I quaderni di ReD OPEN - vol. 1

I princìpi generali del trattamento dei dati sanitari

Dimitri Martignago

ReD OPEN
responsibility & design in open ecosystems

Ledizioni

Quaderno RedOpen I

I principi generali del trattamento dei dati sanitari

Ledizioni

© 2020 Ledizioni LediPublishing
Via Alamanni 11 Milano
http://www.ledizioni.it
e-mail: info@ledizioni.it

Prima edizione Ledizioni: settembre 2020

Quaderno RedOpen I. Dimitri Martignago, *I principi generali del trattamento dei dati sanitari*

ISBN cartaceo 9788855263092

Le riproduzioni a uso differente da quello personale potranno avvenire, per un numero di pagine non superiore al 15% del presente volume, solo a seguito di specifica autorizzazione rilasciata da Ledizioni, Via Alamanni 11 – 20141 Milano, e-mail: info@ledizioni.it

Indice

GUIDA ALLA LETTURA

Questo Quaderno di ReD OPEN può essere considerato un contributo specialistico ad una tematica particolare qual è quella della protezione dei dati sanitari in ogni ambito da essa coinvolto. Accanto a tale focus, tuttavia, questo lavoro può essere letto, soprattutto da un non addetto a simili lavori, come una rappresentazione delle problematiche e delle vicende scarsamente note riguardo al dibattito che si genera alle spalle di quanto il più delle volte viene adottato come una norma operativa e niente di più.

A CHI SI RIVOLGE?

Per questa ragione, accanto ai professionisti della materia giuridica, le persone potenzialmente interessate alla lettura sono anche i responsabili e gli addetti agli istituti di ricerca medica, farmacologica, genetica, e così via, i quali trarranno particolare interesse dai molti dei dettagli ivi raccolti.

Riteniamo possa altresì servire ai DPO di organizzazioni e istituzioni di ogni tipo, ma anche ai loro

referenti come top manager o imprenditori in qualsiasi ambito o settore.

Costoro probabilmente faranno bene, soprattutto a fronte di una prima lettura, a non perdersi eccessivamente nei dettagli tecnico-procedurali per vedere come dietro a tante norme risiedano dibattiti delicati e tutt'altro che uniformi. Molte sono infatti le chiavi di lettura possibili degli elementi messi in discussione, tante quante le vedute ed interpretazioni che, se debitamente traslate, consentono di cogliere le mille sfumature e quindi la ricchezza di sottigliezze che rendono la gestione dei dati personali e del patrimonio dei dati aziendali un autentico tesoro per ognuno di noi come pure per l'immagine dell'organizzazione in chiave di responsabilità, sostenibilità, innovazione e crescita spesso sottovalutata se posta in relazione agli indicatori di business tradizionali.

Detto in parole povere, quello che più conta è comprendere la logica legislativa per considerare la protezione dei dati meno uno spauracchio legale e più una risorsa, uno strumento competitivo degli anni a venire.

1. IL TRATTAMENTO DEI DATI SANITARI ALLA LUCE DEL GDPR

In un momento in cui la maggior parte delle nazioni sta adottando misure straordinarie e imponendo regole specifiche e sempre più restrittive conseguenti al lockdown, gli Stati membri dell'Unione Europea si sono trovati di fronte ad un nuovo problema: tutelare la salute delle persone, bilanciando in maniera proporzionale le misure adottate con i diritti e le libertà da garantire alle stesse. A ciò si aggiunge che molte organizzazioni, per la maggior parte private, hanno optato per un ulteriore inasprimento delle regole e dei controlli, adottando piani specifici spesso criticati per le evidenti invasioni della privacy dei dipendenti con particolare riferimento alle informazioni di carattere sanitario

Simili azioni, sommate al recente aumento esponenziale degli investimenti nel settore della ricerca medica hanno messo in luce come la tutela dei dati relativi alla salute comporti un inevitabile cambiamento culturale e di consapevolezza e l'adozione di misure attuative concrete.

Il GDPR è il primo testo legislativo adottato dall'Unione Europea a fornire una definizione di dati relativi alla salute. Ad essi, il Regolamento dedica un'apposita tutela ritenendoli, per loro natura, particolarmente sensibili: il loro trattamento potrebbe infatti generare rischi significativi tanto per i diritti quanto per le libertà fondamentali delle persone.

Sulla base dell'articolo 4 del dettato legislativo, i «*dati relativi alla salute sono quei dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*». Sono molte le fonti da cui è possibile estrarre i dati relativi alla salute, tra cui: una cartella clinica contenente le informazioni raccolte da un fornitore di assistenza sanitaria; i questionari e i test di autovalutazione compilati direttamente dai pazienti; informazioni raccolte senza fini sanitari, ma che se incrociate tra loro o se utilizzate in uno specifico contesto sono in grado di rivelare lo stato di salute o i rischi relativi alla salute di una persona.

Per questa categoria di dati è fatto espresso **divieto di trattamento** all'articolo 9 del GDPR. Di fronte all'importanza ormai assunta dalla medicina

e dalla ricerca nella nostra società e in considerazione del costante riutilizzo e della condivisione dei **dati sanitari**, è stato però necessario introdurre delle eccezioni per disciplinarne il trattamento anche a fronte del summenzionato divieto.

Sulla base delle **deroghe** introdotte alle lettere h), i) ed j) del secondo comma dell'articolo 9, i dati sensibili, e quindi anche quelli sanitari, possono essere trattati anzitutto se «*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*». *In secondo luogo il trattamento può avvenire laddove «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*» come nel caso della situazione di emergenza sorta con la diffusione del virus SARS-CoV2. Per ultimo poi i dati sanitari possono essere utilizzati nei casi in cui il trattamento è necessario a fini di ricerca scientifica.

Per meglio comprendere la disciplina relativa al trattamento dei dati sensibili e più nello specifico dei dati relativi alla salute è necessario individuare prima di tutto gli elementi chiave la cui applicazione è essenziale per garantire una tutela concreta ed effettiva delle persone fisiche.

A tal riguardo il Considerando 51 del GDPR impone di applicare tanto i **principi generali** quanto le altre norme del regolamento, in particolare per quanto riguarda le **condizioni per il trattamento lecito**, ponendo quindi come punto di partenza fondamentale il rispetto dei *principi generali* e della disciplina del *consenso*.

2. I PRINCIPI GENERALI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

Le disposizioni chiave in merito ai principi generali e alla liceità del trattamento sono lasciate agli articoli 5 (*Principi applicabili al trattamento di dati personali*) e 6 (*Liceità del trattamento*) del GDPR, anche se in entrambi i casi il loro valore deve essere individuato altrove.

I principi fondamentali della protezione dei dati personali del GDPR non hanno subito sostanziali modifiche rispetto a quelli che erano stati individuati nelle linee guida dell'OCSE del 1980 e questo ha contribuito a dimostrarne la capacità di resistere alla prova del tempo. L'ampia portata del loro contesto applicativo e la loro vocazione ad essere «*technology neutral and future-proof*», rendono però le norme in materia di protezione dei dati poco chiare ed autorevoli lasciando spazio a correnti di pensiero, che conferiscono ai singoli principi sfaccettature nuove e questionabili.

2.1. LICEITÀ, CORRETTEZZA E TRASPARENZA

I dati personali devono innanzitutto essere trattati in maniera lecita. Per alcuni questa esigenza comporta che il trattamento debba avvenire in maniera **conforme** all'insieme delle **norme applicabili**, non solo di quelle per la protezione dei dati, ma anche ad esempio di quelle in materia di diritto del lavoro o di segreto professionale. Proprio per queste ragioni il difetto di liceità coinciderebbe «*con l'antigiuridicità, intesa come figura di qualificazione normativa di un fatto come contrario alle norme dell'ordinamento giuridico*».

Di opinione contraria è invece un'altra parte della dottrina, secondo la quale il GDPR avrebbe ristretto la portata del principio di liceità al quale la precedente Direttiva, attribuiva un significato tanto generico da farlo corrispondere ad un semplice requisito di generale osservanza della normativa in materia di protezione dei dati personali. Oggi c'è chi ritiene che nel GDPR, lo stesso concetto di liceità si riferisca esclusivamente ad una specifica necessità ossia che sussista una delle **condizioni per il trattamento** dei dati stabilite dall'**articolo 6** comma 1.

Una simile interpretazione renderebbe più semplice distinguere il significato di legittimità del trattamento da quello di liceità, senza eliminare il requisito del rispetto della legge come principio generale; ribadendo al contrario che, affinché un trattamento possa essere ritenuto lecito, questo è necessario che sia innanzitutto legittimo.

Il trattamento sarà quindi lecito solo nei casi in cui:

a. l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

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;

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;

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.

Nonostante dei leggeri cambiamenti, queste condizioni sono le stesse già individuate dalla Direttiva e le uniche entro cui il trattamento di dati a carattere personale è permesso. La Corte di Giustizia ha già avuto occasione di insistere sulla natura, al contempo esaustiva e limitativa, della lista di ipotesi enunciate nel precedente articolo 7 della Direttiva, sottolineando che, «*a norma dell'articolo 5 della direttiva 95/46, gli Stati membri non possono neppure introdurre principi relativi alla legittimazione del trattamento dei dati personali diversi da quelli enunciati all'art. 7 di tale direttiva, né modificare con requisiti supplementari la portata dei sei principi previsti dal detto art. 7*».

L'articolo 6 stabilisce delle situazioni astratte per le quali comunque sussiste una presunzione di equilibrio degli interessi considerati. Tale presunzione può essere in ogni caso sottoposta ad un **controllo**

concreto, svolto sulla base dell'**articolo 5**, che permette di rilevare una violazione inaccettabile dei diritti e degli interessi fondamentali dell'individuo. Le condizioni di liceità fungono da «*presupposto di legittimazione al trattamento*» e tra le 6 ipotesi previste dall'articolo 6 il trattamento previo espresso **consenso** dell'interessato è certamente il più importante nei casi in cui vengono utilizzati dati che rivelano informazioni relative allo stato di salute.

I dati personali devono poi essere trattati in maniera *corretta* e *trasparente*. Il principio di correttezza assieme a quello di trasparenza «*rappresenta un presupposto indispensabile per la garanzia di una delle componenti essenziali del diritto alla protezione dei dati personali, quale appunto è l'autodeterminazione informativa*» ossia che la garanzia che la raccolta dei dati personali sia preceduta da informazioni adeguate. L'esigenza che i dati siano trattati in maniera **corretta** impone che non siano ottenuti o trattati con mezzi e metodi ingiusti, come avvenne nel caso di Cambridge Analytica. La correttezza del trattamento dipenderà in parte da come sono stati ottenuti i dati e in parte da eventuali raggiri o inganni perpetrati ai danni dei soggetti interessati dal trattamento. Quest'ultimo non potrà quindi

avvenire ad insaputa delle persone a cui i dati si riferiscono e dovrà essere applicato in maniera leale e nella buona fede di chi tratta i dati. Il rispetto del principio di correttezza richiede di valutare non soltanto come processare i dati, ma anche se processarli considerando in maniera più generale se e come il trattamento tocchi gli interessi delle persone coinvolte, individualmente o come gruppo. E se in certi casi questo, pur danneggiando un individuo, potrà non essere necessariamente scorretto, in altre situazioni, anche laddove avvenga in maniera giusta relativamente a molte delle persone interessate ma in maniera ingiusta rispetto ad un singolo individuo, ci sarà sempre una violazione del principio.

Il principio di correttezza contribuisce all'autodeterminazione informativa dell'interessato assieme al principio di **trasparenza**. Quest'ultimo è un principio consolidato all'interno dell'Unione Europea, tanto nei Trattati quanto nel diritto derivato. Il suo fine è volto ad alimentare la fiducia dei cittadini nei procedimenti che li coinvolgono, consentendo loro di comprendere e, se necessario, impugnare questi stessi procedimenti. Inoltre, seppure il GDPR non fornisca informazioni in merito al significato del principio di trasparenza e agli effetti ad esso collegati,

al di fuori di quelle date dal Considerando 39, è oggi possibile ricostruirne le caratteristiche principali.

La trasparenza va applicata a tre aree differenti: al fornire agli interessati informazioni relative ad un trattamento corretto; al come i titolari del trattamento comunicano con gli interessati riguardo ai loro diritti ai sensi del GDPR; a come i responsabili del trattamento dei dati facilitano l'esercizio dei loro diritti da parte degli interessati. Come per il principio di correttezza, anche nell'ambito della trasparenza in base al GDPR il responsabile del trattamento deve quindi fornire in maniera spontanea determinate informazioni alle persone interessate, così da consentire loro di capire lo scopo e le conseguenze che potrebbero derivare dal trattamento. Nel GDPR il concetto di trasparenza viene sviluppato da svariati articoli che impongono il rispetto di specifici requisiti al titolare del trattamento e al responsabile. Se è pur vero poi che il principio di trasparenza va applicato in maniera continuativa durante tutto l'arco del trattamento, indipendentemente dalla base legale, deroghe parziali sono consentite in casi e per finalità precise.

L'articolo 12, intitolato «*Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti*

dell'interessato», stabilisce delle regole generali da applicare tanto laddove si debbano fornire informazioni all'interessato, quanto nelle comunicazioni con l'interessato del trattamento in merito all'esercizio dei suoi diritti e nelle comunicazioni in relazione alle violazioni di dati personali. Le informazioni e comunicazioni dovranno quindi essere fornite «*in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro*». Se trasparenza e concisione comportano un dovere di presentare le informazioni e le comunicazioni in maniera efficiente e succinta, differenziandole da quelle non legate alla privacy; il requisito dell'**intellegibilità** comporta invece che queste possano essere comprese da un componente medio dell'audience a cui sono indirizzate, essendo quindi compito del titolare del trattamento avere la consapevolezza delle persone al cui riguardo i dati vengono raccolti. Perché le informazioni possano dirsi **facilmente accessibili** occorre che sia curato tanto il modo quanto il luogo in cui esse siano reperibili.

Riprendendo le considerazioni espresse nel Considerando 42, il dovere di utilizzare un **linguaggio semplice e chiaro** nelle comunicazioni comporta infine che le informazioni vengano fornite nel-

la maniera più semplice possibile, evitando frasi complesse e un linguaggio strutturato. In merito a ciò il Gruppo di Lavoro Articolo 29 ha poi fornito una spiegazione dettagliata di che cosa questo effettivamente comporti. Perché siano fornite con un linguaggio chiaro, le informazioni dovrebbero essere concrete e definitive, non contenendo termini troppo legalistici e tecnici o un linguaggio troppo specializzato; non dovrebbero lasciare spazio a interpretazioni diverse che rendano poco chiaro lo scopo e la base giuridica del trattamento e, laddove tradotte in uno o più linguaggi diversi, il responsabile del trattamento dovrebbe assicurarsi che tutte le traduzioni siano accurate e che la fraseologia e la sintassi conservino lo stesso significato di modo che il testo non debba essere decifrato o nuovamente interpretato. Nei casi invece in cui il responsabile dovesse decidere di utilizzare un linguaggio indefinito, con termini quali "*può*", "*potrebbe*", "*alcuni*", "*spesso*" "*possibile*", in base al principio di responsabilità costui dovrebbe essere comunque in grado di dimostrare le ragioni per cui non avrebbe potuto evitare un simile idioma senza compromettere la correttezza del trattamento.

2.2. LIMITAZIONE DELLE FINALITÀ

Il principio di finalità o «*limitazione delle finalità*» esige che i dati personali siano «*raccolti per finalità determinate, esplicite e legittime e successivamente trattati in [un] modo che non sia incompatibile con tali finalità*». Il principio è composto da due elementi: innanzitutto lo scopo per cui i dati devono essere raccolti deve essere determinato, esplicito e legittimo; in secondo luogo i trattamenti successivi devono essere compatibili con la finalità per cui i dati sono stati raccolti. Sulla base di questi elementi sarà poi possibile dedurre i dati da raccogliere, il periodo di conservazione e tutti gli altri aspetti essenziali affinché i dati vengano processati in maniera congrua con la finalità perseguita.

Una finalità può dirsi *determinata* solo laddove nota sin dall'inizio del trattamento, non potendo questa essere inesistente o vaga. Si tratta appunto di una caratteristica essenziale che andrà a definire il trattamento, permettendo alla persona interessata di controllare la sorte riservata ai dati coinvolti. La determinazione della finalità dovrà avvenire in maniera precisa al fine di permettere, da un lato all'interessato di effettuare una propria valutazione

e di esercitare i diritti a lui conferiti dalla legge e, dall'altro, al responsabile del trattamento di individuare i dati da raccogliere e trattare. Il responsabile dovrà quindi identificare di quale finalità si tratta, documentandone la valutazione fatta di modo da rispettare il principio di *accountability* presentato in seguito.

Stando all'Opinione rilasciata nel 2013 dal Gruppo di Lavoro Articolo 29, affinché possa essere *determinata*, la finalità andrà individuata prima o comunque non dopo che la raccolta dei dati personali sia stata portata a termine e andrà identificata in maniera chiara e precisa di modo da capire quale trattamento sia o meno incluso. La dottrina ha evidenziato come non rispondano al criterio in questione le finalità troppo vaghe indicate da Facebook quali «*fornire, migliorare e sviluppare servizi, promuovere la sicurezza e mostrare e misurare le pubblicità e i servizi*».

Il grado di dettaglio da adottare nella descrizione della finalità dipende dal particolare contesto in cui i dati sono raccolti e dai dati coinvolti. In determinati casi un linguaggio semplice può essere sufficiente laddove invece altre situazioni richiederebbero maggiori dettagli.

Non mancano poi i casi in cui un'informativa stratificata sia da ritenersi più appropriata. Su Internet, ad esempio, in certi casi è preferibile fornire dapprima le informazioni essenziali in maniera concisa e adatta alle capacità dell'utente, seguite poi da altri elementi aggiuntivi a beneficio di coloro che necessitino di un ulteriore chiarimento. Anche se è vero che più finalità diverse possono essere correlate tra loro, la scelta meno rischiosa per i titolari sembrerebbe essere comunque quella di evitare di utilizzare un'unica finalità generale, entrando più nel dettaglio.

Con il termine *esplicito* invece si intende che la finalità deve essere rivelata, spiegata e espressa con metodi comprensibili. Assieme alle informazioni da fornire all'interessato e alla notifica all'autorità, la necessità che lo scopo venga esplicitato è un elemento costitutivo essenziale del principio della trasparenza. Una finalità non può dunque essere tenuta segreta o camuffata, essendo essenziale comunicare tante informazioni quante siano necessarie ad assicurare che ogni persona coinvolta abbia lo stesso grado di comprensione delle finalità del trattamento senza ambiguità. Per essere esplicita la finalità potrà essere espressa con vari metodi: con

un avviso fornito all'interessato, con una notifica all'autorità posta a supervisione o all'interno delle informazioni fornite al DPO (Data Protection Officer) a patto che sia sufficientemente chiara a tutte le persone coinvolte, indipendentemente dai loro diversi background linguistici/culturali, dai loro livelli di comprensione o dalle loro particolari necessità.

In merito, invece, alla *legittimità* della finalità, come già accennato in precedenza, è utile distinguerla dalla liceità del trattamento, intesa come il ricorrere di almeno una delle condizioni stabilite all'Articolo 6. Secondo alcuni infatti, il requisito della legittimità sembrerebbe avere una portata ben più ampia di quella del principio di liceità. Possono infatti dirsi legittimi solo i trattamenti aventi finalità compatibili tanto con le disposizioni in materia di protezione dei dati personali, quanto con le altre leggi applicabili (ad es. il diritto del lavoro, dei contratti, del consumatore). Secondo questa impostazione, al termine "legge" si dovrebbe perciò attribuire tanto il significato individuato dall'interpretazione delle Corti competenti, quanto quello fornito dalla legislazione primaria o secondaria, dai principi legali e dalla giurisprudenza stessa. Non sembrerebbe quindi appropriato escludere da que-

sto insieme elementi i codici di condotta, le consuetudini, i codici etici o perfino il semplice contesto generale e i fatti del caso specifico, essendo questi parte della relazione che intercorre tra il titolare del trattamento e il soggetto interessato.

La legittimità non va considerata in maniera rigida, ma piuttosto come un concetto in continuo cambiamento, legato all'evoluzione tecnologica e scientifica e ai mutamenti sociali e culturali.

In base al secondo elemento della limitazione delle finalità occorre poi che i trattamenti messi in pratica **non** siano **incompatibili** con la finalità determinata, esplicita e legittima. Non è quindi possibile disporre liberamente dei dati raccolti e solo gli usi compatibili con le finalità determinate e specificate al momento della raccolta saranno ammessi, salvo ovviamente le poche eccezioni previste dal Regolamento, tra le quali appunto, il trattamento a fini sanitari.

L'utilizzo della doppia negazione da parte del legislatore che, invece di definire il concetto di compatibilità, ha preferito autorizzare tutti i trattamenti *non incompatibili* con la finalità originaria, ha spinto vari interpreti a ritenere che si sia preferito lasciare più flessibilità in merito ai successivi utilizzi dei

dati. Per questa ragione anche laddove il trattamento successivo per finalità diversa da quella originaria non sia basato sul consenso, non è detto che questo sia da considerarsi incompatibile con detta finalità. Nel caso infatti in cui un soggetto abbia dato il proprio consenso al trattamento di dati sanitari a scopo di ricerca contro il virus SARS-CoV2 non parrebbe errato pensare che questi possano essere riutilizzati liberamente per poter portare a termine ulteriori ricerche mirate a curare o prevenire patologie diverse.

In determinate circostanze d'altro canto potrebbe presentarsi la necessità di consentire un cambiamento di scopo o di focalizzazione in situazioni in cui le aspettative della società – o degli stessi interessati – siano cambiate riguardo a quale uso ulteriore i dati possono essere destinati.

Caso per caso sarà quindi utile valutare l'esistenza di un'incompatibilità, tramite un'analisi dei criteri stabiliti all'articolo 6 comma 4 per l'esistenza della compatibilità, interpretati alla luce del Considerando 50 del GDPR che disciplina i casi del trattamento ulteriore.

Oltre a verificare che il trattamento successivo soddisfi tutti i requisiti di liceità, nel valutarne la

compatibilità il titolare deve innanzitutto tener conto di ogni **nesso** tra le diverse finalità. Sono quindi compatibili tutti quegli utilizzi successivi che presentino un collegamento logico coerente con la finalità iniziale. Per poter garantire all'interessato il controllo sulla sorte dei propri dati personali, consentendo però che si continui a farne uso, il titolare deve in più considerare «*le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo*». Un trattamento ulteriore è quindi **compatibile** se rispetta le ragionevoli aspettative dell'interessato al momento della raccolta, sulla base del contesto in cui questa è avvenuta. Per queste ragioni la valutazione sulla compatibilità dovrà avvenire, non in termini formalistici, ma «*verificandone la sussistenza, in base a parametri quali il rapporto tra le finalità originarie e quelle dei trattamenti successivi, al contesto della raccolta dei dati, alla ragionevole aspettativa dell'interessato rispetto ai trattamenti futuri anche considerando la relazione tra questi e il titolare, all'impatto dei trattamenti ulteriori, alla necessità delle finalità ulteriori ai fini della realizzazione di quelle originarie, all'esistenza di garanzie adeguate per l'interessato*».

All'articolo 5, lettera c) del primo comma, il Regolamento dispone poi che il titolare debba tener conto *della natura dei dati personali*, sia che si tratti di dati ordinari, ma ancor di più in quei casi in cui ad essere coinvolte siano le categorie di dati disciplinate agli articoli 9 e 10 del GDPR.

Una volta valutate le possibili conseguenze per le persone interessate dal trattamento successivo e l'esistenza di garanzie come quelle misure volte ad assicurare la separazione funzionale dei dati (ad es. pseudonimizzazione e cifratura), il titolare può ritenersi legittimato ad esprimere un giudizio in merito alla compatibilità della finalità del trattamento con quella adottata per la raccolta iniziale. Nel formulare una simile valutazione deve però prestare attenzione a non attenersi ad un metro basato esclusivamente sulla forma che, per quanto all'apparenza più oggettivo e neutrale, rischierebbe di condurre ad un giudizio eccessivamente rigido e povero sotto i profili dell'efficienza e del pragmatismo. Se è pur vero infatti che in certi casi la compatibilità o l'incompatibilità potrebbero essere ovvie sin da una prima lettura, in altre situazioni, solitamente caratterizzate da una maggiore distanza logica tra le due finalità, potrebbe presentarsi la necessità di dover valutare

un numero di fattori più rilevante, tale per cui queste non risultino essere così scontate.

Nonostante ciò, il GDPR ha però introdotto una novità rispetto alla Direttiva, che consente oggi di trattare i dati personali per una finalità diversa e incompatibile con quella originaria. Nei casi in cui vi sia il consenso del soggetto interessato o altrimenti laddove il trattamento, «*misura necessaria e proporzionata in una società democratica*», sia indispensabile per l'esecuzione di un compito d'interesse pubblico o per l'esercizio dei pubblici poteri di cui è investito il titolare del trattamento, potendo «*il diritto dell'Unione o degli Stati membri […] stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile*», è quindi possibile trattare i dati per una finalità diversa da quella originariamente prevista e non compatibile con questa.

2.3. MINIMIZZAZIONE, LIMITAZIONE DELLA CONSERVAZIONE E ESATTEZZA

Costituendo uno dei cosiddetti tre principi sugli standard dei dati, assieme a quello dell'**esattezza** e a quello della **limitazione della conservazione**, il

principio di minimizzazione dei dati comporta che possano essere trattati solo quei dati **necessari alle finalità** per cui sono stati raccolti e trattati. I dati coinvolti in un trattamento devono perciò essere «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità*» e non devono essere trattati in quei casi in cui esse siano ragionevolmente conseguibili con mezzi diversi. Come già nella Direttiva e nei testi nazionali precedenti all'entrata in vigore del GDPR, nel principio di minimizzazione si ritrovano aspetti qualitativi e quantitativi. «*I primi […] attengono alla funzionalità del dato rispetto allo scopo perseguito, in base a un nesso eziologico che deve sussistere lungo tutto l'arco del trattamento. I secondi, propri del canone della limitazione dei dati […], impongono di circoscrivere l'ambito delle operazioni ai soli dati personali appunto indispensabili per la realizzazione dello scopo perseguito*».

Riferendosi ai dati e al loro rapporto con le finalità del trattamento, il legislatore ha infatti preferito utilizzare nel GDPR i termini «*limitati a quanto necessario*» piuttosto che «*non eccessivi*», discostandosi dalla proposta iniziale della Commissione Europea e dalle scelte adottate sia nella Convenzione 108 che nella Direttiva. Una scelta che sembre-

rebbe però avere un valore puramente semantico. Nella sostanza i due termini, entrambi espressione del principio di proporzionalità, sembrerebbero ricongiungersi nella conclusione per cui in entrambi i casi un trattamento conforme al principio di minimizzazione deve avere ad oggetto solo dati necessari al raggiungimento dello scopo ad esso funzionale.

Il Considerando 39 del GDPR instaura una forte connessione funzionale tra il principio di minimizzazione e il secondo principio sugli standard dei dati, quello sulla **limitazione della conservazione** (*data retention*). In base ad esso la durata della conservazione dei dati deve essere limitata allo stretto necessario. Il GDPR non ha apportato alcun cambiamento sostanziale al **divieto** di conservare i dati personali «*in una forma che consenta l'identificazione degli interessati per un arco di tempo […] superiore al conseguimento delle finalità per le quali sono trattati*». Per poter definire il lasso di tempo entro cui i dati possono essere conservati, continua quindi ad essere necessario valutare la finalità scelta per il trattamento. Nel momento in cui i dati non siano più necessari allo scopo per cui sono stati raccolti o alle ulteriori finalità compatibili, il titolare, avendo stabilito magari un termine per la cancellazione o la

verifica periodica, dovrà spontaneamente cancellarli o comunque anonimizzarli, privandoli in maniera irreversibile dei loro elementi identificativi.

Come in quello della compatibilità però, una deroga esplicita è disposta nei casi in cui, fatte salve le adeguate misure tecniche e organizzative, il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89. Solo in questi casi, i dati personali potranno essere conservati più a lungo, indipendentemente dal requisito della necessità.

Il terzo principio è quello dell'**esattezza**. Suddiviso in due distinti obblighi, sancisce, da un lato che i dati trattati oltre ad essere necessari devono anche all'occorrenza essere aggiornati o altrimenti cancellati in maniera costante; dall'altro lato che è necessario che siano «*adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*». Il giudizio in merito al rispetto o meno di tale dovere dipenderà dal contesto del trattamento e quindi dallo scopo per cui le informazioni saranno usate.

In linea generale, agli interessati è comunque consentito esercitare il proprio diritto di accesso e

il diritto alla rettifica in quei casi in cui dovessero ritenere i dati inesatti. «*Complementare al principio di esattezza è infatti l'affermazione all'art. 16 par. 1 del diritto dell'interessato a ottenere, senza ingiustificato ritardo la rettifica dei dati inesatti (anche solo perché non aggiornati) e – ove ciò non sia possibile o comunque non si provveda all'aggiornamento – la loro cancellazione*».

2.4. INTEGRITÀ, RISERVATEZZA E RESPONSABILIZZAZIONE

Un principio di estrema rilevanza nella disciplina del trattamento dei dati personali è quello per cui i dati devono essere trattati così da garantire loro «*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*», assicurandone perciò la loro **integrità e riservatezza**. Mediante questo principio e i precetti puntuali in cui questo si manifesta nel GDPR, il legislatore ha deciso di adottare un approccio generale basato sul rischio e per questo «*ciò che maggiormente differenzia il GDPR dalla dir. 95/46/CE è la qualificazione dell'obbligo di adozione di misure di sicurezza*

"appropriate" non quale mero dovere a sé stante […], ma quale vero e proprio principio generale del trattamento». Il principio di *integrità e riservatezza* rappresenta infatti l'ennesima dimostrazione di come, sotto molti aspetti, gli obblighi normativi attualmente in vigore vadano oltre i requisiti puramente formali che caratterizzavano la precedente Direttiva, valorizzando piuttosto l'insieme delle strategie individuate dalle aziende nella sostanza.

Subito successivo al principio di «*integrità e riservatezza*», il concetto di **responsabilizzazione**, fa da appendice ai precedenti principi, precisandone la dimensione pratica e applicativa.

Considerato che nella parola anglosassone *accountability «l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità»*, il termine responsabilizzazione potrebbe sembrare quasi riduttivo rispetto alla portata insita nel concetto normativo in base al quale il «*titolare del trattamento è competente per il rispetto del comma 1 e in grado di comprovarlo*». Per la prima volta quindi, il GDPR ha imposto al titolare l'obbligo di dimostrare la conformità delle attività di trattamento con il Regolamento, tra cui l'efficacia delle misure adottate e questo si è quindi andato

ad aggiungere al dovere, già precedentemente previsto, di rispettare i principi ex articolo 5 comma 1 del Regolamento, mettendo in atto misure adeguate ed efficaci a garantirne il rispetto.

Il principio generale si dirama in una serie di obblighi ripresi e sviluppati nell'articolo 24 del GDPR sulla «*Responsabilità del titolare del trattamento*». Dovere del titolare sarà di dimostrare l'adempimento agli obblighi imposti e l'efficacia stessa delle misure adottate. Queste dovranno «*tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche*».

3. CONSENSO AL TRATTAMENTO DEI PROPRI DATI PERSONALI

Tra le ipotesi individuate all'articolo 6 del GDPR, il consenso mantiene un ruolo di primo piano, anche se nel caso del divieto di trattamento di categorie particolari di dati personali l'articolo 9 sancisce più deroghe distinte di cui solo una da applicarsi laddove vi sia il consenso esplicito dell'interessato.

Alla luce di ciò parrebbe legittimo domandarsi se e quanto, a fronte di una deroga al requisito del consenso, il trattamento di dati sanitari per una delle altre situazioni previste dall'articolo 9 autorizzi una possibile eccezione al principio di liceità, uno dei principi generali menzionati al Considerando 51 del GDPR, che trova spazio perfino all'articolo 52 della Carta dei diritti dell'Unione Europea secondo cui «*eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge*».

Una riflessione in merito richiede dapprima un'attenta analisi della disciplina sancita tanto per il consenso *ordinario*, quanto per il consenso più specifico definito all'articolo 9 come *esplicito*.

3.1 IL CONSENSO ORDINARIO

La disciplina è rimessa al primo comma dell'articolo 6 del GDPR, non esaurendosi però in esso, ma sviluppandosi poi in svariati articoli. In base all'articolo 6 il trattamento è lecito solo laddove l'interessato abbia espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.

Durante il processo di elaborazione del regolamento, il legislatore ha fortemente insistito sulla necessità di assicurarsi che non vi fosse più un ricorso abusivo al consenso al trattamento e che, nei casi in cui vi si faccia ricorso, questo debba avvenire in un contesto in cui il consenso sia effettiva espressione dell'autonomia del soggetto e garanzia della sua qualità.

Secondo la definizione fornita dall'articolo 4 del Regolamento, per «*consenso dell'interessato*» si intende «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*». Come già durante la vigenza

della Direttiva, il consenso deve essere caratterizzato dai requisiti essenziali di validità che emergono oggi dall'articolo quattro: «*la sua libertà (intesa quale assenza di condizionamenti nella formazione oltre che nella espressione della volontà), la sua specificità (dovendo ciascuna manifestazione di volontà riferirsi a un trattamento determinato), il suo carattere informato (in ragione della necessaria consapevolezza, da parte dell'interessato delle implicazioni e delle caratteristiche del trattamento cui saranno sottoposti i suoi dati), la sua inequivocabilità (non devono cioè sussistere dubbi rispetto all'intenzione dell'interessato né sull'an né sul quomodo, tanto più che in materia vige il principio della libertà delle forme), il suo essere manifestato mediante dichiarazione espressa ovvero mediante azione positiva, appunto inequivocabile*».

Il consenso è *libero* in tutti quei casi in cui l'interessato disponga di una scelta effettiva e sia in grado di esercitare un reale controllo su di esso. Laddove ad esempio il consenso sia stato inserito come parte non negoziabile dei termini e delle condizioni si può quindi presumere che non sia stato espresso liberamente. Allo stesso modo sarà da considerarsi illecita anche l'esecuzione di un contratto condizionata alla prestazione del consenso per un trattamen-

to non necessario alla sua esecuzione. Il consenso infatti deve sempre essere una manifestazione libera di volontà e non può essere confuso con l'esecuzione del contratto, una base per il trattamento diversa dalla prima. Seguendo infatti quanto asserito nel parere 06/2014 del Gruppo di Lavoro Articolo 29, la disposizione in base alla quale il trattamento è lecito solo se e nella misura in cui «*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*» va interpretata in maniera ristretta. Se le situazioni in cui il trattamento non è strettamente necessario a portare a termine la prestazione del contratto sono da considerarsi escluse dall'ambito di applicazione di questa norma, al fine di determinare «*la base su cui si valuterà se il trattamento dei dati è necessario alla esecuzione*» del contratto, bisognerà individuare «*l'esatta ratio del contratto, ossia la sua sostanza e il suo obiettivo fondamentale*». In ogni caso se i dati da trattare sono effettivamente necessari all'esecuzione del contratto, allora il consenso non può comunque essere una base legale appropriata.

La libertà di espressione del consenso è messa fortemente in discussione anche nei casi in cui que-

sto sia utilizzato come base del trattamento da parte di pubbliche autorità o comunque laddove vi sia un evidente squilibrio tra l'interessato e il titolare, come nel rapporto impiegato e datore di lavoro. Dato lo squilibrio di poteri, in questi casi esso può considerarsi libero solo laddove il fatto che l'impiegato abbia dato o meno il proprio consenso al trattamento da parte del datore non sia fonte di conseguenze a lui avverse.

Un ulteriore elemento, costitutivo tanto della libertà quanto della specificità del trattamento, è dato poi dalla **granularità** del consenso. Nei casi in cui un servizio coinvolga molteplici trattamenti con finalità diverse tra loro, il titolare dovrebbe, in virtù del requisito della granularità, consentire all'interessato di scegliere a quali di esse fornire il proprio consenso nello specifico. In caso contrario questo non potrebbe dirsi liberamente espresso, com'anche laddove il titolare non dovesse essere in grado di dimostrare che, se necessario, l'interessato potrebbe rifiutare o ritirare il proprio consenso senza alcun pregiudizio.

«*La specificità del consenso è ritenuta tale quando l'accettazione è correlata ad un trattamento determinato ed analiticamente individuato in tutte le sue*

caratteristiche (oggetto, finalità, ambito di circolazione dei dati, durata, modalità con cui viene posta in essere, ecc…)». In merito alla *specificità*, il consenso dovrà vertere su un trattamento di dati preciso. Non potendo essere generico, dovrà avere una finalità determinata correttamente; in altre parole un consenso generale che non specifichi lo scopo esatto non sarà accettabile. Laddove sufficientemente specifico, il consenso andrebbe applicato ad ogni attività di trattamento svolta per la stessa o le stesse finalità e, ricollegandoci all'idea di granularità, nel caso in cui il trattamento abbia più finalità, l'interessato deve prestare il proprio consenso per ognuna di queste con una scelta unica o altrimenti divisa in vari *opt-in*.

La necessità che il meccanismo alla base del consenso sia granulare serve quindi a far sì che esso sia non soltanto libero, ma anche specifico. Il titolare del trattamento quindi, per far si che questo sia specifico, dovrà innanzitutto adottare una chiara separazione tra le informazioni utili ad ottenere il consenso e quelle informazioni relative ad altre questioni. Dopodiché, con un approccio granulare tale da fornire un singolo *opt-in* per ogni finalità, potrà tutelare l'interessato dal cosiddetto fenomeno

del «*function creep*», in base al quale i dati personali vengono spesso utilizzati per scopi non precedentemente espressi, facendo così venir meno una parte essenziale del controllo dell'interessato.

Un elemento essenziale al fine nuovamente di non rendere illusorio il controllo sui propri dati e di non incorrere in un'invalidazione, risiede poi nell'obbligo di fornire all'interessato le informazioni necessarie al fine di poter esprimere un consenso *informato*, nel rispetto della definizione data all'Articolo 4. Per prevenire violazioni dell'articolo 6, il Gruppo di Lavoro Articolo 29 ha stilato una lista di 6 categorie di informazioni che il titolare del trattamento dovrà quindi fornire all'interessato per poterne ottenere il consenso. L'interessato dovrà quindi essere a conoscenza almeno de:

i. l'identità del titolare del trattamento;

ii. la finalità di ogni trattamento per cui è richiesto il consenso;

iii. che tipo di dati saranno raccolti e utilizzati;

iv. l'esistenza del diritto a ritirare il consenso;

v. laddove rilevante, l'esistenza di un processo decisionale automatizzato nel rispetto dell'articolo 22 (2) (c);

vi. su un possibile rischio di trasferimenti di

dati verso un paese terzo o un'organizzazione internazionale in assenza di un'adeguata decisione e di appropriate garanzie, come descritto nell'articolo 46 del GDPR.

In determinate circostanze questo insieme di informazioni potrebbe comunque non essere sufficiente affinché l'interessato sia messo in una posizione tale da comprendere appieno il trattamento dei suoi dati, necessitando quindi di altre informazioni.

In merito poi al modo in cui queste dovranno essere trasmesse, anche in questo caso il linguaggio utilizzato dovrà essere semplice e chiaro, comprensibile per una persona di media preparazione. Il consenso dovrà essere distinguibile e chiaro e non potrà essere nascosto tra i termini e le condizioni generali.

L'inequivocabilità del consenso «*attiene tanto al suo contenuto quanto alla circostanza che esso sia stato effettivamente prestato*». Già sotto la Direttiva questo doveva essere *inequivocabile* nel caso di trattamento dei dati personali ordinari e *esplicito* per quelli sensibili. Nel GDPR la situazione non è mutata, nonostante Commissione e Parlamento con-

cordassero riguardo al fatto che ormai, nella lotta contro il fenomeno della raccolta indisciplinata dei dati personali su Internet, conservare la suddetta distinzione non avrebbe contribuito in alcun modo. In ogni caso il consenso andrà prestato in una forma espressa, anche orale, «*senza vincoli di forma scritta, né* ad substantiam *né* ad probationem*, salvo che non siano inseriti dal legislatore domestico in forza dei poteri riconosciuti agli stati membri ad opera del Regolamento medesimo*».

Il consenso può quindi dirsi inequivocabile quando, dalla «*dichiarazione o azione positiva inequivocabile*» dell'interessato, risulti ovvio che questo era rivolto ad uno specifico trattamento. Assumendo come inammissibili il silenzio, l'inattività o la precompilazione di caselle, la dichiarazione o azione positiva può dirsi inequivocabile quando espressa attraverso «*dichiarazione scritta, anche attraverso mezzi elettronici, o orale*» tra i quali: «*un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l›interessato accetta il trattamento proposto*», come ad esempio nel caso dei semplici gesti fisici.

Dato l'obbligo del titolare del trattamento di essere in grado di dimostrare che l'interessato vi abbia dato consenso, il metodo più sicuro per raccoglierlo sembrerebbe in ogni caso essere il consenso esplicito, nonostante non sia espressamente imposto dal regolamento per i dati ordinari. Il principio di libertà della forma va infatti «*temperato con l'onere probatorio posto in capo al titolare del trattamento dall'articolo 7 par. 1*». Per i titolari sembrerebbe quindi preferibile sviluppare modelli per il consenso che siano chiari, così da evitare le ambiguità e illustrare all'interessato l'azione da adottare per esprimerlo. Nonostante poi il GDPR non prescriva espressamente l'obbligo di fornire il consenso in via preventiva, questo è comunque implicito e dimostrarlo spetterà al titolare del trattamento, il quale potrà utilizzare ogni mezzo a sua disposizione a patto che questo non conduca ad un numero di trattamenti eccessivo.

3.2 IL CONSENSO ESPLICITO

In questo approfondimento un'ultima digressione la merita il requisito del consenso esplicito. Come visto in precedenza infatti, in base all'articolo

9(2) del GDPR, la possibilità di derogare al divieto di trattare categorie particolari di dati personali è stabilita in 10 ipotesi e alla lettera a) troviamo appunto il caso in cui l'interessato abbia «*prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri [disponga] che l'interessato non possa revocare il divieto di cui al comma 1*». Al di fuori di questa ipotesi, il consenso esplicito è richiesto anche nei casi previsti agli articoli 22 e 49 in materia di processi decisionali automatizzati e di trasferimento dei dati personali verso paesi terzi, pur essendo questi meno rilevanti ai fini della nostra trattazione.

Il consenso esplicito sembrerebbe dunque essere necessario in quelle ipotesi circoscritte da cui emerga un serio rischio per la protezione dei dati, tale per cui risulti essere più appropriato esercitare un livello di controllo maggiormente elevato. Se però, come abbiamo visto, il consenso regolare consiste già in una manifestazione di assenso espressa tramite dichiarazione o azione positiva inequivocabile, sembrerebbe difficile pretendere per il consenso esplicito il raggiungimento di uno standard più alto e complesso da parte del titolare del trattamento.

Il termine esplicito, infatti, si riferisce al modo in cui il consenso è espresso dall'interessato. Questo significa che anche in tal caso il soggetto deve fornire un'espressa affermazione del proprio consenso. Un metodo per fare ciò potrebbe dunque consistere nella dichiarazione scritta, in calce alla quale il titolare si deve assicurare che venga apposta la firma dell'interessato, così da evitare ogni possibile dubbio o la mancanza di prove per il futuro.

Anche nel caso del consenso esplicito è poi possibile utilizzare metodi diversi da quelli scritti. Esso può quindi essere inoltrato compilando un form elettronico, inviando una email, caricando un documento scannerizzato che riporti la firma dell'interessato, utilizzando la firma elettronica o altrimenti, laddove possibile, con una dichiarazione orale o una telefonata che consentano di dimostrare che tutte le condizioni per un consenso esplicito siano state rispettate al momento della registrazione. Scritto o orale, il consenso dovrà comunque essere statuito in un'affermazione chiara con una particolare attenzione nella formulazione. Anche nel caso dei contesti scritti, infatti, non tutti potranno dirsi espliciti, proprio per questo sarà sempre meglio fare uso di una espressione di consenso chiara.

Nel consenso esplicito è infine essenziale un riferimento alla ragione per cui questo viene richiesto. Nel caso di trattamento di categorie di dati sensibili, ad esempio, il titolare non potrà esimersi dallo spiegare che, proprio in ragione dello specifico oggetto del trattamento, il consenso necessario è quello «*esplicito*», così distinguendolo dagli altri richiesti.

Si potrebbe quasi concludere che, nonostante l'originaria volontà del Consiglio d'Europa di conservare la distinzione tra consenso «inequivocabile» ed «esplicito», alla fine, allo stato attuale, quello esplicito è improbabile che possa discostarsi molto dall'elevato standard richiesto per il consenso tradizionale e non sarebbe anzi strano domandarsi se, anche nel caso della deroga al trattamento di dati sanitari per finalità ex art. 9.2, lett. h), i) e j) adottare il requisito del consenso esplicito non possa essere un passaggio obbligato che prescinda dalla sua natura di deroga a sé stante. A tal riguardo è stato però evidenziato come nel GDPR la deroga in caso di consenso esplicito sia da considerarsi indipendente dalle altre, sottolineando come stia in realtà agli Stati membri decidere le modalità per regolarlo nel caso di trattamento dei dati sensibili per questa finalità.