra indicate (che possiamo chiamare: *dati comuni*).

Preso atto che il Regolamento Generale parla di *dato personale*, al singolare, e poi, al plurale, di *categorie particolari di dati personali* e di *dati relativi alle condanne penali e ai reati*, ne segue che:

- la definizione di dato personale è incentrata sul collegamento tra un dato e l'interessato e la sua identificabilità, e dunque su cosa rende un mero dato una informazione riferita ad una certa persona fisica (che viene per questo a qualificarsi come *interessato*), cioè un dato personale;
- le nozioni di *categorie particolari* di dati personali e di *dati relativi alle condanne penali e ai reati*, acquisito che si tratta di informazioni riferibili ad un interessato ovvero di dati personali, si appuntano sul contenuto conoscitivo, sulla specifica tipologia di informazioni che essi sono idonei a rivelare (per quanto riguarda i dati comuni, in via residuale, sulla specifica tipologia di informazioni che essi *non* sono idonei a rivelare).

In breve: la definizione di dato personale ci dice quando un dato ha, appunto, carattere personale; le altre definizioni indicano e classificano le macrotipologie di dati personali,

raggruppate in relazione alle rispettive tipologie di contenuto conoscitivo che esse sono idonee a rivelare; in quanto tali, esse la presuppongono e sottendono, ma ponendosi ad un diverso livello (potremmo dire: *tres res una substantia*).

Tale contenuto conoscitivo, beninteso, può non palesarsi immediatamente, nel senso che le caratteristiche che qualificano un dato come, ad esempio, afferente alle categorie particolari, possono non apparire subito evidenti, ma esser tali da doversi acquisire mediante un «trattamento intellettuale», come un confronto o una deduzione. Ad esempio, con la sentenza sul caso C-184/20, la Corte di Giustizia dell'UE ha stabilito che è possibile dedurre alcune informazioni riguardanti la vita sessuale o l'orientamento sessuale del dichiarante e del suo coniuge, convivente o partner dal nominativo di tale persona, anche se i dati da pubblicare ai sensi della legge «non sono, intrinsecamente, dati sensibili». Così, le opinioni politiche possono essere dedotte dalla destinazione del due per mille con la dichiarazione dei redditi, e l'orientamento filosofico da una donazione. Vero è che, come cerchiamo di argomentare del § successivo, tali estensioni devono essere mantenute su un piano di ragionevolezza, considerato che una finalità di protezione meglio si attua se si riesce a distinguere, al di là del dato formale, la concreta specificità degli oggetti cui si rivolge.

Comunque sia, utilizzando una terminologia ripresa dalla teoria documentale, potremmo dire che all'informazione generica *dato personale*, nel caso delle varie tipologie di dati ad essa si associano ulteriori metadati che ne determinano una caratterizzazione specifica e concreta (così come un documento che abbia certe caratteristiche può essere qualificato come un documento amministrativo).

Cerchiamo di individuare adesso, quali possono essere i metadati che caratterizzano i dati relativi alla salute.

9.3. Quali dati sono qualificabili come relativi alla salute

Coerentemente con quanto sopra osservato, ci interessa una definizione non solo formalmente corretta, ma ragionevole, applicabile e funzionale allo scopo (ovvero alla finalità di protezione). Anche se, da un punto di vista antropologico, oramai la prospettiva della salute (dei rischi per la salute) si è pericolosamente estesa ad ogni aspetto della vita privata e sociale, (gli "stili di vita"), cercheremo comunque di calibrare il campo di applicazione di quella nozione in modo da renderlo coerente con quella finalità, evitando che la sua estensione ne comprometta la specificità, con un approccio dunque di carattere eminentemente consequenziale.

Ciò significa, in pratica, che il tenore della definizione deve essere tale da non comportare conseguenze irragionevoli. La prova del nove della ragionevolezza della definizione è data dal riferimento all'art. 2-septies commi 1 e 8 del Codice, per il quale i dati relativi alla salute non possono essere diffusi: ne segue che l'estensione della nozione di dato relativo alla salute dovrà confrontarsi con una sua comprensione che non comporti, nell'applicazione di tale divieto, conseguenze (nel senso dei divieti) appunto assurde. Ad una età anagrafica avanzata sono senz'altro correlate tipiche patologie, ma se l'età anagrafica in quanto tale fosse classificata come un dato relativo alla salute, considerato che i dati relativi alla salute non possono essere diffusi, ne seguirebbe che non sarebbe possibile pubblicare la foto di un anziano. In realtà, nonostante il giovanilismo corrente, un anziano, con tutti i suoi problemi, e anche se necessita di un bastone per poter camminare, non è un malato, è semplicemente un anziano. Allo stesso modo, sosterremo che l'immagine di un ragazzo in carrozzina non reca una informazione relativa ad un disabile, ma una immagine relativa ad un ragazzo; e così per quella di un fumatore e di una persona che porta gli occhiali. O, almeno, che sono dati relativi alla salute o no non in assoluto, ma a seconda dell'ambito o dello scopo del trattamento.

La definizione di «dati relativi alla salute» ("data concerning health'" nel testo inglese, così come già all'art. 8 comma 1 della Direttiva), offerta dall'art. 4 15 del Regolamento Generale, è la seguente:

> i dati personali attinenti alla (*related to*) salute fisica o mentale di una persona fisica, compresa (*including*) la prestazione di servizi di assistenza sanitaria, che rivelano (*which reveal*) informazioni relative al suo stato di salute

Più articolata e distesa la definizione contenuta nel Considerando n. 35, integrata da una casistica esemplificativa:

> i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso (*all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject*). Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio[14]; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro (*a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test)*.

Riassumendo:

- per l'art. 4 15); i dati relativi alla salute sono:

[14] Direttiva 2011/24/UE del Parlamento Europeo e del Consiglio del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera

> i dati personali attinenti alla salute … di una persona fisica, che rivelano informazioni relative al suo stato di salute.

- per il Considerando n. 35, sono:

> i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso

Le due definizioni appaiono a prima vista tautologiche; ma solo a prima vista, in realtà: dal tenore delle definizioni, si ricava che i dati relativi alla salute non sono *tout court* tutti "i dati personali che rivelano informazioni relative allo stato di salute". I dati in oggetto devono essere dati di per sé, in partenza, "attinenti alla salute" (*related to the physical or mental health*) o "riguardanti lo stato di salute dell'interessato" (*pertaining to the health status)*; *attinenti/riguardanti* (*relating/pertaining*) nel senso di dati che in quel particolare contesto, al di là delle inferenze sullo stato di salute dell'interessato che possono seguirne in via generale (l'anziano ha le patologie tipiche della sua età, chi porta occhiali da vista ha un difetto alla vista), hanno, nello specifico contesto di utilizzo, una relazione *funzionale* o *strumentale* rispetto ad un ambito sanitario o ad una disabilità.

Il Considerando n. 35 ricomprende tra i dati relativi alla salute "le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici"; e, più ampiamente "qualsiasi informazione riguardante, .. lo stato fisiologico o biomedico dell'interessato". Parrebbe tutto ovvio; ma si evidenzia come la nozione non si riferisca solo ad uno stato di salute compromesso, "le informazioni risultanti da esami e controlli effettuati" potendo infatti riguardare un accertamento tanto positivo che negativo (ad es di uno stato di infezione, come il tampone COVID negativo), e dunque qualsiasi informazione circa l'accertamento o il suo esito in sé, piuttosto che di un effettivo stato patologico: non la malattia, dunque ma appunto lo stato di salute, ovvero la caratterizzazione di una persona fisica dal punto di vista sanitario[15].

E' questa fondamentale correlazione, sia diretta che anche indiretta, con l'ambito sanitario che dobbiamo intanto tener presente per una corretta qualificazione del dato relativo alla salute.

Ciò non significa certo ricondurre i dati relativi alla salute ai soli dati clinici. Esemplifichiamo alcune tipologie di informazioni che si è pacificamente convenuto in passato dover rientrare tra i dati relativi alla salute:

[15] Per il Considerando n. 35, nei dati personali relativi alla salute rientrano anche "le informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui (*in the course of the registration for, or the provision of, health care services as referred to in*) alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio". La Direttiva tratta specificamente della «assistenza sanitaria transfrontaliera», ovvero (art. 3 par. 1 e della stessa Direttiva) della "assistenza sanitaria prestata in uno Stato membro diverso dallo Stato membro di affiliazione". Riteniamo sia stata richiamata ad esemplificare un trattamento di dati a scopi amministrativi che integra un trattamento di dati relativi alla salute, in quanto attinenti alla fornitura di prestazioni sanitarie.

1. qualsiasi informazione di ambito sanitario riguardante lo stato fisiologico o biomedico dell'interessato, il rischio di malattie, l'anamnesi medica, i trattamenti clinici e i risultati di prestazioni sanitarie;
2. i dati amministrativi correlati alle prestazioni sanitarie effettuate o ad una situazione di malattia;
3. informazioni relative alla disabilità, anche qualora trattate in ambito amministrativo, ad esempio nell'ambito della gestione del personale o delle procedure di selezione.

Dobbiamo individuare quale sia l'elemento comune a queste informazioni, il *quid* che, pur nella loro diversità, le qualifica appunto tutte come dati relativi alla salute.

Per i punti 1 e 2 nessun problema: si tratta di dati che originano appunto in ambito sanitario e mantengono, nel contesto specifico del trattamento, un rapporto con esso, anche se, per quanto riguarda i dati amministrativi (ad es. un versamento per il pagamento di un ticket sanitario), indiretto.

Per i dati di cui al punto 3, il Considerando 35 definisce relativa alla salute, tra le altre, "qualsiasi informazione riguardante, ad esempio, … una disabilità".

Così, la pubblicazione dei nominativi degli interessati associati all'appartenenza alle particolari categorie previste dalla disciplina sul collocamento obbligatorio, comporta una diffusione (illecita) di dati relativi alla salute. In questo caso, le informazioni sono trattate in diretta correlazione con lo stato di disabilità; quei soggetti sono in quell'elenco *in quanto disabili*: quei nominativi sono qualificabili come dati relativi alla salute, ed esigenze di trasparenza dovranno essere bilanciate con particolari garanzie di riservatezza.

Ricordo che, nei primi tempi di applicazione della L. 675/96 - quando gli apocalittici di turno facevano a gara a delineare incombenti scenari catastrofici per le nostre abitudini e libertà (come l'idea che senza il consenso degli interessati non potevamo più tenere una agenda telefonica o un album fotografico) - fu anche brillantemente sostenuto che non sarebbe più stato possibile esporre la foto di una classe scolastica nella quale fosse presente un alunno in carrozzina, in quanto essa appunto configurava una diffusione di dati relativi alla salute: con l'eccellente (e consueta) conseguenza di stigmatizzare ed escludere ulteriormente l'interessato per il nobilissimo scopo di proteggerlo.

Dunque, perché posso diffondere la foto di un soggetto invalido ma non pubblicare il nominativo del suddetto invalido con il provvedimento che lo elenca tra i vincitori di una selezione per le categorie protette?

Lo abbiamo già capito: perché nel primo caso non viene in primo piano la condizione di disabilità, l'informazione non è rispetto ad essa direttamente funzionale, mentre nel secondo caso (nel quale si intende assicurare un vantaggio compensativo al soggetto in quanto disabile) sì.

Certo, se la stessa foto del disabile in carrozzina, invece, ad esempio, che essere pubblicata sul profilo Facebook della scuola, fosse utilizzata per bullizzare il soggetto ripreso, risulterebbe preponderante l'aspetto della disabilità ed i conseguenti obblighi di protezione.

Dunque, variamente esemplificando sulla base di quanto sopra osservato, integrano dati relativi alla salute le attività relative:

- agli accertamenti ematici a favore dei donatori di sangue, che non sono eseguiti sulla base di una ipotesi diagnostica ma che si svolgono comunque in ambito sanitario ed esitano in un accertamento sullo stato di salute;
- alle informazioni di carattere amministrativo relative alla effettuazione di accertamenti sullo stato di salute, che rivelano non tanto gli esiti ma il fatto in sé di quell'accertamento, ad esempio: informazioni relative al pagamento del ticket per una prestazione sanitaria, indipendentemente dal fatto che si possa evincere quale prestazione sia stata effettuata; prenotazione di servizi sanitari; dati amministrativi relativi alla presenza di un assistito in ospedale, ad un ricovero o ad una terapia, o alla residenza in una residenza sanitaria assistita;
- ad una condizione o status che, pur riferiti ad un ambito non sanitario, sottendano e presuppongano una situazione di carattere patologico o di disabilità: il congedo per malattia del dipendente, anche se privo di alcuna informazione specifica sullo stato di salute che l'ha determinata, la corresponsione di una pensione di invalidità, un ticket ridotto in riferimento ad una – anche indeterminata - esenzione per patologia, i dati relativi al godimento di congedi ex L. 104/92, informazioni relative alla interdizione dal lavoro delle lavoratrici in stato di gravidanza ai sensi dell'art. 17 comma 2 a del D.Lgs. 151/2001 (ovvero qualora vi siano "gravi complicanze della gravidanza o persistenti forme morbose che si presume possano essere aggravate dallo stato di gravidanza", non dunque in riferimento allo stato di gravidanza in quanto tale); il giudizio di idoneità o inidoneità all'esercizio dell'attività sportiva agonistica (in una risalente interpretazione, il Garante invece non identificava un dato relativo alla salute nel giudizio di idoneità all'esercizio dell'attività sportiva agonistica).

Non devono invece ricomprendersi tra i dati relativi alla salute quelli genericamente relativi allo stile di vita (salvo che siano trattati direttamente in ambito sanitario), posto che un certo stile di vita – ad es. quello del fumatore – favorisce ma non comporta sempre e necessariamente la compromissione dello stato di salute, e non è dunque qualificabile come dato attinente la salute (la valutazione opposta comporterebbe comunque, come visto, l'illiceità di riprendere la foto di un fumatore). Oltre a questo, considerato che uno stato di salute è tale anche se non presenta aspetti patologici, dovremmo altrimenti ricomprendere tra i dati relativi alla salute ogni stile di vita (con la conseguenza che alla fine ogni comportamento diventerebbe dato relativo alla salute – cioè allo stato di salute, buono o cattivo che possa essere - il che è assurdo).

10. Dati anonimi e anonimizzazione

Vi sono tipologie di dati e finalità del trattamento che non rientrano nell'ambito di applicazione del Regolamento Generale. Sono i dati anonimi, che non sono dati personali (mentre lo sono i dati cd. pseudonimizzati, cfr. § 11), e i dati trattati per scopi personali (cfr. § 12).

E' stato osservato che anche informazioni ausiliarie, come "l'uomo che indossa un abito nero" possono permettere di identificare qualcuno fra i passanti fermi ad un semaforo (ma non ad es. allo stadio). Insomma, il fatto che una persona cui si riferisce l'informazione venga identificata o meno, subito o successivamente, dipende ordinariamente dalle circostanze dello specifico contesto.

Tale assunto potrebbe apparire contrastante con la valutazione, espressa da varia dottrina nonché seguita dalla Autorità Garante, che quella di dato personale deve considerarsi nozione *assoluta*, per cui una certa informazione o è dato personale oppure non lo è, indipendentemente dal contesto di utilizzo: o meglio, se lo è in uno di tali contesti, lo è in tutti, ed è dunque sufficiente che in un dato ambito una informazione possa avere, variamente combinata con altre, valore identificativo (o distintivo) perché la si debba considerare *tout court* dato personale. Si deve dunque ammettere che la sopra richiamata condizione di avere un abito nero può essere considerata un dato personale quando la persona fisica passa dal semaforo allo stadio? Ovviamente no. Lo sarebbe solo se quella caratteristica restasse chiaramente evidente, caratterizzante, rispetto a quella persona fisica, se conservasse cioè un valore *identificativo*, non solo nel senso della identificazione ma anche della identificabilità; si ricordi che, secondo la nozione di dato personale offerta dal Regolamento, "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un *identificativo* come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più *elementi caratteristici* della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". L'abito nero non rappresenterebbe dunque un elemento identificativo, probabilmente, se la persona fisica si trasferisse dal semaforo allo stadio o forse anche se l'abito dell'uomo al semaforo, invece che nero, fosse descritto più genericamente come "scuro", oppure "non rosso". In tal caso, sono infatti, probabilmente, numerose le persone fisiche alle quali tale informazione potrà correlarsi, così che essa perderebbe valore identificativo. In che senso allora la nozione di dato personale deve considerarsi assoluta? E come è possibile anonimizzare un dato personale?

Anticipiamo, in breve, la risposta: il dato è personale se è costituito da o connesso ad un reticolo di informazioni che, restando stabili, ne determinano in modo assoluto, appunto, la personalità, cioè se sono univocamente riferibili ad un interessato (e ciò, in astratto, resta vero anche in un contesto di utilizzo diverso da quello originario); un dato non è personale se tale riferibilità non ha, o non ha più (attraverso una elaborazione) valore identificativo, ovvero se quella informazione o quelle informazioni sono riferibili a più soggetti, giusta la definizione di dato personale come "qualsiasi informazione riguardante *una* persona fisica identificata o identificabile" (e non *più persone fisiche*).

Secondo il Considerando n. 26:

> I principi di protezione dei dati non dovrebbero … applicarsi a informazioni anonime, vale a dire informazioni che non si

> riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

Si ricomprendono in questo Considerando due piani diversi; anzitutto, si definiscono come anonime le informazioni che, fin da subito o almeno attualmente, "non si riferiscono a una persona fisica identificata o identificabile"; considerato che anonime possono essere non solo informazioni che sono fin da subito tali ma che lo diventano a seguito di un processo di elaborazione, si introduce poi il concetto di anonimizzazione, nel caso appunto di "dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato", ovvero dati che da personali diventano non personali, anonimi.

Il dato anonimo può dunque preesistere, darsi come tale oppure ottenersi successivamente, dopo un processo che ha una sua durata temporale e che viene definito *anonimizzazione*.

L'anonimizzazione è una tecnica che si applica ai dati personali al fine di ottenere una deidentificazione assoluta e irreversibile.

Dato anonimizzato e dato anonimo dovrebbero possedere, ad un certo punto, eguale contenuto informativo, tendente ad un grado zero per quanto riguarda la loro riferibilità, diretta (immediata, fin da subito) o indiretta (attraverso l'utilizzo di ulteriori informazioni, quindi mediatamente, con uno iato logico che è anche temporale), ad una persona fisica.

Con la nozione di dato *reso sufficientemente anonimo* (che non appare, in effetti, felicissima), si intende, evidentemente, che il contenuto informativo di un dato viene progressivamente a ridursi fino ad un punto in cui la sua capacità identificativa si annulla.

Il testo inglese, molto più pianamente, di "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"; definizione questa allineata con quella già offerta dall'art. 4 comma 1 n) del *Codice* pre revisione come "il dato che …, a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile".

Insomma, l'aspetto informativo del dato – dal punto di vista della sua riferibilità ad una certa persona fisica – si attenua fino a scomparire, e se il dato personale è informazione (riferita ad una persona fisica), allora quel dato non è più un dato personale.

Il dato o è personale, cioè può essere associato (immediatamente o poi) ad una persona fisica, o non può esserlo, e allora è un dato anonimo, *tertium non datur* (non è una ulteriore tipologia il dato pseudonimizzato, che resta comunque un dato personale, cfr. il § successivo)[16].

[16] A voler essere precisi, una corretta tassonomia dovrebbe prevedere, nella più ampia categoria dei dati:
- i dati personali (informazioni riferite o riferibili ad una data persona fisica: la temperatura corporea di Tizio);
- i dati anonimi (informazioni non riferite o riferibili ad una data persona fisica, ma che in astratto lo possono essere: un dato di temperatura corporea priva di ogni riferimento ad un soggetto);
- i dati non personali o naturali (es. la temperatura dell'aria).

Quel che è necessario evidenziare è che un set di dati privato dell'anagrafica non è, come secondo la nozione etimologica (*an onoma*) o di senso comune, un dato anonimo: una informazione può non essere immediatamente collegata ad un nominativo, ma esserlo successivamente (cioè ricorrendo ad ulteriori informazioni). Un set di dati è dunque *anonimo*, nel senso tecnico giuridico del termine, solo se è *definitivamente* e *irreversibilmente* privato, anche prospetticamente, di una possibilità di raccordo con la relativa anagrafica, nel senso che questa non è più recuperabile (e non è dunque mai possibile una reidentificazione).

Il Gruppo ex art. 29, il 10 aprile 2014 aveva adottato il Parere 05/2014 *Sulle tecniche di anonimizzazione* (ovviamente ci si riferiva alla regolazione dettata dalla Direttiva 46/95, non essendo il Regolamento ancora stato adottato). Vi si osserva:

> L'anonimizzazione è il risultato del trattamento di dati personali volto a impedire irreversibilmente l'identificazione … costituisce un trattamento successivo dei dati personali; (…) per rendere anonimi determinati dati, gli stessi devono essere privati di elementi sufficienti per impedire l'identificazione della persona interessata. Più precisamente, i dati devono essere trattati in maniera tale *da non poter più essere utilizzati* per identificare una persona fisica utilizzando l'insieme dei mezzi che possono essere ragionevolmente utilizzati ….
> Un fattore importante è che il trattamento deve essere *irreversibile*. La direttiva non specifica come si debba o si possa effettuare il processo di anonimizzazione. L'accento è posto sul risultato: i dati devono essere tali da non consentire l'identificazione della persona interessata mediante l'insieme dei mezzi che "possono" essere "ragionevolmente" utilizzati. (…).
> Il fondamento logico è che il risultato dell'anonimizzazione quale tecnica applicata ai dati personali dovrebbe essere, allo stato attuale della tecnologia, *permanente come una cancellazione, vale a dire dovrebbe rendere impossibile il trattamento dei dati personali*.

Nel Parere si precisa inoltre (nella Direttiva quando si parlava di Responsabile si intendeva quello che nella sistematica del *Codice* e del Regolamento Generale è il Titolare) che:

Tenuto comunque presente che anche alcuni dati ordinariamente 'naturali' possono considerarsi, in certe circostanze, dati personali (il dato ad es. della pressione dell'acqua, nel momento in cui rientra ad es. in una valutazione medico legale quale causa dell'embolia di un sub), ed evidenziato dunque ancora che il dato personale è sempre una informazione di carattere contestuale e circostanziale, di seguito ci occuperemo solo di dati personali vs dati anonimi.

> … *quando un responsabile del trattamento non cancella i dati originali (identificabili) a livello di evento, e trasmette poi parte di questo insieme di dat*i (ad esempio, dopo l'eliminazione o il mascheramento dei dati identificabili), *l'insieme di dati risultante contiene ancora dati personali.* Soltanto se il responsabile del trattamento aggrega i dati a un livello in cui i singoli eventi non sono più identificabili si può definire anonimo l'insieme di dati risultante. Ad esempio, se un'organizzazione raccoglie dati sugli spostamenti delle persone, i tipi di spostamenti individuali a livello di evento rientrano ancora tra i dati personali per tutte le parti coinvolte, fintantoché il responsabile del trattamento (o altri) ha ancora accesso ai dati non trattati originali, anche se gli identificatori diretti sono stati espunti dall'insieme dei dati forniti a terzi. Tuttavia, se il responsabile del trattamento cancella i dati non trattati e fornisce a terzi solamente statistiche aggregate ad alto livello, ad esempio "il lunedì sulla rotta X i passeggeri sono più numerosi del 160% rispetto al martedì", i dati possono essere definiti anonimi.

Riassumendo: la copia di una stringa coerente di informazioni, pur priva degli elementi direttamente identificativi, non reca mai dati che si possano dire anonimi laddove la stringa originale resti integra. Simmetricamente: il requisito fondamentale affinché un insieme di informazioni, ancorché privo di un nominativo di riferimento, non sia qualificabile come dato personale, è che la loro configurazione non possa essere associabile ad una analoga che sia connessa o collegabile ad un interessato, ovvero questa non possa essere individuata, ancorché oggetto di modifiche, come matrice dell'altra.

Considerato che, ordinariamente, una azienda sanitaria trae le informazioni, per la relativa anonimizzazione, da documenti a conservazione obbligatoria ed illimitata, ciò significa che per tali informazioni (per le informazioni caratterizzanti le attività di una azienda sanitaria) una anonimizzazione sia per principio impossibile, sempre che le informazioni che residuano da un intervento di elaborazione non siano dati aggregati o almeno dati che non consentano un collegamento biunivoco con quelli originali; l'esito identificativo si ha infatti sempre qualora vi sia una correlazione biunivoca (uno a uno) tra le configurazioni originali di informazioni e quelle esito di elaborazione o selezione; e non lo si ha solo qualora tale correlazione non si realizzi.

10.1. Tecniche di anonimizzazione

L'anonimizzazione è dunque il risultato di tecniche che vengono applicate ai dati personali col fine di rendere la re-identificazione degli interessati ragionevolmente impossibile. La re-identificazione è la eventualità in cui, partendo da dati erroneamente ritenuti anonimi, si riesca a recuperare informazioni identificative degli interessati, sia direttamente, sia tramite metodi di correlazione e deduzione. Si distingue tra tecniche di randomizzazione e tecniche di generalizzazione.

Tecniche di randomizzazione = consistono nella modifica della veridicità dei dati al fine di eliminare la forte correlazione che esiste tra essi e la persona.

Sostituzione degli attributi . Consiste nel cancellare o modificare l'insieme di dati correlati alle persone atipiche o i valori atipici rispetto all'insieme di attributi complessivo.

Rumore statistico. Consiste nel modificare gli attributi contenuti nell'insieme di dati in modo da renderli accurati a livello di singola attività di informazione. Tale sistema permette l'affiancamento di altre tecniche, di anonimizzazione e generalizzazione, quali la sostituzione o eliminazione degli attributi ad altro valore identificativo

Privacy differenziale. Consiste nell'evitare la pubblicazione dell'intero insieme di dati, ma solo dei sottoinsiemi elaborati in risposta a specifiche query di ricerca.

Permutazione. Consiste nel mescolare i valori degli attributi in modo che essi risultino artificialmente collegati a persone interessate diverse

Tecniche di generalizzazione = consistono nel generalizzare gli attributi delle persone interessate, diluendo i livelli di dettaglio

Generalizzazione dei singoli attributi. Consiste appunto nella generalizzazione dei dati reali: utilizzo di fasce di età rispetto alla data di nascita, generalizzazione dell'area geografica, generalizzazione del dato reale del periodo di ricovero ecc.

Aggregazione / K.-Anonimato. Sono tecniche volte ad impedire l'individuazione di persone interessate mediante il loro raggruppamento con almeno K altre persone (K=valore di soglia). Secondo la *regola della soglia*, le persone cui si riferiscono i dati si considerano non identificabili se il loro numero è superiore ad un certo valore prestabilito (*valore di soglia*). Il valore minimo ordinariamente attribuibile alla soglia è pari a tre (ma nel valutare il valore della soglia si deve tenere conto del livello di sensibilità delle informazioni, e dell'effettivo rischio di danno ad esse correlato: insomma, in riferimento ad es. ai dati relativi alla sieropositività una soglia pari a tre potrebbe apparire insufficiente). La regola della soglia sottende che il valore originale X possa essere riferito non al solo Caio, ma anche a Tizio, Tazio e Sempronio. La relazione biunivoca tra il valore X ed una (una sola) persona fisica viene così meno. A tale scopo, gli attributi possono essere sottoposti a una generalizzazione tale da associare a ciascuno dei K individui del gruppo il medesimo valore.

L-Diversità / C-Vicinanza. Ampliando il principio del K-Anonimato, la L-Diversità si realizza facendo sì che in ciascuna classe di equivalenza ogni attributo abbia almeno L valori diversi, così da limitare la presenza di classi di equivalenza con una scarsa variabilità degli attributi (ogni attributo di equivalenza deve ricorrere almeno L volte). La T-Vicinanza rappresenta un affinamento della L-Diversità, in quanto mira a creare classi equivalenti che assomiglino alla distribuzione iniziale di attributi nella tabella;

non solo devono esistere L valori diversi all'interno di ogni classe, ma ogni valore è rappresentato tante volte quanto sono necessarie per rispecchiare la distribuzione inziale di ciascun attributo.

10.2. Anonimizzazione delle immagini

Questa è questione ulteriore, successiva ed eventuale, ma laddove una immagine consenta anche solo, intanto, di distinguere una persona fisica, siamo già nell'area del dato personale; o meglio: siamo già nella situazione in cui è necessario proteggere una persona dal trattamento di informazioni che, evidentemente, la riguardano, e sono per ciò stesso (funzionalmente allo scopo di protezione) qualificabili come dati personali. Riassumendo il concetto nei termini di una sentenza della Cassazione civile del 2014 (sez. III, 27.01.2014 n° 1608), "... l'individuabilità della persona ... non ne postula l'esplicita indicazione del nominativo, essendo sufficiente che essa possa venire individuata anche per esclusione in via deduttiva, tra una categoria di persone ...".

E contrario, il Garante si è espresso positivamente sulla utilizzabilità di immagini che non permettano, ad es. semplicemente attraverso la solarizzazione del volto, di riconoscere l'interessato. Ovvio che non debbano esservi altre informazioni, ad es. un tatuaggio particolare.

Ragionando nei termini del principio della soglia: l'immagine è dato personale nella misura in cui è riferibile univocamente ad un soggetto, pur se non attualmente identificato; non lo è quando tale univoca riferibilità non è possibile, secondo un criterio di soglia. Ne consegue che, da un punto di vista strettamente formale e consequenziale, un'immagine di diagnostica radiologica – una TAC ad esempio – non potrebbe mai considerarsi anonimizzabile.

10.3. Quali sono i presupposti per poter procedere alla anonimizzazione dei dati?

Posto che la anonimizzazione è definita come un trattamento, che sarà dunque, come qualsiasi altro trattamento, caratterizzato da una determinata finalità, ne segue perciò che il titolare, prima di procedere ad essa, deve già possedere la base giuridica che lo legittima rispetto a tale finalità? Ad esempio: si intendono anonimizzare dati relativi alla salute per scopo di ricerca; posto che la ricerca clinica si legittima ordinariamente con il consenso degli interessati, ciò significa che senza il consenso degli interessati il titolare non può procedere ad anonimizzare quei dati?

Si è visto sopra che il Regolamento è informato ad un generale *principio di necessità*, che possiamo tradurre, in particolare se correlato ad una determinata finalità – attraverso pertinenza e non eccedenza – nel principio di minimizzazione (§ 6.3).

Nella precedente versione del Codice, l'art. 3, oggi abrogato, era appunto rubricato *Principio di necessità nel trattamento dei dati,* e significativamente inserito nel *Titolo I* del *Codice,* dedicato ai *Principi generali*. Esso, soprattutto ma non esclusivamente in riferimento a quando il trattamento viene effettuato con strumenti elettronici – vi si parla

infatti, più in generale, di "sistemi informativi" e non solo informatici - prescriveva di trattare i dati:

> riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Si trattava di una cautela che si traduceva, di fatto, in un obbligo di carattere generale, e dunque in una prerogativa del titolare. Riteniamo, che tale prerogativa sia tuttora riconoscibile, e che pertanto il Titolare possa, con le dovute cautele – in particolare dal punto di vista dell'accesso ai dati identificativi – procedere alla anonimizzazione delle informazioni per qualsivoglia finalità lecita (non, ad esempio, per un ente pubblico, a scopi commerciali).

In accordo con tale impostazione, si rimanda alle considerazioni del *Codice di condotta per l'utilizzo di dati a fini didattici e a scopi di pubblicazione scientifica* della Regione Veneto (cfr. § 20.6), secondo il quale il presupposto giuridico per perseguire tali scopi è rappresentato dal consenso dell'interessato e, in alternativa, dalla anonimizzazione dei dati: così che, in assenza del presupposto giuridico fondamentale del trattamento per quelle finalità, è sempre possibile perseguire queste attraverso una procedura di anonimizzazione delle informazioni.

11. Pseudonimizzazione

Ribadiamo subito cosa i cd. dati *pseudonimizzati* non sono: non sono dati anonimi. I dati pseudonimizzati sono dati personali. Il Regolamento Generale introduce appunto la nozione di pseudonimizzazione, precisando all'art. 4 5 che essa è:

> il 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.

Possiamo definire lo pseudonimo come un *alias* associato a dati personali.

Il sopra citato Parere 05/2014 *Sulle tecniche di anonimizzazione,* precisava correttamente

> …. la pseudonimizzazione non è un metodo di anonimizzazione. Si limita a ridurre la correlabilità di un insieme di dati all'identità originaria di una persona interessata, e rappresenta pertanto una misura di sicurezza utile

Così, il Considerando n. 28 osserva che "L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati".

Di sicuro, la pseudonimizzazione, così come la anonimizzatone, è una operazione di trattamento dei dati.

12. Dati trattati per scopi personali

Ai sensi dell'art. 2 par. 2 lettera c) del Regolamento Generale, esso non si applica ai trattamenti di dati personali … effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Il Considerando 28 specifica che:

> Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

La notazione "personale o domestico" deve intendersi propriamente nel senso di "personale cioè domestico"; non è perciò esente dal rispetto degli obblighi normativi quel trattamento che si traduca in una comunicazione sistematica o diffusione dei dati (come chiaramente specificava l'art. 5 comma 3 della versione previgente del Codice)[17]. Al di fuori di queste situazioni, la disposizione legittima, senza che vi sia necessità di chiedere il consenso al trattamento da parte di ogni soggetto cui le immagini si riferiscano, i trattamenti di dati effettuati ad es. quando si fanno fotografie su una pubblica piazza o alla recita scolastica dei figli. Quando il Considerando specifica che non deve esservi "connessione con un'attività commerciale o professionale", evidenzia come quella esimente non possa operare in ambito aziendale e professionale. In particolare, non è legittimo che il personale di una Azienda Sanitaria utilizzi "a scopo personale" dati dei pazienti che abbia acquisito per finalità istituzionali.

[17] "Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31".

13. Cosa è un trattamento di dati personali

Per raggiungere un proprio determinato scopo o interesse, il Titolare (cfr. § 14) compie delle attività, delle operazioni sui dati: effettua un *trattamento* di dati personali.

La nozione di *trattamento (processing)* offerta dall'art. 4 2) del Regolamento Generale[18] è estremamente ampia, e ricomprende "qualunque operazione o insieme di operazioni" che abbiano ad oggetto ("applicate a") dati personali (e dunque tanto una singola operazione che una serie di operazioni), compiute o meno con l'ausilio di processi automatizzati (cioè di strumenti elettronici: è dunque trattamento di dati anche quello effettuato su supporti cartacei).

Ciò di cui si ha la titolarità non sono i dati quanto piuttosto il loro trattamento - la vigente normativa parla sempre di *titolare del trattamento* - cioè le operazioni effettuate sui dati (dalla raccolta o accesso in poi): con la conseguenza di porre al centro una attività, le operazioni, le azioni sui dati (un *facere*) piuttosto che i dati stessi, staticamente ed isolatamente intesi.

La nozione di trattamento offerta dalla normativa si risolve, essenzialmente, nelle operazioni che lo costituiscono. Quelle elencate dall'articolo sopra richiamato sono le seguenti:

> la raccolta *(collection*), la registrazione (*recording)*, l'organizzazione *(organisation)*, la strutturazione *(structuring)*, la conservazione *(storage)*, l'adattamento (*adaptation)* o la modifica *(alteration)*, l'estrazione *(retrieval)*, la consultazione *(consultation)*, l'uso *(use)*, la comunicazione mediante trasmissione *(disclosure by transmission)*, diffusione (*dissemination)* o qualsiasi altra forma di messa a disposizione *(otherwise making available)*, il raffronto (*alignment)* o l'interconnessione *(combination)*, la limitazione *restriction*, la cancellazione (*erasure)* o la distruzione *(destruction)*.

Rispetto alla posizione di quei commentatori che dall'ampiezza della nozione derivano che tale elenco debba considerarsi meramente esemplificativo, si è opposto un orientamento che lo considera invece tassativo, nel senso che la legge si applica alle sole operazioni che abbiano per effetto taluno dei risultati menzionati nella disposizione. In realtà è la definizione stessa che orienta verso la prima opzione:" *qualsiasi* operazione o insieme di operazioni, … applicate a dati personali o insiemi di dati personali, *come* …".

Ora, una nozione che si risolva in una serie di operazioni è di applicazione abbastanza problematica; ad esempio, l'art. 30 del Regolamento Generale prevede che il Titolare

[18] "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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"

tenga un registro delle attività di trattamento svolte sotto la propria responsabilità[19]. Quali oggetti devono essere censiti in tale registro come "trattamenti"? Come individuarli? Come distinguere un trattamento dall'altro? A tale scopo gli elementi presenti nella definizione – che si risolve appunto in un mero elenco di operazioni - non aiutano affatto in questa identificazione: decine di trattamenti possono infatti essere riassunti nelle operazioni di raccolta, elaborazione, utilizzo, conservazione, accesso.

La nozione di trattamento offerta dall'art. 4 2) del Regolamento Generale, in sostanza, pare avere lo scopo principale di responsabilizzare il soggetto – il titolare, se opera nel proprio interesse o comunque al di fuori di una delega – che effettua alcune operazioni che hanno ad oggetto dati personali. Nel senso che chi effettua operazioni sui dati esegue un trattamento di dati di cui dovrà rendere conto.

Vediamo però se le informazioni richieste per il Registro ex art. 30 del Regolamento Generale possono aiutarci a meglio circoscrivere in qualche modo l'oggetto "trattamento di dati personali". Esse sono:

1. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
6. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento Generale

Alcune di queste informazioni sono descrittive, oppure accessorie e strumentali (ad es. le 1, 4, 5, 6, 7); di carattere più sostanziale quelle dei punti 2 e 3, ovvero:

- le finalità del trattamento;
- le categorie di interessati;
- le categorie di dati personali.

Le categorie di dati (una specificazione dell'elemento astratto dato personale) indicano l'oggetto su cui le operazioni di trattamento effettivamente si esercitano; le categorie di

[19] Tale obbligo riguarda anche il Responsabile del trattamento, per i trattamenti che effettua per conto di altri Titolari.

interessati sono una informazione già implicita nella nozione di dato personale, considerato che laddove vi è un dato personale vi è un interessato (il quale dà dunque un contenuto alla *personalità* del dato); in questo caso occorre indicare le classi di persone fisiche interessate al trattamento (es.: dipendenti, utenti, familiari ecc.).

Per quanto riguarda la finalità (*pourpose*), pur non ricompresa nella definizione di trattamento, essa rappresenta a mio avviso quell'elemento che davvero ne restituisce l'aspetto unitario.

14. Chi è il titolare del trattamento

Ai sensi dell'art. 4 1) del Regolamento Generale, il titolare del trattamento è:

> la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, *determina le finalità e i mezzi del trattamento di dati personali*; 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 designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

Si qualifica dunque titolare del trattamento il soggetto (persona fisica o giuridica, autorità pubblica, servizio o altro organismo) *che determina le finalità e i mezzi del trattamento (which determines the purposes and means of the processing of personal data).*

Precisiamo che, secondo la definizione corrente, per *finalità* può intendersi "un risultato atteso o al quale attendono le azioni pianificate" e per *mezzi* "la modalità con la quale si ottiene un risultato o si raggiunge un fine"[20].

Dunque, non ogni soggetto, anche collettivo, che tratti dati personali è per ciò solo un titolare del trattamento: lo è solo è il soggetto, persona fisica o ente, che, al fine di soddisfare certi suoi scopi o interessi (finalità), decide di trattare (e dunque tratta) i dati personali a ciò necessari, con un apprezzabile margine di autonomia nel decidere i mezzi e le modalità del trattamento e nell'individuare le soluzioni tecniche e organizzative per realizzarli; non lo sarebbe invece il soggetto che tratti dati per conto di un titolare, ovvero per gli scopi di questo (il Responsabile del trattamento, cfr. § 15), né la persona fisica che, nell'ambito della organizzazione del titolare, svolge una attività a favore di questi (la persona autorizzata al trattamento, cfr. § 17).

Queste alcune altre possibili definizioni del titolare:

- una qualificazione che "deriva in primo luogo dal fatto concreto che un'entità ha scelto di trattare dati personali per propri fini" (Parere WP 29 n. 1/2010);

[20] EDPB (European Data Protection Board) .*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR* adottate il 7 luglio 2021, pag. 15.

- il soggetto che "stabilisce il motivo e la modalità del trattamento" *(Manuale di diritto europeo in materia di protezione dei dati);*
- «la persona fisica o giuridica, l'autorità pubblica, il servizio, l'agenzia od ogni altro organismo che, da solo o insieme ad altri, *esercita il potere decisionale sul trattamento dei dati*» (Convenzione n. 108 modernizzata - o anche Convenzione 108+ il cui protocollo di modifica è stato firmato dall'Italia il 5 marzo 2019; n Relazione esplicativa alla Convenzione si precisa che tale potere decisionale riguarda le finalità e i mezzi del trattamento, nonché le categorie di dati da trattare e l'accesso ai dati);
- "una persona fisica o giuridica che, a scopi che le sono propri, influisca sul trattamento dei dati personali e partecipi pertanto alla determinazione delle finalità e degli strumenti di tale trattamento" (Corte di Giustizia Europea – sentenza del 10 luglio 2018);
- Il soggetto che decide "il perché e il come del trattamento" (ovverosia "a quale fine" o "per che cosa" viene svolto), e come tale obiettivo viene raggiunto (ovverosia quali sono i mezzi impiegati per conseguirlo).

E' insomma il grado di influenza esercitata sulla definizione in concreto del *se,* del *perché* e del *come* del trattamento che comporta l'attribuzione ad un soggetto della qualifica di titolare.

Il termine inglese utilizzato nella Direttiva e anche oggi nel Regolamento Generale è *controller*, controllore (il *controllore di volo* è in inglese l'*air traffic controller*), ad indicare il soggetto che appunto controlla il trattamento, in due sensi almeno: è il soggetto che sovrintende complessivamente al relativo processo, determinandone l'attivazione e la continuazione per dati scopi (propri) e secondo certe modalità, e che al contempo se ne responsabilizza, e ciò anche quando l'attività è delegata ad altro soggetto.

Si diceva che il titolare è il soggetto che "determina le finalità e i mezzi del trattamento di dati personali"; certo, questa definizione appare poco soddisfacente nella misura in cui pone sullo stesse piano la finalità e i mezzi del trattamento, considerato che lo scopo che muove un soggetto a trattare dati, in realtà, preesiste alla determinazione di utilizzare certe informazioni secondo certe modalità, essendo lo scopo che le condiziona e seleziona: fatto ancora più evidente nel caso delle finalità istituzionali degli enti pubblici. Potremmo meglio dire che:

> il titolare è il soggetto che, in riferimento a propri scopi e finalità, determina di avviare attività che comportano un trattamento di dati personali individuandone i mezzi e le modalità di esecuzione

Se l'obiettivo, la finalità del trattamento, deve essere senz'altro individuato dal titolare, questi, per poter essere qualificato tale, non deve necessariamente determinare ogni mezzo e modalità del trattamento, ma soltanto quelli ad esso *essenziali*. Per mezzi *essenziali* si intendono quelli strettamente legati alla finalità e alla portata del trattamento, tra i quali:

- Il tipo di dati personali trattati;
- la durata del trattamento;
- le categorie dei soggetti che possono accedere ai dati;

- le categorie di interessati.

I mezzi *non essenziali* riguardano ad es. la scelta del software con il quale effettuare il trattamento, o l'adozione di specifiche misure informatiche di sicurezza: i mezzi non essenziali possono essere lasciati nella disponibilità del responsabile del trattamento.

Il Garante, così come il Gruppo dei Garanti europei, ha ripetutamente osservato che la nozione di *titolare* proposta dalla normativa ha una sua specifica *autonomia,* nel senso che va principalmente interpretata, pur se fonti giuridiche esterne possono aiutare ad identificare tale figura, alla luce delle disposizioni relative alla protezione dei dati, ed adottando un approccio di tipo *fattuale* e *funzionale*.

E' una nozione di carattere *fattuale* perché, al di là di valutazioni di legittimità o liceità, il titolare è anzitutto tale per il solo fatto di determinare - e non "determinare lecitamente" o "avendo titolo o competenza a determinare" - la finalità e i mezzi del trattamento: chi effettua, per proprie finalità, una attività che comporta il trattamento di dati personali, è, per ciò solo, qualificabile come titolare di quel trattamento.

Essendo una nozione di fatto, precisiamo, quella di titolare è una qualificazione che non può che riguardare una situazione *attuale*: il titolare è tale se e quando ha la possibilità, e non la mera intenzione, di trattare i dati, ovvero se e quando ne ha la disponibilità,. Fin quando effettivamente non tratta dati, il Titolare non è Titolare di nulla. Dunque, il titolare è quel soggetto che *tratta* dati per finalità e secondo finalità da esso stesso determinate.

E' una nozione che ha inoltre uno scopo *funzionale*, in quanto è soprattutto finalizzata ad una attribuzione di responsabilità: nell'ambito di una data attività pratica si individua il soggetto che tratta per propri scopi dati personali con un certo ambito di autonomia, determinando finalità e modalità del trattamento (diremmo l'*an* ed il *quomodo* del trattamento), che definirò *titolare* di quel trattamento. Il titolare, per ciò stesso, si assume le responsabilità conseguenti a tale qualificazione, ed alla conseguente attività di trattamento (ad esempio il titolare del trattamento "dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure" Cons. 74). Il titolare del trattamento, così come altre figure del diritto, è insomma una costruzione utile alla imputazione di prerogative/obblighi, è l'esito di un particolare sguardo, dal punto di vista del trattamento dei dati personali, sulla realtà dei soggetti che concretamente agiscono nel mondo. Questo assunto, questa artificialità di base devono essere tenuti presenti quando si parla del titolare come di colui che "decide di trattare dati per propri scopi". Nessuno, di punto in bianco, "decide di trattare dati", normalmente decide di avviare, per propri obiettivi pratici (economici, professionali, sociali, politici ecc.) una attività che comporta la necessità di trattare, cioè di utilizzare, dati personali; il trattamento di dati non è l'obiettivo ultimo del titolare, tutt'altro, è normalmente una operazione strumentale ad altri scopi: è centrale solo per uno sguardo che osservi la realtà fattuale dal punto di vista della tutela, della protezione delle persone fisiche rispetto al trattamento di dati personali che le riguardano.

Per quanto riguarda i titolari, essi lo saranno anzitutto di fatto, per la sola ragione di trattare dati per i propri interessi; alcuni di essi lo saranno poi legittimamente e altri no: ci saranno titolari che si arrogano prerogative di trattamento che non possiedono, e titolari che trattano dati lecitamente, ovvero in riferimento ad una base giuridica che li legittima a farlo. Comunque, al di là di lecito o illecito, sono tutti titolari: è sufficiente compiere una qualche operazione sui dati per un proprio scopo per acquisire il ruolo di titolare del trattamento di quei dati. Non si possono rivendicare prerogative (di trattamento) senza assumersi le conseguenti responsabilità.

In ambito aziendale, titolare del trattamento è la persona giuridica, cioè l'Azienda nel suo complesso, non il Direttore Generale. In realtà amministrative particolarmente complesse,

è possibile individuare come autonomi titolari del trattamento le articolazioni (es. i Dipartimenti) dell'ente

14.1. Contitolarità

In alcuni casi può configurarsi una situazione di Contitolarità.

Ai sensi dell'art. 26 Regolamento Generale, due o più titolari del trattamento si qualificano come contitolari (*joint controller*) del trattamento quando trattano dati sulla base di una determinazione congiunta delle finalità e delle modalità del trattamento. Diremo, meglio: quando, condividendo certe attività (ad es. partecipano congiuntamente ad uno studio), finalizzate ad uno scopo comune (nel caso, la finalità di ricerca), hanno codeterminato le modalità del trattamento atte a realizzarle (nell'esempio, aderiscono al medesimo protocollo).

Al solito, la valutazione della sussistenza di una contitolarità del trattamento deve fondarsi su una analisi fattuale, più che formale, dell'influenza effettivamente esercitata sulla determinazione della finalità e dei mezzi del trattamento.

Una contitolarità è normalmente esito di una decisione congiunta da parte di due o più soggetti; ma potrebbe derivare anche da loro decisioni convergenti: in tal caso occorre verificare se il trattamento non sarebbe possibile senza la determinazione di entrambe le parti circa finalità e mezzi del trattamento, così che i trattamenti svolti da ciascuna parte siano indissociabili, cioè indissolubilmente legati.

Nota bene: il fatto che una delle parti non possa accedere ai dati non esclude una contitolarità del trattamento, laddove quella parte abbia comunque contribuito a determinare finalità e modalità del trattamento (le Linee Guida 7/2020 richiamano una sentenza della Corte di Giustizia dell'Unione Europea - CGUE nella quale la comunità dei testimoni di Geova è stata ritenuta contitolare del trattamento assieme ai suoi membri che effettuavano la predicazione porta a porta, avendo organizzato e coordinato la loro attività dunque condividendo finalità e mezzi del trattamento dei dati ad essa necessari).

Si ha contitolarità del trattamento non solo quando le parti perseguono la stessa finalità del trattamento, ma anche quando perseguano finalità strettamente collegate o complementari.

Relativamente ai mezzi del trattamento, il fatto di utilizzare un sistema o una infrastruttura comuni per il trattamento dei dati non comporta di per sé solo una contitolarità del trattamento.

Tale configurazione di relazioni - orientata nel senso della co-decisione piuttosto che dell'autonomia - può essere utilmente implementata anche nel caso di percorsi di cura condivisi tra diversi enti sanitari (magari attivati in riferimento a progettualità regionali). Essa si conserva pur laddove ciascun ente mantenga un proprio ruolo specifico, cioè anche in caso di *asimmetria* della titolarità, sempre comunque nel contesto di un coordinamento di attività (come ad esempio nei rapporti tipo hub/spoke), che trovi appunto la sua ragion d'essere nella comune finalità e nell'accordo sui mezzi e le modalità per

raggiungerla. La nozione di contitolarità, in breve, può essere strumento utile alla gestione, dal punto di vista della protezione dei dati personali, di percorsi di cura e ricerca programmaticamente ulteriori rispetto all'ambito di un unico titolare, pur nella specificità delle varie fasi in cui si articolano e nella diversità dei rispettivi ruoli e funzioni degli enti coinvolti (dalla quale consegue che i dati necessari per le attività condivise possono essere trattati dai contitolari con una diversa profondità d'accesso).

I contitolari del trattamento devono determinare in modo trasparente (cioè accessibile agli interessati), mediante un accordo *interno* (nel testo inglese dell'art. 26 del Regolamento tale specificazione non è presente), le rispettive responsabilità (i rispettivi ruoli, appunto) in merito all'osservanza degli obblighi derivanti dal Regolamento Generale, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 Regolamento[21] (a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione e dello Stato membro cui i titolari del trattamento sono soggetti). Tale accordo è dunque l'occasione per regolare i rapporti, dal punto di vista del trattamento di dati personali, tra soggetti che condividono determinate attività, specificando distinti obblighi e prerogative. Il contenuto essenziale dell'accordo deve essere messo a disposizione dell'interessato, il quale può comunque esercitare i propri diritti (ad es. di accesso) nei confronti di e contro ciascun contitolare del trattamento.

Attenzione: la soluzione della contitolarità non può essere strumentalmente utilizzata per porre dati personali a disposizione di soggetti che non ne avrebbero la titolarità, concretamente intesa; un percorso di cura, su cui l'interessato sarà debitamente ed analiticamente informato, condiviso tra più enti del Servizio sanitario regionale è di per sé legittimo, e può realizzarsi senza dover acquisire il consenso del paziente per la condivisione delle informazioni tra di essi, ovviamente limitatamente alle rispettive prerogative e necessità; non così qualora il percorso coinvolgesse enti che svolgono un ruolo meramente funzionale rispetto alla finalità principale (in questo caso la finalità di cura), e non possano esercitarla lecitamente in autonomia, i quali dovranno allora essere individuati quali responsabili del trattamento.

15. Chi è il responsabile del trattamento

Dal Titolare del trattamento si distingue il Responsabile del trattamento (*processor)*.

Il termine *Processor* – da *processing*, trattamento - era tradotto, nella versione italiana della Direttiva 46/95, come incaricato (la coppia controller/processor è dunque resa nella versione italiana della Direttiva come responsabile/incaricato), ed in quella del Regolamento Generale come Responsabile (si ha qui dunque, attualmente, il binomio Titolare/Responsabile).

Responsabile del trattamento è:

[21] L'art. 13 riguarda le informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, l'art. 14 qualora i dati non siano stati ottenuti presso l'interessato

> la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali *per conto del titolare del trattamento*[22]

Il Responsabile del trattamento, da un punto di vista soggettivo, si pone sullo stesso piano del Titolare, nel senso che, come esso, può essere una *persona fisica o giuridica, l'autorità pubblica, il servizio o altro organism*.

Il Responsabile del trattamento è dunque il soggetto incaricato dal Titolare di trattare dati (per questo la traduzione italiana del termine Processor nella Direttiva era reso con *incaricato*), cioè di effettuare il trattamento, per conto del (*on behalf of*) Titolare stesso.

Più in concreto: il processor/responsabile è il soggetto al quale il controller/titolare esternalizza una attività, la quale comporta un trattamento di dati personali che sono nella Titolarità di quest'ultimo. Ogni volta che si assiste all'affidamento di una attività che comporta un trattamento di dati ad un soggetto diverso dal Titolare, che non sia in possesso di una autonoma legittimazione a trattare quei dati, ci troviamo dunque di fronte ad un rapporto Titolare/Responsabile. Il rapporto è vicario e funzionale, nell'esclusivo interesse del titolare.

Ai sensi dell'art. 28 paragrafo 3 lettera a) del Regolamento Generale tale incarico deve essere formalizzato in un contratto o altro atto giuridico, che precisi:

- la materia disciplinata
- la durata del trattamento
- la natura e la finalità del trattamento,
- il tipo di dati personali
- le categorie di interessati
- gli obblighi e i diritti del titolare del trattamento.

Tale atto deve poi essere tale che il responsabile

> tratti i dati personali soltanto su istruzione documentata del titolare del trattamento

Il principio è ribadito all'art. 29:

> Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

[22] "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"

La formulazione dell'articolo prevede dunque che il titolare detti istruzioni, oltre che alle persone fisiche che agiscono sotto la propria responsabilità, anche al responsabile del trattamento e alle persone fisiche che agiscono sotto la responsabilità di questo. Anzi, il titolare si caratterizza, tra l'altro, proprio per essere il soggetto che controlla e dirige il trattamento fornendo istruzioni circa la sua effettuazione: le finalità e le modalità del trattamento individuate dal controller si trasferiscono al processor attraverso tali istruzioni.

Per soddisfare a tale scopo, le istruzioni devono essere il meno possibile generiche (non è sufficiente ad esempio limitarsi a scrivere che i dati "devono essere trattati lecitamente e rispettando la normativa in materia di protezione dei dati personali"), e tradursi piuttosto in una specifica regolazione, dal punto di vista del trattamento dei dati, dell'attività delegata. Non è affatto escluso, infatti, che anche una istruzione magari ovvia ma non data e documentata, non comporti l'attribuzione al titolare di una responsabilità in caso di accertamento di trattamento non adeguato.

16. I rapporti tra titolare e responsabile

C'è dunque un soggetto - il titolare - che stabilisce di trattare dati per attività di proprio interesse ed utilizzando mezzi da esso stesso individuati (anche, vedremo, su proposta del responsabile), ed un soggetto - il responsabile - che effettua il trattamento in base alle modalità prescritte o condivise, in funzione degli scopi dell'altro. Tale rapporto è stato qualificato nei termini di una delega di funzioni – nel contesto di una delega di attività - quale atto di autonomia con cui si attua una distribuzione di compiti ed una ripartizione di competenze, e quindi anche di responsabilità.

Quando si caratterizza il titolare come il soggetto che è autonomo nel decidere i mezzi e le modalità del trattamento e nell'individuare gli strumenti per realizzarli, occorre ricordare che tali decisioni si riferiscono all'organizzazione (ed al controllo) generale del trattamento ed al suo coordinamento con le altre proprie attività e non agli aspetti meramente tecnici con cui il trattamento è effettuato. Al titolare restano comunque demandate le questioni sostanziali attinenti ai fondamenti delle modalità e della liceità del trattamento. Il *Manuale di diritto europeo in materia di protezione dei dati* osserva che se il potere di determinare i mezzi del trattamento è delegato a un responsabile, il titolare deve comunque poter esercitare un adeguato controllo sulle decisioni del responsabile in merito ai mezzi del trattamento. Al titolare spetta insomma una responsabilità generale sul trattamento e sulle sue modalità di esecuzione (ed assume dunque anche una responsabilità *in vigilando*).

Ciò non contrasta con il fatto che la qualificazione del rapporto nell'ambito di una delega di funzioni deve assicurare al delegato un qualche margine di autonomia circa i poteri di organizzazione, gestione e controllo necessari per svolgere le funzioni delegate. In particolare, spesso le attività sono delegate ad un soggetto proprio per le sue competenze tecnico organizzative in un determinato settore: se le finalità e le modalità generali sono di spettanza del controller, la concreta identificazione degli strumenti tecnici e delle modalità può essere demandata, su decisione del titolare, al responsabile, che offrirà la propria competenza per individuare le soluzioni idonee a realizzarne gli interessi.

Considerato che il processor acquisisce in via derivativa la propria legittimità al trattamento dal titolare, qualora un responsabile non rispetta le condizioni per il trattamento dei dati come prescritto dal titolare, assume esso stesso, di fatto, il ruolo di titolare (almeno nella misura in cui non si è attenuto alle istruzioni del titolare originario), con le responsabilità che a tale qualifica conseguono (*in primis* quelle relative alla illiceità del trattamento stesso, venendo meno la base giuridica – la delega – in base alla quale i dati erano trattati dal responsabile).

Alla carenza di una autonoma legittimazione ad un particolare trattamento consegue che, ordinariamente, il responsabile conserva i dati solo limitatamente al tempo necessario per effettuare le attività assegnategli dal titolare, *per conto* del quale tratta dati. Per questo, ai sensi dell'art. 28 paragrafo 3 lettera g) del Regolamento Generale, il responsabile deve, su scelta del titolare, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti (salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati).

E contrario, dunque, si può sostenere che, qualora un soggetto, dopo che è terminata la prestazione dei servizi relativi al trattamento, non cancelli o restituisca, tutti i dati personali acquisiti allo scopo, sia ordinariamente (o debba considerarsi) un titolare, salvo che il diritto dell'Unione o degli Stati membri preveda a suo favore la conservazione di quei dati: ma in questo caso si presume che la conservazione sia l'unico scopo lecito, e che tale soggetto non possa utilizzarli per finalità ulteriori (e quindi non può anonimizzarli) o cederli, come potrebbe fare il titolare.

Ciò significa anche che il Titolare non ha, tra le proprie prerogative, la disponibilità dei dati a favore del Responsabile: qualora, anche per gentile concessione del titolare, il Responsabile si trovasse a poter trattare i dati (già trattati per le finalità del titolare) per propri scopi, ne diverrebbe a sua volta titolare: ma tale nuova titolarità non può trovare un fondamento giuridico nella mera volontà del Titolare originario, per cui il trattamento sarebbe perciò stesso illecito (anzi, la stessa trasmissione di dati dal titolare al responsabile, lecita per il rapporto subordinato esistente, diverrebbe retrospettivamente illecita).

Il responsabile può ricorrere a un altro processor, delegandogli alcune attività, ma solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento.

Riassumendo quanto analizzato finora:

il titolare è il soggetto che:

- tratta dati personali nel proprio interesse (o per scopi di interesse pubblico che gli sono istituzionalmente attribuiti) determinando (o perlomeno facendo proprie) le finalità del trattamento e predisponendo (o condividendo) le modalità del trattamento;
- tratta quei dati in maniera esclusiva, sempre che non ci si trovi in un ambito di

contitolarità (vedi *infra*), e può perciò decidere autonomamente se altri soggetti possano collaborare, nel proprio interesse, al trattamento e come e quando questi devono acquisire quei dati e successivamente perderne la disponibilità (cancellarli e restituirli);
- fornisce istruzioni sulle modalità del trattamento ai soggetti, persone fisiche o meno, che lo effettuano sotto la sua autorità o per suo conto;
- può (deve) controllare la correttezza dei trattamenti di dati effettuati sotto la sua autorità o per suo conto;
- detiene i dati e può successivamente utilizzarli per ulteriori finalità.

il responsabile è un soggetto che svolge attività di trattamento "*on behalf of the controller*", *per conto del titolare*, e cioè:

- sulla base di una decisione del Titolare, formalizzata in un contratto o altro atto giuridico, che fornisce al Responsabile la legittimazione in concreto (cioè nel caso specifico) ad effettuarla, della quale sarebbe altrimenti privo (non in generale dunque, ma relativamente a quel particolare trattamento, ovvero a quei dati e a quei soggetti);
- sulla base di istruzioni del Titolare, senza significativi residui ambiti decisionali in proprio (se non, al massimo, circa le modalità tecniche con le quali realizzare quanto dettato dal Titolare);
- detenendo i dati temporaneamente, per il tempo determinato dal Titolare, e non potendo ulteriormente utilizzarli per finalità proprie o per ulteriori finalità.

Si noti che il "contratto" di cui all'art. 28 del Regolamento Generale è la base giuridica del trattamento nel senso che è necessario per poter ricomprendere il responsabile del trattamento nell'ambito di titolarità del controller.

Le traduzioni *responsabile* e *titolare* del termine *controller*, che si sono succedute nelle versioni italiane rispettivamente della Direttiva e del Regolamento, non si pongono, dal punto di vista semantico, sullo stesso piano: se c*ontroller* enfatizza appunto il controllo che un soggetto esercita su un trattamento di dati, *responsabile* evidenzia piuttosto la conseguenza del determinare l'attivazione di un trattamento, ovvero l'assumersene la responsabilità, il doverne rendere conto (da cui peraltro la necessità di controllarlo) e *titolare* punta piuttosto – più di diritto e meno di fatto – sul titolo che un soggetto ha – o se presuma debba avere – per effettuare un dato trattamento. Nel ciclo delle traduzioni, come precedentemente accennato, il termine responsabile, utilizzato prima per *controller*, è poi entrato in uso per *processor*, secondo la tabella seguente:

Direttiva 46/95	Codice pre 101/2018	Regolamento Generale	Codice post 101/2018
responsabile incaricato persone autorizzate	titolare responsabile (interno e esterno) incaricati	titolare responsabile persone autorizzate	titolare responsabile (solo esterno) persone autorizzate e soggetti designati

controller processor persons authorized		controller processor persons authorized	

In effetti, per quanto riguarda il *controller*, indicare il soggetto che determina le finalità e le modalità del trattamento quale *titolare* piuttosto che *responsabile* depotenzia quella correlazione tra attivazione del trattamento per scopi propri e responsabilità che è implicita nella traduzione italiana della Direttiva, per la quale chi determina se, come e con quali strumenti attivare un trattamento ne è responsabile, ne è anzi "il Responsabile"; laddove la dialettica, nel *Codice* come già nella 675/96 e adesso anche nella versione italiana del Regolamento Generale tra Titolare e Responsabile – figura quest'ultima peraltro solo eventuale - tende a dare l'impressione che da un lato vi sia solo titolo e legittimazione, e dall'altra, appunto, la responsabilità.

Per quanto riguarda la nozione di *titolare* appare evidente uno spostamento lessicale e semantico dal piano della *fattualità* a quello della *legittimazione*; in teoria del diritto la nozione di titolarità indica infatti in generale la relazione di appartenenza di una situazione giuridica ad un dato soggetto, per cui titolare è dunque il soggetto che, sulla base di un titolo a lui riferito in ragione di criteri stabiliti dalla norma, è investito della situazione giuridica alla quale il diritto, il potere, il dovere ecc. appartengono, e che in base a tale titolo è legittimato a compiere alcune operazioni: nel nostro caso, appunto, le operazioni di trattamento, o meglio delle attività per la cui realizzazione è necessario un determinato trattamento di dati. Con il termine titolare la fattualità viene decisamente posta in secondo piano: intervenendo solo nelle fattispecie patologiche, nelle quali un trattamento illecito deve comunque ricondursi alla responsabilità di chi lo effettua, per il solo fatto che lo effettua.

17. Persone autorizzate al trattamento

Coloro che effettuano concretamente le operazioni di trattamento sono le persone fisiche *autorizzate al trattamento* dei dati sotto la autorità diretta di Titolare e Responsabile[23].

All'art. 29 del Regolamento Generale tali soggetti sono richiamati come "chiunque agisca sotto la sua - del Responsabile - autorità o sotto quella del titolare del trattamento"[24], e nel Codice post D.Lgs. 101/2018, all'art. 2-quaterdecies comma 2, è precisato che "Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

[23] Tali soggetti sono indirettamente richiamati, quali the *persons who are authorized to process the data,* nella definizione di *Terzo* all'art. 2 paragrafo f) della Direttiva, adesso riproposta all'art. 4 paragrafo 1 10 del Regolamento Generale:

> the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

La Direttiva 46/95 inoltre, all'art. 16 *Confidentiality of processing* prescrive che

> Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Da qui l'art. 8 comma 5 della legge 675/96:

> Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile

e l'art. 30 comma 1 del Codice precedente le modifiche apportate dal D.Lgs. 101/2018:

> Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

[24] "any person acting under the authority of the controller or of the processor"

Si è visto che sempre l'art. 29 del Regolamento Generale prevede che "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"[25].

Il fatto che la previsione delle *istruzioni* sia direttamente nel Regolamento Generale, esenta il legislatore nazionale dal richiamarla nella versione del Codice successiva all'adeguamento, che ne tratta solo all' art. 106 in riferimento alle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ove, al paragrafo 2 lettera g) si prescrive che esse debbano individuare "le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire alle *persone autorizzate al trattamento* dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies".

Quel che caratterizza dunque tali persone fisiche è che trattano dati:

- sotto l'autorità del titolare (o del responsabile);
- con l'autorizzazione di titolare (o responsabile);
- dietro istruzioni fornite dal titolare.

E' opportuno precisare che le istruzioni dettate dal Titolare rappresentano anche il limite della autorizzazione al trattamento, o meglio, in positivo: il *quantum* di trattamento consentito (anche nel senso delle modalità con cui è effettuato) è quello, e solo quello, esplicitato nelle istruzioni. Un soggetto non è autorizzato ad effettuare un trattamento se non nella misura in cui è ad esso istruito.

Qual è la differenza tra responsabile del trattamento e persona autorizzata al trattamento? Anzitutto:

- un soggetto collettivo può essere qualificato solo come responsabile del trattamento;
- una persona fisica, può essere qualificata tanto come persona autorizzata al trattamento che come responsabile del trattamento.

Se il soggetto che effettua il trattamento per il titolare è una persona fisica, quando deve essere qualificato responsabile e quando persona autorizzata? Vi sono casi in cui una esternalizzazione di servizi si traduce in un rapporto tra titolari?

Anzitutto, tanto il responsabile quanto le persone autorizzate effettuano il trattamento dietro istruzioni del titolare – istruzioni che, come vedremo, possono essere più o meno stringenti – ma:

- il responsabile tratta dati "per conto del titolare"
- la persona autorizzata direttamente "sotto l'autorità" del titolare.

[25] The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Il rapporto è di collaborazione in un caso (responsabile), con un qualche margine di autonomia, e decisamente gerarchico/verticale in un altro (persona autorizzata).

Ne segue che il responsabile, pur dietro istruzioni del titolare, può trattare dati con margini di autonomia più ampi di quelli riconosciuti alla persona autorizzata: simmetricamente, il soggetto che tratta dati personali con un certo margine di autonomia rispetto al titolare deve qualificarsi quale responsabile piuttosto che persona autorizzata al trattamento.

17.1. Persona autorizzata e titolarità di fatto

Si è visto (cfr. § 14) che il titolare del trattamento è il soggetto che definisce finalità e modalità del trattamento, e che la persona fisica autorizzata al trattamento è, in quanto tale, legittimata al trattamento dal rapporto con il Titolare che si esplica, dal punto di vista del trattamento dei dati, nella attuazione ed applicazione delle istruzioni da questo dettate.

Perché, relativamente ai trattamenti di dati connessi alla sorveglianza sanitaria dei lavoratori, si individua il medico competente quale Titolare del trattamento? Perché il medico competente, per espressa previsione del D.Lgs 81/2006, svolge le attività di sorveglianza sanitaria in base a prerogative proprie, in via riservata ed indipendentemente rispetto al datore di lavoro, che deve soltanto mettergli a disposizione le risorse umane e strumentali per effettuarla; sul piano dei dati personali, il datore di lavoro non può avere accesso ai dati della sorveglianza sanitaria, che possono appunto essere trattati solo dal medico competente (ciò si riflette, nell'art. 9 del Regolamento Generale, in due diverse basi giuridiche per le attività finalizzate alla tutela della salute dei lavoratori, rispettivamente, per il datore di lavoro ed il medico del lavoro, i parr. 2 lettera b e 2 lettera h). Il medico del lavoro, per i trattamenti di competenza, in quanto titolare del trattamento si assumerà perciò direttamente tutti i rischi, anche di tipo patrimoniale, per illeciti, scorrettezze, violazioni di dati. In questo caso si tratta di una titolarità lecita, che ha una propria specifica base normativa, e che comunque non copre tutte le attività svolte dal medico competente, che per quelle ulteriori rispetto alla sorveglianza sanitaria è legittimato a trattare dati solo quale persona autorizzata al trattamento.

Vediamo ora il caso del Medico competente che, appunto al di fuori delle attività di sorvegliana sanitaria, dunque quale persona fisica autorizzata al trattamento, tratti dati acquisiti in occasione della prestazione lavorativa, per scopi propri, o anche secondo modalità difformi dalle istruzioni ricevute: considerato che tale *autorizzazione* ha un ambito di operatività limitato alle finalità del Titolare ed a quanto da questi prescritto, egli non può più considerarsi una "persona autorizzata" ma, a sua volta, un titolare del trattamento (di fatto).

Allo stesso modo, un medico che, a qualunque titolo (dipendenza, collaborazione, afferenza), operi a favore di un organismo sanitario, tratta i dati dei pazienti non in base a proprie prerogative (i requisiti che ne sostanziano la professionalità rappresentano, in quel contesto, un presupposto per il trattamento ma non per una legittimazione autonoma al trattamento, sempre che un specifica disposizione, come per il medico competente, non

preveda altrimenti), ma nella misura in cui può farlo l'organismo sanitario ed in virtù delle finalità che a questo sono attribuite (in particolare, le "finalità di medicina preventiva …, diagnosi, assistenza o terapia sanitaria" di cui all'art. 9 par. 2 del Regolamento Generale); se questo medico utilizza quei dati per propri scopi personali o utilizzando mezzi diversi da quelli messi a disposizione del Titolare, assume il ruolo di un Titolare di fatto, con tutte le responsabilità conseguenti.

Allo stesso modo, se un medico utilizza i dati personali raccolti per finalità di cura per uno scopo diverso, ad esempio per un convegno, senza alcuna autorizzazione del Titolare (e senza aver acquisito il consenso dell'interessato), è passibile di una sanzione che può essere direttamente posta a suo carico in quanto Titolare del trattamento.

Lo stesso può dirsi se, nonostante la prescrizione aziendale di non trattare dati personali su una casella postale gmail o simile, proceda altrimenti: anche in questo caso la sanzione per una perdita di dati potrà essergli direttamente attribuita.

Perché la finalità di cura è posta in capo all'Azienda e non al professionista (e dunque il titolare del trattamento non è questi ma l'Azienda?) Semplicemente perché il rapporto fondamentale del paziente si stabilisce con questa e non con il singolo professionista (diversamente, ad esempio che per il medico di medicina generale, che infatti è qualificato autonomo titolare del trattamento). Le finalità di tutela funzionali ad assicurare il diritto alla salute sancito dall'art. 32 della Costituzione trovano, quando devono esplicarsi nel caso specifico, il loro diretto e concreto presupposto giuridico nel "contratto di cura" che si stabilisce tra un dato paziente e l'organismo sanitario (non con il singolo professionista) che si assume il compito di tutelarne la salute; si parla di obbligazioni assunte per "*contatto sociale*", per il mero fatto che il paziente viene preso in carico da parte dell'organismo sanitario (trattasi di fattispecie da ricondursi alla categoria dei c.d. *rapporti contrattuali di fatto*). In particolare, la giurisprudenza ha inquadrato il contratto di cura, in riferimento agli organismi sanitari, in un più ampio *contratto di spedalità*, un contratto atipico che ha al centro l'obbligazione primaria di curare il paziente, ma ricomprende anche altre obbligazioni, perché non si esaurisce nella prestazione di cure mediche e chirurgiche, ma ricomprende ad es. anche l'assistenza infermieristica, quella farmaceutica nonché la garanzia di attrezzature tecnologicamente adeguate, oltre ad obbligazioni di carattere strettamente alberghiero quali vitto e alloggio (ed anche la correttezza di trattamenti di carattere amministrativo come quelli riconducibili alla gestione delle cd. liste d'attesa): un contratto che prevede dunque molteplici prestazioni, che non si esauriscono nell'attività strettamente clinica, che comunque vi resta ovviamente centrale.

Quel che preme evidenziare da quanto sopra esposto, è che il medico che tratta dati sotto l'autorità del titolare è qualificata persona autorizzata al trattamento proprio perché non ha autonome prerogative di trattamento (diversamente, si è visto, dal medico competente per i trattamenti di dati connessi alla sorveglianza sanitaria), che acquisisce solo nella misura in cui il titolare la autorizza ed entro i limiti disposti con tale autorizzazione; questa, espressa a mezzo di dettagliate istruzioni, rappresenta il perimetro entro il quale la persona autorizzata può effettuare il trattamento.

17.2. Persone espressamente designate

Il Regolamento Generale ha introdotto la figura della "persona autorizzata al trattamento", a ricomprendere, non differenziate, le precedenti figure del "responsabile" interno e

dell'"incaricato" del trattamento, di cui rispettivamente agli artt. 29 e 30 del D.Lgs. 196/2003, oggi abrogati - quale persona fisica che tratta dati sotto la diretta autorità del Titolare.

Ai sensi dell'art. 2 quaterdecies del D.Lgs. 196/2003, il Titolare del trattamento può comunque prevedere, nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, *espressamente designate*, che operano sotto la sua autorità.

Si evidenziadunque che:

- tale designazione espressa è riferita a chi svolge funzioni e compiti specifici e particolari connessi al trattamento di dati personali, ovvero funzioni di direzione e coordinamento rispetto al trattamento;
- tali soggetti sono assimilabili a quelli già definiti dal previgente art. 29 del Codice come responsabili (interni) del trattamento;
- il termine "responsabili" non appare più utilmente invocabile in riferimento a tali soggetti, in quanto riferito dall'art. 28 del Regolamento Generale ai soli soggetti esterni che effettuano trattamenti di dati per conto del Titolare;

In Azienda si è ritenuto denominare tali soggetti come "preposti", indicandone i rispettivi compiti (vedi Provvedimento del Direttore Generale n. 378 del 24 maggio 2019).

18. Violazione dei dati personali (data breach)

Per *«violazione dei dati personali»* (o *«data breach»*) si intende una violazione di sicurezza che può verificarsi tanto in via accidentale che per atto illecito, e che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, e dalla quale possano derivare rischi per i diritti e le libertà degli interessati. Non ogni violazione di sicurezza si traduce dunque in una violazione di dati personali; per integrare una violazione di dati personali occorrono almeno i seguenti due elementi:

- una violazione di sicurezza;
- un conseguente rischio per i diritti e le libertà degli interessati.

Le violazioni di sicurezza possono essere classificate nelle seguenti tre categorie:

- *violazione della riservatezza*, in caso di divulgazione di dati personali o accesso agli stessi non autorizzati o accidentali;
- *violazione dell'integrità*, in caso di modifica non autorizzata o accidentale di dati personali (i dati sono modificati o incompleti);
- *violazione della disponibilità*, in caso di perdita della possibilità di accesso o distruzione accidentale o non autorizzata di dati personali.

Queste violazioni di sicurezza comportano il mancato rispetto dell'art. 5 par. 1 lettera f) del Regolamento Generale, ai sensi del quale i dati personali devono essere trattati "trattati in maniera da garantire un'adeguata sicurezza …, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

Per *"rischio"* correlato ad una violazione dei dati personali si intende la caratteristica che una violazione di dati ha di poter avere effetti, stimati in termini di probabilità, danno conseguente e rilevabilità, sui diritti e le libertà delle persone cui i dati si riferiscono (gli interessati).

Per quanto concerne gli effetti della violazione, il Titolare deve accertarsi se essa si può tradurre in:

- perdita del controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione d'identità;
- frodi;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- conoscenza da parte di terzi non autorizzati;
- qualsiasi altro danno economico o sociale significativo.

Tali conseguenze determinano senz'altro un rischio per i diritti e le libertà degli interessati:

Il Garante ha esemplificato, in via non esaustiva, quali eventi che integrano senz'altro una violazione di dati personali, i seguenti:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

In presenza di una accertata violazione di sicurezza, il Titolare procederà ad effettuare una valutazione oggettiva - con riguardo alla natura, all'ambito di applicazione, al contesto ed

alle finalità del trattamento - della probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche che ne possono derivare.

La potenziale gravità di una violazione di sicurezza si valuta prendendo in considerazione anzitutto la tipologia e quantità dei dati oggetto della violazione nonché i possibili effetti della violazione stessa.

Per quanto concerne la tipologia di dati, occorre accertarsi se sono stati violate in particolare le categorie di dati di cui all'art. 9 del Regolamento o i dati relativi a condanne penali e reati di cui all'art. 10 del Regolamento, o dati relativi a persone fisiche vulnerabili (ad esempio pazienti o minori), dati che possono avere una capacità lesiva maggiore, o comunque dati riservati (concernenti ad esempio la situazione economica o finanziaria dell'interessato).

Per quanto riguarda la quantità occorre accertarsi se i dati personali violati siano numerosi o comunque relativi ad un significativo numero di interessati. Da ciò non consegue comunque che una violazione di sicurezza riferita ad un solo o pochi interessati non possa essere qualificata come violazione dei dati personali. Si evidenzia anzi che qualsiasi divulgazione non autorizzata di dati relativi alla salute, cioè di dati attinenti alla salute che possono fornire informazioni sullo stato di salute di un interessato identificato o identificabile, comporta di per sé una perdita di riservatezza di dati personali protetti da segreto professionale e determina dunque senz'altro una violazione di dati personali, senza necessità di ulteriori valutazioni.

Al fine di valutare la gravità della violazione, viene utilizzata la metodologia prevista dall'Enisa (European Union Agency for Network and Information Security (ENISA) – Recommendations for a methodology of the assessment of severity of personal data breaches) espressamente richiamata dalla WP 250 Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 " adottata dal WP il 3 ottobre 2017 ed emendata il 6 febbraio 2018.

Il fatto che i dati oggetto della violazione di sicurezza siano pseudonimizzati o cifrati non significa che essa non integri una violazione di dati personali; la circostanza ha comunque effetto sugli obblighi conseguenti.

Ove risulti accertata una violazione di dati personali, il titolare la notifica al Garante utilizzando il modello messo a disposizione sul sito del Garante medesimo, inviandolo con modalità telematica

La notifica al Garante deve essere effettuata senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui il titolare abbia accertato la violazione dei dati personali.

Il titolare deve considerarsi venuto a conoscenza di una violazione dei dati personali quando sia in possesso di un ragionevole grado di certezza tanto, preliminarmente, sul fatto che la violazione di sicurezza di cui è venuto a conoscenza integri i requisiti di una violazione dei dati personali, quanto sulle modalità con cui la stessa si è verificata.

Qualora la notifica non sia effettuata entro 72 ore dall'avvenuta conoscenza della violazione come determinata al comma precedente, è necessario esplicitare i motivi del ritardo. La notifica deve contenere tutte le informazioni previste dal modello messo a disposizione dal Garante; qualora non fosse possibile fornire immediatamente tutte le suddette informazioni, queste possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La notifica della violazione è effettuata dal DPO aziendale (cfr. § 19).

Ove risulti probabile che dalla violazione possa derivare non solo un mero rischio ma un rischio elevato per i diritti e le libertà degli interessati, il titolare, oltre ad effettuare la notifica al Garante, comunica altresì la violazione dei dati personali agli interessati cui i dati si riferiscono, secondo le modalità di seguito precisate. La "soglia" per la comunicazione della violazione all'interessato è dunque più elevata rispetto a quella della notifica al Garante: non un mero rischio, ma un rischio elevato per i diritti e le libertà degli interessati.

La comunicazione della violazione di dati personali all'interessato non è prevista se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure risultano applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura o la pseudonimizzazione;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati (in tal caso si procede a dar conto della violazione sul sito istituzionale pubblicando un avviso per un periodo di trenta giorni).

La comunicazione all'interessato è contestuale o anche successiva a quella al Garante, ma deve comunque essere effettuata senza ingiustificato ritardo, descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali ed informare circa:

- il nome e i dati di contatto del DPO, presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui il titolare non abbia comunicato all'interessato la violazione dei dati personali, il Garante, dopo aver valutato che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà degli interessati, può richiedere che vi provveda, o può invece decidere che una delle condizioni di cui al comma precedente sia soddisfatta.

La comunicazione della violazione è ordinariamente effettuata dal DPO aziendale.

19. Responsabile della Protezione dei Dati (DPO)

Il Regolamento generale prevede un Responsabile della Protezione dei Dati (RPD, o anche Data Protection Officier, DPO), cui dedica il Considerando 97 ed il capo IV sezione 4.

Si tratta di una figura che sostanzialmente ripropone quella del Privacy Officier presente in alcuni paesi europei, o del nostro risalente Referente Privacy; la differenza è che tale figura, appunto già esistente ma non obbligatoria, diventa appunto obbligatoria per alcuni soggetti, in primis per gli enti pubblici, e le si garantisce autonomia e risorse (supporto) per lo svolgimento di compiti che il Regolamento Generale declina puntualmente.

Sul RDP ed i suoi compiti il gruppo europeo dei Garanti ha emesso delle linee guida (*Linee-guida sui responsabili della protezione dei dati RPD*, d'ora in avanti: *Linee guida sul RDP*).

In base all'articolo 37, paragrafo 5, il DPO "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39".
In generale, l'art. 39, paragrafo 1, lettera b), affida al DPO - il compito di sorvegliare l'osservanza del Regolamento. Nel considerando 97 si specifica che il titolare del trattamento dovrebbe essere "assistito [dal DPO] nel controllo del rispetto a livello interno del presente regolamento".

In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" che caratterizza il Regolamento, l'art. 35, secondo paragrafo, prevede in modo specifico che il titolare "si consulta" obbligatoriamente con il DPO quando svolge una DPIA (cfr. § 8), e l'art. 39, primo paragrafo, lettera c) affida al DPO il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento".

Riassumendo, fanno parte dei compiti del DPO:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità;
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile;
- il fungere da interfaccia fra autorità di controllo, interessati, strutture aziendali.

Il trattamento dei dati personali in ambito sanitario

20. Basi giuridiche del trattamento in ambito sanitario

Affinché un trattamento di dati sia lecito esso deve avere una base giuridica, cioè la sua finalità deve essere prevista e consentita dal Regolamento Generale; la base giuridica invocabile può variare in relazione alla tipologia di soggetto che effettua il trattamento, alla finalità dello stesso, alla tipologia di dati utilizzati.

Qui interessa in particolare, illustrare le condizioni di liceità dei trattamenti di *dati relativi alla salute* svolti in ambito sanitario.

Un trattamento di tale tipologia di dati personali, svolto in ambito sanitario, è lecito alle seguenti condizioni, che poi saranno partitamente esaminate:

- l'interessato ha prestato il proprio consenso esplicito al trattamento (art. 9 par. 2 lettera a)
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (art. 9 par. 2 lettera c)
- il trattamento è necessario per motivi di interesse pubblico rilevante (art. 9 par. 2 lettera g)
- il trattamento è necessario per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria (art. 9 par. 2 lettera h e par. 3)
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica (art. 9 par. 2 lettera i)

20.1. Consenso al trattamento

Il consenso non è più indispensabile per poter procedere a trattare dati personali per finalità di cura, essendo il trattamento per tale finalità già di per sé legittimo quando è *necessario* per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria, e tali dati siano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza, ai sensi dell'art. 9 parr. 2 h e 3 del Regolamento Generale). Nell'ambito sanitario, dunque, il Regolamento Generale consente di prescindere, in linea di massima (e comunque non sempre) dal consenso dell'interessato, ed infatti l'art. 76 comma 1 lettera a) del *Codice,* che lo prevedeva in via generale per la finalità di cura, è stato abrogato.

Vero è che, ai sensi dell'art. 9 comma 4 del Regolamento Generale, resta la possibilità per i legislatori nazionali di mantenere o introdurre ulteriori condizioni, comprese limitazioni, sulla base delle quali consentire il trattamento di dati genetici o dati relativi alla salute; un obbligo di consenso, dunque, potrebbe essere successivamente reintrodotto. Comunque l'art. 2 septies del Codice prevede che:

> *1) In attuazione di quanto previsto dall'articolo 9, paragrafo 4 del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo*

2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.
2) 2) Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale...

Il provvedimento non è stato ancora adottato, ad ogni modo il comma 6 secondo periodo del medesimo articolo prevede che:

> *Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, ..., o altre cautele specifiche.*

Non sembra pertanto prevista una reintroduzione del consenso in riferimento ai dati relativi alla salute, se non quando il trattamento ricomprenda i dati genetici.

L'obbligo del consenso viene in causa solo qualora il trattamento, o la modalità in cui è effettuato, non possa essere valutato *necessario*, ovvero *indispensabile*, a scopo di cura.

Si ricordano qui le condizioni ed i limiti per l'utilizzo dello strumento del consenso.

Anzitutto, il «consenso dell'interessato» è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile, con la quale l'interessato manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Il consenso, in quanto "manifestazione di volontà", deve appunto manifestarsi, ed è dunque prestato mediante un atto positivo inequivocabile, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò può comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non configura pertanto consenso il silenzio, l'inattività o la preselezione di caselle. Ad ogni modo, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, con garanzie che assicurino che l'interessato sia consapevole del fatto di prestare un consenso e della misura in cui ciò avviene.

Qualora il trattamento abbia più finalità, il consenso deve essere prestato per ognuna di queste (consenso cd. modulare).

Il consenso non può essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio. In particolare, si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso.

Ma soprattutto, ai sensi del Considerando n. 46, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente. Se ciò non significa certo che un ente pubblico non possa utilizzare lo strumento del consenso, è comunque opportuno:

- limitarne l'utilizzo a casi di stretta indispensabilità;
- proporre modalità di trattamento meno invasive della riservatezza dell'interessato, ad esempio applicando il principio di minimizzazione dei dati.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Di ciò l'interessato è informato prima di prestare il proprio consenso.

20.2. Tutela di un interesse vitale dell'interessato o di un'altra persona fisica

La fattispecie è ampia, potendo ricomprendere anche situazioni nelle quali non viene direttamente in causa la tutela della salute (es. catastrofi umanitarie) e non trovando dunque esclusiva applicazione nell'ambito sanitario. Considerato che essa interviene qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso, in ambito sanitario deve essere pertanto limitata a quei casi in cui il trattamento non è strettamente necessario per una finalità di tutela della salute (ove non si richiede consenso), e la base giuridica è invece appunto individuata nel consenso dell'interessato; a ciò si aggiunge che il trattamento deve essere necessario per tutelare un interesse vitale dell'interessato o di altra persona fisica.

Per la applicabilità di questa norma occorre ovviamente avere ben chiaro quando possa essere necessario il consenso dell'interessato. Poniamo il caso che l'interessato in questione sia un paziente non in grado di esprimere una propria volontà o in emergenza-urgenza; la condizione necessaria è che le informazioni di cui trattasi siano (o si presume che siano) indispensabili per la salvaguardia della salute dell'interessato (o di una diversa persona fisica); variamente esemplificando:

- comunicazione tra due Aziende sanitarie di dati clinici pregressi (es. raccolti in cartelle cliniche relative a precedenti ricoveri) indispensabili ad evitare un rischio incombente sulla salute del paziente;

- trasferimento tra due Aziende sanitarie del paziente accompagnato da copia della cartella clinica;
- accesso ad immagini radiologiche detenute da diversa Azienda sanitaria;
- utilizzo dei dati personali dell'interessato per la tutela della salute di un diverso paziente.

Cosa accadrebbe se queste necessità fossero riferibili ad un paziente cosciente? Dovrebbe essere chiesto il consenso (e dunque la base giuridica sarebbe quella di cui al § 20.1) o si può accedere alla nozione ampia di trattamento necessario per finalità di cura? Anzitutto, di quale operazione si tratta? Raccolta o comunicazione di dati? La *raccolta* si identifica con acquisizione del dato, vale a dire con il momento in cui si verifica l'ingerenza nella sfera esistenziale della persona cui esso si riferisce, ed è operazione che prescinde dall'accesso, ovvero dalla conoscenza del dato stesso; la *comunicazione* del dato è il dare di esso conoscenza, ovvero renderlo accessibile anche in termini cognitivi: possiamo dire che, nella fattispecie esaminata, i due termini si integrino in un prima/dopo temporale. In effetti il Garante ha sempre sotteso nelle sue interpretazioni, in particolare in ambito sanitario, che la raccolta/comunicazione di informazioni pregresse presso un diverso titolare del trattamento debba essere sostenuta da un consenso dell'interessato o da parte dei soggetti di cui all'art. 82 comma 2 lettera a) del Codice, nelle situazioni da esso previste[26]. La norma di cui all'art. art. 9 par. 2 lettera c offre dunque una base giuridica per quelle stesse operazioni di trattamento, quando non sia possibile raccogliere il consenso dell'interessato, perché questi si trova nell'incapacità fisica o giuridica di prestarlo.

La disposizione prevede anche la possibilità che l'interesse vitale da tutelare sia ascrivibile ad una persona fisica diversa dall'interessato; questa norma appare meno comprensiva di quella prevista dall'abrogato art. 76 comma 1 lettera b) del Codice, per la quale il trattamento di dati per finalità di cura era lecito, se la finalità riguardava un terzo o la collettività, con il consenso dell'interessato oppure prescindendo da esso, ma previa autorizzazione del Garante (che provvedeva con una Autorizzazione Generale reiteratamente rinnovata); in questo caso si richiede infatti che l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso, laddove ovviamente sia previsto: la disposizione appare cioè giustificata non solo dalla finalità, cioè la salvaguardia di un interesse vitale di una persona fisica diversa dall'interessato, ma anche dalla condizione dell'interessato (tale da non consentirgli di poter prestare il consenso al trattamento, qualora previsto). Per la complessiva copertura giudica della fattispecie già prevista dall'art. 76 comma 1 lettera b) del Codice, si veda il § 20.4.

[26] "impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato".

20.3. Motivi di interesse pubblico rilevante

I trattamenti in oggetto sono quelli effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, come la nostra Azienda. Si tratta, in breve, per quanto riguarda l'ambito sanitario, di trattamenti di carattere in senso lato amministrativo o certificatorio che concorrono allo scopo di tutela della salute ma sono per essa meramente strumentali e non essenziali.

Esemplificando, la fattispecie ricomprende non solo tutte le attività di prenotazione ed accettazione o in generale di gestione amministrativa del paziente e della prestazione, ma anche, ad esempio, la redazione della cartella clinica. In proposito, occorre comunque evidenziare che una cosa è la corretta redazione e tenuta della cartella, altra l'utilizzo dei dati della cartella clinica per la cura dell'interessato o di un altro soggetto, che trovano copertura nella base giuridica di cui al § 20.4; insomma, il trattamento dei dati contenuti nella cartella clinica può essere legittimato da disposizioni diverse a seconda della finalità; non esiste dunque una norma unica che li riguardi in quanto tali, staticamente considerati, ma più disposizioni e basi giuridiche che ne rendono lecito il trattamento, dinamicamente, a seconda dello scopo.

Stesso discorso per un certificato o referto: c'è un obbligo giuridico ulteriore rispetto a quello prestazionale che, per motivi di interesse pubblico rilevante, ne impone la redazione ed eventualmente la conservazione; sarà ugualmente un obbligo giuridico declarato in una norma di legge o regolamentare che può prevederne la comunicazione ad un ente per scopi ed es. medico legali o autorizzatori; ma la sua comunicazione per finalità di cura è coperta dalle basi giuridiche di cui al § 20.1 o eventualmente § 20.4.

L'interesse addotto per giustificare il trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato: in breve, occorre un bilanciamento tra l'interesse pubblico, cioè l'interesse del titolare che se ne fa latore ed interprete, da un lato, ed il diritto alla protezione dei dati dell'interessato dall'altro, nella consueta prospettiva della proporzionalità e minimizzazione del trattamento.

Si può sostenere che, prima delle modifiche apportate dal D.L. 8 ottobre 2021 n. 139, tale bilanciamento fosse direttamente rimesso alla normativa - lasciando un margine di discrezionalità, e correlata responsabilità, solo per gli aspetti tecnici delle modalità di trattamento - poiché il trattamento era consentito qualora previsto dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specificassero i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali. Dunque:

- norma UE;
- legge;
- regolamento, se previsto dalla legge (ad integrazione e specificazione di essa).

Raramente una legge prevede tutti gli aspetti del trattamento che la norma prescrive, per cui ci si doveva orientare verso l'integrazione di carattere regolamentare; è ad es. la soluzione rappresentata dal Decreto del Presidente della Giunta Regionale Toscana 26 ottobre 2021, n. 37/R *Regolamento di attuazione dell'articolo, 1 comma 1, della legge regionale 3 aprile 2006, n. 13 (Trattamento delle categorie particolari di dati personali e di quelli relativi a condanne penali e ai reati da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo),* di seguito Decreto del Presidente della Giunta Regionale Toscana 26 ottobre 2021, n. 37/R, Regolamento del quale esistono due precedenti versioni, del 2006 e del 2013.

Si tratta dunque di un sistema di strettissima giuridicità, caratteristico del Codice fin dalla sua prima versione relativamente al trattamento di dati sensibili (oggi categorie particolari di dati) da parte degli enti pubblici.

Il trattamento è invece, oggi, consentito, ai sensi dell'art. 2-sexies comma 1 del Codice così come modificato dal D.L. 8 ottobre 2021 n. 139:

> … qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Segue, al comma 2 - secondo la consueta tecnica già utilizzata ad es. dagli artt. 85-86 della prima versione del Codice, per la declinazione finalità di interesse pubblico perseguite dal Servizio Sanitario Nazionale – l'elenco delle materie i cui trattamenti sono effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, delle quali si rileva la rilevanza per l'interesse pubblico.

Quel che occorre sottolineare è che, nell'attuale formulazione dell'art. 2-sexies, il comma 2 offre una indicazione meramente ricognitiva e orientativa, laddove il compito di specificare "i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" resta indifferentemente affidato, nell'ordinamento interno, a:

- disposizioni di legge;

oppure

- disposizioni di regolamento;

oppure

- atti amministrativi generali.

Pur volendo restare all'interno delle materie elencate dall'art 2 sexies comma 2, che del resto forniscono un quadro sufficientemente esaustivo delle finalità istituzionali della P.A., resta il fatto che quel sistema di strettissima giuridicità che sopra si richiamava – molto formale e rigido, ma anche estremamente oggettivo e trasparente - con le modifiche apportate dal D.L. 8 ottobre 2021 n. 139, è stato fortemente posto in dubbio, anche se sarà necessario comprendere quale tipologia di atto amministrativo generale sia in grado di assumere tale efficacia (non certo, per intendersi, un Provvedimento del Direttore Generale).

20.4. Finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria

Per la finalità di cura (o meglio "finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità"), i dati devono essere trattati o da un professionista soggetto al segreto professionale o sotto la sua responsabilità (o da altra persona anch'essa soggetta all'obbligo di segretezza).

Attenzione: l'esistenza di una autonoma base giuridica non significa che, per scopi di cura, i dati possano sempre essere sempre trattati senza necessità di acquisire il consenso.

La base giuridica si qualifica come autosufficiente in riferimento al trattamento dei dati *strettamente necessari* (nel senso di *oggettivamente indispensabili*) alla prestazione sanitaria, ed immediatamente funzionali all'atto medico. Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, anche se effettuati da professionisti della sanità, una diversa base giuridica, che dovrà essere individuata o nel consenso dell'interessato (§ 20.1) o in quella di cui al § 20.2. Inoltre alcuni trattamenti, o meglio alcune operazioni di trattamento, sono oggettivamente non strettamente funzionali alla prestazione (si pensi agli obblighi informativi ad es. verso l'ente Regione), e possono trovare una base giuridica nei motivi di interesse pubblico rilevante di cui al § 20.3.

Una APP sanitaria troverà perciò la sua base giuridica nel consenso dell'interessato (dunque nell'art. 9 par. 2 a del Regolamento Generale, e non nell'art. 9 par. 2 h), in quanto non può essere considerata direttamente funzionale o indispensabile alla cura (e neppure è normata da una disposizione di carattere generale, che la ricondurrebbe all'interesse pubblico rilevante di cui al § 20.3); per quanto riguarda sistemi elettronici di controllo della condizione di salute questi sono certamente direttamente funzionali alla cura (in

particolare quando prevedono dei sistemi di alert in caso di condizioni particolari), ma, per la particolarità e novità delle modalità di funzionamento, il Garante ne rimette ugualmente l'attivazione alla autodeterminazione dell'interessato (implicitamente argomentando, evidentemente, che se una modalità di trattamento dei dati non è diffusa ovunque essa non deve ritenersi indispensabile, e da tale assunto, e dal minore o nullo controllo che l'interessato può avere sui dati gestiti elettronicamente, facendo conseguire la necessità di un bilanciamento che si attua e dimostra con la previsione del formale atto di assenso dell'interessato).

In tale condizione di liceità rientrano anche i casi degli interventi di emergenza-urgenza, o comunque quelli elencati nell'art. 82 commi 2 e 3 del Codice: impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato; rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato; casi in cui la prestazione medica che può essere pregiudicata in termini di tempestività o efficacia (in tali casi, come si è detto, non è possibile fare riferimento alla base giuridica del punto 2, perché non è previsto il consenso).

Si evidenzia che la finalità in oggetto non è riferita in via esclusiva all'interessato. Questa norma può pertanto offrire copertura alle casistiche sopra richiamate già autorizzate dall'art. 76 del Codice, cioè ai trattamenti per finalità di cura del terzo o della collettività.

20.4.1. Titolarità della finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria

Si ricorda che la titolarità dei trattamenti di dati necessari per la tutela della salute del paziente è della Azienda Ospedaliero-Universitaria, e non dell'Università degli studi: il contratto di cura con il paziente si stabilisce con la sola Azienda - come d'altronde dimostra il fatto che il risarcimento per un sinistro in ambito sanitario è a carico dell'Azienda, anche quando riguarda il personale universitario in afferenza, e non dell'Università – ed i trattamenti di dati necessari ad adempiere alle obbligazioni di tale contratto sono senz'altro riferibili alla titolarità dell'Azienda.

Il personale universitario accede a tali dati e può trattarli per quella finalità proprio in quanto in afferenza all'Azienda, cioè quale collaboratore di questa e, dal punto di vista del trattamento dei dati, quale persona autorizzata al trattamento da parte dell'Azienda. In quanto universitario, non ha dunque autonome prerogative di trattamento dei dati per finalità di cura.

20.4.2. Rapporto tra finalità di cura e motivi di interesse pubblico rilevante

La Direttiva UE trattava il "processing of special categories of data" - quello che il Regolamento richiama, con lieve integrazione, nella rubrica dell'art. 9 come *processing of special categories of personal data* - all'art. 8; relativamente ai trattamenti di ambito strettamente sanitario - preso atto che comunque il Regolamento introduce il trattamento di dati relativi alla salute per finalità di sanità pubblica, ed in generale sviluppa le finalità di ambito sanitario in modo più articolato - le disposizioni sono sostanzialmente compatibili, anche se non del tutto sovrapponibili (se non altro per il diverso statuto normativo degli atti che le contengono); lo schema dei due articoli è analogo, ponendo ambedue un divieto

generalizzato di trattare dati riconducibili alle categorie particolari se non per alcune finalità, tra le quali appunto quelle riconducibili alle attività in ambito sanitario.

Per l'art. 8 par. 3 della Direttiva il trattamento era lecito quando:

> … è necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura e quando il trattamento dei medesimi dati viene effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale, comprese le norme stabilite dagli organi nazionali competenti, o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente[27]

Per l'art. 9 par. 2 lettera h del Regolamento, il trattamento è lecito se:

> … è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

Per il par. 3 dell'art. 9 del Regolamento, inoltre, i dati personali di cui sopra possono essere trattati per dette finalità

> se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti[28].

[27] 3) …processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecv .

[28] (h) … processing is necessary for reasons of purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
3.Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. 4.Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Ora, rispetto alla fattispecie prevista dell'art. 8 par. 3 della Direttiva, prima la L. 675/96 e poi il Codice si erano "ritagliati" un ambito di applicazione più ristretto: le "finalità di tutela dell'incolumità fisica e della salute dell'interessato" o di terzi o della collettività nella L. 675/96 (art. 24), le stesse (es. art. 76 comma 1), ma anche, più in particolare, le finalità di "prevenzione, diagnosi, cura e riabilitazione" nel Codice; una scelta che riconduceva il trattamento ad attività di ambito strettamente sanitario-professionale, rimandando quanto ad esse non potesse essere ricondotto a scopi cosiddetti "amministrativi", riconducibili ai motivi di interesse pubblico rilevante.

In pratica, il legislatore nazionale aveva preso in considerazione, rispetto all'art. 8 della Direttiva, solo la finalità di "prevenzione … diagnostica medica, … somministrazione di cure" piuttosto che quella, più ampia, relativa alla "gestione di centri di cura". Se tale selezione è stata possibile in riferimento alla Direttiva, non lo è però adesso in relazione al Regolamento, che, come abbiamo visto, si riferisce anch'esso, ma con valore direttamente prescrittivo, alle attività di ambito sanitario nel senso più ampio, compresi gli aspetti di carattere organizzativo.

L'art. 9 par. 2 del Regolamento, infatti - preso atto che, così come già nella Direttiva (che parlava di "obbligo di segreto equivalente"), oltre al segreto professionale vi si richiamano anche altri obblighi di segretezza (per soggetti che evidentemente non svolgono una attività professionale - fa ampio riferimento (tralasciamo pure i "servizi sociali") a:

> diagnosi, assistenza o terapia sanitaria … ovvero gestione dei sistemi e servizi sanitari …

La "gestione di sistemi e servizi sanitari" non è evidentemente la "diagnosi, assistenza o terapia sanitaria", che sono attività di ambito strettamente professionale (qualche anno fa le avremmo tipicamente identificate con "l'atto medico"), è piuttosto la contestualizzazione di questi in un ambito più direttamente organizzativo, nella consapevolezza che l'atto medico, isolato dal sistema che lo promuove, non esiste (chiamiamola di seguito, per intenderci, *finalità di cura e di gestione di sistemi e servizi sanitari*).

Tra l'altro, è opportuno osservare che i *motivi di interesse pubblico rilevante*, nella Direttiva, erano richiamati dal solo art. 7 (il trattamento "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati"), rubricato *Condizioni per il trattamento dei dati*, e non nell'art. 8; l'art. 7 è insomma l'analogo dell'art. 6 del Regolamento, *Liceità del trattamento* (non a caso si parla di *condizioni di liceità*); rispetto a quest'ultimo l'art. 9 del Regolamento reitera – cfr. art. 9 par. 2 lettera g ed art. 6 par. 1 lettera e - il riferimento ai motivi di interesse pubblico rilevante, per cui le due basi giuridiche *motivi di interesse pubblico rilevante/ finalità di cura e di gestione di sistemi e servizi sanitari* sono compresenti nel medesimo articolo, autonomi seppur sempre funzionalmente integrabili nella prospettiva (spesso riproposta dall'EDPB, l'*European Data Protection Board*, il Comitato Europeo per la Protezione dei Dati) della pluralità delle basi giuridiche di ogni singolo trattamento.

Si può legittimamente ritenere che un organismo sanitario debba individuare anzitutto nell'art. 9 par. 2 lettera h) e par. 3 del Regolamento la base giuridica delle proprie attività; ciò non significa che non occorra poi confrontarsi con obblighi di carattere normativo, laddove siano stati esplicitati, ma che in generale vi è comunque una specificità dei trattamenti di dati effettuati in ambito sanitario – cioè delle attività cui essi sono funzionali – che non può sempre ricondursi, considerata la loro peculiarità e dinamicità, a preesistenti specifiche norme positive. Quando vi sono esse si affiancano, condizionandolo, al trattamento per finalità di cura e gestione dei sistemi sanitari, ma se non vi sono ciò di per se stesso non rende inconsistente ed inutilizzabile quella base giuridica.

La necessità di strutturare percorsi di cura, nella complessità della medicina attuale, precede, certo da un punto di vista logico e ordinariamente anche da quello cronologico, le disposizioni che poi eventualmente li regoleranno: soprattutto, l'attività in ambito sanitario non può essere assimilata ad attività di ambito diverso che hanno interamente la propria genesi nella disposizione o nelle disposizioni che le regolano, il cui scopo cioè si pone come necessario (e lecito) solo dal momento in cui una norma lo rende obbligatorio.

Così, una modalità organizzata di cura che non sia prevista da una norma di legge o di regolamento, sarà comunque lecita in quanto riconducibile alla finalità di cura e gestione dei sistemi e servizi sanitari; quando la previsione normativa vi sarà, ne regolerà meglio il *quomodo*, laddove la legittimità dell'*an* deve però già considerarsi garantita dalla finalità fondamentale.

Vero è che comunque, laddove si volesse ad ogni modo accompagnare un trattamento per finalità di cura e gestione dei sistemi e servizi sanitari con un supporto amministrativo che ne definisse limiti e condizioni, sarebbe sempre possibile utilizzare l'atto amministrativo generale di cui all'art. 2-sexies del Codice (cfr. § 20.3).

20.5. Motivi di interesse pubblico nel settore della sanità pubblica

La sanità pubblica deve essere intesa, secondo il Considerando 54 del Regolamento Generale, così come è definita dall'art. 3 par. 1 lettera c) del Regolamento UE 1338/2008, ovvero: "tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale ad essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità". Si tratta di trattamenti di dati direttamente finalizzati alla conoscenza piuttosto che alla cura, quand'anche della collettività, ed infatti si richiamano quali scopi "la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici", ed al collegato Considerando 53 quelli "di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta".

È una finalità molto prossima a quella esemplificata nel trattamento denominato, nel Decreto del Presidente della Giunta Regionale Toscana 26 ottobre 2021, n. 37/R, "Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria", che l'Autorità riconduce a quelli che adesso si definiscono *motivi di interesse pubblico rilevante* (§ 20.3). Ciò nonostante, l'art. 75 del Codice riferisce evidentemente all'art. 9 par. 2 i) del Regolamento Generale il trattamento "per finalità di tutela della salute e incolumità fisica… della collettività".

20.6. Scopi didattici e scopi di formazione professionale

Esistono nel Regolamento Generale basi giuridiche specificamente e direttamente riferite alla formazione professionale e alla didattica in ambito sanitario (nel senso di formazione professionale e di didattica per le quali debbano essere trattati dati relativi alla salute), in particolare nelle aziende integrate? La risposta è negativa.

Una base giuridica di carattere generale, cioè una finalità lecita cui possa essere ricondotto il riutilizzo dei dati raccolti per finalità di cura per attività didattiche e di formazione professionale (la partecipazione a convegni, i case study a fini didattici e di formazione professionale ecc., le tesi di laurea ecc.), è rappresentata dall'interesse pubblico rilevante di cui all'art. 9 par. 2 lettera g) del Regolamento; nel Codice, l'interesse pubblico rilevante è trattato all'art. 2-sexies (relativo al *Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*), che si articola, al comma 2, in una serie di finalità; tra queste (lett. bb)., quella di "Istruzione e formazione in ambito scolastico, professionale, superiore o universitario".

Si è visto (§ 20.3) che, secondo il comma 1 dell'art. 2-sexies del Codice, tali trattamenti "sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, dell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

La previsione di legge l'abbiamo: l'articolo del Codice ora richiamato o altri che normino l'attività didattica e di formazione professionale; ma certamente, questi, non specificano "i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato"; dobbiamo tentare perciò di trovare questi ulteriori elementi in "disposizioni … di regolamento" o in "atti amministrativi generali".

Per quanto riguarda le disposizioni di carattere regolamentare, se andiamo ad esaminare il Decreto del Presidente della Giunta Regionale Toscana 26 ottobre 2021, n. 37/R, quella base giuridica è richiamata soltanto nella scheda 11 dell'Allegato A, riferita ai Trattamenti di competenza della Regione, dell'ARPAT, delle Agenzie Servizi alla Persona e dell'Istituto degli Innocenti (solo alcuni trattamenti dell'allegato A sono riferibili anche agli "enti controllati"); essa è inoltre dedicata alla "Gestione dei dati relativi ai partecipanti a corsi ed

attività formative": gli interessati sono cioè i discenti, non i pazienti (ovvio, essendo la scheda riferita ad enti diversi dalle Aziende Sanitarie); nessuna scheda specifica è invece presente nell'allegato B, dove sono elencati i trattamenti di competenza delle Aziende sanitarie.

Posto che finora nessuno ha mai visto un "atto amministrativo generale" adottato da una Azienda sanitaria ai fini dell'art. 2-sexies del Codice, in assenza di disposizioni di legge o regolamentari che specifichino tutti gli elementi richiesti dall'art. 2-sexies del Codice sopra richiamato, resta disponibile, quale base giuridica "residuale", il consenso dell'interessato.

E infatti, il Garante ha validato un *Codice di condotta per l'utilizzo di dati a fini didattici e a scopi di pubblicazione scientifica* della Regione Veneto, per il quale il presupposto giuridico per perseguire tali finalità – nella modalità dell'accesso (ed utilizzo) della documentazione clinica - è rappresentato dal consenso dell'interessato; in alternativa, quando il consenso dell'interessato non è acquisito, dalla anonimizzazione dei dati (che non essendo più dati personali, non sono perciò soggetti alla normativa in materia di protezione, appunto, dei dati personali).

Dunque, il trattamento di dati per scopi didattici e di formazione professionale si dovrebbe legittimare attraverso il consenso dell'interessato o l'anonimizzazione del dato.

Il fatto che l'accesso per tali finalità sia esercitato, piuttosto che da uno studente, da un medico in specializzazione (che è appunto un medico) o anche da un medico strutturato (ad es. nel riutilizzo di dati raccolti per finalità di cura per l'intervento ad un convegno), non rileva, non essendo questione meramente soggettiva, ma oggettivamente relativa alla finalità del trattamento. Il medico (strutturato o specializzando) che operi in un reparto può certo accedere alla documentazione clinica del reparto per scopi di cura (quando deve trattare il paziente cui la documentazione si riferisce o altro paziente che rappresenta un caso analogo), ma per quanto riguarda il riutilizzo di essa per ulteriore finalità (es. ricerca, o, appunto, didattica o formazione professionale) la questione è oggettiva, cioè relativa alla finalità ed alla relativa base giuridica, nel rispetto appunto di un principio di limitazione della finalità (§ 6.1).

Esemplifichiamo il principio in riferimento al caso di utilizzo di riprese foto-video per finalità didattiche e di aggiornamento professionale: anche per esse è necessario o che si acquisisca il consenso dell'interessato o che le immagini siano raccolte anonime, o che si proceda ad una loro compiuta anonimizzazione prima dell'utilizzo. Si può approssimare la seguente casistica, con le relative modalità di legittimazione:

- le immagini foto/video (non immagini di diagnostica) sono acquisite per una diversa finalità (es. di documentazione sanitaria), e sono anonimizzate dal Reparto che le ha raccolte prima del loro utilizzo per finalità didattiche e di aggiornamento professionale: è sufficiente l'indicazione offerta nella informativa generale;

- le immagini foto/video (comprese le immagini di diagnostica) sono acquisite anonime (ogni riferimento personale è originariamente assente) o sono successivamente anonimizzate, a scopo didattico o di aggiornamento professionale: comunque, ogni eventuale informazione personale correlata alle immagini deve essere eliminata, e in Azienda quelle immagini non dovranno, in nessun archivio, essere accompagnate da informazioni che possano determinare una identificabilità dell'interessato; dovrà essere fornita adeguata specifica informativa (sostanzialmente allo scopo di evitare che l'interessato possa poi essere indotto a pensare ad una loro conservazione con modalità identificativa a tempo indeterminato, come appunto per la documentazione clinica, con conseguente possibilità d'accesso);
- le immagini (comprese le immagini di diagnostica) sono acquisite a scopo didattico o di aggiornamento professionale non anonime (immagini e riprese non contengono informazioni direttamente identificative)): dovrà essere fornita adeguata specifica informativa all'interessato e dovrà esserne acquisito il consenso (ciò vale anche per tutte le attività effettuate in live surgery);
- le immagini sono acquisite anonime o meno, ma comunque con l'intervento di soggetti esterni alla equipe chirurgica (come tipicamente quando si proceda alla videoregistrazione e trasmissione ad es. di una sessione operatoria): dovrà essere fornita adeguata specifica informativa all'interessato, acquisito il suo consenso ed occorrerà inoltre individuare i soggetti che effettuano le riprese come responsabili o persone autorizzate al trattamento. Si evidenzia che, nel caso di riprese "in diretta", tipologia di intervento, medico operatore, tempistica, rappresentano elementi tali da rendere le immagini messe a disposizione per scopi di formazione professionale, pur se la ripresa si limita al campo operatorio, non anonime.

Se le immagini, non originariamente anonime, hanno subito un processo elettronico di solarizzazione, occorre accertarsi che questo non sia reversibile, ed altrimenti non lasciarle nella disponibilità dei destinatari: così, nel corso di un convegno, si dovrà fare in modo che le immagini non siano rilasciate in formato elettronico. Tale problema è evidente nel caso di messa a disposizione delle immagini secondo una modalità *e-learning*; in questi casi, sarebbe preferibile che le immagini riprendessero fin dall'inizio un paziente con il volto non riconoscibile.

20.7. Dati relativi alla salute e contratto

Il trattamento di dati relativi alla salute non può essere legittimato per la sola via contrattuale; ovvero, quando si stipula un contratto o convenzione, il trattamento di dati relativi alla salute – ad es. la loro comunicazione alla controparte - non trova nel solo strumento contrattuale la sua legittimazione, che deve essere recuperata *aliunde* (consenso dell'interessato, rapporto titolare/responsabile, finalità di interesse pubblico

rilevante ecc.); il contratto non è una condizione di liceità se non per i dati comuni, come è evidente dal fatto che di contratto si parli solo nell'art. 6 del Regolamento Generale, che appunto pone delle condizioni di liceità di carattere generale, ma sconta poi il divieto di trattamento delle categorie di dati di cui all'art. 9 par. 1, fatte salve le finalità elencate dall'art. 9 par. 2.

A quanto sopra osservato consegue che, se è vero che per il datore di lavoro la principale base giuridica del trattamento è il contratto, quando il trattamento riguardi categorie particolari di dati, ad esempio dati relativi alla salute o alla appartenenza sindacale, la base giuridica dovrà individuarsi in particolare nell'art. 9 par. 2 lettera g) (motivi di interesse pubblico rilevante), nell'art. 9 par. 2 lettera b) (assolvimento dei compiti in materi di diritto del lavoro) del Regolamento.

20.8. Trattamento di dati per scopi di ricerca

20.8.1. L'articolo 110 del Codice

Nonostante l'evidente favore per la ricerca presente nel Regolamento UE 2016/679, l'utilizzo della prerogativa, da parte del legislatore nazionale, ai sensi dell'art. 9 par. 4 del Regolamento medesimo, di poter "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di … dati relativi alla salute", ha determinato, con le modifiche apportate dal D.Lgs. 101/2018, un sostanziale aggravamento degli adempimenti già previsti dalla precedente redazione dell'art. 110 del D.Lgs. 196/2003 intitolato alla *Ricerca in ambito medico, biomedico ed epidemiologico*.

L'attuale impostazione dell'articolo 110 del Codice, dedicato alla *Ricerca medica, biomedica ed epidemiologica*, è rimasta, pur a seguito degli adeguamenti apportati dal D.Lgs. 101/2018, sostanzialmente immutata, rispetto alla versione originaria, nel prioritario riferimento, quale base giuridica del trattamento, al consenso dell'interessato:

> il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico ed epidemiologico, non è necessario quando …

Ovvero: il consenso è appunto la base giuridica ordinaria per il trattamento di dati personali a scopo di ricerca scientifica in ambito medico ecc. , fatte salve alcune eccezioni. E comunque, anche qualora tali eccezioni siano verificate sussistenti, il trattamento può essere avviato soltanto a seguito di ulteriori adempimenti. Infatti:

- "quando la ricerca è effettuata in base a disposizioni di legge o di regolamento … ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502" deve essere "condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento";

- "quando … 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" … :
    - ✓ "il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato";
    - ✓ "il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale";
    - ✓ il programma di ricerca "deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento".

Nel primo caso, appare ovvio che si tratta di studi che hanno quella particolare copertura normativa proprio perché si ritiene necessario ampliare la casistica utilizzabile evitando il *bias* rappresentato dal dissenso degli interessati.

Nel secondo caso, invece, la non necessità del consenso è conseguente alla impossibilità (es. pazienti defunti), difficoltà (pazienti dei quali non si riescono a recuperare i dati di contatto), inopportunità (pazienti affetti da patologie con prognosi infausta o che possono non conoscere la diagnosi) di informare gli interessati ed acquisirlo: in tali fattispecie, però, il "programma di ricerca" viene sottoposto a consultazione preventiva presso l'Autorità Garante. E' ovvio che queste situazioni si presentano negli studi osservazionali, e soprattutto in quelli retrospettivi (ma anche in quelli prospettici laddove i motivi per cui non è possibile informare gli interessati sono quelli di carattere etico).

Lo studio osservazionale retrospettivo rappresenta il tipico caso di "utilizzo secondario" dei dati per finalità *ulteriori* rispetto a quelle per le quali sono stati raccolti (si avrebbe invece un "utilizzo primario" quando i dati relativi alla salute fossero stati raccolti direttamente per scopi di studio, come accade per gli IRCCS, cfr. § 20.8.3). E, come precisano le *Linee Guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nell'ambito dell'emergenza legata al COVID-19* adottate dall'EDPB il 21 aprile 2020), al paragrafo 3.3:

> La distinzione tra ricerca scientifica basata sull'utilizzo primario o secondario dei dati relativi alla salute assume particolare importanza al fine di determinare la base giuridica del trattamento, gli obblighi di informazione e l'applicazione del principio della limitazione delle finalità a norma dell'art. 5, paragrafo 1, lettera b) del RGPD …

In breve, la distinzione tra finalità primarie e secondarie significa, applicato alla casistica d'interesse, che il fatto di detenere dati relativi alla salute per finalità di cura non legittima di per sé all'utilizzo di tali dati per una diversa finalità quale quella di ricerca (si tratta del principio di "limitazione della finalità" di cui all'art. 5 par. 1 lettera b del Regolamento Generale); è vero che c'è una generale compatibilità di principio tra tali finalità, ma esse

restano però diverse e separate, e vi sono dunque correlate basi giuridiche (e dunque condizioni e presupposti) distinte.

Prima del Regolamento Generale e dell'adozione del D.Lgs. 101/2018, l'Autorità Garante poteva emanare, ai sensi dell'art. 40 del Codice, delle autorizzazioni generali. Tale possibilità è venuta meno in forza dell'art. 27 comma 1 lett. a) n. 2 del D.Lgs. 101/2018, che ha appunto abrogato il suddetto art. 40. Infatti, tra i compiti ed i poteri riconosciuti alle Autorità di controllo dal dal Capo VI del Regolamento Generale o dal Titolo II del Codice, la possibilità di procedere ad Autorizzazioni Generali, che consistono nell'individuare alcune fattispecie riconducendosi alle quali un certo tipo di trattamento è consentito, non è prevista.

L'art. 21 del d.lgs. n. 101/2018, inoltre, ha demandato al Garante il compito di individuare, con proprio provvedimento di carattere generale – che è poi stato il *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101* n. 146 del 5 giugno 2019 - le prescrizioni, contenute nelle autorizzazioni generali già adottate, che risultino compatibili con le disposizioni comunitarie.

L'allegato n. 5 al Provvedimento 146/2019 reca le *Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica.*

E' del tutto evidente che una *prescrizione* non equivale ad una *autorizzazione*, ed anzi, dal punto di vista semantico, è forse il suo opposto. Il provvedimento reca appunto prescrizioni che si inquadrano nel quadro normativo vigente, e che specificano ed articolano, in via appunto prescrittiva, quali "particolari ragioni" – cioè quali presupposti di fatto - possano addursi quando si sostiene che "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" (art. 110 comma 1 e 110 bis comma 1).

Quel provvedimento non contiene una deroga rispetto alle disposizioni contenute nell'art. 110, ma indica i presupposti, e non le eccezioni, dell'obbligo di svolgere il procedimento indicato dal terzo periodo del primo comma dell'art. 110 (venendo meno tali presupposti, la consultazione preventiva non è accessibile). Inoltre dispone circa adempimenti che sono immediatamente conseguenti rispetto alla disposizione normativa:

> quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali 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;

> Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento.

Ciò, a ribadire che il parere positivo del Garante all'esito di una consultazione preventiva resta comunque una base giuridica subvalente rispetto degli interessati, che non esime dall'ottenerlo quando, anche in una seconda fase, è possibile farlo.

La precedente redazione del primo comma dell'art. 110 comma 1 secondo periodo si muoveva su un piano giuridico diverso, investendo direttamente il Garante – in quella prospettiva di *legal implementation* che fin dall'inizio ne ha caratterizzato, anche rispetto a quella di altre Autorità Amministrative Indipendenti, l'attività - di una regolazione additiva, da attuarsi sia in riferimento al singolo progetto che attraverso una autorizzazione generale, come tale *una tantum*, in relazione ad una fattispecie complessivamente intesa:

> Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40.

L'autorizzazione generale consentiva di far sì che, motivatamente sussunta la condizione particolare dello studio nella fattispecie più ampia *impossibilità di informare gli interessati*, e positivamente valutato dal competente comitato etico tale collegamento, lo studio poteva senz'altro effettuarsi.

Questa è l'attuale redazione del passo sopra riportato dell'art. 110:

> Il consenso non è inoltre necessario 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 della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

Posto che il richiamo all'art. 36 non può certo essere riferito al comma 4 (che riguarda atti legislativi o regolamentari), e che non pare utilizzabile neppure il comma 5 (che si riferisce "al trattamento da parte di un titolare del trattamento di un compito di interesse pubblico,

tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica"), sembra che la "preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento" potrà avviarsi solo a seguito della effettuazione di quella Valutazione d'impatto (o DPIA Data Protection Impact Assestment) di cui tratta l'art. 35 del Regolamento, in quanto è questa il presupposto previsto dai parr. 1 – 3 dell'art. 36 del Regolamento per attivare appunto una preventiva consultazione.

E' vero che, mentre il primo periodo del comma 1 dell'art. 110 richiama tanto l'art. 35 che l'art. 36 del Regolamento, il terzo richiama, in riferimento alla casistica del secondo periodo, solo l'art. 36. Se ne potrebbe allora dedurre che, per le fattispecie di cui al secondo periodo la consultazione preventiva può prescindere dalla redazione di una valutazione d'impatto? Sarei contrario a questa interpretazione.

Anzitutto, banalmente, perché la Valutazione d'impatto è regolarmente richiamata nei Pareri in materia emanati dall'Autorità. Si veda ad esempio il Provvedimento n. 406 del 1° novembre 2021, pag. 4:

> la consultazione preventiva del Garante, ai sensi dell'art. 36 del Regolamento, implica che il titolare del trattamento sottoponga all'Autorità la valutazione di impatto sul trattamento dei dati personali necessari per la realizzazione del progetto di ricerca.

Si noti la logica dell'argomentazione: non è la Valutazione di impatto – ovvero un certo esito della valutazione d'impatto che determina il ricorso alla consultazione preventiva (posto che, in generale, questa si avvia ex art. 36 par. 1 del Regolamento, obbligatoriamente, "qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio"); piuttosto, è la previsione, all'art. 110 comma 1 terzo periodo del Codice, della consultazione preventiva obbligatoria (""il programma di ricerca …deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento") in riferimento a certe condizioni di fatto, ad implicare appunto, retroattivamente, "che il titolare del trattamento sottoponga all'Autorità la valutazione di impatto sul trattamento dei dati personali necessari per la realizzazione del progetto di ricerca". Così comunque salvaguardando il legame inscindibile tra Valutazione d'impatto e Consultazione preventiva.

Più in generale, prendendo in considerazione anche il primo periodo del comma 1 dell'art. 110, possiamo anzi sostenere che l'art. 110 associa all'assenza di consenso – ordinaria base giuridica dell'attività di ricerca - l'obbligo della redazione di una valutazione d'impatto. Infatti, anche il primo periodo dell'art, 110 comma 1, rispetto alla precedente redazione dell'art. 110, introduce un aggravamento del procedimento, prevedendo appunto una valutazione di impatto obbligatoria anche per quelle tipologie di studi per le quali "il consenso … non è necessario" in quanto "la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9,

paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992 n. 502": anche in tutti questi casi infatti "è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento".

E' vero che nel terzo periodo del primo comma dell'art. 110 non si richiama esplicitamente, come nel primo, la obbligatoria redazione di una Valutazione d'impatto: tralasciando che essa, come sopra ricordato, è prevista dall'art. 36 par. del Regolamento, e dunque che sarebbe comunque singolare che la si prevedesse in casi nei quali le ricerche sono previste da basi normative (art. 110 comma 1, primo periodo), ed hanno perciò comunque assicurata una qualche pubblicità, e non per ricerche rispetto alle quali gli interessati non avrebbero simili garanzie.

Dunque, riassumerei l'impostazione ed il senso dell'art. 110 come segue. Stabilito il consenso al trattamento come base giuridica ordinaria (cui si potrebbe aggiungere il parere del competente comitato etico), per ogni attività di ricerca in ambito medico, biomedico ed epidemiologico, si prevede, tanto per i casi nei quali l'acquisizione del consenso non sia *necessaria* che per quelli nei quali, pur essendo dovuta, sia oggettivamente impossibile ecc., un procedimento aggravato che ricomprende comunque la redazione di una Valutazione di impatto, e rispettivamente la sua diffusione (la valutazione d'impatto è "resa pubblica") o comunicazione (s'intende, al Garante).

Di queste Valutazioni d'impatto (diversamente da quelle volontariamente effettuate dal titolare nell'ottica dell'accountability, che devono solo essere redatte, conservate ed eventualmente messe a disposizione dell'Autorità qualora lo richiedesse), l'art. 110 prevede dunque non solo la redazione obbligatoria e la loro conservazione, ma anche:

- la pubblicazione nel caso di progetti di ricerca previsti da disposizioni normative;
- la comunicazione al Garante nel caso di progetti di ricerca nei quali l'acquisizione del consenso non sia oggettivamente possibile.

Nell'ambito della ricerca, perciò:

assenza di consenso > valutazione di impatto (e conseguente, diversificata, sua divulgazione).

Viene comunque meno, in questa prospettiva di carattere sistemico, l'ipotesi che la sottoposizione del progetto di ricerca a consultazione preventiva sia condizionato dalla sussistenza di un "rischio elevato per i diritti e le libertà delle persone fisiche", e che sia sufficiente non riconoscere la presenza di un rischio elevato per far venir meno l'obbligo del passaggio dal Garante.

La correlazione *necessaria* tra i casi in cui "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" e l'obbligo di una consultazione preventiva ("il programma di ricerca … deve essere sottoposto a preventiva consultazione") è esplicitato, ad esempio (in questo caso rispetto a dati già raccolti in un registro di patologia), nel Provvedimento n. 238 del 30 giugno 2022, nei seguenti termini:

> L'Azienda Ospedaliera Universitaria Integrata di Verona … ha presentato un'istanza di consultazione preventiva, ai sensi dell'art. 110, comma 1, ultimo capoverso del Codice e dell'art. 36 del Regolamento, in qualità di promotore dello studio osservazionale interdipartimentale, prospettico, retrospettivo, non farmacologico … trasmettendo il protocollo e la relativa valutazione di impatto, redatta ai sensi dell'art. 35 del Regolamento, *in ragione del fatto che tra i pazienti arruolati rilevano anche soggetti deceduti o non più contattabili*.

Come si vede, è individuato un rapporto di causalità diretta tra il fatto che "tra i pazienti arruolati rilevano anche soggetti deceduti o non più contattabili" e la trasmissione del protocollo e della relativa valutazione di impatto. La consultazione, ovviamente, riguarda dati retrospettivi. E' anzi espressamente dichiarato che:

> Con riferimento ai pazienti non contattabili è la consultazione preventiva in esame, unitamente al parere favorevole del Comitato etico territorialmente competente, a costituire il presupposto giuridico equipollente al consenso, per la raccolta e la conservazione dei dati nel data base

Dunque: la base giuridica del trattamento, nei casi di cui all'art. 110 comma 1 secondo e terzo periodo, quando non è possibile informare gli interessati ed acquisirne il consenso, è rappresentata tanto dal parere del comitato etico che dalla consultazione preventiva con l'Autorità; ricordato che ci è adesso consentito di acquisire il parere del Comitato etico anche successivamente rispetto all'esperimento della consultazione preventiva, si evidenzia che quest'ultima comporta la redazione di una valutazione d'impatto e non vi è spazio per condizionare la consultazione alla sussistenza di rischi più o meno elevati rilevati con la Valutazione d'impatto.

Un caso leggermente diverso, che però conferma il principio generale, è rappresentato dal caso in cui "motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato" gli rendono impossibile "comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso". In tali casi, sono previste le seguenti "prescrizioni":

- "lo studio deve essere volto al miglioramento dello stesso stato clinico in cui versa l'interessato";
- "occorre comprovare che le finalità dello studio non possano essere conseguite 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", con "riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all'attendibilità dei risultati conseguibili in relazione alle specifiche finalità dello studio".
- deve essere acquisito il consenso delle persone indicate nell´art. 82, comma 2, lett. a), del Codice" (cioè chi esercita legalmente la rappresentanza, ovvero un prossimo congiunto, un familiare, un convivente o unito civilmente ovvero un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, il responsabile della struttura presso cui dimora l'interessato).

Quale è la differenza rispetto alle altre situazioni? In questo caso un recepimento dell'informativa e l'espressione di un consenso, da parte di un soggetto collegato all'interessato, sussiste, in accordo con un principio di carattere generale: ai sensi dell'art. 82 comma 2 del Codice, si prevede appunto che in caso di "impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato" è possibile "rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato"; questa disposizione, nella precedente versione dell'articolo, riguardava anche il consenso, riferimento adesso venuto meno (ma probabilmente recuperabile secondo le modalità di cui all'art. 22 comma 11 del D.Lgs. 101/2018, richiamato al § 1).

Ulteriori prescrizioni, nel caso che gli interessati non siano contattabili, devono essere tratte dall'art. 6, comma 3 *delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica adottate dal Garante, ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101*, Allegato A 5 al Codice, il quale dispone che:

> Quando i dati sono raccolti presso terzi, ovvero il trattamento effettuato per scopi statistici o scientifici riguarda dati raccolti per altri scopi, e l'informativa comporta uno sforzo sproporzionato rispetto al diritto tutelato, il titolare adotta idonee forme di pubblicità, ad esempio, con le seguenti modalità:
>
> - per trattamenti riguardanti insiemi numerosi di soggetti distribuiti sull'intero territorio nazionale, inserzione su almeno un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale;
> - per trattamenti riguardanti insiemi numerosi di soggetti distribuiti su un'area regionale (o provinciale), inserzione su un quotidiano di larga diffusione regionale (o

provinciale) o annuncio presso un'emittente radiotelevisiva a diffusione regionale (o provinciale);
- per trattamenti riguardanti insiemi di specifiche categorie di soggetti, identificate da particolari caratteristiche demografiche e/o da particolari condizioni formative o occupazionali o analoghe, inserzione in strumenti informativi di cui gli interessati sono normalmente destinatari".

Si evidenzia che il Garante intende tali condizioni estensivamente, nel senso di un dovere di informare gli interessati non contattabili, così come, per quelli deceduti, a beneficio di eventuali terzi legittimati ex art. 2-terdecies del Codice), e tale obbligo viene normalmente espletato, qualora riguardi dati detenuti dall'Azienda, mediante pubblicazione dell'informativa sul sito istituzionale.

Ai sensi dell'art. 166 del D.Lgs. 196/2003, colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma, è soggetto alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento (fino a 10 milioni di euro).

20.8.2. L'articolo 110 bis del Codice

Alcuni interpreti, alquanto creativamente, hanno ritenuto di poter riferire gli studi osservazionali non l'art. 110 ma all'art. 110 bis.

Occorre ricordare che dell'articolo 110 bis esisteva una precedente versione, introdotta dall'articolo 28, comma 1, lettera b) della legge 20 novembre 2017, n. 167, recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017":

> Nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati.
>
> Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli

interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza.

Evidenzio che si parla di autorizzazione e del termine dei 45 giorni, che allora l'art. 110 riportava all'art. 39 del Codice, successivamente abrogato con il D.Lgs. 101/2018, e che si esclude il trattamento di dati genetici.

Tale versione era rubricata *Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici* (oggi l'art. 110 bis reca: *Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici*).

La attuale versione dell'art. 110 bis è la seguente:

1. Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività 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 della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza.
3. Il trattamento ulteriore di dati personali da parte di terzi per le finalità di cui al presente articolo può essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore
trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati. I provvedimenti adottati a norma del presente comma sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana.

> 4. Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

E' immediato osservare due caratteri distintivi dell'art. 110 bis (in ambedue le redazioni), rispetto all'art. 110:

- dal punto di vista oggettivo, se l'art. 110, tanto nella versione precedente come in quella successiva al D.Lgs. 101/2018 si riferisce alla *Ricerca medica, biomedica ed epidemiologica* (e, al comma 1, al "trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico ed epidemiologico") il 110 bis si riferisce, meno specificamente, alla *Ricerca scientifica o a fini statistici* (si può pensare alla ricerca in ambito sociologico, economico ecc., oltre che alla ricerca statistica);
- dal punto di vista soggettivo, l'art. 110 bis riguarda i soggetti "terzi" (*Trattamento ulteriore da parte di terzi).*

Nel primo caso, si evidenzia una maggior specificità dell'art. 110 rispetto all'art. 110 bis. Tale osservazione parrebbe però contraddetta dal richiamo, al comma 4 dell'art. 110 bis, agli IRCCS. Ugualmente, le Regole deontologiche - pur se si applicano a trattamenti per scopi, appunto, *statistici e scientifici* non connessi "con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attività comparabili in termini di significativa ricaduta personalizzata sull´interessato"- sono regolarmente richiamate dal Garante nei provvedimenti sugli studi clinici (non interventistici).

Circa il secondo aspetto, occorre osservare che la versione attuale dell'art. 110 bis si riferisce, fin dalla rubrica, non solo a trattamenti di dati ulteriori, ma anche svolti da "soggetti terzi", terzi evidentemente riguardo a chi ha raccolto i dati per la primaria finalità clinica: quindi, non solo riutilizzo secondario di dati raccolti per una diversa finalità primaria, ma riutilizzo da parte di soggetto terzo.

Sono terzi, ai sensi dell'art. 4 10 del Regolamento i soggetti diversi rispetto a

> l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

Si tratta di soggetti esterni all'ambito del trattamento, che ne acquisiranno poi la titolarità, non avendo di partenza particolari prerogative sui dati (se non per il fatto "che svolgano

principalmente tali attività", si presume quelle con finalità scientifiche e statistiche) dopo il provvedimento autorizzatorio, particolare o generale, del Garante.

Oggetto del nuovo 110 bis è dunque il trattamento *ulteriore* di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte non del titolare, ma di soggetti *terzi* rispetto a questo, che svolgano principalmente tali attività di ricerca.

Tralascio la curiosa notazione, nel primo comma, "*trattamenti speciali* di cui all'articolo 9 del Regolamento" (Il Regolamento, nella versione inglese, parla ovviamente di "Processing of special categories of personal data", laddove "special" – particolari – sono appunto le "categories of personal data", non i processings, i trattamenti).

Nell'art. 110 bis, la fattispecie affrontata è sempre comunque la medesima dell'art. 110: dati raccolti per una primaria finalità, che si intende utilizzare ulteriormente per finalità di ricerca ma rispetto ai quali non è possibile informare gli interessati ed acquisirne il consenso; il riutilizzo interesserà però non il soggetto che ha raccolto i dati per la finalità primaria, ma appunto soggetti terzi, cioè esterni rispetto al primario ambito di titolarità e che comunque hanno la ricerca scientifica o i fini statistici tra le proprie principali attività. Potrebbe essere il caso di una casa farmaceutica, ma anche dell'Università, qualora volesse condurre in proprio uno studio utilizzando i dati aziendali.

La soluzione qui prospettata, come per l'art. 110 comma 1 terzo periodo, comporta un passaggio dal Garante: nel 110 bis si parla però precisamente di *autorizzazione* del Garante, proprio spendendo quel termine (*unicum*, riferito al Garante, nell'attuale redazione del Codice), pure con la risalente tempistica dei 45 giorni, ma non si prevede esplicitamente, in questo caso, né la preventiva trasmissione di una Valutazione d'impatto, non essendovi alcun riferimento all'art. 35 o 36 del Regolamento, né il parere del Comitato etico (il che è di per sé impossibile); e non si capisce dunque su quale documentazione possa fondarsi questa "autorizzazione" del Garante: sempre che le "misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati" non si debbano intendere comunque documentate – dove altrimenti? – in una Valutazione d'impatto.

Secondo alcuni giuristi, l'art. 110-bis del Codice andrebbe letto in combinato con l'art. 21 del d.lgs. 10 agosto 2018, n. 101 e con le Prescrizioni già sopra richiamate.

L'art. 110 bis infatti prevede, al comma 3, che il trattamento ulteriore di dati personali da parte di terzi per le finalità di ricerca "può essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati".

Tale provvedimento generale dovrebbe appunto individuarsi nel Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101: da tale individuazione si fa derivare che se il trattamento resta entro l'ambito descritto all'art. 5.3 delle Prescrizioni, il secondo comma dell'art. 110 (quello che dispone l'obbligo di consultazione preventiva del Garante) non troverebbe applicazione.

Mi sembra però si dimentichi quanto sopra osservato, cioè che gli artt. 110 e 110 bis non hanno il medesimo ambito di applicazione: in forza di tale assunto non può sostenersi che, per il combinato tra Prescrizioni, artt. 110-bis del Codice Privacy e 21 del D.Lgs. 101/2018, il secondo comma dell'art. 110 (quello che dispone l'obbligo di consultazione preventiva del Garante) non troverà applicazione, proprio per l'immediata (e impropria) correlazione tra i due articoli che così verrebbe a realizzarsi.

Inoltre, se quello recante le Prescrizioni dovesse individuarsi quale uno dei *provvedimenti generali* dell'art. 110 bis comma 3, nella sezione 5 delle Prescrizioni medesime, al trattamento da parte di *terzi (*al quale solo potrebbe applicarsi, visto che analoga previsione non vi è nell'art. 110*)*, magari, almeno un richiamo sarebbe stato fatto.

Per quanto riguarda, poi, i Provvedimenti o autorizzazioni generali, tante sono le specificità degli studi, dal punto di vista del trattamento dei dati, ed in così rapida evoluzione, che è estremamente difficile ricondurli, senza semplificazioni, a casistiche univoche (magari diversamente rispetto a ricerche di ambito statistico).

Credo che una possibile applicazione dell'art. 110 bis comma 3, con la previsione di provvedimenti generali, potrebbe riferirsi all'accesso, da parte diverso titolare, dei Sistemi di sorveglianza sanitaria o i Registri di patologia elencati dal Dpcm) del 3 marzo 2017.

In tali casi, sarebbe accettabile che il soggetto esterno, terzo rispetto al titolare che ha raccolto i dati (nel caso di utilizzo secondario) o che ha comunque il rapporto fondamentale con gli interessati (nel caso di raccolta di dati direttamente finalizzati alla ricerca) rivendichi una esclusiva titolarità del trattamento (cfr. il § successivo).

20.8.3. L'articolo 110 bis e gli IRCCS

Maggiori problemi interpretativi ci pone comunque il comma 4 dell'art. 110 bis:

> Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

Si può interpretare la disposizione riferendo agli Istituti di ricovero e cura a carattere scientifico la raccolta dei dati nell'ambito dell'attività clinica, come segue:

> Non costituisce trattamento ulteriore da parte di terzi il trattamento, a fini di ricerca, dei dati personali *raccolti per l'attività clinica da parte degli Istituti di ricovero e cura a carattere scientifico* …

Però questa impostazione - che assicurerebbe agli IRCCS la immediata liceità del trattamento per finalità di ricerca dei dati raccolti *nel proprio ambito di attività assistenziale* senza necessità di una base giuridica ulteriore rispetto a quella rappresentata dall'art. 9 par. 2 lettera J del Regolamento, che infatti richiama l'art. 89, qui citato (appunto "in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca", loro primaria finalità) – richiederebbe di perdere il riferimento ai terzi, che in tal caso proprio non verrebbero in causa: trattamento ulteriore sì, ma non da parte di terzi.

Conservando e valorizzando invece il riferimento ai terzi, e così giustificando la faticosità di scrittura della redazione attuale, con quella giustapposizione di cause, attraverso l'inciso ("il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte …"), la lettura più diretta parrebbe la seguente:

> Non costituisce trattamento ulteriore da parte di terzi il trattamento, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, dei dati personali raccolti per l'attività clinica, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

I primi 3 commi concernono il trattamento ulteriore (riutilizzo, rispetto a chi ha raccolto i dati per scopi di cura) di dati personali da parte di terzi i quali svolgano principalmente attività di ricerca o per finalità statistiche; relativamente a tale trattamento ulteriore del terzo, si prevede, qualora non sia possibile raccogliere il consenso degli interessati, il ricorso ad una decisione autorizzatoria del Garante. Relativamente agli IRCCS, invece, tale riutilizzo non deve qualificarsi come "trattamento ulteriore da parte di terzi", per cui è possibile prescindere dalla autorizzazione del Garante. Il riferimento al "carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca" dovrebbe essere interpretato come riconoscimento di una legittimazione di carattere generale al trattamento di dati, raccolti da terzi, per gli scopi di ricerca degli IRCCS. Resta ovviamente il problema che nessuna disposizione offre agli IRCCS, come parrebbe logico, la possibilità di un utilizzo immediato dei dati raccolti presso i propri pazienti: sempre che la notazione circa il "carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca", individuando l'attività di ricerca

come una finalità a sua volta primaria per gli IRCCS, non sia di per sé valutata sufficiente a superare lo iato tra attività di cura (primaria) e attività di ricerca (secondaria) che determina il ricorso al consenso o alla legge, ai regolamenti ecc. come ulteriore base giuridica necessaria per la liceità dei trattamenti a scopo di ricerca.

20.9. Ruoli privacy del Centro di sperimentazione e del Promotore

Si è recentemente notato un deciso riposizionamento dei Promotori relativamente al rapporto con i Centri di sperimentazione circa la qualificazione dei rispettivi ruoli in materia di protezione dei dati personali, motivato da presunte disposizioni del Regolamento, fino ad un sostanziale rovesciamento delle impostazioni che avevano a suo tempo portato l'Autorità Garante ad adottare il Provvedimento n. 52 del luglio 2008. Fino a tale determinazione, si ricordi, le case farmaceutiche tendevano a rifiutare la qualificazione di titolari del trattamento, sostenendo che esse trattassero dati di fatto anonimi ancorché codificati, per l'impossibilità di correlarli a soggetti identificati o identificabili. L'Autorità Garante aveva all'opposto evidenziato come si trattasse di informazioni che, seppur non direttamente identificative (appunto, codificate), era comunque necessario qualificare come dati personali per la possibilità che una identificazione fosse, nonostante la codificazione, successivamente recuperabile (la reidentificazione era cioè certo improbabile, ma non impossibile): ne seguiva che tanto il Centro di sperimentazione che il Promotore esterno assumevano il ruolo di (autonomi) titolari del trattamento, con diverse profondità di accesso ai dati (solo il Centro, fatta salva l'attività di monitoraggio, poteva conoscere i dati identificativi dei partecipanti allo studio): la titolarità autonoma si giustificava per il fatto che, pur condividendo la finalità di ricerca, i due soggetti trattavano i dati secondo diverse modalità, l'uno secondo una modalità identificativa e l'altro non identificativa; l'uno inoltre raccoglieva i dati, anche in diretto rapporto con l'interessato, oppure acquisiva i dati già raccolti per la primaria finalità di cura per la finalità di ricerca ecc.

Sempre più frequentemente, adesso, il Promotore propone invece di qualificare la relazione con il Centro di sperimentazione nei termini di un rapporto tra titolare (il Promotore) e responsabile (il Centro di sperimentazione). Alcune proposte, estremizzando la medesima logica, propongono addirittura che lo sperimentatore principale si qualifichi come *persona fisica espressamente designata*, ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003, che opera sotto la autorità del Promotore, non riconoscendo evidentemente al Centro di sperimentazione alcun ruolo nel trattamento dei dati.

I Promotori giustificano tale nuova impostazione richiamando un passo delle *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR* adottate il 7 luglio 2021 dall'EDPB (European Data Protection Board); si tratta di un documento di carattere generale, che al punto 68, nella versione italiana, recita:

> *Un prestatore di assistenza sanitaria (lo sperimentatore) e un'università (lo sponsor) decidono di avviare congiuntamente una sperimentazione clinica avente la medesima finalità.*

Collaborano all'elaborazione del protocollo di studio (ossia finalità, metodologia/progettazione dello studio, dati da raccogliere, criteri di esclusione/inclusione dei soggetti, riutilizzo delle banche dati, se del caso, ecc.).
Possono essere considerati contitolari del trattamento per detta sperimentazione clinica in quanto stabiliscono e concordano congiuntamente una stessa finalità e i mezzi essenziali del trattamento. La raccolta di dati personali dalla cartella clinica del paziente ai fini di ricerca va distinta dalla conservazione e dall'uso degli stessi dati ai fini dell'assistenza del paziente, per i quali il fornitore di assistenza sanitaria rimane titolare del trattamento.
Nel caso in cui lo sperimentatore non partecipi alla stesura del protocollo (in quanto accetta semplicemente il protocollo già elaborato dallo sponsor) e il protocollo sia elaborato solo dallo sponsor, ai fini della sperimentazione clinica il ricercatore dovrebbe essere considerato responsabile del trattamento e lo sponsor il titolare del trattamento[29].

L'argomentazione è dunque la seguente: se la nozione di titolare del trattamento indica il soggetto che decide finalità e modalità del trattamento, e lo sponsor ha redatto in autonomia il protocollo di studio (che prescrive, tra l'altro, come si debbano trattare i dati personali nell'ambito dello studio), laddove invece "lo sperimentatore … accetta semplicemente il protocollo già elaborato dallo sponsor", ne segue che la titolarità compete esclusivamente al Promotore, ed il ruolo dello Sperimentatore deve essere recuperato dalle prerogative del Promotore, e non potrà essere che quello di Responsabile. La prospettiva non è quella, delineata nel Provvedimento 52/2008, di una collaborazione finalizzata ad un obiettivo comune - lo sviluppo della ricerca e delle conoscenze in campo medico - ma quasi quella di una accettazione di una proposta contrattuale, finalizzata alla esecuzione di un servizio per conto del proponente.

La esclusiva titolarità dello sponsor si costituisce dunque in rapporto al ruolo svolto (o non svolto) dall'Azienda sanitaria rispetto alla redazione del protocollo; se ha contribuito a redigerlo, si qualificherà come titolare (o contitolare) del trattamento, altrimenti come responsabile del trattamento: a seguito dell'accordo con lo Sponsor e l'accettazione del

[29] "A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller. In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial".
Al testo è associata una nota secondo la quale "L'EDPB prevede di fornire ulteriori orientamenti in relazione alle sperimentazioni cliniche nel contesto delle prossime linee guida sul trattamento dei dati personali a fini medici e di ricerca scientifica".

protocollo di studio, si procederà a pseudonimizzare i dati necessari allo studio, ed a metterli a conoscenza dello sponsor in tale modalità.

Circa questa impostazione, occorre, a mio avviso, non dimenticare che, se è vero che l'art. 4 1 del Regolamento definisce titolare il soggetto "che, singolarmente o insieme ad altri, *determina le finalità e i mezzi del trattamento di dati personali*", quella di titolare, come più volte i Garanti europei hanno precisato, è una nozione *di fatto* (finalizzata ad una attribuzione di responsabilità, nel senso che chi tratta dati determinando scopi e modalità del trattamento è di per ciò stesso, al di là di ogni valutazione di liceità, titolare del trattamento): è perciò una qualificazione che non può che riguardare una situazione *attuale* e non meramente prospettica o ipotetica, che riguarda chi tratta o può comunque già adesso trattare i dati e non chi li tratterà o ha intenzione di trattarli: il titolare è insomma tale se e quando ha la prerogativa, e non la mera intenzione, di trattare i dati, in breve se e quando ne ha la disponibilità. Fin quando effettivamente non tratta dati, o non ne ha lecitamente la disponibilità, il Titolare non è Titolare di nulla, se non di una aspirazione alla titolarità.

D'altronde, nella configurazione del rapporto tra titolare e responsabile, è il titolare che mette a disposizione del responsabile i dati che deve trattare per suo conto, e non viceversa, e può costituirlo come tale solo se ha la disponibilità dei dati che vuol fare trattare per proprio conto.

Insomma, il Promotore di uno Studio non diventa Titolare del trattamento nel momento in cui idea uno studio. Lo è se e quando, oltre a ciò, ha la disponibilità dei dati.

Un accordo contrattuale, relativo a categorie particolari di dati, e segnatamente a dati relativi alla salute, può consentire ad un titolare, ai sensi dell'art. 28 par. 3 del Regolamento Generale, di costituire un soggetto come responsabile del trattamento; ma un accordo contrattuale, nel caso in esame la sottoscrizione di una convenzione o del protocollo di studio, non può costituire come titolare del trattamento dei dati un soggetto che non abbia alcuna pregressa prerogativa rispetto a quei dati.

In alcuni contratti si distingue tra titolarità del Centro di sperimentazione sui dati clinici (identificativi) e titolarità del Promotore sui dati di ricerca (pseudonimizzati). Più precisamente, si sostiene che i dati clinici (identificativi) sono nella titolarità delle Aziende per la finalità di cura, mentre quelli trattati per finalità di ricerca (ovvero quegli stessi dati, una volta pseudonimizzati) sono invece nella titolarità esclusiva del Promotore. Questa parrebbe una applicazione delle Linee Guida 7/2020 sopra citate, laddove si prevede che "La raccolta di dati personali dalla cartella clinica del paziente ai fini di ricerca va distinta dalla conservazione e dall'uso degli stessi dati ai fini dell'assistenza del paziente, per i quali il fornitore di assistenza sanitaria rimane titolare del trattamento", correlando alle due diverse finalità due diverse modalità di trattamento dei dati: identificativi per la cura, pseudonimizzati per la ricerca. Mediante un accordo interno, lo Sponsor e l'Azienda decidono che questa proceda a pseudonimizzare i dataset clinici indicati nel protocollo e

tali dati, per ciò solo (accordo e operazione di pseudonimizzazione) transitano (o sono creati) nell'ambito della titolarità dello sponsor.

Ricordo che la pseudonimizzazione (§ 11) è "il 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 …", è insomma una operazione di trattamento che si risolve esclusivamente in una misura di sicurezza, appunto riducendo il rischio di identificazione dell'interessato: i dati non possono essere attribuiti all'interessato senza l'utilizzo di informazioni ulteriori che vengono mantenute riservate dal Titolare.

La pseudonimizzazione, come qualsiasi altra operazione di trattamento sui dati personali, è prerogativa del Titolare del trattamento: chi pseudonimizza i dati è quel soggetto che può già qualificarsi come titolare del trattamento rispetto a quei dati.

Più precisamente: la titolarità, come abbiamo sopra argomentato, non si riferisce ai dati, ma al trattamento dei dati; e il trattamento dei dati, si è già notato, è essenzialmente caratterizzato dalla finalità, ovvero dallo scopo, che deve essere già del soggetto che la persegue. In altre parole: se un soggetto compie una operazione di trattamento (in questo caso, la pseudonimizzazione) per una certa finalità (la ricerca), deve già avere tra le sue prerogative quella finalità.

Dal dimenticare questo fondamentale assunto – ovvero che, nella protezione dei dati, la finalità, e la relativa base giuridica, hanno una fondamentale centralità – deriva che abbiamo un sedicente titolare che (tranne che nel caso, del tutto particolare, e che conferma il principio, dell'attività di monitoraggio e auditing, nella quale però il Monitor e l'Auditor assumono per l'appunto un ruolo indipendente rispetto al Promotore) ha una minore profondità d'accesso del responsabile, che pure da quello dovrebbe avere trasmesse tutte le sue prerogative. Ma, come recita il noto brocardo: *nemo plus iuris ….*

Inoltre, vi sono dati che i Centri di sperimentazione trattano per scopo di ricerca in costanza di rapporto con il paziente, e dunque in modalità forzatamente identificativa: si pensi a studi che prevedano prestazioni o attività aggiuntive rispetto all'ordinario percorso di cura (ed in generale tutti gli studi interventistici). La correlazione finalità/modalità, così come proposta in quei contratti, non può dunque considerarsi rigida e dirimente in ordine alla titolarità.

Ulteriore problema è posto dagli studi osservazionali per i quali non sia possibile richiedere il consenso agli interessati, così che debba attivarsi la procedura dettata dall'art. 110 comma 1 secondo periodo del D.Lgs. 196/2003: chi è il soggetto in grado di effettuare la valutazione d'impatto da trasmettere al Garante per la consultazione preventiva? Non certo il Promotore, che non ha cognizione di come sono saranno trattati i dati clinici da utilizzare (a seguito della autorizzazione dell'Autorità) a scopo di ricerca. Il soggetto deputato a redigere la DPIA è il titolare del trattamento rispetto alla finalità perseguita. E quando si attivano le procedure previste dall'art. 110, siamo già nell'ambito di una finalità

di ricerca. Dunque, se la DPIA deve essere effettuata dal titolare, se il soggetto che può effettuare la DPIA è solo l'Azienda sanitaria, e se la finalità per la quale si effettua una DPIA è già quella di ricerca, ne segue che l'Azienda sanitaria, in questa fattispecie, deve individuarsi quale titolare del trattamento per finalità di ricerca.

Il presupposto dell'esempio portato dall'EDPB è appunto che lo sperimentatore (o il Centro di sperimentazione) si limiti "semplicemente" ad accettare passivamente il protocollo già elaborato dallo sponsor. Il Provvedimento del Garante del 2008 dimostrava invece una miglior cognizione del setting di studio, e muoveva correttamente dall'assunto che l'accettazione del protocollo di studio non è un atto meramente passivo, ma è, piuttosto, funzionale ad una "partecipazione" del Centro di sperimentazione, attiva e non acritica, alla ricerca. Il Centro di Sperimentazione non opera "per conto" del Promotore, in un rapporto gerarchico e funzionale rispetto ad esso, opera per scopi di ricerca che condivide con il Promotore (e che possiede "originariamente" tra le proprie finalità istituzionali):

> … va rilevato che il centro non è assoggettato a vincoli di subordinazione nei confronti del promotore: accetta il protocollo concordandone con il promotore alcuni aspetti, compresi quelli relativi alla formulazione del consenso informato delle persone partecipanti in ottemperanza al parere del comitato etico di riferimento; esegue la sperimentazione con propria autonomia organizzativa, sebbene nel rispetto del protocollo, delle procedure operative standard e delle direttive del promotore; per l'esecuzione della sperimentazione si avvale di collaboratori che ritiene idonei ed è responsabile del loro operato; fornisce l'informativa alle persone coinvolte nello studio e acquisisce il loro consenso anche per ciò che attiene al trattamento dei dati che le riguardano; permette che i collaboratori del promotore accedano alla documentazione medica originale dei soggetti coinvolti per svolgere le attività di monitoraggio; gestisce e custodisce sotto la propria responsabilità tale documentazione.

In effetti il Promotore, appunto, *promuove* lo studio, lo propone, non lo svolge esclusivamente in proprio, o attraverso un terzo servente, e con la sottoscrizione del protocollo acquisisce non i dati e i risultati, ma la partecipazione e collaborazione attive dei Centri che vi aderiscono. E infatti spesso non fornisce esaustive istruzioni sul trattamento dei dati.

Il Garante, proprio sulla base dell'assunto che il Promotore e i singoli centri di sperimentazione "hanno in genere responsabilità distinte", aveva indicato la soluzione delle autonome titolarità, o in alternativa, una ipotesi di contitolarità (anch'essa peraltro percorribile, considerato che la contitolarità non vieta profondità di accesso differenziate tra i vari titolari che pure abbiano concordato le finalità e le modalità, appunto anche

articolate e differenziati nei ruoli, del trattamento). Tale soluzione ci sembra a tutt'oggi quella più razionale ed obiettiva.

D'altronde, questa pretesa dello Sponsor all'immediata titolarità - Sponsor che è soggetto terzo rispetto a quello che ha che raccolto i dati per la primaria finalità di cura e li vuole riutilizzare per un trattamento ulteriore - consentirebbe di bypassare il processo previsto dall'art. 110 bis.

Si potrebbe anzi argomentare, generalizzando, che l'art. 110 dovrebbe essere riferito esclusivamente agli studi che sono strutturati, dal punto di vista dei soggetti che trattano dati, secondo l'impostazione delle autonome titolarità (o della contitolarità) delineata nel provvedimento 52/2008, laddove, qualora si volesse riconoscere ai terzi (tra questi, ad es. anche agli sponsor) una titolarità esclusiva del trattamento (con quindi un ruolo vicario dell'Azienda sanitaria), potrebbero essere utilizzati i commi 1 – 3 dell'art. 110 bis.

Analogamente, si dovrebbe argomentare in relazione al ruolo dell'Università: ribadendo le prerogative dell'Azienda sanitaria quale titolare del trattamento per la finalità di cura, si osserva che qualora si intendano utilizzare i dati già raccolti per quella finalità primaria per una ulteriore finalità secondaria con essa compatibile – ad esempio quella di ricerca - solo il soggetto titolare del trattamento per la finalità primaria potrà attivare, con le modalità previste dalla legge, quel trattamento ulteriore; quindi, nel nostro caso, solo l'Azienda, e non l'Università degli Studi, considerato che questa deriva la sua legittimazione a poter trattare dati clinici per scopi di ricerca solo da una collaborazione con l'Azienda (non dalla generica relazione che si stabilisce nell'Azienda integrata), che dovrà essere formalizzata in riferimento ad ogni specifico progetto di ricerca; in alternativa, qualora volesse rivendicare una esclusiva titolarità del trattamento, l'Università dovrebbe ottenere una autorizzazione ai sensi dell'art. 110 bis (trattamento ulteriore da parte di soggetto terzo).

21. Creazione di banche dati

Si ricorda che il Codice di deontologia medica prescrive all'art. 11 comma 2 che "Il medico non collabora alla costituzione, alla gestione o all'utilizzo di banche di dati relativi a persone assistite in assenza di garanzie sulla preliminare acquisizione del loro consenso informato e sulla tutela della riservatezza e della sicurezza dei dati stessi."

Garantire la "tutela della riservatezza e della sicurezza dei dati", nell'ambito di un organismo sanitario, significa, anzitutto, che ogni registro o banca dati devono essere preventivamente valutati dal punto di vista della complessiva responsabilizzazione del Titolare, cioè degli elementi che assicurano tale responsabilizzazione: limitazione della finalità, base giuridica, minimizzazione dei dati, sicurezza (ivi compresa l'accessibilità).

Osservo che, pur restando nell'ambito della finalità primaria (di cura), anche le modalità con cui perseguo tale finalità (i mezzi del trattamento) qualificano lo specifico trattamento,

e la loro modifica o alterazione determina l'attivazione di un trattamento diverso la cui adeguatezza deve essere valutata dal Titolare. Cioè: si sono raccolti dati personali per scopo di cura che sono archiviati su un applicativo aziendale, secondo modalità che (si presume) il Titolare ha già valutato adeguate dal punto di vista della protezione dei dati personali; potrei trasferire ed utilizzare questi dati, sempre per finalità di cura, creando una ulteriore banca dati: i nuovi mezzi che utilizzo sono tali da modificare – ad esempio dal punto di vista della sicurezza – il trattamento effettuato sulla banca dati originaria, si effettua un diverso trattamento che deve essere esaminato ed autorizzato dal titolare, ad esempio attraverso una valutazione d'impatto.

Tale valutazione è ovviamente necessaria anche quando i dati raccolti per la finalità primaria sono estratti dall'applicativo ed utilizzati per una finalità diversa, venendo in tal caso in causa la base giuridica di tale nuovo trattamento, ed a maggior ragione quando sono archiviati in una nuova banca dati, che può presentare particolari problemi di sicurezza.

In assenza di tale valutazione (positiva), tutte le basi dati non autorizzate sono illecite, ed espongono chi le crea o utilizza a responsabilità personale.

22. Videosorveglianza in Azienda

Per videosorveglianza si intende:

- attività di videosorveglianza propriamente detta, effettuate attraverso sistemi e dispositivi che permettono al visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche dati di immagini di aree o zone delimitate;
- attività di videocontrollo, effettuate attraverso sistemi o dispositivi che permettono unicamente la visione in tempo reale di aree o zone delimitate.

Si precisa che un'Azienda pubblica ha generali obblighi di tutela delle cose e delle persone che si trovano nelle aree di pertinenza, e che tali obblighi rientrano tra i propri compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, di cui all'art. 6 par. 1 lettera e) e 9 par. 2 lettera g) del Regolamento; si ricorda altresì che i compiti istituzionali di un ente pubblico non devono essere necessariamente specificati in uno specifico atto legislativo (Considerando 45 del Regolamento).

I trattamenti di dati attraverso gli impianti di videosorveglianza possono avere le seguenti finalità:

1. protezione delle persone all'interno e all'esterno delle strutture aziendali
2. tutela dei beni e in particolare prevenzione dei reati contro il patrimonio dell'azienda, dei dipendenti e degli utenti;
3. sicurezza degli ambienti di lavoro;
4. gestione dell'accesso di persone fisiche ed automezzi ad aree ad accesso controllato;

5. tutela della salute attraverso il videocontrollo a distanza dei pazienti;
6. controllo della procedura di raccolta di campioni biologici a fini certificatori o di cura.

Il consenso dell'interessato, di cui agli artt. 6 comma 1 lettera a) e 9 comma 2 lettera a) del Regolamento, non rappresenta base giuridica necessaria per la liceità del trattamento. Le basi giuridiche del trattamento sono da individuarsi rispettivamente:

- per il punto 1, nell'art. 6 par. 1 lettera e) del RGPD (perseguimento di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri);
- per il punto 2, nell'art. 6 par. 1 lettera e) del RGPD (perseguimento di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri);
- per il punto 3, nell'art. 6 par. 1 lettera e) e nell'art. 9 par. 2 lettera g) del RGPD (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri);
- per il punto 4, nell'art. 6 par. 1 lettera e) del RGPD (perseguimento di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri);
- per il punto 5, nell'art. 9 par. 2 lettera g) (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) e nell'art. 9 par. 2 lettera h) del RGPD (attività di assistenza sanitaria);
- per il punto 6, nell'art. 9 par. 2 lettera g) (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) e nell'art. 9 par. 2 lettera h) del RGPD (attività di assistenza sanitaria).

L'attività di videosorveglianza, inoltre, quando comporta, o può comportare anche incidentalmente, la ripresa di lavoratori, deve essere attivata con le modalità previste dall'art. 4 della L. 300/70.

Il rifiuto di conferire i dati comporta l'impossibilità da parte dell'interessato di accedere alle aree videosorvegliate dell'Azienda. L'accesso alle zone videosorvegliate comporta, senza necessità del consenso dell'interessato, la raccolta, la registrazione, la conservazione e, in generale, il possibile utilizzo delle immagini degli interessati.

Destinatari (cioè i soggetti che ricevono *comunicazione* di dati personali) dei dati di videosorveglianza possono essere:

- magistratura o forze dell'ordine;
- soggetti legittimati all'eccesso ai dati in quanto titolari di un interesse giuridicamente qualificato.

I dati sono trattati in qualità di Responsabili del Trattamento (ai sensi dell'art.28 del Regolamento generale):

- dalla ditta che supporta il servizio di videosorveglianza;
- dalle ditte fornitrici dei servizi di gestione e manutenzione degli impianti.

I dati sono inoltre trattati in ambito aziendale da persone specificamente autorizzate al trattamento, espressamente designate e autorizzate per l'accesso sia ai locali dove sono situate le postazioni di controllo che agli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Il personale autorizzato riceve istruzioni specifiche ed è dotato di livelli differenziati di accesso, a seconda delle mansioni effettuate.

I dati trattati non sono oggetto di diffusione.

I dati, qualora registrati, saranno conservati - salvo necessità di utilizzo da parte dell'Azienda o eventuali richieste d'accesso o speciali esigenze di ulteriore conservazione in relazione tanto a indagini di Polizia giudiziaria che a richieste dall'Autorità giudiziaria - per un massimo di 96 ore.

I sistemi sono programmati in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili o accessibili i dati cancellati. Le informazioni memorizzate su supporto che non consenta la sovra-registrazione sono ugualmente distrutti entro il termine massimo sopra indicato.

E' opportuno prevedere, in attuazione del principio di minimizzazione, che le immagini riprese siano limitate, laddove opportuno, tanto dal punto di vista della loro eventuale registrazione che da quello dell'orario di ripresa (es. solo riprese notturne).

I dati personali raccolti mediante le attività di videosorveglianza non saranno elementi a supporto di alcun processo decisionale automatizzato.

Il Provvedimento dell'Autorità Garante n. 467 dell'11 ottobre 2018, 'nell'allegato 1 recante l' *Elenco delle tipologie di trattamenti da sottoporre … a valutazione d'impatto*, sono ricompresi i trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti.