Azienda Ospedaliero Universitaria Careggi

Glossario privacy

Guida tematica all'applicazione del Regolamento UE 2016/679

Rev. 1

Sommario

Premessa normativa

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);
- 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 Regolamento ha abrogato la *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* (di seguito anche: Direttiva 95/46). Da essa erano derivati tanto la L. 31 dicembre 1996 n. 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali,* che poi il Codice stesso nelle sue versioni precedenti al D.Lgs. 10 agosto 2018, n. 101.

Si è preferita l'adozione di un Regolamento piuttosto che procedere all'aggiornamento della Direttiva in quanto un Regolamento entra direttamente in vigore nei paesi aderenti all'Unione (una Direttiva solo in casi particolari e residuali).

Ciò che ha spinto la Commissione Europea verso il superamento della *Direttiva 95/46* sono stati gli sviluppi della rivoluzione tecnologica degli ultimi decenni, 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*), scarsamente controllabili entro un orizzonte nazionale, consigliando perciò l'adozione di un atto applicabile in via diretta in tutti i Paesi UE; si è così evitato, o almeno contenuto, il proliferare di disposizioni che interpretavano ed adattavamo la norma europea secondo una prospettiva nazionale, determinandone una applicazione non omogenea.

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.

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

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.

Il Regolamento Generale, comunque, condivide con la Direttiva 95/46 molti tratti, particolari e generali, e tra questi ultimi:

- la previsione di diverse modalità di legittimazione di un soggetto (il cd. *Titolare*) 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.

Un Regolamento Europeo (così come peraltro una Direttiva) si struttura su una serie di Considerando e su un successivo articolato. Il *Manuale interistituzionale di convenzioni redazionali dell'Unione Europea* (§ 2.2) 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.

***

Linee Guida e pareri interpretativi del Regolamento sono forniti dall'European Data Protection Board (Comitato Europeo per la Protezione dei Dati, EDPB), un coordinamento, principalmente, di rappresentanti delle Autorità di controllo nazionali, costituito ai sensi degli artt. 68-76 del Regolamento, che dal 25 maggio 2018 ha sostituito il Gruppo dei Garanti ex art 29 della Direttiva 95/46/UE (appunto previsto dall'art. 29 della Direttiva 46/95 e anche richiamato come WP 29).

***

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. 101/2018:

> 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 provvedimenti già definiti 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 almeno sì, siamo certi).

***

L'art. 27 comma 1 lett. a) n. 2 del D.Lgs. 101/2018 ha abrogato l'art. 40 del Codice; e infatti, tra i compiti ed i poteri riconosciuti alle Autorità di controllo 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 ha demandato al Garante il compito di individuare, con proprio provvedimento di carattere generale le prescrizioni, contenute nelle autorizzazioni generali a suo tempo adottate, che risultassero compatibili con le disposizioni comunitarie. Tale provvedimento 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, e contiene prescrizioni relativamente al trattamento:

- di categorie particolari di dati nei rapporti di lavoro;
- di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose;
- di categorie particolari di dati da parte degli investigatori privati;
- dei dati genetici dei dati personali effettuato per scopi di ricerca scientifica.

Accesso ai documenti

Occorre anzitutto evidenziare che per la L. 241/90 l'accesso si riferisce ad atti e documenti amministrativi, vale a dire a rappresentazioni materiali che fanno parte di un procedimento amministrativo e che sono formate, con carattere di originalità, da un soggetto privato o pubblico. La protezione dei dati personali qualifica invece come documento ogni supporto che contiene dati personali, a prescindere dalla tipologia del supporto. La differenza tra atti e documenti da un lato, e dati dall'altro non potrebbe essere, concettualmente, più profonda, poiché i primi si riferiscono ad un oggetto materiale, una *res*, i secondi ad una informazione, cioè ad una rappresentazione ideale della realtà.

Da un punto di vista pratico-operativo, si deve prendere atto che la L. 241/90 definisce in effetti il "diritto di accesso" come "il diritto degli interessati di prendere visione e di estrarre copia di *documenti amministrativi*" (art. 22 comma 1 a) e che "Non sono accessibili le informazioni in possesso di una pubblica amministrazione *che non abbiano forma di documento amministrativo*, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, *in materia di accesso a dati personali da parte della persona cui i dati si riferiscono*" (art. 22 comma 4); secondo tale impostazione, del diritto di accesso ai documenti (amministrativi) si occupa la L.241/90, di quello ai dati personali (da parte del solo interessato), il *Codice*; in realtà, il *Codice* interferisce più sostanzialmente con la normativa in materia di accesso agli atti, in quanto individua condizioni e requisiti di accessibilità differenziati in relazione alle diverse tipologie di dati contenuti nel documento, o anche del soggetto cui i dati si riferiscono (es. se la persona fisica è deceduta).

Ad ogni modo, il D.Lgs. 33/2013 prevede all'art. 1 comma 1 che "La trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche" (laddove appunto la L. 241/90 all'art. 24 comma 3 prevede all'opposto che "Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni").

L'accessibilità riferita non solo ai documenti, che pure contengono ordinariamente dati personali, ma appunto direttamente a "dati e documenti" – presumendo che continui a valere il principio per cui tali dati debbano preesistere alla richiesta d'accesso (pur se non già ricompresi in un documento) e non debbano pertanto essere oggetto di elaborazione - permette di evidenziare come l'art. 22 comma 4 della L. 241/90 non sia più applicabile in via esclusiva, per cui ne risulta ulteriormente confermata la portata applicativa del *Codice* in materia, in generale, di diritto d'accesso.

In generale, i requisiti di legittimità all'accesso da parte di soggetti terzi – diversi dunque dalla persona cui i dati si riferiscono - e nel loro proprio interesse (non è insomma il caso di soggetto delegato

dall'interessato), a documenti contenenti dati personali, variano a seconda che tali dati siano o non siano dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale.

I requisiti per l'accesso a documenti contenenti dati personali esclusi quelli genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale sono i medesimi in generale previsti per l'accesso ai documenti amministrativi: in breve l'interessato deve dimostrare di avere "un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso" (L. 241/90 art. 22 comma 1 b); l'art. 59 del *Codice* prevede infatti che:

> 1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò
> che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
> 1-bis. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.

Invece, ai sensi dell'art. 60:

> Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti
> amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Tali indicazioni, qui riferite in generale ai *dati* sono ripetute dall'art. 92 comma 2 in particolare per la documentazione sanitaria (esemplificata attraverso il richiamo alla cartella clinica ed alla SDO):

> 2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o
> in parte, solo se la richiesta è giustificata dalla documentata necessità:
> a) di esercitare o difendere un diritto in sede giudiziaria, ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;

> b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

La stessa necessità di esercitare o difendere un diritto in sede giudiziaria, ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento, non è dunque sufficiente a legittimare l'accesso, laddove tale diritto non sia, anch'esso, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale. Non è perciò possibile aderire alla richiesta di accesso da parte del terzo se i dati o il documento sono utili per tutelare in giudizio un interesse legittimo o anche un diritto soggettivo non di pari rango - cioè non riconducibile alla categoria dei diritti della personalità o se non è compreso tra altri diritti o libertà fondamentali ed inviolabili - che possono essere anche di rilievo, ma che restano comunque subvalenti rispetto alla concorrente necessità di tutelare la riservatezza, la dignità e gli altri diritti e libertà fondamentali dell'interessato. Si pensi al caso dell'accesso volto a soddisfare meri diritti di credito, o anche generiche esigenze basate sulla prospettiva solo eventuale di apprestare la difesa di diritti in quel momento non ancora posti in discussione.

L'Azienda, nel valutare il "rango" del diritto di un terzo che può giustificare l'accesso, deve utilizzare come parametro di raffronto non tanto il "diritto di azione e difesa" che pure è costituzionalmente garantito (e che merita in generale protezione a prescindere dall'"importanza" del diritto sostanziale che si vuole difendere), quanto il diritto sottostante che il terzo intende far valere sulla base del materiale documentale che chiede di conoscere.

In relazione a questioni di carattere patrimoniale nell'ambito della responsabilità medica, l'Autorità Garante ha suggerito che si possa comunque valutare positivamente, con cautela, caso per caso, la possibilità di consentire *al curante* l'accesso ad una cartella clinica - prima della sua probabile acquisizione su iniziativa del giudice - in caso di controversia risarcitoria per danni ascritti all'attività professionale medica documentata nella cartella, considerando il fatto che qui l'esigenza di riservatezza appare attenuata trattandosi di medico che ha avuto in carico il paziente ed ha partecipato alla redazione della documentazione sanitaria stessa (anche per finalità medico legali, e dunque non nel solo interesse del paziente).

Rispetto alle indagini difensive ex 391 *quater* CPP, la pregressa analoga impostazione, prescritta dall'art. 71 del Codice, è venuta meno con l'abrogazione di tale articolo.

Analisi dei rischi

L'art. 32 del Regolamento, dedicato alla "Sicurezza del trattamento" prescrive che, nel valutare l'adeguato livello di sicurezza del trattamento, il titolare deve tenere conto in special modo dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, avvengano essi per causa accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Qualora dalla valutazione, nonostante le misure attivate, residui ancora un rischio elevato per la libertà e i diritti degli interessati (anche per la tipologia in sé dei dati trattati, per il contesto, per la particolare accessibilità delle informazioni) il titolare effettua, prima di avviare il trattamento, una Valutazione d'impatto sulla protezione dei dati (DPIA - Data Protection Impact Assessment).

Anonimizzazione

L'anonimizzazione è una tecnica che si applica ai dati personali al fine di ottenere una loro deidentificazione assoluta e irreversibile (in modo cioè che l'informazione perda la sua "personalità", il suo essere riferibile ad una persona fisica): assoluta, in particolare, nel senso che ciò deve essere vero in qualsiasi contesto di trattamento, per cui se in uno di tali contesti la identificazione o la reidentificazione è possibile, il dato non potrà essere considerato anonimo.

Dati anonimi (le informazioni che, fin da subito o almeno attualmente, non si riferiscono a una persona fisica identificata o identificabile) e dati anonimizzati (i dati personali elaborati in modo tale da impedire o da non consentire più l'identificazione dell'interessato) 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 locuzione del Considerando n. 26 "dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato" (che non appare, in effetti, felicissima), si intende, evidentemente, che il contenuto informativo dei dati viene progressivamente a ridursi fino ad un punto in cui la loro capacità identificativa si annulla.

Il testo inglese parla, 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).

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).

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.

Comunque, quel che, ai nostri fini, è anzitutto necessario evidenziare è che un dataset privato dell'anagrafica non reca, come secondo la nozione etimologica (*an onoma*) o di senso comune, dati anonimi: infatti, 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 (e non di una probabilità) 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.*

Per quanto di interesse, veramente chiarificatore questo passo, sempre ricompreso nel citato Parere (nella Direttiva quando si parlava di Responsabile si intendeva quello che nella sistematica del *Codice* e del Regolamento Generale è il Titolare):

> … *quando un responsabile del trattamento non cancella i dati originali (identificabili) a livello di evento, e trasmette poi parte di questo insieme di dati* (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: il requisito fondamentale affinché un insieme di informazioni, ancorché privo di una anagrafica di riferimento, non sia qualificabile come dato personale, è che la sua configurazione non possa essere (anche solo ipoteticamente, al di là delle difficoltà che ciò comporterebbe) associabile ad una analoga che sia connessa o collegabile ad un interessato, ovvero quest'ultima non possa essere individuata, ancorché oggetto di elaborazioni, come matrice dell'altra.

Insomma, un set di dati è compiutamente anonimizzato solo se non è qualificabile come un sottoinsieme diretto o univoco di un insieme di dati originali che ricomprendono o sono comunque connessi o collegabili ad informazioni di carattere identificativo.

Dunque, la copia o l'estrazione di una stringa coerente di informazioni, pur privata degli elementi direttamente identificativi, non reca dati che si possano dire anonimi laddove:

- la stringa primaria, collegata o collegabile ad elementi identificativi, resti integra (cioè non sia modificata o eliminata);
- la stringa secondaria non possa essere riferibile a più interessati (solitamente, almeno 3).

Già ad una prima lettura del parere di cui sopra, non è chi non avverta una frizione tra la anonimizzazione come equivalente, per la sua assolutezza, alla cancellazione (il dato anonimizzato, dunque, come il dato in cui ogni riferimento di carattere personale è assente, e la personalità del dato, e con essa il dato personale, è come cancellata), ed il riferimento ai mezzi che possono essere ragionevolmente utilizzati per una reidentificazione, la "ragionevolezza", con il suo carattere di soggettività, riconducendoci dall'ambito dell'assoluto a quello del relativo.

I mezzi "ragionevolmente utilizzabili per identificare un interessato" sono indicati, a livello categoriale, all'art. 4 delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica del19 dicembre 2018, per il quale:

> a) 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;

In effetti, qui il criterio della "assolutezza" parrebbe contemperarsi con elementi più disponibili, quali la "ragionevolezza" (i mezzi "ragionevoli" o "ragionevolmente utilizzabili") e la "probabilità ("un'associazione significativamente probabile …"), solitamente e preferibilmente declinate in riferimento alle "risorse economiche" e a quelle "di tempo", per le quali sono in effetti più facilmente possibili valutazioni di carattere soggettivo, e dunque meno stringenti.

Il suddetto articolo, al punto b, propone un elenco di "mezzi ragionevolmente utilizzabili per identificare un interessato":

> b) 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;…"

In realtà, quando si dice che "i mezzi ragionevolmente utilizzabili per identificare un interessato" afferiscono tra le altre, alle categorie "archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione" o "archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione", ci troviamo davanti agli elementi da noi definiti "oggettivi" sopra richiamati, in quanto parrebbe ci si limitasse a considerare il dato di fatto della loro mera esistenza, e non della loro più o meno facile accessibilità.

Possiamo trovare un bilanciamento tra tali possibili interpretazioni, sostenendo comunque che una compiuta anonimizzazione dovrebbe verificarsi dimostrando che nessun soggetto, ivi compreso quello che l'ha effettuata, sarà in grado di procedere, a partire dalle informazioni finali, e pur conoscendo le tecniche di elaborazione utilizzate, ad una reidentificazione degli interessati (non reversibilità del processo di anonimizzazione). Ciò vale anche rispetto allo stesso interessato: se questi si riconosce in un insieme di informazioni che oggettivamente (documentalmente) in effetti lo riguardano, tali per cui sarebbe

possibile recuperare una collegamento con i dati anagrafici, appare evidente che il trattamento di deintificazione effettuato su di esse non si è perfezionato.

Questo anonimato sarà dunque, più che assoluto, "oggettivo" (non soggettivo, cioè legato a particolari prerogative o contesti di trattamento), nel senso che sarà oggettivamente impossibile recuperare le informazioni di partenza, come se fossero "cancellate": non realmente, ma quantomeno dall'orizzonte informativo dei dati finali.

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 estremamente improbabile; appare possibile solo qualora le informazioni che residuano da un intervento di elaborazione 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, fatte salve situazioni di "soglia", cfr. infra la nozione di k-anonimato) tra le configurazioni originali di informazioni e quelle esito di elaborazione o selezione.

***

L'anonimizzazione è il risultato di tecniche che vengono applicate ai dati personali col fine di rendere la reidentificazione degli interessati ragionevolmente impossibile. La re-identificazione è la eventualità in cui, partendo da dati erroneamente ritenuti anonimi, si riescano a recuperare informazioni identificative degli interessati, sia direttamente, sia tramite metodi di correlazione (si parla di *correlabilità* dei dati per la possibilità di correlare almeno due dati concernenti il medesimo interessato) e deduzione (si parla di *deduzione* relativamente alla possibilità di desumere, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi). 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.

***

Relativamente alle immagini, occorre osservare che, 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 ...".

Coerentemente, 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.

E' stato osservato, in un diverso contesto, che un volto è anonimo non se è senza nome, ma se è senza tratti, con fattezze indistinte, cancellate o perdute, e che quel che ci spaventa nel teschio è anche, appunto, il suo anonimato, il suo relegarci nella specie.

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.

***

Posto che la anonimizzazione è definita come un trattamento, il quale sarà dunque, come qualsiasi altro trattamento, caratterizzato da una determinata finalità, deve perciò seguirne 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, da ciò segue che senza il consenso degli interessati il titolare non possa procedere ad anonimizzare quei dati?

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.

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/dovere del titolare.

E' stato, di conseguenza, regolarmente ritenuto che tale prerogativa fosse tuttora riconoscibile, e che pertanto il Titolare potesse, con le dovute cautele – in particolare dal punto di vista dell'accesso ai dati identificativi – procedere in generale alla anonimizzazione delle informazioni per qualsivoglia finalità lecita (non, ad esempio, per un ente pubblico, a scopi commerciali).

Vero è che la disposizione citata non chiarisce quando "le finalità perseguite nei singoli casi" siano perseguite lecitamente: pare che ci muoviamo più sul piano della modalità che della finalità del trattamento.

In accordo con una impostazione, che apre alla anonimizzazione a prescindere dal possesso di una causa di liceità (anzi, partendo proprio dal presupposto che essa è carente), è la soluzione proposta dal *Codice di condotta per l'utilizzo di dati a fini didattici e a scopi di pubblicazione scientifica* della Regione Veneto, per la quale il presupposto giuridico per perseguire tali scopi è rappresentato, in assenza di una base giuridica specifica, dal consenso dell'interessato o, in alternativa, dalla anonimizzazione dei dati.

Nella stessa direzione è orientata la previsione delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, laddove all'art. 7 comma 1 "Le particolari categorie di dati di cui all'art. 9, § 1 e i dati relativi a condanne penali e reati di cui all'art. 10, trattati per scopi statistici e scientifici devono essere di regola in forma anonima", che, al di là della resa non felice (un dato personale non può essere in forma anonima, per l'evidente contraddizione), significa semplicemente che certe tipologie di informazioni devono essere, ad una certa altezza del trattamento, anonimizzate qualora gli scopi del trattamento siano quelli statistici e scientifici.

Recentemente, però, il Provvedimento del 24 febbraio 2022 con il quale il Garante ha sanzionato alcune Regioni e Province autonome perché, per rispondere ad una richiesta del Ministero della salute, ha aggregato informazioni in suo possesso non avendo una specifica base giuridica per farlo, pare aver seguito un diverso orientamento.

Attestazioni a scopo amministrativo

Occorre mettere in atto specifiche procedure per prevenire che soggetti estranei possano facilmente evincere lo stato di salute del paziente attraverso la correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato; se la prescrizione non riguarda soltanto la documentazione, ciò comporta comunque la necessità, nel caso di richieste di certificazioni o attestazioni a scopi amministrativi e non sanitari (ad es., attestazione della presenza di un dato soggetto presso le strutture aziendali per giustificare un'assenza dal lavoro), di non evidenziare, appunto, neppure indirettamente (a mezzo di intestazioni, timbri ecc.), il reparto presso cui l'interessato è stato assistito, ed a maggior ragione, ovviamente, le prestazioni effettuate, limitandosi a certificare la sua presenza in Azienda; per garantire ciò, in breve, occorre che:

- la modulistica sia intestata all'Azienda e non al reparto;
- si eviti l'apposizione di timbri che identifichino la struttura di appartenenza;
- si eviti l'apposizione di timbri che identifichino la specializzazione dell'addetto.

Per quanto riguarda le attestazioni degli accessi degli accompagnatori, sono necessarie le seguenti considerazioni:

- l'Azienda non ha alcun titolo ad effettuare una preventiva registrazione dei soggetti che accompagnano i pazienti alle prestazioni (così come dei visitatori);
- le informazioni rispetto alle quali poter eventualmente, successivamente, valutare la veridicità di quanto certificato (o autocertificato) sono riferibili esclusivamente al paziente, con il quale l'Azienda stabilisce il rapporto fondamentale (documentandolo);
- normalmente, l'incaricato non è in grado di verificare l'effettiva continuità della presenza dei soggetti che si presentano per ottenere l'attestazione, ed il documento che va a rilasciare deve dichiarare quanto effettivamente accertato dall'incaricato;
- la normativa sulla autocertificazione legittima l'Azienda quantomeno a confermare informazioni, non dettagliate, sui pazienti di cui le venisse chiesta una verifica, senza aggiungere dati ulteriori rispetto a quelli già in possesso del richiedente (restando assolutamente escluso qualsiasi riferimento alle prestazioni effettuate ed alla struttura di erogazione);

Ovviamente, se l'incaricato è in grado di accertare la effettiva continuità della presenza dei richiedenti, di ciò potrà tranquillamente dare evidenza:

> Su istanza dell'interessato, si attesta che il sig./la sig.ra … , si è trattenuto presso questa Azienda dalle ore … alle ore … del giorno ….

In caso contrario, si propongono due soluzioni:

- attestazione riferita al paziente, redatta (con le varianti del caso) nella forma:

Su istanza dell'interessato, si attesta che il sig./la sig.ra (*Nome/Cognome del paziente*), recatosi/recatasi presso questa Azienda per poter effettuare una prestazione sanitaria, si è presentato/a al sottoscritto (o: presso questi uffici) con il sig./sig.ra (*Nome/Cognome dell'accompagnatore*), per segnalare la propria effettiva presenza, il giorno … alle ore …, e nuovamente alle ore … per ottenere la presente attestazione.

- attestazione riferita all'accompagnatore, redatta (con le varianti del caso) nella forma:

Su istanza dell'interessato, si attesta che il sig./la sig.ra (*Nome/Cognome dell'accompagnatore*), recatosi/recatasi presso questa Azienda per accompagnare un paziente alla effettuazione di una prestazione sanitaria, si è presentato/a al sottoscritto (o: presso questi uffici), per segnalare la propria effettiva presenza, il giorno … alle ore …, e nuovamente alle ore … per ottenere la presente attestazione.

Categorie particolari di dati

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 - 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 ricomprese dall'art. 9 tra le *categorie particolari di dati personali*.

Sono categorie particolari (*special categories of personal data*, dove speciali o particolari sono le categorie, non i dati, perché, in relazione alla loro sensibilità per i diritti della persona (nel Codice pre-adeguamento si chiamavano appunto 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 al par. 1 ne vieta anzi in assoluto, *prima facie* il trattamento, salvo poi indicare al par. 2 alcune finalità per le quali il trattamento è consentito. 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, o possono rappresentare elementi di controllo della persona.

In particolare, la preoccupazione del legislatore di prendere atto di rischi storicamente accertati può evidenziarsi nell'accogliere 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, e che si vorrebbe dunque non dicibile.

Tale inclusione ribadisce il fatto che finalità 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.

Si precisa che, altra cosa, comunque, è l'utilizzo di riferimenti a razza/etnia in ambito sanitario, dove il concetto di etnia è utilizzato senza alcuna implicazione di carattere biologico/razziale, per scopi meramente pratici, al fine di raggruppare alcune caratteristiche morfologico/somatiche, ricondotte a classi cui si attribuiscono i nomi delle popolazioni nelle quali più frequentemente, mediamente e non deterministicamente, si ritrovano.

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* (all'art. 10), ne segue che:

- la definizione di dato personale è incentrata sulla connessione tra dato, interessato e sua identificabilità, e dunque su cosa rende un mero dato una informazione riferita o riferibile 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;
- il concetto di dati cosiddetti *comuni* – diversi sia da quelli afferenti alle categorie particolari che da quelli relativi alle condanne penali - si appunta invece, in via residuale, sulle tipologie 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: *una substantia, tres res*).

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 pubblicate riguardanti la vita sessuale o l'orientamento sessuale del dichiarante e del suo coniuge, convivente o partner, dal nominativo di tale persona (nel caso, i nominativi sono dello stesso genere), 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, l'orientamento filosofico da una donazione, l'orientamento politico da una lista di prestiti in biblioteca. Vero è che 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 (o non 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*).

Chat

E' assolutamente vietato utilizzare strumenti social quali chat whatsapp e similari per condividere, anche tra professionisti, dati relativi alla salute. La ragione è intuitiva: si tratta di soluzioni che prevedono condizioni di servizio non contrattualizzate ed imposte unilateralmente agli utenti, che spesso si traducono nella condivisione indifferenziata (senza il necessario consenso specifico) di tutti o gran parte dei dati personali trasmessi, che insomma soddisfano senz'altro efficacemente lo scopo di socializzazione di persone e contenuti per cui sono nati; scopo evidentemente incongruo rispetto ad attività che devono essere connotate, piuttosto, da riservatezza e confidenzialità.

Consenso

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 (cioè possa no essere) oggetto di trattamento.

Il consenso, in quanto "manifestazione di volontà", deve appunto manifestarsi, cioè esternarsi e dimostrarsi mediante un atto positivo inequivocabile, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. E' un "atto positivo" anche 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 un particolare 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 prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre e in forma comprensibile, utilizzando un linguaggio semplice e conciso, con modalità 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.

Consenso a fasi progressive

I requisiti del consenso, ed in particolare la sua specificità - il Garante parla di "granularità" del consenso - comportano ordinariamente che il consenso prestato circa un determinato trattamento non legittimi ulteriori trattamenti ad esso conseguenti o comunque connessi: ad es. il consenso per la raccolta dei dati in un cd. "registro di patologia" non legittima di per sé gli studi che in riferimento ai dati raccolti nel registro possono essere effettuati.

In effetti, il considerando 50 del Regolamento offre una apertura circa la possibilità di svolgere ulteriori trattamenti sul presupposto di liceità del trattamento originario. Si richiede, in particolare, che il titolare possa verificare, in concreto, che la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti e che la base giuridica del primo trattamento possa supportare anche eventuali trattamenti ulteriori; tale secondo presupposto, nel caso di dati raccolti per finalità di ricerca utilizzati per ulteriori ricerche parrebbe senz'altro soddisfatto.

L'elemento della "specificità" orienta il Garante a considerare invece soprattutto il considerando 33 del Regolamento, per il quale:

> In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista.

Il Garante parla, rispetto a tale fattispecie, di "consenso a fasi progressive". Il fatto è che il Garante ritiene che una finalità di ricerca non sia invocabile se generica (quand'anche riferita a macro aree di ricerca), e che, in accordo con le Linee guida 5/2020 sul consenso del Board europeo, per "ricerca scientifica" in questo contesto debba sempre intendersi "un progetto di ricerca istituito in conformità con le pertinenti norme metodologiche e deontologiche settoriali, in linea con le buone prassi", e che in tale settore lo scopo del trattamento debba sempre essere individuato nello specifico progetto di ricerca che si intende realizzare. Anche le citate Regole deontologiche sulla ricerca (art. 3) prevedono espressamente che la ricerca deve essere effettuata sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare, esitando dunque in un protocollo di ricerca. Insomma, una finalità di ricerca (una ricerca) esiste solo se strutturata in un progetto di ricerca, documentato in un protocollo di ricerca, che verrà sottoposto al Comitato etico territorialmente competente per l'acquisizione del previsto parere. La finalità determinata e specifica del trattamento verrà dunque individuata, appunto, a fasi progressive, completandosi solo all'esito dell'approvazione dei futuri progetti (protocolli) di ricerca.

Consenso e finalità di cura

Il consenso non è più base giuridica ordinaria per poter procedere a trattare dati personali per finalità di cura, essendo il trattamento per tale scopo già di per sé legittimo quando è, ai sensi dell'art. 9 parr. 2 h e 3 del Regolamento Generale, *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, per scopi di cura, si prescinde dunque, in linea di massima dal consenso dell'interessato, ed infatti l'art. 76 comma 1 lettera a) del *Codice,* che lo prevedeva in via ordinaria, è stato abrogato. Il superamento di tale obbligo sconta due condizioni.

Anzitutto, l'art. 9 parr. 2 h e 3 del Regolamento Generale assicura una copertura sufficiente ed autonoma al trattamento per finalità di cura solo qualora tale trattamento, o la modalità in cui è effettuato, possano essere valutati *necessari*, ovvero *indispensabili* per quello scopo: ad es. il trattamento effettuato mediante una app sanitaria, o un dossier sanitario non saranno qualificati come necessari (e dovranno integrare la base giuridica della cura con quella rappresentata dal consenso dell'interessato.

In secondo luogo, ai sensi dell'art. 9 comma 4 del Regolamento Generale, relativamente ai dati genetici o dati relativi alla salute resta la possibilità per i legislatori nazionali di mantenere o introdurre ulteriori condizioni, comprese limitazioni, sulla base delle quali consentire il trattamento; un obbligo di consenso, dunque, potrebbe essere successivamente reintrodotto. L'art. 2 septies del Codice, ad oggi, si limita a prevedere 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) Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale...".

Le *condizioni* cui ci si riferisce sono le condizioni di liceità del trattamento, le sue basi giuridiche: ad esempio il consenso, la finalità di cura, le finalità di rilevante interesse pubblico ecc.; la *limitazione* richiamata, relativamente ai dati relativi alla salute trattati per finalità di cura (esclusi i dati genetici), pare riguardare solo le "*misure di garanzia disposte dal Garante*", poiché il comma 6 secondo periodo del medesimo articolo prevede la possibilità di reintrodurre il consenso solo per il trattamento di questi:

> 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.

Preso atto che non è pertanto prevista una generale reintroduzione del consenso in riferimento ai dati relativi alla salute trattati per finalità di cura, se non quando il trattamento ricomprenda i dati genetici, occorre osservare che il Garante non ha disposto, relativamente a questi ultimi, nessun obbligo particolare, per cui il consenso, ad oggi, non è necessario per nessuna tipologia di dati, compresi quelli genetici (fatto salvo il caso della comunicazione di questi ultimi a soggetti terzi).

Consultazione preventiva

All'esito di una DPIA, il titolare potrà decidere in autonomia se iniziare il trattamento ovvero, qualora la valutazione indichi un rischio residuo elevato ove non siano attivate ulteriori azioni correttive, consultare l'autorità di controllo prima dell'inizio del trattamento per ottenere indicazioni su come gestire il rischio residuale.

Si parla allora (art. 36 del Regolamento) di Consultazione preventiva (Prior consultation).

L'autorità – che risponderà entro otto settimane, prorogabili di ulteriori sei settimane per trattamenti particolarmente complessi - avrà il compito 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).

La Consultazione preventiva è ordinariamente un processo che il Titolare attiva volontariamente, sulla base delle proprie valutazioni, nell'ottica della accountability.

Il diritto degli stati membri può, comunque, sempre prescrivere, nell'ambito di un compito di interesse pubblico, che il titolare consulti obbligatoriamente l'autorità di controllo e ne ottenga la autorizzazione al trattamento.

Contitolarità

La contitolarità, ai sensi dell'art. 26 Regolamento Generale, è la situazione nella quale due o più titolari del trattamento (contitolari: *joint controller*) 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), e la stessa base giuridica (se il trattamento condiviso vuol avere i crismi della liceità), 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.

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.

Sono dunque indizio di una situazione di contitolarità del trattamento:

- una decisione congiunta da parte di due o più soggetti sullo scopo e le modalità del trattamento;
- decisioni convergenti da parte di due o più soggetti sullo scopo e le modalità del trattamento, qualora 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;
- il fatto che le parti perseguono 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 la specificazione "mediante un accordo interno" 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 (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.

La contitolarità si dispiega lecitamente quando i vari soggetti contitolari condividono la medesima base giuridica del trattamento. Ciò significa che 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), ma che non potrebbero esercitarla lecitamente in autonomia, i quali dovranno allora essere individuati quali responsabili del trattamento.

Quanto sopra significa anche che, se si comunicano dati ad un diverso soggetto in riferimento ad una base giuridica – che potrebbe essere il consenso – e questo soggetto intende condividere tali dati con altri soggetti con i quali si trova in una situazione di contitolarità, le informazioni che precedono il consenso devono prevedere tale situazione, così che la base giuridica legittimi la comunicazione dei dati anche a tali altri soggetti.

Significa anche che non sarebbe possibile che la situazione di contitolarità si definisse successivamente alla comunicazione dei dati a quel soggetto. Si suggerisce che, quando si intendono comunicare dati a più soggetti che operano in contitolarità, la liceità di tale comunicazione sia valutata come se ciascuno di essi si trovasse in una condizione di autonoma titolarità.

La contitolarità del trattamento parrebbe non determinare un superamento, nella trasmissione delle informazioni tra i contitolari, di una operazione di *comunicazione* dei dati (come accade invece nel rapporto titolare/responsabile); la nozione di comunicazione di dati personali resa dall'art. 2-ter comma 4 lettera

a) del Codice ("il dare conoscenza dei dati personali a uno o più soggetti determinati …") esclude infatti che essa si attui soltanto qualora i dati siano posti a conoscenza dell'interessato, del responsabile, delle persone autorizzate al trattamento. Così come l'atto di cui all'art. 28 par. 3 del Regolamento legittima il responsabile a trattare i dati per conto del titolare – ma in quel caso il titolare è uno, e non si ha comunicazione del dato - si potrà sostenere che tale comunicazione è legittimata dall'art. 26 del Regolamento.

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* (si tratta della buona fede in senso oggettivo, ovvero quel principio che impone ad una parte di salvaguardare la ragionevole 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 – *by default* - le buone pratiche della sicurezza.

Creazione di banche dati

Si ricorda anzitutto 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 Titolare e autorizzati (dall'Azienda) dal punto di vista della propria complessiva responsabilizzazione nonché del rispetto dei principi che la assicurano: limitazione della finalità, base giuridica, minimizzazione dei dati, sicurezza (ivi compresa l'accessibilità), esattezza, integrità.

Uno specifico trattamento è qualificato non solo dalla sua finalità, ma anche dalle modalità (i mezzi del trattamento) con cui tale finalità è perseguita: la loro modifica o alterazione rispetto a quelle definite dal Titolare determinano l'attivazione di un trattamento diverso, la cui adeguatezza dovrà essere valutata ex novo dal Titolare stesso. Esempio: si sono raccolti dati personali per scopo di cura, archiviati su un applicativo aziendale, secondo modalità che (si dà per acquisito) il Titolare ha valutato adeguate dal punto di vista della protezione dei dati personali; si intendono estrarre ed utilizzare questi dati, sempre per finalità di cura, creando una ulteriore banca dati di più facile accesso: la finalità è la medesima, ma i nuovi mezzi che si utilizzano sono tali da modificare – anche solo dal punto di vista della sicurezza – il trattamento effettuato con la banca dati originaria: si realizza dunque un diverso trattamento che deve essere esaminato ed autorizzato dal Titolare. Va da sé che analoga valutazione è ancor più necessaria quando i dati raccolti per la finalità primaria sono estratti dall'applicativo aziendale ed archiviati per una finalità diversa, ulteriore, venendo in tal caso in causa anche la questione della base giuridica (la condizione di liceità, cioè i presupposti normativi che la legittimano) di tale nuovo trattamento

Se tale autorizzazione è assente, una banca dati creata ex novo deve ritenersi per ciò stesso, dal punto di vista della protezione dei dati personali, illecita, esponendo chi la crea o utilizza a responsabilità personale.

Un frequente equivoco è quello per cui un medico che opera (a qualunque titolo: dipendenza, collaborazione, afferenza) a favore dell'Azienda, presume trattare i dati dei pazienti in base a proprie prerogative: i requisiti che ne sostanziano la professionalità rappresentano in realtà, in questo contesto, un presupposto per il trattamento piuttosto che una legittimazione autonoma al trattamento. Il medico deriva una legittimazione al trattamento – quale, appunto, *persona autorizzata* (dal Titolare) *al trattamento* - dall'Azienda, Titolare del trattamento: legittimazione che si conserva se si perseguono le finalità che a questa sono attribuite, secondo le modalità e i mezzi (anche da intendersi come: gli strumenti, ad es. i sistemi informatici) da questa valutati ed adottati: se si opera, cioè, sotto l'autorità e secondo le istruzioni del Titolare.

Come qualificare, tra i soggetti che trattano dati personali, la persona fisica che si sottrae all'autorità del Titolare e tratta dati secondo proprie finalità e/o modalità?

Ora, il Titolare è il soggetto (persone fisica, giuridica ecc.) che, di fatto (potrà farlo più o meno lecitamente) tratta dati per una propria finalità e/o secondo modalità da esso stesso determinate; è il Titolare che, nell'ottica della responsabilizzazione, risponde per un trattamento da esso o per esso effettuato non adeguatamente. Se sistema aziendale subirà un accesso illecito o una sottrazione di dati, ne sarà dunque responsabile il Titolare del trattamento, appunto l'Azienda. Qualora però un dipendente/collaboratore tratti quei dati per propri scopi personali o comunque mediante modalità o mezzi diversi da quelli messi a disposizione del Titolare, assumerà esso stesso un ruolo di Titolare (di fatto), accollandosi in proprio, direttamente, tutte le conseguenti responsabilità (e correlate sanzioni). Se dunque una banca dati autonomamente costituita subirà un accesso illecito o una sottrazione di dati, ne sarà responsabile non l'Azienda, ma la persona fisica che l'ha realizzata.

Dati genetici

I dati genetici, secondo la definizione offerta dall'art. 4 13 del Regolamento, sono dati personali:

- relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica
- che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica
- che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Essi trovano adesso collocazione tra le categorie particolari di dati; giustamente, la definizione, pur mantenendo una autonomia del concetto, ricorda che il dato genetico può essere interpretato anche come un dato relativo alla salute ed essere trattato per finalità sanitarie.

Ai sensi dell'art. 9 parr. 2 h e 3 del Regolamento Generale, per i trattamenti di dati finalizzati alla cura si prescinde, in linea di massima, dal consenso dell'interessato. 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. L'art. 2 septies del Codice, ad oggi, si limita a prevedere 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) Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale...".

Il comma 6 secondo periodo del medesimo articolo prevede la possibilità di reintrodurre, attraverso le suddette Misure di garanzia, il consenso per il trattamento dei dati genetici. Preso atto che non è pertanto prevista una generale reintroduzione del consenso in riferimento ai dati relativi alla salute trattati per finalità di cura, se non quando il trattamento ricomprenda i dati genetici, occorre osservare che il Garante non ha ad oggi disposto, relativamente a questi ultimi, nessun obbligo particolare, per cui il consenso, ad oggi, non è necessario per nessuna tipologia di dati, compresi quelli genetici (fatte salve le eccezioni sotto specificate).

Non vi è dunque, in via generale, alcun obbligo di consenso per trattare i dati genetici per l'esecuzione della prestazione. A seconda della tipologia di esame, può però essere necessario informare l'interessato sulle seguenti due situazioni:

- i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici;
- la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di tali dati per ulteriori scopi.

Se nel primo caso si tratta solo di una integrazione informativa, nel secondo caso viene ovviamente in causa l'acquisizione di una specifica (ripeto specifica, non per il trattamento in generale) manifestazione di volontà dell'interessato.

I dati genetici, secondo la definizione offerta dall'art. 4 13 del Regolamento, sono dati personali:

- relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica
- che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica
- che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Essi trovano adesso collocazione tra le categorie particolari di dati; giustamente, la definizione, pur mantenendo una autonomia del concetto, ricorda che il dato genetico può essere interpretato anche come un dato relativo alla salute ed essere trattato per finalità sanitarie.

I dati genetici sono dati che hanno un valore costitutivo della sfera intima tendenzialmente più forte di ogni altra tipologia di dato personale (tanto che certa dottrina li qualificava come dati *supersensibili*) e che inoltre, caratteristicamente, si collocano tanto oltre la sfera giuridica di un soggetto, coinvolgendo quella del gruppo parentale, come anche al di là di un dato ambito temporale. Si tratta infatti di informazioni:

- che identificano l'individuo in maniera univoca;
- non modificabili (che lo identificano dunque stabilmente);
- con la peculiare caratteristica di porre un soggetto in relazione con altri soggetti, con un gruppo parentale, così che gli effetti di un trattamento si estendono necessariamente dalla sfera personale di un individuo a quella del gruppo (famiglia, razza) di appartenenza;
- dotate, in riferimento tanto all'individuo che ai soggetti geneticamente collegati, di natura predittiva.

E' stato addirittura affermato che, in riferimento al trattamento dei dati genetici, sia emerso un nuovo gruppo sociale, giuridicamente rilevante, ossia il gruppo biologico, il gruppo di consanguinei, non coincidente, in termini tecnici, a quello della famiglia. Questo gruppo non comprende infatti familiari

come il coniuge o i figli adottivi o agli affini, ma altri soggetti che non fanno parte della cerchia familiare, in termini giuridici o di fatto, come i donatori di gameti o la donna che non ha riconosciuto il figlio al momento della nascita e ha chiesto di non rivelare la sua identità.

In effetti, riportare il dato genetico, come caratteristicamente riferibile ad una pluralità di soggetti, alla nozione di dato personale, univocamente riferita ad una (sola) persona fisica, non è cosa immediata.

In questo contesto ci si può chiedere se i dati genetici appartengano esclusivamente all'individuo presso cui sono stati raccolti o se i soggetti appartenenti alla medesima linea genetica dell'interessato abbiano il diritto di accedere ai dati anche senza il consenso di quella persona. Nella misura in cui i dati genetici hanno una dimensione familiare, si potrebbe infatti sostenere che si tratta di informazioni "condivise" e che i familiari hanno il diritto ad avere informazioni che possono avere ripercussioni sulla loro salute e vita futura.

Si possono immaginare almeno due scenari. Il primo è che anche gli altri soggetti appartenenti alla medesima linea genetica dell'interessato possono essere direttamente considerati "persone interessate" con tutti i diritti che ne derivano. Un altro è che essi hanno un diritto ad essere informati di tipo diverso, basato sul fatto che i loro interessi personali possono essere direttamente coinvolti.

Le Prescrizioni, così come a suo tempo il Codice, hanno optato per la seconda soluzione, individuando i soggetti appartenenti alla medesima linea genetica dell'interessato come soggetti terzi ma senza richiamare se non obliquamente il cd. *principio dei diritti di pari rango* (principio di carattere generale che richiedeva una valutazione di accessibilità effettuata caso per caso).

Al § 4.6 delle Prescrizioni, dedicato in generale a *Comunicazione e diffusione dei dati*, è previsto che

> I dati genetici devono essere resi noti, di regola, direttamente all'interessato o a persone diverse dal diretto interessato solo sulla base di una delega scritta di quest'ultimo, adottando ogni mezzo idoneo a prevenire la conoscenza non autorizzata da parte di soggetti anche compresenti. La comunicazione nelle mani di un delegato dell'interessato è eseguita in plico chiuso".

In questo caso, ovviamente, siamo sempre nell'ambito del trattamento di dati nell'interesse della persona cui i dati si riferiscono, non di terzi; la *persona diversa dall'interessato* interviene solo in qualità di messo, a seguito di specifica delega da parte dell'interessato.

Il § 4.7 è invece dedicato alla *Tutela della salute di un soggetto terzo*; esso recita:

> Ferme restando le specifiche condizioni in ambito sanitario previste dall'art. 75 del Codice, il trattamento di dati genetici per finalità di tutela della salute di un soggetto terzo può essere effettuato se questi appartiene alla medesima linea genetica dell'interessato e con il consenso di quest'ultimo.

> Nel caso in cui il consenso dell'interessato non sia prestato o non possa essere prestato per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere, nonché per effettiva irreperibilità, il trattamento può essere effettuato limitatamente ai dati genetici disponibili qualora sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole o sia giustificato dalla necessità, per il terzo, di interventi di natura preventiva o terapeutica. Nel caso in cui l'interessato sia deceduto, il trattamento può comprendere anche dati genetici estrapolati dall'analisi dei campioni biologici della persona deceduta, sempre che sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole o sia giustificato dalla necessità, per il terzo, di interventi di natura preventiva o terapeutica (cons. 27, Regolamento UE 2016/679).

Dunque: le condizioni ordinarie affinché un terzo possa accedere ai dati genetici dell'interessato per finalità di tutela della propria salute sono le seguenti:

- il terzo deve appartenere alla medesima linea genetica dell'interessato;
- l'interessato deve prestare un consenso alla comunicazione.

Qualora non siano compresenti ambedue tali condizioni, la comunicazione di dati non può essere effettuata (fatto salvo quanto specificato *infra*).

Si tratta della applicazione di un principio di carattere generale, secondo il quale, se non sono presenti altre cause di liceità, e nulla osta al ricorrervi, la acquisizione del consenso dell'interessato, ai sensi dell'art. 9 par. 2 lettera a) del Regolamento, può essere idonea base giuridica per legittimare la comunicazione dei dati ad altri soggetti diversi dall'interessato, nel loro specifico interesse.

Il riferimento all'art. 75 del D.Lgs. 196/2003 deve intendersi come segue: in ambito sanitario, il professionista può sempre accedere ad informazioni riguardanti un paziente per la cura di un altro paziente che presenta analoga casistica; ciò non si traduce in una comunicazione di dati ai soggetti appartenenti alla medesima linea genetica dell'interessato, ma appunto nell'accesso del professionista, prescindendo da qualsiasi autorizzazione dell'interessato, ai dati che lo riguardano qualora necessari per la tutela della salute di un diverso soggetto.

Il secondo paragrafo del § 4.7 delle Prescrizioni introduce il caso per il quale il consenso dell'interessato non sia prestato o non possa essere stato prestato per:

- impossibilità fisica,
- incapacità di agire
- incapacità d'intendere o di volere,
- per effettiva irreperibilità.

In tal caso, il trattamento può essere effettuato limitatamente ai dati genetici disponibili, ma solo qualora:

- sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole
- sia giustificato dalla necessità, per il terzo, di interventi di natura preventiva o terapeutica.

Si tratta a ben vedere, in riferimento a tali soggetti non utilmente contattabili, di una specificazione dell'art. 9 par. 2 lettera c) del Regolamento, per il quale è lecito il trattamento necessario per tutelare un interesse vitale di una persona fisica diversa dall'interessato qualora l'interessato si trova nell'incapacità fisica o giuridica (in questa si ricomprende evidentemente la "effettiva irreperibilità") di prestare il proprio consenso.

Diversa considerazione occorre fare relativamente al caso in cui "il consenso non sia prestato", nel senso evidentemente di un dissenso espresso (altrimenti, anche qualora la richiesta all'interessato non fosse stata posta, occorrerebbe ricontattarlo, e se non è possibile si rientrerebbe nell'altra fattispecie).

Qui si tratta piuttosto della applicazione del principio dei diritti di pari rango declinato, relativamente alla documentazione sanitaria, dall'art. 92 comma 2 lettera b) del Codice:

> 2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:
> …
> b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ((...)).

In questi casi, la situazione "giuridicamente rilevante di rango pari a quella dell'interessato", è appunto rappresentata dal diritto del terzo di poter compiere una scelta riproduttiva consapevole o di poter effettuare interventi di natura preventiva o terapeutica.

Nel caso in cui l'interessato sia deceduto, il trattamento, sempre per le finalità suddette, può ricomprendere anche dati genetici che vengano successivamente estrapolati dall'analisi dei campioni biologici della persona deceduta (quindi non solo i dati attualmente "disponibili"), sempre e solo per gli scopi sopra richiamati (scelta riproduttiva consapevole o interventi di natura preventiva o terapeutica). In questo caso è esplicito il richiamo al Considerando 27 del Regolamento, secondo il quale

> Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.

In questo caso è ribadito che la normativa nazionale prevede una tutela anche delle persone decedute, ma che questa è meno stringente (per cui appunto l'accesso non si limita ai dati già disponibili, ma anche a quelli che è possibile estrapolare successivamente dall'analisi dei campioni biologici della persona deceduta).

Da quanto sopra esaminato, trovandosi sempre in una situazione per la quale dover rispondere a richieste di soggetti (interessato, terzo) portatori di propri interessi, appare evidente che all'ente che detiene i dati non è imputabile l'obbligo di farsi parte attiva per individuare i soggetti potenzialmente interessati dalle informazioni detenute per effettuare una comunicazione nel loro interesse.

Dati relativi alla salute

Premetto, considerata l'importanza, per una Azienda sanitaria, dei dati relativi alla salute, che ci interessa acquisirne una definizione non solo formalmente e astrattamente corretta, ma ragionevole, applicabile e funzionale allo scopo (ovvero alla finalità di protezione e tutela). 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, anche se non esclusivamente, consequenziale (ritenendo intellettualmente onesta quella definizione che contemperi correttezza analitica e consapevolezza delle sue concrete applicazioni). Insomma, il tenore della definizione deve soddisfare criteri di esattezza e sostenibilità, ma anche essere tale da non comportare conseguenze irragionevoli.

Ritengo che la prova del nove della ragionevolezza della definizione del dato relativo alla salute sia offerta 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. Esemplificando; 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, anche di salute, e pur 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 quelle informazioni sono dati relativi alla salute o no non in assoluto, ma a seconda dell'ambito o dello scopo del trattamento. Ciò non contraddice il principio di assolutezza del dato personale, perché qui non si tratta di discutere della eventuale personalità del dato, ma della sua capacità informativa, e del contesto in cui essa può essere tipicamente apprezzata.

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; 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:

  > 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, "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 un tampone 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.

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.

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:

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 regolare) 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. Lo stesso, se il disabile venisse ripreso mentre segue un percorso di riabilitazione in Unità Spinale.

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, es. per le dipendenze da alcool o da fumo), 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).

***

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, 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.

Dato anonimo

Vi sono tipologie di dati che non rientrano nell'ambito di applicazione del Regolamento Generale: sono i dati anonimi, che appunto non sono dati personali.

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. 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 (fatte salve le tecniche di aggregazione). Si deve dunque ammettere che la sopra richiamata condizione di avere un abito nero può essere considerata un dato personale anche 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* in qualsiasi contesto di utilizzo, non solo nel senso della identificazione ma anche della identificabilità; 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 tali casi e situazioni, infatti, saranno probabilmente, numerose le persone fisiche alle quali tale informazione potrà correlarsi, così che essa perderebbe valore identificativo: sempre che, ad esempio, quell'uomo con l'abito scuro non fosse stato continuativamente videoripreso, nei suoi spostamenti, o magari ci trovassimo in agosto e l'abito nero fosse un cappotto.

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: una informazione è qualificabile come dato personale se è costituita da o connessa 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, può restare 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, nel diverso contesto, 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*.

I cd. dati sintetici sono esito di anonimizzazione nella misura in cui aggregano dati preesistenti, sono dati nativamente anonimi se vengono prodotti sulla base di criteri predefiniti e sono indipendenti da dati originari.

Dato 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 fattura, all'acquisto di un libro, ha significato e qualificazione diversi rispetto alla medesima anagrafica associata ad una fattura relativa ad una prestazione sanitaria (e, nel primo caso, avremo ordinariamente un documento che reca dati comuni, nel secondo un documento – della stessa tipologia, una fattura – che reca dati relativi alla salute);
- un insieme di dati relativi alla salute può avere un significato diverso, se associato ad altri dati relativi alla salute riferiti allo stesso interessato (sono sempre dati relativi alla salute, ma si modifica il loro contenuto informativo dal punto di vista clinico).

Una informazione di carattere personale potrà anche avere significati diversi per i diversi titolari che lo utilizzano (magari per finalità differenti) o per l'interessato: l'informazione sull'acquisto di un testo di carattere politico potrà essere diversamente interpretata ed utilizzata dal venditore, dall'interessato o dalla DIGOS.

Saranno poi coessenziali 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, in generale 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, adesso ma anche successivamente, cioè a seguito del collegamento con altri dati, non solo quelli al momento disponibili, ma anche quegli altri prospetticamente accessibili.

La nozione di dato personale non può essere apprezzata solo dal punto di vista della sua correttezza logico formale, e dunque staticamente; essa è funzionale ad uno scopo di protezione, e viene dunque conformata dalla prospettiva del rischio e della necessità di prevenirlo o attenuarlo. 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 (il rischio) 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 (l'interessato, appunto) cui si riferisce.

Per essere qualificata come personale, una informazione deve comunque avere i caratteri dell'oggettività: non nel senso di dover essere una verità obiettiva e stabile, cioè statica e non modificabile, ma in quello che non può consistere in un sapere meramente soggettivo, intimo e non espresso, di colui che effettua il trattamento. Rientra certo nella definizione anche qualsiasi informazione o elemento che abbia un'efficacia informativa tale da fornire un contributo di conoscenza rispetto ad un soggetto identificato o identificabile e dunque anche i giudizi, le analisi e le valutazioni di tipo soggettivo (ad es. il parere sulla capacità professionale di un dipendente), purché in qualche modo, appunto, oggettivati (ad es. in un documento, ma non soltanto: anche in una testimonianza, una dichiarazione ecc.); tali *dati di tipo valutativo* sono dunque considerati dati personali (ma avranno un peculiare regime di accesso, in particolare non possono essere oggetto di pretese di rettificazione o integrazione); sono tra l'altro dati che, in specifici contesti, possono essere anche qualificati come dati particolari (es. dati di valutazione clinica relativa a diagnosi o prognosi, giudizi sui comportamenti del pazienti riportati nell'anamnesi, perizie redatte dal medico legale ecc.).

Il dato personale è 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 esse 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 (considerate e giuridicamente qualificate) *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", che ha una relazione più o meno stabile e personale con i dati. Non è comunque proprietario dei dati che lo riguardano.

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.

Il dato personale è dunque quel dato che ha, 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 distinguere, e poi magari 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 e 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 identificabilità come riconoscibilità, che può essere propedeutica ad una possibile identificazione nominativa dell'interessato ma che non è necessario si risolva in questa: il bullismo on line o il revenge porn funzionano benissimo, nei loro effetti, senza necessità di spendere il nome delle persone riprese; posso riconoscervi una persona nota anche se non ne conosco il nome. 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 valutata in riferimento alla possibilità e probabilità che possano determinarsi su di essa, attraverso tale riconoscibilità, effetti concreti.

Riteniamo dunque, in via generale, che la nozione di dato personale ricomprenda la riferibilità di una informazione ad una persona fisica *identificabile*, intesa come la persona fisica che "può essere identificata", non nel senso che questa possibilità debba risolversi poi in una effettiva identificazione – e solo allora il dato sarebbe personale - ma perché gli effetti del trattamento su di essa potrebbero già aversi a questo primo livello informativo.

La definizione di dato personale offerta dal Regolamento Generale ricomprende infatti, 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).

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").

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 *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: il dato personale, infatti, si qualifica sempre quale un sistema, un coordinamento di informazioni entro un dato contesto.

Posto che, in astratto, qualunque soggetto è identificabile nel proprio 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

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 (fatto salvo quanto sopra osservato circa la possibilità che tali informazioni possano comunque avere un effetto su una persona fisica).

Diciamo che, in generale, occorre applicare un principio di precauzione, ma sempre con ragionevolezza, assumendosi, al solito, la responsabilità (non solo giuridica, ma anche etica) di una equilibrata valutazione.

Documento

Le *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101*, adottate dal Garante per la protezione dei dati personali il 19 dicembre 2018, propongono la definizione di documento come "qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali".

Dossier sanitario

Che cos'è?

Il Dossier sanitario, come descritto nelle Linee Guida del Garante per la protezione dei dati personali del 4 giugno 2015 (in particolare v. Allegato A), rappresenta uno strumento di ausilio nei processi di diagnosi e cura dei pazienti poiché garantirebbe la predisposizione di un sistema informativo in grado di gestire potenzialmente l'intera storia clinica di un individuo.

Si può quindi rappresentare il dossier sanitario come l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato (paziente), che vengono condivisi tra i professionisti sanitari che lo assistono presso un'unica struttura sanitaria (differentemente dal Fascicolo Sanitario Elettronico che consente la raccolta di dati e informazioni sanitarie che costituiscono la storia clinica e di salute dell'interessato ed è alimentato dai soggetti che lo prendono in cura nell'ambito del Servizio Sanitario Regionale).

È importante evidenziare come il Dossier sanitario sia uno strumento informativo *incompleto* in due sensi: anzitutto in quanto "include solo le informazioni cliniche derivanti dagli accessi del paziente nella struttura sanitaria che utilizza il Dossier e non anche quelle relative agli accessi effettuati presso altre strutture pubbliche e private"; in secondo luogo perché sugli stessi dati che il Titolare potrebbe rendere accessibili attraverso il Dossier, l'interessato può intervenire rendendo disponibili solo alcune informazioni e non altre.

Il dossier sanitario, dunque, è un sistema integrato di dati che ha lo scopo di mettere a disposizione dei medici e dei professionisti sanitari che hanno in cura un assistito, nella sua più ampia configurazione, tutti i dati e i documenti relativi al suo stato di salute in possesso dell'Azienda. Questo consente ai soggetti autorizzati, formati e istruiti, di aver una migliore e più accurata evidenza della storia clinica del paziente per garantire una migliore prestazione e assistenza medica.

Il trattamento dei dati sanitari effettuato tramite il dossier costituisce, pertanto, un trattamento ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso.

In assenza del dossier sanitario, infatti, il professionista avrebbe accesso alle sole informazioni fornite in quel momento dal paziente e a quelle elaborate in relazione all'evento clinico per il quale lo stesso ha richiesto una prestazione sanitaria; attraverso l'uso del dossier sanitario, invece, il professionista pone in essere un ulteriore trattamento di dati sanitari mediante la consultazione delle informazioni elaborate nell'ambito dell'intera struttura sanitaria e non solo del suo reparto e, quindi, da professionisti diversi, in occasione di altri eventi clinici occorsi in passato all'interessato che siano riferibili anche a patologie differenti rispetto all'evento clinico in relazione al quale l'interessato riceve la prestazione sanitaria.

Quali sono le finalità del dossier sanitario?

L'obiettivo è quello di garantire una migliore diagnosi, assistenza e cura attraverso un sistema integrato di informazioni circa lo stato di salute del paziente.

Ciascuna delle Strutture Aziendali dispone singolarmente della tecnologia digitale indispensabile alla gestione ed archiviazione dei dati sanitari: immagini radiografiche, tracciati, referti ed ogni altra tipologia di informazione sanitaria; tuttavia, nel pieno rispetto della Riservatezza, ogni struttura aziendale può consultare esclusivamente le informazioni sanitarie prodotte e prescritte all'interno della struttura stessa.

All'interno del Dossier Sanitario, una volta costituito previo consenso del paziente, potranno confluiranno tutte le informazioni sanitarie che lo riguardano e che sono state acquisite ed elaborate all'interno dell'Azienda e ove le stesse siano prodotte in un formato compatibile.

Come chiarito dalle Linee Guida in materia di Dossier Sanitario adottate con deliberazione del Garante per la protezione dei dati personali del 4 giugno 2015, il Dossier Sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, rappresenta un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal Professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico e si configura, quindi, come trattamento facoltativo.

Per quanto appena evidenziato e per migliorare i processi di cura, è necessario che il paziente fornisca uno specifico consenso alla costituzione del Dossier. Un ulteriore consenso sarà chiesto anche per inserire gli eventi clinici pregressi. In assenza del consenso, invece, il professionista che prenderà in cura il paziente avrà a disposizione solo le informazioni rese in quel momento.

Il rifiuto a prestare il consenso al trattamento dei dati personali mediante il Dossier sanitario, comunque, NON inciderà sulla possibilità di accedere alle cure mediche richieste.

È importante evidenziare che i dossier sanitari non certificano lo stato di salute dei pazienti, in quanto consistono in strumenti che possono aiutare il clinico ad inquadrare meglio e più rapidamente lo stato di salute di questi, nel rispetto del diritto dovere del medico di effettuare gli accertamenti che riterrà -anche deontologicamente- più opportuni.

L'informativa all'interessato

L'obbligo di informare l'interessato in via preventiva rispetto al trattamento dei dati personali trova piena applicazione anche in relazione al Dossier Sanitario.

In particolare, nell'informativa al dossier deve essere evidenziata l'intenzione del titolare del trattamento di costituire un insieme di informazioni personali riguardanti l'interessato il più possibile completo che documenti parte della storia sanitaria dello stesso al fine di migliorare il suo processo di cura attraverso un accesso integrato di tali informazioni da parte del personale sanitario coinvolto.

L'interessato deve essere informato inoltre che l'eventuale mancato consenso al trattamento dei dati personali mediante il dossier sanitario non incide sulla possibilità di accedere alle cure mediche richieste.

Deve essere resa nota all'interessato anche la circostanza che, qualora acconsenta al trattamento dei suoi dati personali mediante il dossier sanitario, questo potrà essere consultato anche qualora ciò sia ritenuto indispensabile per la salvaguardia della salute di un terzo o della collettività.

L'informativa al dossier è resa dal titolare del trattamento con riferimento al trattamento effettuato da parte dei professionisti e dei reparti o unità interne che prenderanno in cura l'interessato.

Nell'informativa è necessario, inoltre, che sia specificata l'eventualità che il dossier sanitario sia consultabile anche da parte dei professionisti che agiscono in libera professione intramuraria -detta anche intramoenia- ovvero nell'erogazione di prestazioni al di fuori del normale orario di lavoro utilizzando le strutture ambulatoriali e diagnostiche della struttura sanitaria a fronte del pagamento da parte del paziente di una tariffa.

Al fine di informare adeguatamente l'interessato in relazione, in particolare, delle opportunità correlate all'istituzione e alla implementazione del dossier è necessario illustrargli l'utilità, per l'operatore sanitario, di disporre di un quadro clinico il più possibile completo della sua salute. In tal senso, devono essere compiutamente illustrate a quest'ultimo le conseguenze collegate al mancato consenso ovvero all'esercizio del diritto di oscuramento, nonché il significato clinico dell'informazione che si intende oscurare.

Qual è il presupposto di liceità del trattamento?

Per condizione di liceità del trattamento si intende il presupposto giuridico che consente al Titolare di trattare i dati personali e, nel caso di specie, anche quelli di cui alle categorie particolari (es. dati relativi alla salute).

Il dossier sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo.

All'interessato deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale strumento. Ciò significa che qualora l'interessato non manifesti il proprio consenso al trattamento dei dati personali mediante il dossier sanitario, il professionista che lo prende in cura avrà a disposizioni solo le informazioni rese in quel momento dallo stesso interessato (ad es., raccolta dell'anamnesi e delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista.

Analogamente, in tale circostanza il personale sanitario di reparto/ambulatorio avrà accesso solo alle informazioni relative all'episodio per il quale l'interessato si è rivolto presso quella struttura e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio (c.d. accesso agli applicativi verticali dipartimentali).

L'eventuale mancato consenso al trattamento dei dati personali mediante il dossier sanitario non deve incidere negativamente sulla possibilità di accedere alle cure mediche richieste.

Ai fini dell'accesso al dossier da parte del personale sanitario non è necessario che venga acquisito volta per volta il consenso dell'interessato; il dossier, infatti, sarà accessibile nel tempo da parte di tutti gli operatori sanitari che lo prenderanno in cura sulla base del consenso che l'interessato avrà inizialmente prestato per il trattamento dei suoi dati personali mediante il dossier. Ciò stante, il professionista che a vario titolo (ad es., prestazione specialistica, nuovo ricovero, attività riabilitativa) interverrà nel processo

di cura di un paziente che avrà già manifestato in passato il consenso al dossier, potrà accedere a tutti i dati ivi presenti.

Anche l'inserimento delle informazioni relative ad eventi sanitari pregressi all'istituzione del *dossier* sanitario deve, inoltre, fondarsi su un nuovo, specifico e informato consenso dell'interessato; potendo quest'ultimo anche scegliere che le informazioni sanitarie pregresse che lo riguardano non siano trattate mediante il *dossier*.

Si evidenzia che in caso di incapacità di agire dell'interessato deve essere acquisito il consenso di chi esercita la potestà legale su di esso. In caso di minori, raggiunta la maggiore età, deve essere acquisito -al primo contatto utile- nuovamente il consenso informato dell'interessato divenuto maggiorenne.

Particolari casi di consenso

Le citate Linee Guida del Garante stabiliscono alcune particolari condizioni al ricorrere delle quali è necessario acquisire uno specifico consenso.
Si tratta dei casi riferiti a informazioni relative a prestazioni sanitarie offerte a soggetti nei cui confronti l'ordinamento vigente ha posto specifiche disposizioni a tutela della loro riservatezza e dignità personale. Si tratta, in particolare, dei dati soggetti a maggiore tutela dell'anonimato, ovvero relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all' uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari. In tali casi, infatti, l'interessato può legittimamente richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti dallo stesso individuati (ad es., solo dallo specialista presso cui è in cura), fermo restando la possibilità che agli stessi possano sempre accedere i professionisti che li hanno elaborati.
Nel caso in cui il titolare intenda trattare anche tali dati personali mediante il dossier è pertanto necessario che acquisisca un autonomo e specifico consenso dell'interessato, che può essere raccolto unitamente a quello sul dossier o anche in occasione dell'erogazione della specifica prestazione sanitaria.

Prestazioni in emergenza

Una volta prestato il consenso al trattamento dei dati personali mediante il dossier sanitario, quest'ultimo sarà accessibile da parte di tutti gli operatori sanitari che, nel corso del tempo, lo prenderanno in cura, senza che l'interessato debba manifestare tale volontà ogni volta che accede per vari motivi alla struttura sanitaria.

La revocabilità del consenso

In considerazione del carattere facoltativo del Dossier Sanitario e la sua costituzione e implementazione solo a seguito del consenso dell'interessato (paziente), il consenso potrà essere revocato e/o modificato in qualsiasi momento.
L'Azienda ha, a tal proposito, adottato specifica modulistica per consentire all'interessato il pieno esercizio di tali diritti.

Il Dossier Sanitario nell'Azienda Ospedaliero-Universitaria di Careggi

L'Azienda Ospedaliera Universitaria di Careggi effettua solo parzialmente i trattamenti previsti nell'ambito del Dossier Sanitario ovvero allo stesso riconducibili.

Ferma la descrizione della natura del Dossier, del suo funzionamento e delle finalità per le quali lo stesso viene istituito e gestito (come puntualmente evidenziato nelle Linee Guida in materia di Dossier Sanitario dell'Autorità Garante per la protezione dei dati personali del 4 giugno 2015) nonché gli ulteriori requisiti organizzativi e tecnici richiesti per la sua implementazione, l'AOU-Careggi consente la visibilità di solo alcune informazioni, come di seguito dettagliato.

Pertanto, ove il paziente fornisca il proprio consenso, i soggetti abilitati e autorizzati potranno avere la visibilità delle seguenti informazioni e documenti:

- Cartella ambulatoriale e di degenza (clenco degli accessi ai reparti, referti esami strumentali - referti di laboratorio);
- Relazione di degenza / Lettera di dimissione;
- Lettera al medico curante della visita ambulatoriale.

Si precisa, quindi, che l'eventuale attivazione del Dossier Sanitario è sempre collegata all'apertura della cartella clinica e ambulatoriale collegata all'accesso a un percorso clinico (ambulatoriale o di ricovero). Il personale sanitario sarà autorizzato all'accesso con diversi livelli di profondità e differenti privilegi di visibilità delle informazioni garantendo che solo le informazioni necessarie e assegnate allo specifico profilo (es. medico o infermiere) possano essere consultate.

In relazione alla struttura informatica delle cartelle ambulatoriali o di ricovero attraverso le quali l'Azienda ha implementato le sopra descritte funzionalità proprie del Dossier Sanitario, si evidenzia che le informazioni accessibili e, di conseguenza, oscurabili, sono unicamente quelle sopra indicate: cartella nel suo complesso; la relazione di degenza; la lettera al curante.

L'Azienda non effettua trattamenti anonimizzati per finalità di didattica, studio e ricerca attraverso il Dossier Sanitario.

I Diritti dell'interessato

La struttura sanitaria presso la quale è effettuato il trattamento dei dati personali mediante il dossier sanitario e, segnatamente nel nostro caso l'Azienda Ospedaliero-Universitaria Careggi, deve garantire che l'interessato possa esercitare nei confronti di tale trattamento i diritti indicati negli articoli 15 e seguenti del Reg.UE 2016/679.

In particolare, l'interessato ha diritto di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la

cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo"

Si evidenzia che essendo il dossier sanitario un trattamento di dati personali effettuato con modalità elettroniche atte a consentire una forte integrazione di dati e documenti contenenti informazioni idonee a rivelare lo stato di salute, assume particolare rilievo il diritto riconosciuto all'interessato di poter ottenere l'indicazione della logica applicata a tale trattamento, ovvero l'indicazione dei criteri utilizzati nell'elaborazione elettronica dei dati.

Qualora l'interessato richieda di integrare, rettificare, aggiornare i dati trattati mediante il dossier sanitario, trattandosi di documentazione medica, in analogia a quanto disposto dall'Autorità in tema di ricerche in ambito medico, biomedico ed epidemiologico, il riscontro a istanze di integrazione, aggiornamento e rettificazione dei dati deve essere fornito annotando le modifiche richieste senza alterare la documentazione di riferimento.

L'oscuramento

Un'importante garanzia a tutela della riservatezza dell'interessato che abbia manifestato la propria volontà in merito al trattamento dei dati personali mediante il dossier sanitario consiste nella possibilità che lo stesso decida di oscurare taluni dati o documenti sanitari consultabili tramite tale strumento. Ciò in analogia a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di alcuni eventi sanitari che lo riguardano. Ciò, anche nel rispetto della legittima volontà dell'interessato di richiedere il parere di un altro specialista senza che quest'ultimo possa essere influenzato da quanto già espresso da un collega.
Ferma restando, infatti, l'indubbia utilità di un *dossier* sanitario il più possibile completo, il titolare del trattamento deve garantire la possibilità per l'interessato di non far confluire in esso alcune informazioni sanitarie. Al riguardo, si evidenzia che di per sé il *dossier* sanitario costituisce uno strumento informativo incompleto. Indipendentemente dalle ipotesi di oscuramento, infatti, il *dossier* include solo le informazioni cliniche derivanti dagli accessi del paziente nella struttura sanitaria che utilizza il *dossier* e non anche quelle relative agli accessi effettuati presso altre strutture pubbliche e private.
È, inoltre, importante evidenziare che i dossier sanitari non certificano lo stato di salute dei pazienti, in quanto consistono in strumenti che possono aiutare il clinico ad inquadrare meglio e più rapidamente lo stato di salute di questi, nel rispetto del diritto dovere del medico di effettuare gli accertamenti che riterrà -anche deontologicamente- più opportuni.

L'"oscuramento" dell'evento clinico (revocabile nel tempo) deve avvenire con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").
Proprio in considerazione di quanto sopra, il Professionista deve essere consapevole in ordine alla possibilità che i Dossier ai quali può accedere possono non essere completi, in quanto l'interessato potrebbe aver esercitato il suddetto diritto di oscuramento.

Nel caso in cui l'interessato richieda l'oscuramento delle informazioni e/o dei documenti oggetto dello stesso, questi restano comunque disponibili al professionista sanitario o alla struttura interna al titolare che li ha raccolti o elaborati (ad es., referto accessibile tramite dossier da parte del professionista, che lo ha redatto, cartella clinica accessibile da parte del reparto di ricovero). La documentazione clinica relativa all'evento oscurato deve essere comunque conservata dal titolare del trattamento in conformità a quanto previsto dalla normativa di settore.

Diritto alla visione degli accessi al dossier

Al fine di contrastare i rischi di accesso non autorizzato ai dati personali trattati mediante il dossier sanitario, è necessario predisporre l'adozione di adeguate misure di sicurezza, contestuale a una puntuale individuazione dei profili e dei livelli di autenticazione e di accesso ai sistemi, per consentire l'accesso solo da parte dei professionisti autorizzati.

In tale ottica, l'Azienda è tenuta a comunicare all'interessato che abbia manifestato il proprio consenso al trattamento dei dati personali mediante il dossier sanitario, un riscontro alla richiesta avanzata dallo stesso o da un suo delegato, volta a conoscere gli accessi eseguiti sul proprio dossier con l'indicazione della struttura/reparto che ha effettuato l'accesso, nonché della data e dell'ora dello stesso.

La tracciabilità degli accessi, pertanto, si caratterizza quale specifica misura di sicurezza.

Organizzazione interna e accesso al dossier sanitario

Come già rappresentato, il dossier sanitario costituisce uno strumento di ausilio per il personale sanitario consultabile da parte dello stesso nel processo di cura del paziente. La finalità perseguita attraverso tale strumento è, pertanto, quella di prevenzione, diagnosi, cura e riabilitazione dell'interessato. In quanto tale, l'accesso al dossier deve essere limitato al personale sanitario che interviene in tale processo di cura e deve essere posto in essere esclusivamente da parte dei soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico nell'esercizio di attività medico-legale.

Come riportato nelle citate Linee Guida, è necessario evidenziare che l'insieme delle informazioni sanitarie trattate mediante il dossier sanitario costituisce una banca dati di significativo rilievo non solo clinico ma anche economico. È facilmente intuibile, infatti, l'interesse economico che vari soggetti potrebbero vantare nei confronti di tale insieme di dati, la consultazione del quale rende agevolmente possibile ricostruire una significativa parte della storia clinica di un individuo. Al fine di scongiurare il rischio di un accesso a tali informazioni da parte di soggetti non autorizzati o di comunicazione a terzi delle stesse da parte di soggetti a ciò abilitati, è necessario, pertanto, che il titolare ponga una particolare attenzione nell'individuazione dei profili di autorizzazione e nella formazione dei soggetti abilitati.

L'accesso al *dossier* deve essere limitato, quindi, al solo personale sanitario che interviene nel tempo nel processo di cura del paziente. Sono pertanto previste specifiche modalità tecniche di autenticazione al dossier.

L'accesso al dossier deve essere limitato, poi, al tempo in cui si articola il processo di cura, ferma restando la possibilità di accedere nuovamente al dossier qualora ciò si renda necessario in merito al tipo di trattamento medico da prestare all'interessato.

L'Azienda ha inoltre previsto soluzioni che siano in grado di garantire l'accesso alle sole informazioni necessarie in relazione al profilo autorizzato (c.d. profondità dell'accesso). In risposta ai principi stabiliti dalla normativa, pertanto, il personale amministrativo dell'Azienda non avrà accesso ai dati trattati attraverso il Dossier.

A livello organizzativo, nel rispetto delle regole generali fissati dalla normativa posta a protezione delle persone fisiche con riguardo al trattamento dei dati personali, l'Azienda ha specificamente identificato e autorizzato i Professionisti autorizzati all'accesso definendo specifici profili.

Esattezza e aggiornamento dei dati

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 – che magari non è più attuale ma non per questo è/era inesatto - conservato.

Qualora 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. Dire oggi che sono celibe è inesatto. 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 legittimamente (anzi devono) essere conservate.

In alcune circostanze, dunque, 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.

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.*

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.

Informazioni/informativa sul trattamento dei dati

Se il diritto alla protezione dei dati personali si declina come diritto al controllo sul trattamento dei dati personali che riguardano una certa persona fisica, questa ha anzitutto il diritto di essere informata, direttamente o meno, che un certo trattamento la riguarda sta per essere o è già effettuato.

Il titolare deve informare l'interessato mettendogli a disposizione alcuni elementi, precisati agli artt. 13 e 14 del Regolamento.

L'art. 13 si riferisce al caso in cui "i dati personali siano raccolti *presso* l'interessato" ("personal data are collected *from* the data subject") ed è fornita all'interessato "nel momento in cui i dati personali sono ottenuti"; l'art. 14 a quello in cui "i dati personali non siano stati ottenuti *presso* l'interessato" ("personal data have not been obtained *from* the data subject").

Parrebbe che *from*, più che *presso*, sia proprio da intendersi come *da*, come sinonimo di *by*, evidenza di un rapporto diretto con l'interessato, nel senso che è l'interessato che conferisce i dati. *Presso* suggerisce l'idea di una vicinanza fisica, ma l'informativa può essere prestata all'interessato ed i dati ottenuti da questi anche telematicamente.

La pubblicazione on line dell'informativa, anche preventiva, nella misura in cui non viene data "nel momento in cui i dati personali sono ottenuti", è da riferirsi all'art. 14 del Regolamento.

L'Autorità parla, quando "i dati personali siano raccolti *presso* l'interessato", di interessato "contattabile", e quando ""i dati personali non siano stati ottenuti *presso* l'interessato" di interessato "non contattabile". Ciò significa che, quand'anche abbia raccolto i dati per scopo di cura presso l'interessato, se ne faccio un uso secondario per finalità di ricerca e non riesco a ricontattare l'interessato per informarlo (ed ottenerne il consenso), mi trovo nella situazione di un interessato non contattabile (ed infatti pubblicherò una informativa ex art. 14 del Codice): i dati, allora saranno raccolti, nel rispetto del principio di limitazione della finalità, per la ulteriore finalità di ricerca, come ex novo, e non saranno ottenuti "presso l'interessato", cioè previo un contatto con esso.

I soggetti che non sono stati contattati per raccoglierne i dati e che possono quindi avere eventualmente cognizione del trattamento solo in un secondo tempo, potrebbero anche essere di fatto non contattabili: ad esempio perché non si hanno i dati di contatto o perché troppo numerosi, o semplicemente perché defunti. In tali casi non viene meno un obbligo di informativa, e se ne prevede comunque la pubblicazione, ad esempio sul sito istituzionale di una P.A. (nel caso dei defunti, ovviamente, l'informativa potrebbe interessare i soggetti legittimati, ai sensi dell'art. 2-terdecies del Codice, o da un interesse proprio o che agiscono comunque a tutela dell'interessato o per ragioni familiari meritevoli di protezione).

Le seguenti *informazioni* sono quelle comuni alle due fattispecie:

- 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;
- l'eventuale esistenza di un processo decisionale automatizzato.

Se l'informativa è prestata ai sensi dell'art. 13 del Regolamento, l'interessato deve inoltre essere informato "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";

Se l'informativa è prestata ai sensi dell'art. 14 del Regolamento, occorre specificare "le categorie di dati personali in questione" e "la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico".

In ambedue i casi è previsto che qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti/ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui sopra: in breve, ad un trattamento ulteriore di dati per una finalità diversa è correlato l'obbligo, nel rispetto del principio di limitazione della finalità, di una ulteriore informativa preventiva.

Se l'informativa riguarda il trattamento di dati genetici, essa è integrata con le seguenti informazioni:

- i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici;
- la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di tali dati per ulteriori scopi.

Interessato

L'interessato è "la persona fisica cui si riferiscono i dati".

La Direttiva 95/46 parlava di "interessato" (data subject) offrendone una definizione ricompresa in quella di dato personale: "'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject')"; laddove la *natural persona* è la persona fisica, distinta dalla *legal person,* la persona giuridica. E' la stessa definizione offerta dal Regolamento all'art. 4.1: "'personal data' means any information relating to an identified or identifiable natural person ('data subject')".

In realtà, L.675/96 all'art. 2 f) ne aveva estesa la nozione, ponendo l'interessato come "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali", definizione transitata senza modifiche all'art. 4 comma 1 i) della prima versione del Codice; tanto per la L. 675/1996 che nella prima redazione del D.Lgs. 196/2003 potevano dunque essere qualificati "interessati" sia persone fisiche che persone giuridiche, enti o associazioni, estendendo la tutela appunto oltre le persone fisiche.

Successivamente, l'art. 40, comma 2, lett. b), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214, aveva già riportato le nozioni di dato personale e di interessato a quelle della Direttiva 95/46.

L'interessato è dunque la persona fisica alla quale i dati personali oggetto di trattamento si riferiscono (o potrebbero riferirsi), appunto *interessata* dal trattamento ed alla protezione assicurata dalla normativa.

Quella dell'interessato è una situazione: la situazione della persona fisica di cui si trattano dati che la riguardano. L'interessato è tale di fatto, nella misura in cui se ne trattano o possono trattare i dati, e non è richiesta alcuna sua formale individuazione o qualificazione, o una sua manifestazione di volontà in tal senso.

L'interessato ha una serie di diritti, riconducibili a categorie 3 principali.

Ha anzitutto il diritto a conoscere se è stato iniziato un trattamento che lo riguarda: ciò significa che può utilizzare le prerogative dell'interessato anche qualora, ad una successiva verifica, si accerti che in effetti non lo era.

Ha inoltre il diritto di effettuare controllo sulla liceità e qualità del trattamento (ad es. sulla esattezza ed aggiornamento dei dati personali trattati).

Oltre a questi diritti "di conoscenza", ha anche un diritto positivo di intervento sul trattamento (limitazione, blocco, ecc.)

Si noti come il termine interessato abbia una connotazione passiva/attiva: è la persona interessata "dai dati", il *soggetto* in senso proprio (passivo), ma anche la persona interessata "ai dati", che cioè 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 è, appunto, l'oggetto del trattamento, così che l'interessato subisce il trattamento del dato o il dato stesso (che normalmente è il prodotto, l'esito di una altrui attività, si pensi ai dati sanitari), 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).

Legittimo interesse

La direttiva 46/95 non vietava espressamente ai soggetti pubblici di trattare dati per il perseguimento del proprio interesse legittimo (articolo 7, lettera f).

Nella versione del Codice pre adeguamento, si richiamava il legittimo interesse solo all'art. 24, ricompreso nel Capo III, dedicato a Regole ulteriori per privati ed enti pubblici economici, dunque non riferibile agli enti pubblici.

L'articolo 7, lettera f della Direttiva è sostanzialmente simile all'art. 6 par 1 lettera f del Regolamento, tranne il fatto che a questo è di seguito aggiunto un addendum per il quale "La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche (*public authority*) nell'esecuzione dei loro compiti" (stessa previsione nel Considerando n. 47: "la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti").

Ora, nel Regolamento si parla ordinariamente di "autorità pubbliche e organismi pubblici" (*public authorities and bodies*). L'Autorità di controllo è senz'altro qualificata come autorità pubblica all'art. 4 21.

In effetti, il fatto che il Regolamento non offra una definizione di tali termini - che hanno un significato peculiare nel diritto anglosassone, non facilmente trasferibile nell'ambito nazionale - ha portato gli interpreti a considerare quei termini come endiadi per "ente pubblico" o "settore pubblico" in senso ampio.

La questione dell'impraticabilità del "legittimo interesse" da parte delle PP.AA. è stata perciò ricondotta al principio generale secondo cui queste, di norma, devono trattare dati, nell'esercizio dei loro compiti, purché siano opportunamente autorizzate da qualche disposizione normativa ad agire in tal senso.

Si potrebbe pensare ad una possibilità di accesso a tale base giuridica anche per le PP.AA. quando svolgono attività di diritto privato.

Ad ogni modo si tratta di una base giuridica non replicata all'art. 9, e dunque non utilizzabile in riferimento alle categorie particolari di dati.

Liceità e base giuridica del trattamento

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

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.

Gli artt.. 13 e 14 del Regolamento, relativi alle Informazioni da mettere a disposizione dell'interessato distinguono 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 il motivo per il quale e l'obiettivo pratico in vista del quale si trattano informazioni di carattere personale, è dunque una situazione di fatto.

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 tratta 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 sorprendentemente esterno rispetto alla definizione di trattamento offerta dal Regolamento[1], 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.

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/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 lecito il trattamento dei dati per quella certa finalità, spesso in riferimento ad una certa categoria di titolari: cioè il trattamento è lecito se una certa base giuridica è utilizzata da determinati soggetti e non da parte di altri. In alcuni casi, dunque, 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 relativi alla salute per finalità di "diagnosi assistenza o terapia sanitaria".

Le basi giuridiche del trattamento sono indicate, per quanto di nostro interesse, agli artt. 6 e 9 del Regolamento. Sono definite in tali articoli, rispettivamente, condizioni o casi che rendono lecito il trattamento.

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 a quelle categorie di dati personali che sono definite "particolari" ("categorie particolari di dati personali", "special categories of personal data"; 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

Ciò significa che, in riferimento a tali dati, le basi giuridiche consentite dall'art. 6 sono dichiarate insufficienti; tale divieto non si applica però se si verificano, appunto, alcuni "casi", ovvero in presenza di specifiche, ulteriori basi giuridiche indicate al par. 2 dell'art. 9.

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, 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.

Il titolare, comunque, 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, deve accertare se, oltre che ad essere funzionali ad 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 potrà essere documentata 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.

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. 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..

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, gli artt. 13 e 14 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", certo indizio dell'ignoranza della medesima da parte di chi ciò ha scritto. 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 riutilizzare i dati per una diversa finalità.

Madre che non vuole essere nominata

I documenti relativi all'evento nascita sono i seguenti:

- la dichiarazione di nascita;
- l'attestazione di avvenuta nascita;
- il certificato di assistenza al parto.

La *dichiarazione di nascita* può essere resa indistintamente da uno dei soggetti legittimati nel comma 1 dell'articolo 30 del D.P.R. 3 novembre 2000, n. 396 *Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile*: uno dei genitori, procuratore speciale, medico, ostetrica, altra persona che ha assistito al parto. Essa è corredata da una *attestazione di avvenuta nascita,* il primo documento che appunto attesta l'evento nascita e che prevede l'identificazione della partoriente, ma che non ricomprende i dati identificativi del neonato, indicato solo in riferimento al sesso (i dati necessari alla attestazione di nascita sono indicati all'art. 30 comma 2 del D.P.R., ovvero "le generalità della puerpera nonché le indicazioni del comune, ospedale, casa di cura o altro luogo ove è avvenuta la nascita, del giorno e dell'ora della nascita e del sesso del bambino").

Il Certificato di Assistenza al Parto (CAP) ed il relativo flusso informativo sono previsti dal DM sanità n. 349/2001 *Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"*, e dalla DGR 68/2008 (le Regioni potendo integrare le informazioni ricomprese nel flusso) e viene compilato in occasione di ogni parto.

La possibilità ex lege per la madre di non essere indicata nell'atto di nascita è assicurata in pochi Stati membri del Consiglio d'Europa, Francia, Italia, Lussemburgo e, più recentemente, Austria e Slovacchia. In Francia l'anonimato della madre costituisce una tradizione risalente, formalizzata per via legislativa nel 1941 e ridisciplinata nel 2002 e successivamente, senza significative variazioni. La legge ha istituito un organo e un procedimento amministrativo volti, su istanza dei figli, a ricontattare, ove possibile, le madri anonime, per una eventuale revoca del segreto. Negli altri Stati, invece, il rapporto di filiazione tra madre e figlio si costituisce automaticamente per il fatto del parto.

Nell'ordinamento francese l'aspirazione a conoscere le origini integra un'esigenza giuridicamente tutelata ma non un diritto costituzionale. In breve arco di tempo, seguendo un'onda montante nel diritto internazionale e in altri ordinamenti, improntata alla riscoperta dei legami di sangue rispetto alla famiglia sociale o, come è stato detto, "ad una vittoria della biologia sulla biografia", la conoscenza delle origini, da mera aspirazione, ha assunto la consistenza di diritto legislativo (con la l. n. 149/2001, di modifica della l. n. 183/1984) e poi di vero e proprio diritto costituzionale, componente dell'identità personale ai sensi dell'art. 2 Cost., quale «elemento significativo nel sistema costituzionale di tutela della persona» (Corte cost. n. 278/2013, ritenuta apice di un «processo di valorizzazione del diritto all'identità personale» da Corte cost. n. 286/2016.

Vediamo comunque i diritti che, nel nostro sistema normativo, devono essere garantiti alla madre "che non vuole essere nominata"; essi sono i seguenti:

- ai sensi dell'art. 30, comma 1 del D.P.R. n. 396/2000, la *dichiarazione di nascita* deve rispettare l'eventuale volontà della madre di non essere nominata;
- ai sensi dell'art. 93 commi 2 e 3 del D.Lgs. 196/2003, il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata, possono essere rilasciati in copia integrale a chi vi abbia interesse decorsi cento anni dalla formazione del documento; durante tale periodo la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Per individuare la ratio di tali disposizioni, è utile considerare che non vi viene fatta menzione dell'*attestazione di nascita*; perché per l'attestazione di nascita, che viene pure trasmessa all'ufficiale di stato civile, non si prevede alcuna tutela della riservatezza della partoriente? Il fatto è che l'attestazione di nascita si riferisce propriamente al fatto fisiologico dell'avvenuto parto, e dunque alla donna come "partoriente", la quale in un secondo momento può o meno – in accordo con l'assunto che il solo fatto della procreazione non è fattispecie in sé e per sé sufficiente a determinare la costituzione di un rapporto giuridico di filiazione e di uno status di figlio - diventare madre (per mezzo della dichiarazione di nascita, che, ai sensi dell'art. 30 comma 4 del DPR 396/2000, " può essere resa, entro dieci giorni dalla nascita, presso il comune nel cui territorio è avvenuto il parto o in alternativa, entro tre giorni, presso la direzione sanitaria dell'ospedale o della casa di cura in cui è avvenuta la nascita. In tale ultimo caso la dichiarazione può contenere anche il riconoscimento contestuale di figlio nato fuori del matrimonio e, unitamente all'attestazione di nascita, è trasmessa, ai fini della trascrizione, dal direttore sanitario all'ufficiale dello stato civile del comune nel cui territorio è situato il centro di nascita o, su richiesta dei genitori, al comune di residenza …, nei dieci giorni successivi, anche attraverso la utilizzazione di sistemi di comunicazione telematici tali da garantire l'autenticità della documentazione inviata secondo la normativa in vigore"). Ne segue che la madre "che non vuole essere nominata" è dunque, propriamente, la partoriente che non vuole essere nominata nella dichiarazione di nascita, ovvero la *potenziale* madre che rinuncia ad esserlo *in effetto*; ci si trova insomma di fronte ad un rapporto giuridico che non si è perfezionato; per questo la tutela ricomprende appunto:

- la garanzia di una dichiarazione di nascita priva dei riferimenti alla partoriente, che è la dichiarazione di nascita di una madre che non è (voluta diventare) tale, ma restare solo una partoriente (assumendo solo gli obblighi di questa, pure sussistenti – per questo il legame non può essere rescisso - e non quelli correlati allo status di madre);
- l'oscuramento dei legami tra il neonato e la donna che, pur partorendo, ha appunto scelto di non diventarne madre.

Il diritto della madre *a non essere nominata* limita evidentemente quello dei figli a conoscere le proprie origini biologiche; si tratta oggi comunque di una limitazione meno ampia di quella assicurata dalla previgente normativa.

Anzitutto, a far data dal 1 gennaio 2004, la limitazione all'accesso è prevista non genericamente in riferimento alla madre che non abbia proceduto al riconoscimento, ma solo a quella che, avvalendosi della possibilità prevista dall'art. 30 comma 1 del D.P.R. n. 396/2000, abbia specificamente dichiarato alla nascita *di non volere essere nominata* (nell'atto di nascita).

Se la L. 4 maggio 1983 n. 184 *Disciplina dell'adozione e dell'affidamento dei minori*, nella sua prima versione, aveva infatti confermato il divieto per l'adottato di conoscere le proprie origini biologiche - sostanzialmente al (ragionevole) scopo di salvaguardarne l'inserimento nella nuova famiglia - con le modifiche apportate dalla L. 149 del 28 marzo 2001 la nuova redazione dell'art. 28 comma 5 assicurava la possibilità per l'adottato venticinquenne (è dunque richiesta una capacità d'agire speciale) di accedere alle informazioni che riguardano la sua origine e l'identità dei genitori biologici ("L'adottato, raggiunta l'età di venticinque anni, può accedere a informazioni che riguardano la sua origine e l'identità dei propri genitori biologici. Può farlo anche raggiunta la maggiore età, se sussistono gravi e comprovati motivi attinenti alla sua salute psico-fisica. L'istanza deve essere presentata al tribunale per i minorenni del luogo di residenza").

Tale diritto viene appunto meno, ai sensi dell'art. 28 comma "nei confronti della madre che abbia dichiarato alla nascita di non volere essere nominata ai sensi dell'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396".

La Corte Costituzionale, con sentenza 18 - 22 novembre 2013, n. 278 (in G.U. 1a s.s. 27/11/2013, n. 48), ha però dichiarato l'illegittimità costituzionale dell'articolo 28, comma 7, della legge 4 maggio 1983, n. 184" nella parte in cui non prevede - attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza - la possibilità per il giudice di interpellare la madre - che abbia dichiarato di non voler essere nominata - su richiesta del figlio, ai fini di una eventuale revoca di tale dichiarazione.

Tale sentenza è applicazione della sentenza *Godelli contro Italia* della Corte di Strasburgo, che nel 2012 aveva condannato l'Italia per la prevalenza assoluta e permanente assicurata all'anonimato della madre rispetto al diritto del figlio a conoscere le proprie origini, ledendo il principio personalistico assicurato dall'art. 8 CEDU (Convenzione Europea sui Diritti dell'Uomo). L'art. 8 prevede che "Ogni persona ha diritto al rispetto della propria vita privata e familiare …". Tale diritto deve intendersi in senso ampio: fra le questioni rilevanti per lo sviluppo personale devono essere infatti ricomprese le informazioni relative all'identità di una persona in quanto essere umano e l'interesse a ottenere le informazioni necessarie a scoprire la verità su importanti aspetti dell'identità personale, quali appunto l'identità dei genitori, la propria origine e aspetti relativi alla propria infanzia e alla propria adolescenza. La nascita e, in particolare, le circostanze in cui è avvenuta, fanno parte della vita privata di un minore e successivamente dell'adulto, garantita dall'articolo 8 della Convenzione.

Laddove il comma 3 dell'art. 93 del *Codice* accenna a richieste d'accesso che durante tale periodo di possono essere accolte "relativamente ai dati relativi alla madre, osservando le opportune cautele per evitare che quest'ultima sia identificabile" ci si riferisce verosimilmente ad una situazione quale ad es. la seguente: il figlio, affetto da una data patologia, chiede all'ospedale presso il quale è nato un riscontro sulla familiarità della stessa, che gli verrà fornito senza allegare informazioni identificative, diretta o indiretta, della madre. Si tratta, in questo caso, di una particolare specificazione del principio dei "diritti di pari rango".

Il diritto della madre a non essere nominata, quale diritto della personalità, è riconosciuto anche alla madre di nazionalità straniera, ed è prevalente su ogni difforme diritto che una legge straniera eventualmente accordasse ai genitori biologici.

Quanto sopra conferma che un diritto del paziente all'anonimato, se per anonimato si intende, secondo la definizione tecnico-giuridica, l'impossibilità di riferire una informazione ad un interessato individuato o individuabile, non ha fondamento, né – diciamo così – prospetticamente (paziente che accede alle strutture senza essere identificato), né retrospettivamente (anonimizzazione successiva dei dati riferiti al paziente). Anche altre disposizioni normative che assicurano appunto, letteralmente, un cosiddetto anonimato del paziente - oltre alle donne che decidono di partorire in anonimato, vi sono i casi delle vittime di atti di violenza sessuale o di pedofilia (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (l. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (D.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza (l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349) - fanno riferimento piuttosto all'obbligo di un trattamento dei dati del paziente con modalità non immediatamente identificativa, che si realizza normalmente attraverso l'utilizzo di codici alfanumerici, che comunque il Titolare, ovvero uno o più dei suoi incaricati a ciò specificamente autorizzati hanno sempre la possibilità di ricondurre ad un determinato soggetto.

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), per il quale i dati devono essere

> 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»)

Leggendo la disposizione citata, in realtà 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.

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 di cui il titolare ha già la disponibilità (l'art. 5 del Regolamento di focalizza sui dati, anche se in realtà oggetto della disposizione è a ben vedere la raccolta dei dati e dunque una operazione di trattamento, tanto che poi si parla, coerentemente, di un trattamento ulteriore) - 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.

Comunque, la *finalità* è il motivo per il quale e l'obiettivo pratico in vista del quale si trattano informazioni di carattere personale. In tale nozione, di per sé, non viene in causa la questione di una eventuale liceità/illiceità di tale scopo (infatti è stato necessario specificare "finalità … legittime"), questione che coinvolge il concetto di "base giuridica" del trattamento.

Dunque, l'art. 5 par. 1 lettera b) del Regolamento 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 lecitamente raccolti per una specifica finalità (ad es. quella di cura) *ad libitum*, per finalità ulteriori, avendone invece un possesso *condizionato,* e appunto *limitato* a quella prima finalità; 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 senz'altro 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 ed 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.

Medicina preventiva, diagnosi, assistenza o terapia sanitaria

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

Per l'art. 8 par. 3 della Direttiva il trattamento di categorie particolari di dati (tra i quali i dati relativi alla salute) è lecito, tra l'altro, 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

Per l'art. 9 par. 2 lettera h del Regolamento, il trattamento di categorie particolari di dati (tra i quali i dati relativi alla salute) è lecito, tra l'altro, quando:

> … 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;

Le differenze tra i due articoli, per quanto riguarda la parte strettamente sanitaria, è soprattutto da ricondursi alla diversa traduzione; vengono poi specificate le attività di medicina del lavoro e valutazione del dipendente, a creare una articolazione rispetto ai trattamenti svolti dal datore di lavoro ai sensi dell'art. 9 par. 2 lettera b), e aggiunte quelle relative all'assistenza sociale):

Direttiva	Regolamento
prevenzione medica / preventive medicine	medicina preventiva / preventive medicine
diagnostica medica / medical diagnosis	diagnosi sanitaria / medical diagnosis

somministrazione di cure / provision of care or treatment	assistenza o terapia sanitaria / provision of health care or treatment
gestione di centri di cura / management of health-care services	gestione dei sistemi e servizi sanitari / management of health systems and services
	medicina del lavoro / occupational medicine
	valutazione della capacità lavorativa del dipendente / assessment of the working capacity of the employee
	assistenza sociale / provision of social care or treatment
	gestione dei sistemi e servizi sociali / management of social care systems and services

Nel par. 3 dell'art. 9 del Regolamento, inoltre, si specifica ulteriormente il riferimento al "contratto con un professionista della sanità" di cui alla lettera h) (una simile ulteriore precisazione non è prevista nell'art. 8 della Direttiva) indicando le peculiari "condizioni e … garanzie" poste a salvaguardia:

> 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.

Ora, rispetto alla fattispecie prevista dell'art. 8 par. 3 della Direttiva, prima la L. 675/96 e poi il Codice nella stesura originaria, si erano "ritagliati" un ambito di applicazione ben 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 riportava il trattamento ad attività di ambito strettamente sanitario-professionale, rimandando quanto ad esse non potesse essere direttamente ricondotto agli scopi cosiddetti "amministrativi", riconducibili ai motivi di interesse pubblico rilevante.

In realtà, la previsione della Direttiva era diversa, se esaminiamo, assieme al par. 3 dell'art. 8, anche il par. 4:

> Il paragrafo 1 (*il divieto di trattamento*) non si applica quando il trattamento dei dati 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.

> Purché siano previste le opportune garanzie, gli Stati membri possono, per motivi di interesse pubblico rilevante, stabilire ulteriori deroghe oltre a quelle previste dal paragrafo 2 sulla base della legislazione nazionale o di una decisione dell'autorità di controllo.

I motivi di interesse pubblico rilevante erano individuati come utilizzabili in riferimento ad ulteriori finalità di trattamento, non connesse con l'ambito sanitario (e infatti il richiamo è al par. 2, non al par. 3).

Nel Codice, però, il legislatore nazionale aveva preso in considerazione e valorizzato, rispetto all'art. 8 par. 3 della Direttiva, solo la finalità di "prevenzione … diagnostica medica, … somministrazione di cure", tralasciando piuttosto che quella, più ampia, relativa alla "gestione di centri di cura", pur presente in quell'articolo. La impostazione dell'art. 9 par. 2 lettera h) e par. 3 è intermedia; i motivi di interesse pubblico rilevante hanno una loro autonomia, all'art. 9 par. 2 lettera g), e per finalità sanitarie la finalità di cura può fondarsi tanto su questi che, semplicemente, sul fatto che il trattamento viene effettuato da professionisti sanitari soggetti al segreto o anche (evidentemente per le attività di supporto alla cura) da parte di personale soggetto al segreto d'ufficio.

Se quella 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 ("sistemi e servizi sanitari"). Se non è possibile curare una persona in elettiva senza effettuare una prenotazione, siamo certi che questa non possa rientrare nella finalità di cura, cui è strettamente funzionale ed anzi indispensabile? E, a parte questo, proprio da un punto di vista pratico, sarebbe pensabile una disposizione che dettagli i tipi di dati trattabili e le operazioni effettuabili per l'attività di prenotazione?

L'art. 9 par. 2 del Regolament dunque 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, regola e sostiene, non esiste (chiamiamola di seguito, complessivamente, per intenderci, *finalità di cura e di gestione di sistemi e servizi sanitari*).

Nella versione inglese del Regolamento, si parla proprio di "management of health … care systems and services", utilizzando un termine – *management* – assolutamente esplicito e caratterizzato sugli aspetti organizzativi.

Il problema, veramente decisivo, che si pone, è allora il seguente: in un ambito di fortissimo interesse pubblico come quello della tutela della salute (e possiamo accostarvi anche i motivi di interesse pubblico nel settore della sanità pubblica di cui all'art. 9 par. 2 lettera j del Regolamento) laddove vi è una larga

presenza normativa (e giurisprudenziale) a regolarne le attività, come si articola la pluralità delle basi giuridiche, in questo caso quelle appunto previste dall'art. 9 par. 2 lettera h) e par. 3 da un lato e dall'altro dall'art. 9 par. 2 lettera g) del Regolamento? E' possibile, almeno per i trattamenti caratterizzanti l'ambito sanitario, sostenere una sufficienza della base giuridica *finalità di cura e di gestione di sistemi e servizi sanitari*?

Si può ipotizzare 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: infatti, il trattamento è legittimo:

> sulla base del diritto dell'Unione o degli Stati membri *o conformemente al contratto con un professionista della sanità* …soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti …

La locuzione "sulla base del diritto dell'Unione o degli Stati membri" occorre altre tre volte nell'art. 9 par. 2 del Regolamento (lettere g, i, j), ed è sempre stata interpretata dal Garante - considerato che il diritto dell'Unione o degli stati membri deve appunto prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato - come un rimando alla esistenza di disposizioni puntuali che prevedano e legittimino il 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*;
> i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, … *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*;
> j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, *sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.*

Ma se in questi casi la base giuridica trova una sua necessaria integrazione e avveramento nel "diritto dell'Unione o degli Stati membri", nell'art. 9 par. 2 lettera h) questo è richiamato in via alternativa e sussidiaria. Ciò non significa che non occorra poi confrontarsi con obblighi di carattere normativo, laddove siano stati esplicitati ai sensi dell'art. 9 par. 2 lettera g (e saranno questi che dovranno avere i requisiti previsti dall'art. 2-sexies del Codice) ma che in generale vi è comunque, a mio avviso, una specificità dei trattamenti di dati effettuati in ambito sanitario che non può sempre ricondursi, considerata la loro peculiarità e dinamicità, a preesistenti specifiche norme positive. Quando vi sono esse si affiancheranno, anche condizionandolo, al trattamento per finalità di cura (e gestione dei sistemi sanitari) – e la loro presenza sarà significativa di una particolare attenzione del legislatore, o di chi per lui, circa

una specifica modalità di trattamento dei dati connessi a certe attività, e dunque di effettuazione di quelle attività - ma, se non vi sono, ciò di per se stesso non rende inconsistente ed inutilizzabile, da sola, quella base giuridica, ed effettuabile quel trattamento.

Ecco allora che la scheda n. 17 del Decreto del Presidente della Giunta Regionale Toscana 26 ottobre 2021, n. 37/R, dedicata alla *Attività amministrativa, programmatoria gestionale e di valutazione relativa all'assistenza ospedaliera in regime di ricovero*, ricomprende, indicandole come di propria competenza:

> cartelle cliniche di ricovero; diari clinici (es. infermieristici, riabilitativi, ecc.) relativi ai ricoverati; registri delle prenotazioni (L. 23 dicembre 1994, n.724); relazione clinica di dimissione, che viene trasmessa al medico di famiglia, con il previo e specifico consenso dell'interessato per finalità di cura e tutela della salute; archivi di attività diagnostiche/terapeutiche svolte per i pazienti ricoverati; registri di sala operatoria (Circolare del Ministero della Sanità n. 900 del 14.03.1996); registri delle trasfusioni (DM Sanità 01.09.1995); registri e documenti relativi alle sperimentazioni cliniche; raccolte di dati con finalità amministrativo-contabili; raccolte di dati relativi ad esposti/lamentele/opinioni degli utenti

Ciò significa null'altro che la cartella clinica o il diario clinico, o il verbale operatorio, che contengono informazioni con valore clinico rispetto alle attività effettuate, ne assumono anche uno di carattere amministrativo o giuridico-probatorio. Occorre cioè sempre distinguere la cartella clinica come obbligo documentale, la cui redazione è regolata da puntuali norme (in una considerazione, per così dire, retrospettiva), dalla cartella clinica prospetticamente intesa come collazione e fonte di dati necessari per l'inquadramento clinico del paziente durante il ricovero (o per le prestazioni ad esso successive).

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 (la finalità di interesse pubblico rilevante è applicabile *omnibus*) che hanno interamente, e geneticamente, la propria legittimazione 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. E' questo assunto che sostanzia l'idea di uno "specifico sanitario" anche nell'ambito del trattamento dei dati, riflesso nella autonoma finalità prevista dall'art. 9 par. 2 lettera h) e 3 del Regolamento; vero è che la giurisprudenza ci ha talmente abituati ad una visione strettamente ed astrattamente prescrittiva, in riferimento a regole per la verità quasi mai preventivamente o chiaramente esplicitate, e comunque molto sempre molto lontane dalle concrete e complesse realtà operative cui si vogliono poi, *ex post*, applicare, che tale specificità ed autonomia oramai non appare affatto evidente.

Su tale linea, la DGRT n. 495 del 22 aprile 2024, relativa alle Centrali Operative Territoriali (COT) di cui al DM 77/2022, ha potuto sostenere:

> La COT è un modello organizzativo che svolge una funzione di coordinamento della presa in carico della persona e raccordo tra i servizi e professionisti coinvolti nei diversi setting assistenziali: attività territoriali,

sanitarie e sociosanitarie, ospedaliere, telemedicina. Tali attività comportano la necessità di accedere a informazioni sanitarie che in alcuni casi afferiscono a Titolari diversi. Le COT coordinano, tracciano e monitorano le prese in carico e le transizioni fra luoghi di cura dei pazienti. In considerazione del fatto che la transizione tra un setting e l'altro è da considerarsi come logica prosecuzione del percorso di cura di un interessato, il quale prosegue afferendo a diversi servizi/strutture nel corso del tempo, il trattamento dei dati "comuni" e "particolari" strettamente necessari, viene effettuato dai titolari del trattamento ai sensi dell'art. 9, par. 2, lettera h) e par 3 del GDPR 679/2016, relativo al trattamento di dati necessario, tra l'altro, per finalità di diagnosi, assistenza o terapia sanitaria o sociale, ovvero gestione dei sistemi e servizi sanitari e sociali, effettuato da o sotto la responsabilità di un professionista soggetto al segreto professionale 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 dell'interessato

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 o in quella della tutela di un interesse vitale dell'interessato o di un'altra persona fisica (laddove l'interessato non sia nella condizione di poter prestare un valido consenso . Inoltre, alcuni trattamenti, o meglio alcune operazioni di trattamento, sono oggettivamente non funzionali alla cura (si pensi agli obblighi informativi ad es. verso l'ente Regione), e possono trovare una base giuridica nei motivi di interesse pubblico rilevante.

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 comunque indispensabile alla cura; 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 consapevole determinazione dell'interessato: implicitamente argomentando che al minore o nullo controllo che l'interessato può avere sui dati gestiti elettronicamente consegue 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 riguarda in via esclusiva all'interessato. In effetti, le disposizioni di cui all'art. 9 par. 2 lettera h) e par. 3 non riferiscono la finalità di cura al solo interessato; perciò l'art. 75 del Codice recita:

> Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-septies del presente codice, nonché' nel rispetto delle specifiche disposizioni di settore.

Si precisa che il riferimento all'art- 2-septies è quello relativo alle misure di garanzia che il Garante deve emanare con proprio provvedimento.

***

In una Azienda Ospedaliero-Universitaria, la titolarità dei trattamenti di dati necessari per la tutela della salute del paziente è della Azienda, 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 esclusiva 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.

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 *necessità*, oppure di *pertinenza o non eccedenza*.

La *non eccedenza* derivava dalla lettera dell'art. 6 della Direttiva 46/95 , per la quale "Member States shall provide that personal data must be : … (c) adequate, relevant and *not excessive* in relation to the purposes for which they are collected and/or further processed ; …"; la *non eccedenza* diventa all'art. 5 del Regolamento precisamente, e significativamente, una *limitazione*: "Personal data shall be: … c) adequate, relevant and *limited* to what is necessary in relation to the purposes for which they are processed ('data minimisation'). Il periodo, si osservi, è modificato anche in riferimento al rapporto tra dati e scopi per i quali sono trattati: da "*in relation to the purposes* for which they are collected and/or further processed" a "*to what is necessary in relation to the purposes* for which they are processed", spendendo proprio il termine "necessary". Nella Direttiva, si trattava di una prescrizione allora direttamente interpretabile come una versione aggiornata del principio di *minimalizzazione* che figura nel dall'art. 3a) del *Bundesdatenschutzgesetz* tedesco del maggio 2001, che parla di "parsimonia e misura nell'utilizzo dei dati personali", e prevede appunto che siano applicate ai dati modalità di trattamento che riducano al minimo l'utilizzazione di dati personali e permettano di identificare l'interessato solo quando necessario: "*Parsimonia e misura nell'utilizzo di dati personali*. La configurazione e la scelta di sistemi di elaborazione dati devono avere come obiettivo quello di evitare o ridurre quanto più possibile la raccolta, il trattamento o l'utilizzazione di dati personali. In particolare, occorre fare uso delle opportunità offerte dall'anonimizzazione e dalla pseudonimizzazione nella misura in cui ciò sia possibile ed il loro impiego risulti proporzionato alla finalità di protezione perseguite."

Comunque sia, ne segue che adeguatezza, pertinenza e limitazione dei dati non sono elementi assoluti, ma relativi allo scopo, o meglio a quanto necessario (*scil*: indispensabile, essenziale) per perseguire un dato scopo: sarà lecito utilizzare, tanto da un punto di vista qualitativo che quantitativo, solo le informazioni indispensabili per la specifica finalità perseguita, anche se lecita, che deve perciò essere sufficientemente definita e dettagliata, anche in tutte le sue articolazioni. Sono elementi che trovano dunque una loro misura in riferimento ad un principio di necessità non assolutizzabile, ma da valutare e motivare volta a volta.

La disposizione dell'art. 5 paragrafo 1 c) della Direttiva 46/95 citata, 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". Si noti che non si parla solo di sistemi informatici ma, più ampiamente, di sistemi informativi. Tale disposizione, che si può anche leggere come una prima, embrionale, apparizione del principio della privacy by design, connette la minimizzazione ("ridurre al minimo") dei dati personali e di quelli, in particolare, identificativi, ed un principio di necessità (anche se riferito, tralasciati i dati anonimi che personali non sono, solo alla possibilità di identificazione dell'interessato).

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, magari in una DPIA). Potrà poi esservi, eventualmente, una verifica da parte dell'Autorità di controllo.

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 …" ("processing is necessary for..."). In questo caso, in generale, la nozione di necessità è riferita al trattamento nel suo complesso, piuttosto che ai dati. 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". Ma una valutazione circa la minimizzazione dei dati effettivamente efficace rispetto ad un principio di protezione dei dati, dovrà essere svolta non rispetto ad una tipologia di trattamento riferibile ad una finalità generalmente considerata (ad es. la finalità di cura in astratto), ma in riferimento al trattamento in concreto e dunque ai dati ad esso specificamente necessari: i dati, appunto, *essenziali* per il raggiungimento di una o più finalità determinate.

Motivi di interesse pubblico

Si evidenzia che per il Regolamento il trattamento è complessivamente lecito in riferimento ad una certa base giuridica, ivi compresa evidentemente ogni operazione di trattamento eseguibile: non distingue cioè, relativamente alla liceità, tra le varie operazioni di trattamento; gli artt. 6 e 9 del Regolamento illustrano insomma la liceità di un trattamento considerandolo nel suo insieme, nella forma "il trattamento è necessario per …".

Relativamente ai trattamenti che hanno per scopo l'adempimento di un obbligo legale o l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri – quelli di cui qualche anno fa si parlava come di "scopi amministrativi" - il Considerando 45 sollecita la possibilità di integrazioni normative a livello UE o nazionale:

> È opportuno che il trattamento … necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. …. tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto.

Il legislatore nazionale – ma era così già nelle precedenti versioni del Codice – ha provveduto ad attuare questa sollecitazione in modo estremamente rigoroso.

Il comma 4 dell'art. 2-ter del Codice integra anzitutto la definizione di trattamento di dati offerta dall'art. 4 2) del Regolamento, nel quale si distingue dalle altre operazioni di trattamento la

> comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione ("disclosure by transmission, dissemination or otherwise making available)

Il testo avrebbe essere più precisamente ed utilmente tradotto con: "divulgazione attraverso comunicazione, diffusione o ogni altra modalità di messa a disposizione"; comunque, il legislatore nazionale offre una più analitica definizione delle operazioni di comunicazione e diffusione di dati personali; tale specificazione è ovviamente funzionale alla introduzione di una base giuridica più specifica, o anche di un particolare divieto, per tali operazioni (ad es. la diffusione di dati relativi alla salute o genetici è vietata ai sensi dell'art. 2-septies comma 8 del Codice).

> 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.

Riassumendo: si possono divulgare dati personali in qualsiasi modo, non necessariamente trasferendoli ma anche semplicemente mettendoli a disposizione o consentendo loro l'accesso (dunque senza un loro effettivo spostamento); si parla di comunicazione quando i soggetti che la ricevono sono preventivamente determinati o determinabili (ad es. i soggetti che possono accedere ad un documento amministrativo), di diffusione quando tali soggetti sono indeterminati (ad es. la pubblicazione di un documento amministrativo).

Relativamente alla base giuridica per poter effettuare operazioni di comunicazione o diffusione di dati comuni, l'attuale redazione dei primi 4 commi dell'art. 2-ter del Codice precisa:

> 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.

Allora: 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[i] o da atti amministrativi generali[ii]; 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, 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, che in un certo senso ha gli stessi effetti autorizzatori di una norma di legge o regolamento.

Coerentemente con tale impostazione, ma più radicalmente in relazione alla sensibilità di certe tipologie di dati (appunto quelli afferenti alle categorie particolari), la prima versione dell'art. 2-sexies del Codice (precedente alle modifiche apportate dal D.L. 8 ottobre 2021 n. 139) prescriveva che il trattamento fosse 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 e, se previsto dalla legge, regolamento.

Considerato che raramente una legge prevede tutti gli aspetti del trattamento che la norma prescrive, ci si doveva comunque orientare verso l'integrazione di carattere regolamentare laddove disponibile; 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 trattava effettivamente di un sistema di strettissima ed esclusiva 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, pur nella medesima impostazione analitica, è, oggi, invece consentito, ai sensi dell'art. 2-sexies comma 1 del Codice così come modificato dal D.L. 8 ottobre 2021 n. 139, più ampiamente, come segue:

> … 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.

E' stato intanto superato l'obbligo che l'atto regolamentare fosse previsto dalla norma di legge: questa doveva prevedere appunto "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", e se non era possibile o opportuno inserire tutti questi elementi nella stessa legge, questa doveva demandarli ad una integrazione di carattere regolamentare.

Era questa una impostazione in linea con quella dell'art. 20 del Codice pre-adeguamento, secondo il quale per effettuare un trattamento di dati sensibili sarebbe stata necessaria una legge che riconducesse tale trattamento ad una finalità di rilevante interesse pubblico, e che di tale trattamento specificasse i tipi di dati trattati e quali operazioni su di essi (comunicazione ecc.) possono essere eseguite (una disposizione di legge, insomma, centrata direttamente sul trattamento, e simmetricamente un trattamento direttamente ed integralmente legittimato da una norma di legge); in alternativa, in riferimento ad un trattamento ricondotto da una norma di legge ad una finalità di rilevante interesse pubblico (e tale requisito era in larga parte soddisfatto dal *Codice* stesso, dunque da una disposizione non indirizzata ad un particolare trattamento), è sufficiente che la specificazione dei tipi di dati trattati e di quali operazioni su di essi possono essere eseguite sia prevista da una disposizione di carattere regolamentare (un trattamento, insomma, legittimato – soddisfatta la previsione per legge della finalità di rilevante interesse pubblico – da una disposizione regolamentare). Tale disposizione regolamentare si caratterizzava ad ogni modo per il fatto di doversi conformare ad uno schema tipo sul quale l'Autorità Garante abbia espresso un proprio parere di conformità.

Nella nuova redazione dell'art. 2-sexies viene inoltre aggiunto, come base giuridica, l'atto amministrativo generale.

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 così come a 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, e 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); lasciando in secondo piano la questione fondamentale, che già si è presentata in via di principio con i livelli essenziali di assistenza (LEA), di come consentire che un diritto fondamentale come la protezione dei dati personali possa trovare una diversa assicurazione a seconda del titolare preso in considerazione (qui con l'aggravante che, se un titolare ha previsto, a mezzo di un atto amministrativo generale, di poter lecitamente comunicare dati personali ad un altro titolare, anche questo deve aver previsto di poterli ricevere).

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 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 54 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". La finalità è ampia, e non si riferisce dunque ai compiti del solo Servizio sanitario pubblico.

Sono trattamenti di dati direttamente finalizzati alla conoscenza piuttosto che, direttamente, alla cura, quand'anche della collettività, ed infatti l'art. 75 del Codice riferisce all'art. 9 par. 2 i) del Regolamento Generale il trattamento "per finalità di tutela della salute e incolumità fisica… della collettività".

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.

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.

Oblio

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

Il diritto all'oblio si sostanzia in effetti in un diritto alla cancellazione del dato, pur se, solitamente, relativa, ovvero riferita ad alcuni titolari, e dunque spesso traducibile in una limitazione del trattamento.

Il diritto all'oblio si confronta in particolare, 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 scriveva 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 in conformità all'articolo 9 paragrafi 2 lettere h e i) e dell'articolo 9 paragrafo 3, cioè in senso lato in ambito sanitario. Vero è che, in quest'ambito, il trattamento di alcuni dati può essere meramente accessorio, ed alla richiesta di cancellazione alcune informazioni (es. i dati di contatto) possono bene essere cancellate.

Oblio oncologico

La legge 7 dicembre 2023, n. 193 reca *Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche* definisce oblio oncologico il diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica limitatamente ad alcuni ambiti: l'accesso ai servizi bancari, finanziari, di investimento e assicurativi, in sede di indagini sulla salute dei richiedenti un'adozione e per l'accesso alle procedure concorsuali e selettive, al lavoro e alla formazione professionale.

La condizione di persona guarita da una malattia oncologica è attestata in un apposito certificato, redatto da una struttura sanitaria pubblica o privata accreditata, da un medico dipendente del Servizio sanitario nazionale nella disciplina attinente alla patologia oncologica di cui si chiede l'oblio, dal medico di medicina generale oppure dal pediatra di libera scelta. Esso è ottenibile può essere presentata decorsi 10 anni dalla conclusione del trattamento attivo, cioè dell'ultimo trattamento farmacologico antitumorale, radioterapico o chirurgico senza episodi di recidiva (potendo prevedersi termini inferiori di guarigione per specifiche patologie oncologiche).

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[iii].

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", 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".

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".

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.

Riassumendo: la persona fisica che tratta dati sotto l'autorità del titolare è qualificata persona *autorizzata* al trattamento proprio perché non ha autonome prerogative di trattamento, 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.
E' ovvio che un medico è autorizzato, in astratto, a trattare dati per finalità di cura: ma i mezzi e le modalità con cui può farlo sono nella disponibilità esclusiva del Titolare, che detta le regole con cui il

trattamento concretamente può essere effettuato. Ne consegue che ogni trattamento che ecceda oppure non rispetti l'ambito e le modalità di trattamento autorizzati attraverso le istruzioni è illecito, e comunque non riconducibile al Titolare, e può dunque essere direttamente imputato alla responsabilità della persona fisica che lo pone – scorrettamente – in essere, così come le eventuali conseguenti sanzioni.

La autorizzazione al trattamento concerne non solo una certa base dati, ma la finalità per la quale questa diventa accessibile: se un medico è autorizzato ad accedere alle cartelle di reparto per finalità di cura non lo è – come co-sperimentatore in uno studio – per quella di ricerca (trattandosi appunto di un trattamento diverso, diverso appunto per quanto riguarda lo scopo), così che per tale finalità occorrerà una specifica autorizzazione.

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.

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.

Si è visto 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 sorveglianza 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 (di fatto) del trattamento.

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 primis, le "finalità di medicina preventiva …, diagnosi, assistenza o terapia sanitaria" di cui all'art. 9 par. 2 lettera h e par. 3 del Regolamento Generale, e quindi le finalità "amministrative" di cui all'art. 9 par. 2 lettera g); se questo medico utilizza quei dati per propri scopi personali o utilizzando mezzi diversi da quelli messi a disposizione del Titolare, assume egualmente il ruolo di un Titolare di fatto, con tutte le responsabilità conseguenti.

Esempio: se un medico utilizza i dati personali raccolti per finalità di cura 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 qualificato 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 è autorizzata ad effettuare il trattamento.

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 evidenzia dunque 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).

Posta elettronica

All'interno dell'organizzazione del titolare, la trasmissione/accessibilità informatica di dati (direttamente o indirettamente identificativi) afferenti alle categorie particolari o relativi a condanne penali e reati dovrebbe ordinariamente realizzarsi attraverso strumenti/soluzioni informatiche dedicate (utilizzo dello stesso applicativo verticale, applicativi verticali diversi e operanti in collaborazione applicativa, piattaforme/spazi digitali condivisi etc..), con l'obiettivo di contenere l'informazione all'interno di un ambito predefinito, controllato e strettamente monitorabile attraverso i log di procedura. L'utilizzo del sistema di posta elettronica ordinaria del titolare (e-mail) dovrebbe considerarsi dunque soluzione residuale da porre in essere solo ove risulti indispensabile e con l'obbligo di attenersi alle seguenti modalità:

- divieto di riportare in chiaro nel corpo della mail contenuti riferibili a informazioni personali cd sensibili (dati particolari/relativi a condanne penali e reati)
- spedizione del documento contenente i dati personali in forma di allegato al messaggio e non come testo del messaggio
- l'allegato deve essere criptato e protetto da password (ad. es. file compresso zip e protetto da password) e la password deve essere comunicata al destinatario con canale diverso dalla mail (telefono, sms,fax etc.).

La comunicazione/trasmissione dei dati verso/da soggetti terzi rispetto all'organizzazione del titolare può avvenire, in presenza di idonea base giuridica:

- verso/da altro soggetto pubblico (altra azienda sanitaria, ente pubblico etc..);
- verso/da soggetto privato (MMG/PLS, struttura accreditata, fornitore etc);
- verso il paziente.

In caso di comunicazione con altri soggetti istituzionali, premesso che è preferibile attivare canali specifici di comunicazione mediante strumenti quali accesso via web e accesso in modalità di collaborazione applicativa, per comunicazioni la cui periodicità è limitata e la quantità dei dati è contenuta, utilizzare lo strumento di Posta Elettronica Certificata con l'obbligo di attenersi alle seguenti modalità:

- le informazioni devono essere inviate in forma di allegato al messaggio (e non come testo compreso nella body part del messaggio allegato contenente le informazioni) zippato e protetto da password;
- la password deve essere comunicata mediante un invio diverso e ulteriore rispetto a quello utilizzato per trasmettere i dati;
- deve essere prevista apposita procedura per interrompere l'invio per PEC a un destinatario che abbia comunicato il furto o lo smarrimento delle credenziali di autenticazione per l'accesso al proprio sistema di PEC o altre condizioni di possibile rischio per la riservatezza dei dati.

Nel caso di comunicazione verso/da soggetto privato (MMG/PLS, struttura accreditata, fornitore etc) i si individua, quale modalità ordinaria e corrente, lo strumento di Posta Elettronica Certificata con l'obbligo di attenersi alle modalità di cui al precedente punto.

Relativamente all'invio al paziente del referto o di altra documentazione sanitaria o comunque recante informazioni direttamente/indirettamente riferite al suo stato di salute, si evidenzia che, in presenza di idonea base giuridica, e fermo restando che sarebbe opportuno attivare soluzioni di cooperazione applicativa, la messaggistica elettronica è utilizzabile con le seguenti cautele:

- nel caso di invio tramite posta elettronica ordinaria
    - convalida dell'indirizzo mail esterno con procedura di verifica apposita in modo da impedire che il documento, anche se criptato, sia recapitato a soggetto diverso dall'interessato;
    - referto/documentazione spediti in forma di allegato a un messaggio e non come testo compreso nel corpo del messaggio;
    - allegato protetto con tecniche di cifratura e accessibili tramite una password per l'apertura del file consegnata separatamente all'interessato;
    - possibilità per il paziente di confermare l'indirizzo di posta elettronica cui ricevere l'invio in occasione di successivi accertamenti clinici;

- nel caso di invio tramite Posta Elettronica Certificata
    - convalida dell'indirizzo mail esterno con procedura di verifica apposita in modo da impedire che il documento, anche se criptato, sia recapitato a soggetto diverso dall'interessato;
    - referto/documentazione spediti in forma di allegato a un messaggio e non come testo compreso nel corpo del messaggio;
    - possibilità per il paziente di confermare l'indirizzo di posta elettronica certificata cui ricevere l'invio in occasione di successivi accertamenti clinici.

La necessità di assicurare una consulenza specifica nell'effettuazione di alcuni test genetici fa ritenere in tali casi possibili servizi di tele refertazione solo nel caso in cui l'interessato si sottoponga a tali indagini cliniche nell'ambito di un complessivo servizio di tele consulenza; in tal caso occorre seguire 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 del 5 giugno 2019, ovvero:

- utilizzo della Posta Elettronica Certificata;
- trasmissione dei dati in forma di allegato e - trasmissione dei dati in forma di allegato e non come testo compreso nel corpo del messaggio;
- cifratura dei dati avendo cura di rendere nota al destinatario la chiave crittografica tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati;

E' comunque vietato l'utilizzo della posta elettronica/Posta Elettronica Certificata per l'invio al paziente nei casi di accertamenti sull'HIV.

Privacy by default e privacy by design

Alla responsabilizzazione del titolare di conformare i trattamenti da esso effettuati a dati principi è consustanziale un onere della prova.

Tale assunto viene ribadito all'articolo 24, paragrafo 1 del Regolamento, intitolato alla "Responsabilità del titolare del trattamento" (Responsability of the controller") 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*: ciò si traduce senz'altro in un obbligo di valutazione e documentazione preventiva

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), tanto dal punto di vista della sua liceità che della sua sicurezza.

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.

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. Analisi dei Rischi ed eventuale *Valutazione d'impatto sulla protezione dei dati* e le istruzioni a Responsabili e persone autorizzate al trattamento. Con le prime, il Titolare valuta la liceità del trattamento e si predefiniscono le misure, tecniche ed organizzative che ne assicurano, più ampiamente, l'adeguatezza ed in particolare la sicurezza; 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.

Protezione dei dati personali

Tanto il Regolamento che il Codice, come d'altronde le disposizioni europee e 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*.

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 (soprattutto) 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*).

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 acquisite, connesse, fatte circolare, in generale "trattate", deriva l'esigenza di ampliare l'oggetto di una possibile tutela, rivendicando, quale indispensabile sviluppo di quell'*habeas corpus* - "abbi il [tuo] corpo", cioè, ti sia restituita la libertà personale - dal quale si è storicamente sviluppato appunto il diritto alla libertà personale, una sorta di *habeas data* – "abbi le informazioni" che ti riguardano, almeno nel senso che ti sia restituito il controllo su di esse - e qualificando la tutela rispetto al trattamento dei dati come un diritto fondamentale della persona, una componente essenziale della nuova cittadinanza.

Infatti, pur se spesso si parla di *data protection*, di protezione dei dati personali, occorre non dimenticare che la tutela non è diretta ai dati, se non strumentalmente, 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, la rubrica completa del Regolamento Generale, pur se spesso riassunto in Regolamento sulla protezione dei dati, è *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* ….

Così era naturalmente anche 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 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".

Dunque, la tutela riguarda i dati solo nella misura in cui la loro protezione è strumentale alla tutela della persona cui essi si riferiscono: la qual cosa induce anche a porsi la questione del 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, dalla presa d'atto, 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 essi possano essere utilizzati e circolare, come è loro essenziale, però solo secondo principi e regole trasparenti che assicurino la giusta tutela delle persone fisiche cui essi si riferiscono.

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. Inoltre, 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 una protezione che può prevalere su una sua opposta scelta: la nozione individualistica del diritto alla privacy deve dunque considerarsi oramai superata, a fronte di una tutela che si realizza attraverso una disciplina regolata, che un'autorità pubblica di controllo – il Garante per la protezione dei dati personali - implementa e sorveglia. Simmetricamente, viene meno l'utilizzo di strumenti di carattere contrattualistico, e segnatamente del consenso, che ha un ruolo sempre più residuale.

Pseudonimizzazione

Precisiamo anzitutto 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 in generale lo pseudonimo come un *alias* associato a dati personali.

La pseudonimizzazione - non *pseudo-anonimizzazione*, come si trova talvolta scritto (se il significato etimologico di *pseudo* è, genericamente, quello di "falso", volontario o meno, si capisce che associare tale qualificazione ad *anonimo*, ovvero "senza nome", ad intendere un nome falso ma assente, *pseudo/an*, è assurdo) consiste perciò nell'associare dei dati (es. quelli relativi alla salute riferibili ad un interessato) ad una informazione di carattere non identificativo, appunto uno pseudonimo, un *alias*, (in pratica, un codice), sostituendo con essa quella di carattere identificativo, ad es. il nome/cognome dell'interessato, e mantenendo riservata, con specifiche misure di sicurezza, la correlazione tra dato identificativo e dato non identificativo (tra anagrafica e codice). Essa è una operazione di trattamento che si traduce in una misura di sicurezza e di minimizzazione dei dati.

Il sopra citato Parere 05/2014 *Sulle tecniche di anonimizzazione,* precisava infatti 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".

Non ogni codificazione può tradursi in una pseudonimizzazione dei dati: non lo è certo l'utilizzo del codice fiscale (anche più identificativo del mero nome giuridico). Inoltre, se si crea un elenco, e questo ha una sua logica (ad es. alfabetica o cronologica), non è sufficiente togliere l'anagrafica ed inserire ad es. dei codici progressivi, occorre che siano non sequenziali e randomizzati (almeno se l'estrazione dei dati è eseguibile una seconda volta con identici risultati). Insomma, il codice di pseudonimizzazione non può contenere elementi oggettivi – siano essi informativi che di carattere procedurale – che rendano possibile una identificazione dell'interessato a prescindere dalla chiave di pseudonimizzazione.

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

Registri di patologia

Diversamente dai registri istituiti per previsione normativa (per scopi epidemiologici, di sorveglianza sanitaria e in generale di sanità pubblica), i cd. registri di patologia istituiti acquisendo il parere del competente Comitato etico si qualificano per una finalità di ricerca e trovano la loro base giuridica nell'art. 110 del Codice. Si tratta di basi di dati, relative ad una certa tipologia di pazienti che si legittimano dunque o attraverso il consenso oppure, se questo non può essere acquisito, con le modalità di cui all'art. 110 primo comma secondo periodo (parere positivo del competente Comitato etico e applicazione delle misure di garanzia proposte dal garante con Provvedimento del 9 maggio 2024).

Quel che preme evidenziare è che la legittimazione acquisita in tali modi si riferisce alla sola raccolta dei dati nel Registro, non al loro utilizzo per studi successivi che possano beneficiare di essi. Ogni singolo studio dovrà poi recuperare autonomamente le proprie condizioni di liceità (ancora: o con il consenso degli interessati o con le modalità sopra richiamate di cui all'art. 110 primo comma secondo periodo del Codice). L'Autorità Garante parla in tali casi di "consenso a fasi progressive"; in effetti, si tratta di un consenso (la considerazione vale anche per la base giuridica rappresentata dalla condizione di liceità rappresentata dal parere positivo del competente Comitato etico e dalla applicazione delle misure di garanzia) riferito a due diverse fasi della ricerca: la raccolta dei dati prima ("primo consenso"), il loro utilizzo in riferimento ad uno specifico protocollo di studio ("secondo consenso"): la condizione di liceità, insomma, deve ricercarsi ed attuarsi in riferimento ad ogni fase del processo, ognuna delle quali ha sì una propria autonomia ma è comunque funzionale alla realizzazione di un progetto di ricerca.

L'Autorità Garante ha evidenziato che una raccolta dati così legittimata per scopi di ricerca non può essere a tempo indeterminato: deve dunque prevedersi un termine, che può essere anche non breve ma deve essere comunque chiaramente determinato ed indicato nell'informativa.

Registri di patologia possono essere istituiti anche per finalità di cura, ovvero per la creazione di casistiche, come accade ad esempio nell'ambito delle malattie rare. La particolare modalità di gestione e condivisione delle informazioni su piattaforme informatiche – anche internazionali - consigliano l'acquisizione di un consenso come base giuridica aggiuntiva rispetto a quella, normalmente autosufficiente, prevista dall'art. 9 par 2 lettera h del Regolamento per la finalità di cura.

Responsabile del trattamento

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

Il termine *processor* – da *processing*, elaborazione, trattamento - era tradotto, nella versione italiana della Direttiva 46/95, come incaricato (la coppia controller/processor era 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:

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

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 organismo.*

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 è 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

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.

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 (la base giuridica che rende lecito il trattamento da parte del Titolare), qualora un responsabile non rispetti le condizioni per il trattamento dei dati quali prescritte 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 stessa 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	titolare	titolare	titolare

incaricato persone autorizzate	responsabile (interno e esterno) incaricati	responsabile persone autorizzate	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.

Responsabile della Protezione dei Dati (DPO)

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

Già la Direttiva 46/95 prevedeva ai Considerando 49 e 54 la possibilità che il titolare (allora "Responsabile") individuasse un "incaricato della protezione dei dati" ("data protection official"), cui sarebbe stato demandato, ai sensi dell'art. 18 par. 2 "di assicurare in maniera indipendente l'applicazione interna delle disposizioni nazionali di attuazione della presente direttiva" e "di tenere un registro dei trattamenti effettuati dal responsabile del trattamento". Era una figura non obbligatoria, che pure ha trovato attuazione nel Privacy Officier presente in alcuni paesi europei, e che ha analogie con il nostro risalente Referente Privacy; la differenza è che tale figura, con il Regolamento,Generale, 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 DPO ed i suoi compiti il gruppo europeo dei Garanti ha emesso delle linee guida (d'ora in avanti: Linee guida sul DPO).

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 , 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.

Responsabilizzazione/Accountability

Nel parere 3/2010 il Gruppo dei Garanti ex art 29 della Direttiva 95/46/UE, richiamando un proprio precedente documento del dicembre 2009, aveva evidenziato come il quadro giuridico derivato dalla Direttiva 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:

- un primo livello costituito da un obbligo di base vincolante per tutti i responsabili del trattamento (e comprensivo di due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove);
- un secondo livello che include sistemi di responsabilità di natura volontaria eccedenti gli obblighi vigenti, tali da fornire garanzie più elevate di quelle prescritte, in termini di modalità di attuazione oppure 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).

L'art. 5 del Regolamento (*Principi applicabili al trattamento di dati personali*, cd. principi base del trattamento) al par. 1 prescrive analiticamente alcuni principi la cui attuazione è richiesta per assicurare l'adeguatezza del trattamento; la *responsabilizzazione* del Titolare (art. 5 par. 2) consiste appunto 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»);
> 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»

Dunque, il titolare del trattamento è responsabile del rispetto dei seguenti principi, che poi sono, nel presente testo, analizzati 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).

Il trattamento, per essere conforme ai principi del Regolamento, sarà dunque: limitato ad una finalità determinata, esplicita e legittima, lecito, corretto, trasparente, effettuato utilizzando solo dati pertinenti, non eccedenti, esatti e aggiornati, conservati per un periodo di tempo limitato e gestiti con idonee misure di sicurezza.

Si noti: 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 necessari; il Regolamento, possiamo dire, è informato ad un generale *principio di necessità/indispensabilità*.

Dunque (cfr. Considerando 74-75) il titolare del trattamento:

- è responsabile di ogni trattamento da esso effettuato (anche attraverso soggetti terzi);
- deve valutare ed accertare la complessiva liceità e conformità del trattamento al Regolamento;
- deve implementare misure adeguate ed efficaci per garantire tale conformità;
- deve individuare i possibili rischi del trattamento per gli interessati e valutarne l'entità e la probabilità in riferimento alla natura, all'ambito di applicazione, al contesto ed alla finalità del trattamento stesso, mettendo a punto misure in grado di ridurli;
- deve documentare le proprie valutazioni circa l'adeguatezza conclusiva del trattamento.

Da un principio di maggior responsabilizzazione del Titolare consegue anche che con il Regolamento l'intervento delle autorità di controllo è 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 (unica significativa eccezione, la consultazione preventiva di cui all'art. 36 del Regolamento).

Riassumendo, il Regolamento pone una serie di principi 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.

Scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico da parte di soggetti terzi

Al "Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici" è dedicato l'art. 110 bis del Codice.

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", rubricata "Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici":

> 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 parlava 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 escludeva il trattamento di dati genetici.

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.

Comparando l'art. 110 con l'art. 110 bis si osservano immediatamente due caratteri distintivi di quest'ultimo:

- 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*;
- dal punto di vista soggettivo, l'art. 110 bis riguarda i soggetti "terzi" (*Trattamento ulteriore da parte di terzi).*

Circa quest'ultimo punto, 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 di una Università, qualora volesse condurre in proprio uno studio utilizzando i dati dell'Azienda sanitaria con la quale è integrata.

La soluzione prospettata nel 110 bis comporta un intervento del Garante: si parla precisamente di *autorizzazione* del Garante, proprio spendendo quel termine (*unicum*, riferito al Garante, nell'attuale redazione del Codice), per di più con la risalente tempistica dei 45 giorni; 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 (d'altronde, lo studio non coinvolgerebbe il titolare se non come una sorta di database); 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.

L'art. 110 bis 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, per alcuni interpreti, dovrebbe 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 evidenza 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, anche 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 propria titolarità del trattamento.

Se riferiamo i primi tre commi dell'articolo 110 bis ai trattamenti, da parte di terzi, per finalità ulteriori di dati raccolti da un diverso soggetto, si capisce l'incipit del comma 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.

A seguito delle FAQ messe a disposizione dal Garante nel giugno 2024, la norma deve interpretarsi 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* …

Qui i dati da utilizzare per scopi di ricerca da parte degli IRCCS sono solo i dati clinici raccolti dagli stessi IRCCS.

La norma, in sostanza, ci dice che l'attività di ricerca, per gli IRCCS, non comporta un trattamento per una finalità ulteriore e secondaria, ma per una finalità qualificabile come primaria tanto quanto quella di cura (trattandosi di istituti che curano ma caratterizzati da una peculiare connotazione "sceintifica")

Tale soluzione - che assicura 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) – richiedere comunque di perdere il riferimento ai terzi, che in tal caso proprio non verrebbero in causa: trattamento ulteriore sì, ma non da parte di terzi. E' evidente che tale comma avrebbe trovato una più idonea collocazione nell'art. 110.

La disposizione è riconducibile alla previsione dell'art. 110 comma 1 primo periodo, che consente una deroga al generale obbligo di consenso "quando la ricerca è effettuata in base a disposizioni di legge"; ne segue, come per quella fattispecie, l'obbligo della pubblicazione della DPIA. Riassumendo:

- i primi 3 commi dell'art. 110 bis concernono il trattamento ulteriore (il riutilizzo) di dati personali, da parte di soggetti terzi (rispetto a chi ha raccolto i dati per scopi di cura) 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;
- il comma 4 è relativo ai soli IRCCS, per i quali il riutilizzo non deve qualificarsi come "trattamento ulteriore", cioè per una finalità secondaria rispetto a quella primaria di cura; essendo trattamenti così qualificati dalla legge – lo stesso art. 110 bis – ciò richiede comunque di adempiere agli obblighi previsti dal primo comma dell'art. 110 comma 1 per i progetti di ricerca per il quali "il consenso …non è necessario", ovvero condurre e rendere pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento (oltre ad una informativa ex art. 14 del Regolamento, come da previsione delle Regole deontologiche).

Nel caso di studi multicentrici promossi da un IRCCS, i centri satelliti, ancorché titolari del trattamento, acquisiscono – rispetto all'obbligo di consenso - le medesime prerogative del promotore.

Scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico

Il Regolamento prevede, per la ricerca scientifica in senso ampio, una base giuridica comune, rappresentata dall'art. 9 par. 2 lettera j). Tale base giuridica non è sempre, da sola, sufficiente.

Anzitutto, l'art. 9 par. 4 del Regolamento consente ai legislatori nazionali di poter "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici… o dati relativi alla salute". Inoltre, l'art. 9 par. lettera j) del Regolamento richiama anch'esso una integrazione normativa nazionale, nei seguenti termini:

> il trattamento è necessario a fini … di ricerca scientifica … in conformità dell'articolo 89, paragrafo 1, *sulla base del diritto* dell'Unione o *nazionale*, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Insomma, l'art. 9 par. 4 del Regolamento riconosce al legislatore nazionale prerogative di intervento in riferimento alle tipologie di dati trattati, l'art. 9 par. 2 lettera j) in riferimento alla finalità (in questo caso, di ricerca scientifica).

Si precisa che il dettato dell'art. 9 par. 2 lettera j) quando introduce la relativa "che è proporzionato alla finalità perseguita…" (nel testo inglese "which shall be proportionate to the aim pursued …") non riconduce tale obbligo al trattamento, ma proprio al "diritto dell'Unione o nazionale".

Non è dunque possibile fare riferimento al solo art. 9 par. 2 lettera j) del Regolamento quale condizione di liceità per quei trattamenti, con la conseguente necessità di una base giuridica ulteriore, che è poi, ordinariamente, il consenso dell'interessato.

Così è appunto previsto dall'art. 110 del Codice, per il quale "Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando …", il che significa che è sempre necessario, tranne eccezioni.

Non sempre uno studio che tratta dati sanitari è qualificabile come studio in campo medico, biomedico o epidemiologico, determinando l'applicazione delle prescrizioni dell'art. 110 del Codice. Quest'ultimo si applica appunto, quale *lex specialis*, solo alla ricerca scientifica in tale ambito: se una ricerca non rientra in tale fattispecie, ma si tratta genericamente di una ricerca scientifica che anche utilizzi dati sanitari (ad es. una ricerca di carattere sociologico o antropologico sulla medicina popolare), ne segue che non può essere inquadrata nell'art. 110.

In tali casi, una prescrizione circa la modalità di legittimazione al trattamento è direttamente offerta dal Garante (che, ai sensi dell'art. 2-quater del Codice, è legittimato ad adottare regole deontologiche, il cui

rispetto "costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali", e che vengono pubblicate in Gazzetta). Nelle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*, laddove all'art. 7 comma 2 "I soggetti di cui all´art. 2, comma 1, possono trattare categorie particolari di dati personali per scopi statistici e scientifici quando: a) l´interessato ha espresso liberamente il proprio consenso sulla base degli elementi previsti per l´informativa…". La regola, in generale, è dunque la medesima, tanto per la ricerca scientifica in generale che per quella in ambito clinico, traslando di fatto il principio del "consenso informato" da questa a quella, dunque anche a tipi di attività di ricerca molto lontani da quelli in ambito medico. E si può osservare, in generale, che certi ambiti di ricerca qualitativa, spesso induttiva e fondati su una epistemologia della scoperta, processuale, piuttosto che su una epistemologia della progettazione, mal si accordano, proprio da un punto di vista strutturale, sulla privacy by design.

Cosa si intende comunque per ricerca in ambito medico? Già nel provvedimento 52/2008 Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali, si distingueva la ricerca clinica da studi che:

> non siano strettamente associati ad attività di tutela della salute svolte da medici o organismi sanitari, ovvero - a differenza delle sperimentazioni cliniche sui medicinali - non possano ritenersi comparabili a tali attività in termini di ricaduta personalizzata sull'interessato.

I criteri di qualificazione di uno studio nell'ambito della ricerca medica o clinica sono dunque i due seguenti, anche in alternativa:

- studi che sono strettamente associati ad attività di tutela della salute svolte da medici o organismi sanitari;
- studi che possano ritenersi comparabili alle sperimentazioni cliniche sui medicinali in termini di ricaduta personalizzata sull'interessato.

Il Garante è rimasto fedele a questa impostazione, come è stato confermato anche da recenti Provvedimenti (ad es. le *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica* sopra richiamate, all'art. 2 comma 2).

La maggior parte degli studi osservazionali su dati sanitari, se non possono ritenersi "comparabili alle sperimentazioni cliniche sui medicinali in termini di ricaduta personalizzata sull'interessato", devono evidentemente valutarsi per lo più come "strettamente associati ad attività di tutela della salute svolte da medici o organismi sanitari"; diremo che sono studi che si svolgono in un contesto clinico.

Sono però sempre più numerose le ricerche che utilizzano dati sanitari per testare la funzionalità di algoritmi; in questi casi, vi sono due possibilità: sostenere che ci troviamo di fronte a trattamenti che, per la preminente importanza degli aspetti informatico-matematici, non sono "strettamente associati ad attività di tutela della salute svolte da medici o organismi sanitari" e dunque non rientrano tra gli studi

clinici, anche se trattano dati relativi alla salute; oppure che il fatto stesso di utilizzare dati sanitari che nascono in un contesto clinico e sono utilizzati per addestrare strumenti che saranno alfine deputati a elaborare dati sanitari con lo scopo ultimo di mettere a disposizione elementi di supporto alla cura, consiglia di considerali, già adesso come "strettamente associati ad attività di tutela della salute". La stessa ragione potrebbe essere addotta per il fatto di aver voluto ricomprendere nella finalità anche la ricerca epidemiologica. Riteniamo di dover propendere per tale ultima opzione.

Esaminiamo adesso analiticamente il testo dell'art 110 comma 1 del Codice; il terzo periodo di tale comma è stato recentemente oggetto di modifica da parte della L. 56/2024 (si evidenzia anche la precedente versione, barrata):

Periodo 1

> Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando 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, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

Periodo 2

> 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.

Periodo 3

> 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~~. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice.

Il comma è impostato in negativo, come previsione di una serie di eccezioni (primo periodo: "non è necessario", secondo periodo: "non è inoltre necessario") rispetto ad una condizione presunta, appunto, come ordinariamente necessaria. Quel che in determinate situazioni non è necessario è appunto "Il

consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico". Ciò significa dunque che il consenso è la base giuridica ordinaria per il trattamento di dati personali a scopo di ricerca clinica, fatte salve le seguenti eccezioni:

- "quando 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";
- "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"

Nel primo caso (periodo 1), appare ovvio che si tratta di studi che hanno quella particolare copertura normativa proprio perché si ritiene evidentemente necessario ampliare al massimo la casistica utilizzabile evitando il *bias* rappresentato dal dissenso degli interessati, e non ci si pone dunque la questione se l'interessato sia o meno contattabile (anche ai pazienti contattabili, dunque, non dovrebbe essere richiesto il consenso al trattamento). Non è in causa tanto la quantità dei dati da raccogliere, quanto la loro qualità, nel senso della completezza (si precisa, per quanto riguarda "la ricerca … effettuata in base …al diritto dell'Unione europea", che non tutti i progetti che hanno una copertura UE vi possono rientrare; vi rientra invece, ad es. il programma Horizon, che è istituito attraverso una serie di atti normativi del Parlamento Europeo e del Consiglio).

Nel secondo caso (periodi 2 e 3), 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.

Una volta accertata la sussistenza di tali situazioni, il trattamento non può ancora essere lecitamente avviato, essendo necessari ulteriori adempimenti.

Quando cioè la ricerca è effettuata in base a disposizioni di legge o di regolamento ecc.":

- "è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento".

"*Q*uando … 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";

- si applicano le misure di garanzia individuate dal Garante.

Tali "misure di garanzia" sono state offerte con un Provvedimento del 9 maggio 2024.

La precedente versione del terzo periodo del primo comma dell'art. 110 del Codice prevedeva l'obbligo ("e deve essere sottoposto …") della consultazione preventiva del Garante; il richiamo era generico all'art. 36 del Regolamento. Considerato che ordinariamente, ai sensi dell'art. 36 par. 1 del Regolamento, la Consultazione preventiva del Garante è una prerogativa del Titolare, che "consulta l'Autorità di controllo qualora la valutazione d'impatto … a norma dell'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento pe attenuare il rischio", pareva qui doversi richiamare piuttosto all'eccezione rappresentata dal par. 5 dell'art. 36, secondo il quale:

> Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica

Le Misure di garanzia di cui al Provvedimento del 9 maggio 2024 prevedono che il titolare rispetti i seguenti obblighi:

> … il titolare del trattamento oltre ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca come previsto dall'art. 110 del Codice, deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando altresì i ragionevoli sforzi profusi per tentare di contattarli. Nei predetti casi, i titolari del trattamento di dati sulla salute per finalità di ricerca medica, biomedica e epidemiologica riferiti a soggetti deceduti o non contattabili devono altresì svolgere e pubblicare la valutazione di impatto, ai sensi dell'art. 35 del Regolamento, dandone comunicazione al Garante.

La "comunicazione al Garante" sembra dover riguardare non tanto, direttamente, la valutazione di impatto, quanto il fatto della sua pubblicazione, e si realizzerà dunque trasmettendo al Garante stesso il link della avvenuta pubblicazione della valutazione sul sito istituzionale.

Allo stato attuale, 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, dunque 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, nonché la sua diffusione (la valutazione d'impatto è "resa pubblica"). Nell'ambito della ricerca clinica, perciò:

assenza di consenso > valutazione di impatto > sua diffusione

Il consenso al trattamento dei dati personali nell'ambito della ricerca deve essere preventivo, specifico (ossia riferito ad un singolo progetto di ricerca, redatto conformemente alla norme di settore), libero, informato (ossia preceduto da idonea informativa sul trattamento), espresso, inequivocabile, reso o documentato per iscritto e sempre revocabile.

***

Lo studio osservazionale retrospettivo rappresenta un 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). 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 …

La distinzione tra finalità primarie e secondarie significa, in breve, 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 appunto 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 cioè condizioni e presupposti) distinte.

Si ricorda che, 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; la questione affrontata nell'art. 110 comma 1 secondo e terzo periodo era così risolta dalla precedente versione dell'art. 110 comma 1 secondo periodo:

> 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, il trattamento fosse valutato come lecito e la ricerca potesse senz'altro avviarsi.

La precedente redazione 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 D.Lgs. 101/2018 ha abrogato l'art. 40 del Codice, circa la possibilità di procedere ad Autorizzazioni Generali. La Autorizzazione Generale n. 9 (2012/2014/2016), relativa al trattamento dei dati personali effettuato per scopi di ricerca scientifica, non è dunque più valida.

L'art. 21 del d.lgs. n. 101/2018 ha demandato al Garante il compito di individuare, con proprio provvedimento di carattere generale le prescrizioni, contenute nelle autorizzazioni generali a suo tempo adottate, che risultassero compatibili con le disposizioni comunitarie. Tale provvedimento è poi stato il *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati* …; l'allegato n. 5 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 magari il suo opposto. Alcune indicazioni, già richiamate nelle Autorizzazioni con scopo appunto autorizzatorio, sono adesso recuperate in un diverso contesto, cioè per una finalità prescrittiva.

La Autorizzazione n. 9, nel caso dei pazienti con contattabili, consentiva il trattamento dei dati; la Prescrizione, invece, chiede di specificare ed articolare, 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". Ciò attestato, non si procede immediatamente al trattamento, ma occorre adempiere ad alcuni obblighi.

Il Provvedimento 146/2019 non reca una deroga rispetto alle disposizioni contenute nell'art. 110, limitandosi ad indicare i presupposti che consentono di accedere alle fattispecie indicate nel terzo periodo del primo comma dell'art. 110: venendo meno tali presupposti il trattamento non potrà essere effettuato. Inoltre dispone circa ulteriori adempimenti che sono immediatamente conseguenti:

> 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.

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.

Qual è la differenza rispetto alle altre fattispecie indicate nel secondo periodo del comma 1 dell'art. 110? In questo caso, informare, se non l'interessato, qualcuno a lui prossimo - in accordo con il principio di carattere generale dettato dall'art. 82 comma 2 del Codice, per il quale, 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" – è possibile. Questa disposizione, nella precedente versione dell'articolo, riguardava anche il consenso, riferimento adesso venuto meno (ma recuperato secondo le modalità di cui all'art. 22 comma 11 del D.Lgs. 101/2018, per il quale "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, … 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, …).

A questa fattispecie non si applicano le Misure di garanzia di cui al Provvedimento del 9 maggio 2024, in quanto riferite a soggetti deceduti o non contattabili per motivi etici (riconducibili alla circostanza che l'interessato ignora la propria condizione) o organizzativi.

Ulteriori prescrizioni, nel caso che i dati non siano raccolti in un rapporto diretto con l'interessato – cioè quando gli interessati o non sono contattabili o non debbano essere contattati – in breve quando ci troviamo nella situazione che comporta la redazione di una informativa ex art. 14 del Regolamento, derivano 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".

In effetti, le Regole Deontologiche non si applicherebbero agli studi clinici. Anche in riferimento a questi, comunque, si è visto che vi sono situazioni in cui "i dati sono raccolti presso terzi", ed il Garante chiede che si proceda a rendere disponibile una informativa ai sensi dell'art. 14 del Regolamento in riferimento agli interessati non contattabili o non contattati. Si evidenzia che il Garante intende tali soggetti estensivamente, nel senso del dovere di attivarsi anche relativamente ai deceduti, in questo caso per poter informare eventuali terzi legittimati ex art. 2-terdecies del Codice; tale obbligo viene normalmente espletato, qualora riguardi dati detenuti dall'Azienda, mediante pubblicazione dell'informativa sul sito istituzionale.

Circa, in particolare, i dati personali dei deceduti, alcuni interpreti sostengono che questi non rientrino nelle competenze del Garante e che siano pertanto liberamente utilizzabili. In effetti, per il Considerando n. 27 del Regolamento

> Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme ("rules") riguardanti il trattamento dei dati personali delle persone decedute.

L'art. 2-terdecies del Codice si limita in effetti a disciplinare la sola fattispecie i diritti della persona deceduta (artt. 15-22 del Regolamento, cioè diritto di accesso, rettifica, oblio, limitazione ecc.). La previsione circa i dati dei pazienti deceduti è però nelle Prescrizioni, al § 5.3:

> le seguenti prescrizioni concernono anche il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nello studio: *deceduti* o non contattabili.

Si tratterebbe dunque di sostenere non solo che una serie di provvedimenti del Garante, adottati in applicazione delle Prescrizioni, sono illegittimi, ma che alle stesse Prescrizioni non deve essere riconosciuto valore "normativo" o che sono illegittime esse stesse, nel senso che la valutazione effettuata dal Garante ai sensi dell'art. 21 comma 1 del D.Lgs. 101/2018, nell'individuare "le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere *c)* ed *e)* , 9, paragrafo 2, lettera *b)* e 4, nonché al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento", è errata. E' ovvio che si tratta di una posizione alquanto temeraria.

Si è recentemente evidenziato un deciso riposizionamento di alcuni Sponsor 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, gli Sponsor tendevano a rifiutare la qualificazione di titolari del trattamento, sostenendo che essi 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, lo Sponsor propone invece di qualificare la relazione con il Centro di sperimentazione nei termini di un rapporto tra titolare (lo Sponsor) 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 dello Sponsor, non riconoscendo evidentemente al Centro di sperimentazione alcun ruolo nel trattamento dei dati.

Si giustifica 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; 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*[iv].

L'argomentazione è dunque la seguente: se il titolare del trattamento è 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 allo Sponsor, ed il ruolo dello Sperimentatore deve essere recuperato dalle prerogative di questi, e non potrà essere che quello di Responsabile.

La esclusiva titolarità dello sponsor si costituisce dunque in rapporto al ruolo svolto (o non svolto) dal *prestatore di assistenza 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 protocollo di studio, si procederà a pseudonimizzare i dati necessari allo studio, ed a metterli a conoscenza dello sponsor in tale modalità. 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.

Circa questa impostazione, occorre, a mio avviso, non dimenticare che quella di titolare è una nozione *di fatto* finalizzata ad una attribuzione di responsabilità, e che in quanto tale non può che riguardare una situazione *attuale* e non meramente ipotetica, che riguarda chi tratta o ha comunque già adesso i titoli per trattare i dati, piuttosto che chi ha intenzione di trattarli esplicitando un proprio interesse verso di essi ed indicando le modalità procedurali, le modalità, con cui soddisfare tale interesse.

Possiamo dunque definire il titolare nell'ambito della ricerca come quel soggetto che attualmente tratta o comunque già attualmente possiede le prerogative, i titoli per poter trattare certi dati per realizzare un determinato studio, secondo modalità da esso determinate o comunque condizionate o condivise: presupposto per tale qualificazione è dunque che quel soggetto possieda già adesso i titoli per perseguire quella finalità.

Comunque, fin quando effettivamente non ha la disponibilità, il possesso dei dati, o comunque non possieda già adesso i titoli per vantare tale ruolo, il Titolare non è Titolare di nulla, se non, al limite, di una aspirazione alla titolarità.

Ed infatti, 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 appunto ha la disponibilità, il possesso di quei dati.

Insomma, il Promotore di uno Studio non diventa Titolare del trattamento nel momento in cui idea uno studio e lo propone. Si richiama allo scopo il Provvedimento del Garante del 24 febbraio 2022: "La circostanza che un soggetto terzo, … chieda a un titolare … di effettuare operazioni di trattamento su dati personali rispetto ai quali quest'ultimo è titolare, indicandone anche le modalità, non comporta … l'automatica attribuzione della titolarità in capo al richiedente, né tantomeno la perdita della titolarità da parte del soggetto che legittimamente detiene i dati. (…). Diversamente opinando, si determinerebbe il paradosso secondo cui chiunque richiedesse a un titolare di effettuare operazioni di trattamento sulle banche dati di quest'ultimo, ne diverrebbe automaticamente titolare".

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 di specie 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 alcune proposte contrattuali si esplicita una distinzione 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", specifica il testo italiano), 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 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 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 o dà ad altri l'incarico di pseudonimizzarli per proprio conto, può essere soltanto quel soggetto che già può 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 fatto di dimenticare questo assunto – ovvero che, nella protezione dei dati, la finalità, e la relativa base giuridica, hanno una centralità fondamentale – consegue che ci viene proposta una situazione nella quale il sedicente titolare avrebbe una minore profondità d'accesso del proprio responsabile, che pure da quello dovrebbe derivare tutte le sue prerogative: lo Sponsor accede infatti solo ai dati pseudonimizzati, (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 allo Sponsor). 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.

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 può 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 studio; 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).

In assenza del consenso degli interessati, i campioni biologici prelevati e i dati genetici raccolti per scopi di tutela della salute possono essere conservati e utilizzati per finalità di ricerca scientifica o statistica nei seguenti casi:

- indagini statistiche o ricerche scientifiche previste dal diritto dell'Unione europea, dalla legge o, nei casi previsti dalla legge, da regolamento;
- limitatamente al perseguimento di ulteriori scopi scientifici e statistici direttamente collegati con quelli per i quali è stato originariamente acquisito il consenso informato degli interessati.

Il secondo punto non riguarda dati e campioni già raccolti per scopi di ricerca, ma per finalità di cura. Dunque, il riferimento è agli scopi scientifici sottesi al trattamento per finalità di cura, nel caso cioè la ricerca sia impostata in modo tale da rivelare informazioni immediatamente utili per la cura (ovviamente di pazienti con casistiche analoghe). In effetti, sarebbe più logico riferirlo a dati già raccolti per scopi di ricerca: utilizzabili per una ricerca ulteriore direttamente collegata alla precedente senza ulteriori condizioni, presenti invece (una ricerca di analoga finalità non può essere realizzata mediante il trattamento di dati riferiti a persone dalle quali può essere o è stato acquisito il consenso informato e: aa) il programma di ricerca comporta l'utilizzo di campioni biologici e di dati genetici che in origine non consentono di identificare gli interessati, ovvero che, a seguito di trattamento, non consentono di identificare i medesimi interessati e non risulta che questi ultimi abbiano in precedenza fornito indicazioni

contrarie; bb) ovvero il programma di ricerca, preventivamente oggetto di motivato parere favorevole del competente comitato etico a livello territoriale, è sottoposto a preventiva consultazione del Garante ai sensi dell'art. 36 del Regolamento (UE) 2016/679) se il progetto di ricerca è diverso da quello originario.

Scopi di ricerca storica

Al trattamento di dati personali per "scopi storici" sono dedicati l'art. 89 del Regolamento UE 2016/679, gli artt. 99 e 101-103 del Codice, nonché le *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101*, adottate dal Garante per la protezione dei dati personali il 19 dicembre 2018.

Anzitutto, ai sensi dell'art. 89 par 1 del Regolamento, il trattamento a fini di ricerca storica è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, che assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Ricordo che il principio di minimizzazione richiede, ai sensi dell'art. 5 par. 1 lettera c) del Regolamento, che i dati siano "adeguati, pertinenti e limitati rispetto alle finalità per le quali sono trattati", e preciso inoltre che la normativa nazionale tutela anche il diritto alla protezione dei dati personali del defunto.

Il trattamento di dati personali effettuato per scopi storici, ai sensi dell'art. 99 del Codice, è considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati, e può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

Ai sensi dell'art. 101 comma 2 del *Codice*, i documenti contenenti dati personali, trattati per scopi storici, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.

L'art. 102 comma 2 b) rimanda per una dettagliata regolamentazione, alle *Regole deontologiche* adottate dal Garante, in particolare per le cautele da garantire per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse debba essere informato dall'utente della prevista diffusione di dati.

L'art. 103, in relazione alla consultazione dei documenti conservati negli archivi storici degli enti pubblici, rimanda a sua volta alla disciplina dettata dal D.Lgs. 22.06.2004 n. 42 *Codice dei beni culturali e del paesaggio*. Il Capo 3 (art. 122-127) del Titolo II Sezione 2 del *Codice dei beni culturali* è rubricato *Consultabilità dei documenti degli archivi e tutela della riservatezza*. Ai sensi dell'art. 126 comma 3 del Codice dei beni culturali, inoltre, "La consultazione per scopi storici dei documenti contenenti dati personali è assoggettata anche alle disposizioni del codice di deontologia e di buona condotta previsto dalla normativa in materia di trattamento dei dati personali".

Le *Regole deontologiche* del 19 dicembre 2018 (che sostituiscono il precedente *Codice di deontologia e di buona condotta)* richiamano appunto l'art. 122 del *Codice dei beni culturali* dettando disposizioni per i trattamenti di dati personali effettuati per scopi storici in relazione ai documenti (per *documento* intendendosi "qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali") conservati

presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico, in particolare prescrivendo principi-guida di comportamento per l'accesso ai documenti conservati , nei riguardi tanto degli archivisti (per *archivista* intendendosi "chiunque, persona fisica o giuridica, ente o associazione, abbia responsabilità di controllare, acquisire, trattare, conservare, restaurare e gestire archivi storici, correnti o di deposito della pubblica amministrazione, archivi privati dichiarati di notevole interesse storico, nonché gli archivi privati"), che degli utenti (è definito *utente* "chiunque chieda di accedere o acceda per scopi storici a documenti contenenti dati personali, anche per finalità giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero").

Premesso, ai sensi dell'art. 10 comma 1 delle *Regole deontologiche*, che "L'accesso agli archivi pubblici è libero" e che "Tutti gli utenti hanno diritto ad accedere agli archivi con eguali diritti e doveri", il comma 2, richiamando appunto l'art. 122 del Codice dei beni culturali, precisa che, tra gli altri, fanno eccezione, ai sensi delle leggi vigenti quelli contenenti i dati di cui agli artt. 9, par. 1, e 10 Regolamento (categorie particolari di dati e dati relativi alle condanne penali e ai reati), che divengono liberamente consultabili quaranta anni dopo la loro data, mentre il termine è di settanta anni se i dati sono relativi alla salute ovvero alla vita o all'orientamento sessuale oppure rapporti riservati di tipo familiare.

Particolare attenzione deve essere prestata al principio della pertinenza e all'indicazione di fatti o circostanze che possono rendere facilmente individuabili gli interessati.

Ai sensi dell' art. 11 comma 2 delle Regole deontologiche, nel far riferimento allo stato di salute delle persone l'utente si astiene dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad una determinata persona identificata o identificabile.

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 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 Codice di condotta della Regione Veneto prevede l'istituzione di un ufficio – lì denominato *Centro elaborazione data-set* – al quale appunto il professionista inoltra le richieste di dati per finalità didattiche o di formazione professionale. Il Centro crea il data-set di interesse, gli assegna un codice, e se, per la tipologia di informazioni raccolte, non se ne può assicurare la compiuta anonimizzazione, chiederà il consenso all'interessato all'utilizzo di quei dati, non anonimi ma semplicemente non direttamente identificativi.

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.

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.

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 18 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 ("purely personal or household activity and thus with no connection to a professional or commercial activity"). 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.

Il Considerando 12 della Direttiva 46/95 esemplificava tale ambito di attività a carattere personale o domestico in riferimento a "la corrispondenza o la raccolta di indirizzi".

La notazione "personale o domestico" deve dunque 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)[v]. 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.

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 non riguardano solo gli aspetti tecnici ma al contempo misure tecniche e organizzative, e 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 si parla conseguentemente solo di misure adeguate – individuate come tali dal Titolare - e non più di misure minime di sicurezza, normativamente stabilite (come già nel Codice); 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.

Titolare del trattamento

Ai sensi dell'art. 4 7) 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 anzitutto 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).*

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);
- 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; nella 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);
- il soggetto sul quale ricadono le decisioni di fondo relativamente alle finalità e ai mezzi del trattamento dei dati personali, nonché la responsabilità generale sui trattamenti posti in essere dallo stesso o da altri "per [suo] conto" (Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale – settembre 2023)

Precisiamo che, secondo la definizione corrente, per *finalità* può intendersi "un risultato atteso o al quale attendono le azioni pianificate" (in breve, uno scopo pratico) e per *mezzi* "la modalità con la quale si ottiene un risultato o si raggiunge un fine"[vi].

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 o tratterà) 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), né la persona fisica che, nell'ambito della organizzazione del titolare, svolge una attività a favore di questi (la persona autorizzata al trattamento).

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, che sovrintende complessivamente al relativo processo, determinandone l'attivazione e la continuazione per dati scopi (propri) e secondo certe modalità; a tale "controllo" consegue la responsabilizzazione di chi lo esercita, e ciò anche quando l'attività è delegata ad altro soggetto.

Sorge immediatamente un quesito: un Titolare si qualifica come tale, in riferimento ad un certo trattamento, dal momento in cui effettua concretamente quel trattamento, oppure già quando soltanto, in riferimento ad un proprio interesse, decide di effettuarlo (ma senza averlo ancora attivato)?

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 trattare i dati - e non "trattarli lecitamente" o "avendo titolo o competenza a trattarli" – per una finalità da esso assunta ed utilizzando mezzi del trattamento da esso stesso determinati: chi tratta dati personali - o meglio, chi svolge, nel proprio interesse (il che, per un ente pubblico, significa soprattutto, *per realizzare le proprie finalità istituzionali*) una attività che comporta il trattamento di dati personali - è, per ciò solo, qualificabile come titolare di quel trattamento.

Quella di Titolare è inoltre una nozione che ha 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.

Ai fini dell'attribuzione della titolarità di un trattamento, anche in base al principio di legalità, è comunque necessario valutare la sussistenza di una idonea base giuridica che conferisca a tale soggetto il compito di svolgere il trattamento, non potendo questi assumere automaticamente le prerogative del titolare sulla base di un mero presupposto fattuale, come, ad esempio, la realizzazione di un progetto che appunto prevede il trattamento dei dati personali. I titolari saranno tali, anzitutto, di fatto, per la sola ragione di trattare dati per i propri interessi, ma 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, formalmente, 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), anche non lecite, senza poi assumersi le conseguenti responsabilità.

Essendo una nozione di fatto, quella di titolare è una qualificazione che non può che riguardare una situazione effettiva, attuale: il titolare è tale se, adesso, effettivamente controlla il trattamento, ovvero lo determina, anche se il trattamento non è ancora iniziato o se i dati non sono ancora per esso disponibili. Possiamo, per illustrare tale interpretazione, richiamare due pronunce.

Una, in realtà, è relativa alla nozione di contitolarità, ma è comunque utile allo scopo. Le Linee Guida EDPB 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. Simmetricamente, così si è espresso il Garante nel Provvedimento del 24 febbraio 2022:

> La circostanza che un soggetto terzo, … chieda a un titolare … di effettuare operazioni di trattamento su dati personali rispetto ai quali quest'ultimo è titolare, indicandone anche le modalità, non comporta … l'automatica attribuzione della titolarità in capo al richiedente, né

> tantomeno la perdita della titolarità da parte del soggetto che legittimamente detiene i dati. (…)
> Diversamente opinando, si determinerebbe il paradosso secondo cui chiunque richiedesse a un titolare di effettuare operazioni di trattamento sulle banche dati di quest'ultimo, ne diverrebbe automaticamente titolare.

Si diceva che il titolare è il soggetto che "determina le finalità e i mezzi del trattamento di dati personali"; è certo una definizione 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.

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.

Potremmo dunque precisare questa nozione di Titolare del trattamento:

> quel soggetto che, in riferimento a propri interessi e scopi pratici, svolge o svolgerà attività che comportano un trattamento di dati personali dei quali ha o prevede di poter avere la disponibilità, e che di tale trattamento, possedendo o meno la base giuridica per effettuarlo lecitamente, determina (o comunque condivide o condiziona) i mezzi e le modalità

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

Trasferimento di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo

Le condizioni per il trasferimento dei dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE oltre a Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono indicate agli artt. 45, 46, 47 e 49 del Regolamento Generale. Il trasferimento è anzitutto consentito a condizione che:

- l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del Regolamento Generale).

In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento Generale). Possono costituire, per quanto di nostro interesse, garanzie adeguate:

- gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
- le clausole tipo (art. 46, par. 2, lett. c e lett. d) e le clausole contrattuali ad hoc (art. 46, par. 3, lett. a)
- i codici di condotta (art. 46, par. 2, lett. e) e i meccanismi di certificazione (art. 46, par. 2, lett. f)
- gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b)

In assenza di ogni altro presupposto, è inoltre possibile trasferire i dati personali in base a:

- alcune deroghe che si verificano in specifiche situazioni (art. 49 del Regolamento Generale).

Nelle Reccommendations 01 - 02/2020 del 10 novembre, l'EPDB fornisce alcuni suggerimenti delle misure da adottare in caso di trasferimento. Gli step sono i seguenti:

- mappare i trasferimenti: identificare tutti i responsabili, subresponsabili al di fuori del territorio UE, comprese le terze parti che hanno un mero accesso da remoto ai sistemi del titolare
- identificare la base giuridica: indicare gli strumenti di trasferimento su cui si fa affidamento tra quelli previsti nel Capo V del Regolamento Generale
- valutare l'efficacia dello strumento alla luce di tutte le circostanze del trasferimento: es. legge o prassi del paese terzo, attori coinvolti nel trattamento e possibili ulteriori attività di trasferimento)
- adozione di misure supplementari: se lo strumento di trasferimento non è efficace, allora sarà necessario considerare, se del caso in collaborazione con l'importatore, se è necessario adottare misure supplementari (contrattuali, organizzative o tecniche)
- adozione di step procedurali: SCC, BCR o Clausole contrattuali ad hoc, in base al tipo di garanzie/strumenti individuati
- monitoraggio continuo sulle leggi del Paese Terzo e sulle caratteristiche del trasferimento

- ***

***

La Commissione europea può stabilire, valutati gli elementi indicati nell'art. 45, par. 2 del Regolamento Generale e sulla base di un procedimento che prevede il parere del Comitato europeo per la protezione dei dati, che il Paese terzo (ma anche un territorio o un settore specifico al suo interno) o l'organizzazione internazionale garantiscano un livello di protezione adeguato e che pertanto è possibile trasferirvi dati personali. Il Regolamento prevede un'attività di monitoraggio da parte della Commissione mediante riesame delle decisioni a cadenza periodica, almeno ogni quattro anni, che può concludersi con una modifica della decisione o la sua sospensione o revoca. Sono ad oggi oggetto di decisioni di adeguatezza:

Svizzera
Andorra
Isole Fær Øer
Guernsey
Jersey
Isola di Man
Argentina
Giappone
Canada
Israele
Nuova Zelanda
Uruguay
Regno Unito
Repubblica di Corea (Corea del sud)
USA (nei limiti del Data Privacy Framework)

Relativamente agli USA, la Commissione europea ha appunto adottato il 10 luglio 2023 una decisione in merito al cosiddetto EU-US Data Privacy Framework, l'accordo che regolamenta il trasferimento di dati personali tra Unione europea e USA.

Quest'ultimo tutela i diritti fondamentali degli individui nell´UE le cui informazioni personali vengano trasferite negli Stati Uniti ad imprese che si sono certificate aderendo al Data Privacy Framework (l'elenco delle imprese è consultabile sul sito dedicato). La nuova disciplina prevede:

- obblighi di protezione stringenti per le imprese nell'UE/EEA che trasferiscono i dati personali;
- garanzie vincolanti in materia di accesso ai dati da parte dei soggetti pubblici statunitensi per finalità di intelligence e law enforcement;
- strumenti di tutela per gli interessati quali il ricorso gratuito a organismi indipendenti di risoluzione delle controversie o la possibilità di rivolgersi alle Autorità europee di protezione dei

dati. Gli interessati, inoltre, indipendentemente dallo strumento utilizzato per trasferire i dati personali negli Stati Uniti, possono presentare un reclamo al Garante per avvalersi del nuovo meccanismo di ricorso nel settore della sicurezza nazionale;
- il riesame congiunto, a cadenza periodica, dell'accordo per monitorarne l'attuazione.

I trasferimenti possono essere effettuati anche da autorità pubbliche o da organismi pubblici verso altre autorità pubbliche o organismi pubblici, o nei confronti di organizzazioni internazionali con analoghi compiti o funzioni, stabiliti in Paesi terzi. In tal caso i dati personali possono essere trasferiti:

- sulla base di uno «strumento giuridicamente vincolante e avente efficacia esecutiva» (art. 46, par. 2, lett. a) del Regolamento Generale), quale un accordo amministrativo, di natura internazionale e di ambito bilaterale o multilaterale,

ovvero

- previa autorizzazione dell'autorità di controllo competente, mediante «disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati» (art. 46, par. 3, lett. b) del Regolamento Generale), quali ad esempio i protocolli d'intesa.

La Commissione europea o l'autorità di controllo competente previa approvazione della Commissione può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi o organizzazioni internazionali (art. 46, par. 2, lett. c) e lett. d). In pratica, incorporando il testo delle clausole contrattuali in questione («Standard Contractual Clauses» o «SCC») in un contratto utilizzato per il trasferimento, l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nel Regolamento anche nel Paese terzo o all'interno dell'organizzazione di destinazione. È importante sottolineare che le clausole tipo di protezione dati non ammettono emendamenti e devono essere sottoscritte dalle parti. Tuttavia, esse possono essere incorporate in un contratto più generale e vi si possono aggiungere clausole ulteriori purché non in conflitto, direttamente o indirettamente, con le clausole tipo così adottate.

"Il 4 giugno 2021, la Commissione europea, con decisione n. 2021/914/UE, ha stabilito che le clausole tipo allegate alla decisione rappresentano garanzie adeguate, ai sensi dell'articolo 46, par. 1, e par. 2, lett. c), del Regolamento (UE) 2016/679, ai fini del trasferimento di dati da un titolare o un responsabile del trattamento soggetto al Regolamento Generale (esportatore) a un titolare o un (sub-)responsabile del trattamento rispetto al quale non trova applicazione il predetto Regolamento (importatore).

Le SCC sono valide solo se:

- le parti confermano l'adeguatezza della legge applicabile nel paese terzo considerato
- possono effettivamente essere rispettate dall'importatore.

I titolari e i responsabili del trattamento potranno avvalersi, a determinate condizioni, anche di codici di condotta o meccanismi di certificazione senza che ciò comporti alcuna autorizzazione da parte dell'autorità competente. I primi, purché approvati a norma dell'art. 40, possono costituire adeguati strumenti per il trasferimento, qualora accompagnati dall'«impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati» (art. 46, par.2, lett. e) del Regolamento Generale); i meccanismi di certificazione purché approvati a norma dell'art. 42, «unitamente all'impegno vincolante ed esigibile del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati» (art. 46, par.2, lett. f) del Regolamento Generale).

In via residuale e solo a determinate condizioni (specificatamente individuate per singola situazione), è possibile trasferire dati personali nell'ambito delle c.d. "deroghe" di cui all'art. 49 del del Regolamento Generale (consenso, contratto, interesse pubblico, difesa in giudizio, interesse vitale, registro pubblico, cogente interesse legittimo del titolare). In merito, è opportuno considerare che il termine "deroga" include di per sé una connotazione di eccezionalità rispetto al principio dell'adeguatezza e alle altre garanzie e che, pertanto, l'ambito di operatività delle suddette deroghe deve essere soggetto ad un'interpretazione restrittiva.

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 dunque nella messa a disposizione degli interessati di idonee *informazioni* (prima si parlava di *informativa*).

Trattamento di dati personali in ambito sanitario

Si è visto che, 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)

Trattamento di dati personali

Per raggiungere un proprio determinato scopo o interesse, il Titolare 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[vii] 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:

> 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)*.

A tali termini posso associarsi le seguenti definizioni:

- Adattamento (individuazione di dati personali nell'ambito di un gruppo di dati già memorizzati)
- Cancellazione (eliminazione dei dati)
- Comunicazione (far conoscere i dati ad uno o più soggetti determinati diversi dall'interessato, dal responsabile o dal titolare)
- Conservazione (il mantenere memorizzate le informazioni su un qualsiasi supporto, indipendente dal loro utilizzo)
- Consultazione (accesso alle informazioni già archiviate)
- Diffusione (divulgazione di dati al pubblico o, comunque, a soggetti indeterminati)
- Distruzione (eliminazione dei supporti che contengono i dati)

- Estrazione (estrapolazione di dati personali da un gruppo di dati già memorizzati)
- Interconnessione (utilizzo di più banche dati)
- Limitazione (possibilità di limitare il trattamento dei dati solo per determinate finalità
- Modifica (attività con la quale il dato personale subisce una modifica non sostanziale, diversamente si preferisce parlare di Elaborazione)
- Organizzazione (classificazione dei dati secondo un metodo prescelto)
- Raccolta (attività di acquisizione del dato, è il momento in cui si verifica l'ingerenza nella sfera esistenziale della persona cui esso si riferisce, anche disgiuntamente dall'accesso)
- Raffronto (operazione di confronto tra dati)
- Registrazione (fissazione dell'informazione su un supporto dal quale poterla poi recuperare)
- Strutturazione (attività di organizzazione sistematica dei dati)
- Uso (attività generica che ricopre qualsiasi tipo di impiego dei dati)

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 tenga un registro delle attività di trattamento svolte sotto la propria responsabilità[viii]. 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 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.

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

Il trattamento è lecito allorquando "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".

La fattispecie è ampia, potendo ricomprendere anche situazioni (es. catastrofi umanitarie) che non riguardano l'ambito sanitario strettamente inteso. 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 dell'interessato (per le quali il consenso non è più previsto).

Per la applicabilità di questa norma occorre dunque 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; 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.

Cosa accadrebbe se queste necessità fossero riferibili ad un paziente cosciente? Dovrebbe essergli chiesto il consenso (e dunque la base giuridica sarebbe quella di cui all'art. 9 per. 2 lettera a del Regolamento) 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[ix]. 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, o di altri soggetti legittimati anche ai sensi dell'art. 82 comma 2 lettera a) del Codice.

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).

Valutazione d'impatto (DPIA)

Alla DPIA (Data Protection Impact Assessment) 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 Valutazioni d'impatto (*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[x].

La DPIA deve soddisfare alcuni requisiti basilari, indicati 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.

Una DPIA è obbligatoria allorquando il trattamento "possa presentare un rischio elevato" per i diritti dell'interessato, e dunque è ordinaria 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.

Se la DPIA accerta la adeguatezza, la conformità, la sicurezza di un trattamento, non può essere un'attività *ad libitum* o *una tantum*, ma un processo (qualora ne ricorrano i presupposti, ma in ambito sanitario è difficile che non accada) necessario permanente e continuativo, soprattutto se si ha a che fare con un trattamento dinamico e soggetto a continue trasformazioni/innovazioni.

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento ovvero, qualora la valutazione indichi un rischio residuo elevato qualora non siano attivate ulteriori azioni correttive, consultare l'autorità di controllo in consultazione preventiva per ottenere indicazioni su come gestire il rischio residuale.

Spetta al titolare garantire l'effettuazione della DPIA (art. 35, paragrafo 2 del Regolamento). consultandosi con il DPO (art. 35, paragrafo 2 del Regolamento); 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, 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. Oltre a ciò è anche l'unico strumento che consente di acquisire un parere preventivo da parte del Garante.

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.

Videosorveglianza

Il Garante è in passato intervenuto sulle problematiche della Videosorveglianza con due provvedimenti di carattere generale, uno dell'aprile 2004 ed uno successivo, sostitutivo del primo, dell'aprile 2010.

Riassuntivamente, si definisce *videosorveglianza* tanto l'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, che l'attività di videocontrollo, effettuata attraverso sistemi o dispositivi che permettono unicamente la visione in tempo reale di aree o zone delimitate.

D'ora in avanti intenderemo la videosorveglianza in senso ampio, comprensivo di entrambe le fattispecie di cui al punto precedente.

In generale, l'attività di videosorveglianza può essere:

- continua;
- non continua ad orario programmato (es. solo notturna);
- attivabile con un sistema di allarme programmato (ovvero in connessione con un determinato evento, come il passaggio di una persona fisica o di un automezzo).

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 videomonitoraggio a distanza dei pazienti;
6. controllo della procedura di raccolta di campioni biologici a fini certificatori o di cura.

Come è evidente, l'attività di videosorveglianza, per un ente pubblico, è riconducibile ad attività istituzionali di tutela di beni e persone o di organizzazione dei servizi. In effetti non esiste, per le PP.AA, un obbligo né di sorveglianza in senso lato né di sorveglianza effettuata secondo modalità normativamente determinate. Non è un caso che, quando siamo andati a definire la base giuridica che consente il trattamento dei dati per scopi di videosorveglianza, ci siamo orientati, in un primo tempo, verso il legittimo interesse, proprio per l'assenza di puntuali obblighi nel merito. Successivamente, considerato che tale attività coinvolge comunque diversi operatori aziendali e comporta ingenti costi – così che diventa difficile sostenere che si tratti di attività non istituzionale - e visto che il legittimo interesse non è utilizzabile, da parte delle PPAA, in riferimento ai propri compiti istituzionali, si è deciso, anche su un input dell'Autorità Garante, di ricondurla ad un "interesse pubblico" genericamente inteso, cioè al di qua di specifiche prescrizioni.

Da ciò segue che il consenso dell'interessato, di cui agli artt. 6 comma 1 lettera a) e 9 comma 2 lettera a) del Regolamento Generale, non rappresenta base giuridica idonea 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 Regolamento Generale (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 Regolamento Generale (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 Regolamento Generale (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 Regolamento Generale (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) Regolamento Generale (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 Regolamento Generale (attività di assistenza sanitaria).

L'attività di videosorveglianza, quando comporta, o può comportare anche incidentalmente, la ripresa di lavoratori, deve essere attivata con le modalità previste dall'art. 4 (Impianti audiovisivi e altri strumenti di controllo) della L. 20 maggio 1970 n. *300 Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento* (cd. *Statuto dei lavoratori*) così come modificato dai dal d.lgs. 14 settembre 2015, n. 151 e dal D.Lgs. 24 settembre 2016, n. 185:

> 1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.
>
> ((In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della

> sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.))
> 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
> 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

L'installazione dell'impianto di videosorveglianza deve essere autorizzata dalla Commissione tecnica di unica valutazione (CTUV) aziendale, acquisito, se ritenuto opportuno, il parere del Responsabile della Protezione dei dati, nonché, ma nei casi in cui dall'attività di videosorveglianza possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, con il coinvolgimento della U.O. Politiche e formazione del personale e relazioni sindacali per procedere all'accordo con le Organizzazioni Sindacali (oppure, in sua assenza, per precedere all'autorizzazione dell'Ispettorato del lavoro).

L'attività di videosorveglianza è limitata ai locali ed alle pertinenze aziendali, nonché alle relative aree d'accesso.

Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili.

I monitor degli impianti di videosorveglianza devono essere collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

In particolare, per quanto riguarda le finalità di *rilevazione di situazioni di pericolo per la sicurezza pubblica e di tutela del patrimonio*, i sistemi di videosorveglianza sono introdotti come misura complementare volta a migliorare la sicurezza all'interno o all'esterno degli edifici aziendali, anche allo scopo di agevolare l'eventuale esercizio, in sede di giudizio, dei diritti del Titolare del trattamento o di terzi.

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini. Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa In particolare:

- in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini; gli

incaricati o, eventualmente, i responsabili del trattamento, laddove tecnicamente possibile, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

- laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare tanto in sincronia con la ripresa, che in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
- nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele: in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
- qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale;
- la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless.

Chi accede ad una zona videosorvegliata deve anzitutto esserne informato a mezzo di idonea informativa breve.

Il supporto con l'informativa deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera, e deve comunque avere un formato ed un posizionamento tale da essere chiaramente visibile.

In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, saranno installati più cartelli.

Il modello va integrato con una informativa completa che riporti tutti gli elementi dell'art. 13 del *Regolamento*, con particolare riguardo alle finalità e all'eventuale conservazione. Tale informativa va resa disponibile sul sito istituzionale (il modello semplificato riporta anzi l'URL presso la quale è accessibile l'informativa) e presso i locali dell'Azienda (ad esempio presso l'URP)

Qualora l'attività di videosorveglianza sia cessata e la relativa telecamera rimossa, deve esserlo anche l'informativa: se nel caso di informativa assente, si ha appunto un'*omissione*, nel caso di informativa

presente in mancanza della relativa attività di videosorveglianza si avrebbe appunto una informativa *inidonea*.

L'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita. L'Autorità garante prescrive che la conservazione sia "limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria".

Si ritiene congrua, in riferimento alle finalità nonché tenuto conto dell'attuale logistica ed organizzazione dell'Azienda (con chiusura degli uffici URP, cui l'interessato dovrebbe rivolgersi per proporre istanza di accesso alle immagini prima della loro cancellazione automatica, nel fine settimana), una conservazione delle immagini videoregistrate per un tempo non superiore a 96 ore. E' comunque opportuno mettere a punto misure organizzative tese ad assicurare un termine di conservazione non superiore alle 48-72 ore.

L'ulteriore conservazione delle immagini rispetto a tale termine può essere disposta dalla persona espressamente designata (oltre che nel caso di indagini delle autorità giudiziarie o di polizia) in relazione a illeciti che si siano verificati e dei quali l'Azienda abbia avuto notizia.

Il sistema deve essere programmato in modo da operare l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere comunque non riutilizzabili i dati cancellati.

In presenza di impianti non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di *expiring* dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile dalla fine del periodo di conservazione fissato dal Titolare.

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.

Persona espressamente designata per il trattamento dei dati di videosorveglianza per finalità di rilevazione di situazioni di pericolo per la sicurezza pubblica e per la tutela del patrimonio, nonché per finalità di gestione dell'accesso ad aree ad accesso controllato, è il direttore della U.O: ….

Persona espressamente designata per il trattamento dei dati di videosorveglianza per finalità di cura e tutela della salute di pazienti (videomonitoraggio), è il Direttore/Responsabile del reparto nel quale le telecamere sono installate.

Tali soggetti devono individuare le categorie di persone autorizzate al trattamento, legittimate ad utilizzare gli impianti, ad accedere alle immagini e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni, mettendo loro a disposizione idonee istruzioni. Devono altresì individuare

diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

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 …. 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*, ricomprende anche 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.

In relazione alle immagini videoregistrate, è assicurato agli interessati l'esercizio dei diritti di accesso di cui alla L. 241/90: si considera cioè l'attività di videosorveglianza quale attività amministrativa, in linea con quanto sopra osservato sulla base giuridica del trattamento, e la relativa documentazione come documentazione amministrativa, in quanto rappresentazione di tale attività.

Il soggetto interessato, per l'esercizio di tali diritti, deve avanzare apposita istanza indirizzata al Titolare o al responsabile del trattamento, anche attraverso l'U.R.P. aziendale, precisando a quale impianto di videosorveglianza o a quale area o reparto si fa riferimento; chi riceve la richiesta deve immediatamente attivare l'Area Tecnica per la sospensione del processo di cancellazione delle immagini; l'Area Tecnica, quale responsabile del procedimento d'accesso provvederà ad effettuare le necessarie valutazioni in ordine alla legittimità della stessa (con l'eventuale supporto del Responsabile della protezione dei dati), accogliendola o respingendola con atto motivato. Al richiedente potrà essere altresì richiesto di fornire

ulteriori indicazioni, finalizzate a facilitare il reperimento delle immagini stesse, tra cui il giorno e l'ora in cui l'interessato potrebbe essere stato oggetto di ripresa.

Nel caso che le immagini di possibile interesse non siano più conservate, di ciò dovrà essere data formale comunicazione al richiedente.

Il responsabile del trattamento, nel caso di accertamento positivo, fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà visionare le immagini che lo riguardano. Le immagini possono altresì essere trasmesse in copia a seguito di formale richiesta.

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. L'interessato ha comunque diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

L'accesso da parte di terzi è consentito nei limiti in cui sia strettamente *necessario* per curare o per difendere i propri interessi giuridici.
Sono previsti rimborsi per i costi effettivamente sostenuti dall'Azienda, quantificabili in:

- … euro per l'esame di ogni singola registrazione (cioè di ogni singola telecamera);
- … euro per la digitalizzazione delle immagini su supporto informatico.

Nel caso le immagini siano qualificabili come dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'accesso da parte di terzi è consentito nei limiti in cui sia strettamente *indispensabile* per curare o per difendere i propri interessi giuridici e solo qualora la situazione giuridicamente rilevante che si intende tutelare attraverso l'accesso sia di rango almeno pari ai diritti dell'interessato, cioè consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

L'autorità Giudiziaria o di Pubblica Sicurezza può legittimamente accedere alle immagini videoregistrate, a seguito di formale richiesta.

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.

***

Particolare finalità, che in certo modo la distingue rispetto alle attività di videosorveglianza propriamente dette, ha l'attività di videomonitoraggio, relativa alla sorveglianza remota di pazienti ricoverati, per finalità di cura e tutela della salute. Non si ricomprende nel videomonitoraggio la gestione delle immagini integrata in apparecchiature elettromedicali.

L'attività di videomonitoraggio non prevede ordinariamente la registrazione delle immagini.

Essa dovrà essere limitata ai casi di stretta indispensabilità per la tutela della salute del ricoverato, e circoscrivendo le riprese solo ad uno o più pazienti interessati; sono adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate. In particolare, potranno accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico), nella misura della stretta indispensabilità: ovvero solo i soggetti che avrebbero avuto accesso ai pazienti laddove non fosse stato attivato il monitoraggio a distanza.

Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali deve essere consentita, con gli adeguati accorgimenti tecnici, esclusivamente la visione dell'immagine del proprio congiunto o conoscente.

Le immagini idonee a rivelare lo stato di salute non devono - nel rispetto del divieto dell'art. 2-septies comma 8 del *Codice* - essere comunque diffuse, per cui, ad esempio, va assolutamente evitato il rischio di diffusione delle immagini di pazienti su *monitor* collocati in locali liberamente accessibili al pubblico o a soggetti non legittimati: anzi, in questo caso può integrare una diffusione di dati idonei a rivelare lo stato di salute, semplicemente, la loro messa a disposizione di soggetti indeterminati, e dunque, posto che l'accesso deve essere consentito solo a incaricati chiaramente individuati, a qualunque soggetto, pur se integrato nell'organizzazione aziendale, ulteriore rispetto a quelli autorizzati.

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.

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.

[i] Quest'ultima non deve essere più, a sua volta, prevista da una norma di legge, come nella redazione precedente al D.L. 139/2021 comma 1.

[ii] 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.

[iii] 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.

[iv] "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".

[v] "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".

[vi] 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.

[vii] "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"

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

[ix] "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".

[x] 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.