PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Linee guida sulle questioni etiche e legali della protezione dei dati nella ricerca e nell'innovazione delle TIC

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR) – CONCETTI PRINCIPALI

Questo progetto è stato finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea con l'accordo di sovvenzione n. 788039. Il presente documento riflette esclusivamente il punto di vista degli autori e l'Agenzia non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.

2 Concetti principali

2.1 Dati personali

Simona Sobotovicova (UPV/EHU)

Questa parte delle Linee guida è stata rivista da Daniel Jove VIllares, Universidade Da Coruna, Spagna

Questa parte delle Linee guida è stata rivista e convalidata da Marko Sijan, Senior Advisor Specialist, (HR DPA)

2.1.1 Il concetto di dati personali

Per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile ("persona interessata"). La definizione di dati personali secondo il GDPR aggiunge che una persona fisica identificabile è quella che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificatore come un nome, un numero di identificazione, dati di localizzazione, un identificatore online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica[54]. Non c'è dubbio che l'obiettivo delle norme contenute nel GDPR è quello di proteggere i diritti e le libertà fondamentali delle persone fisiche e in particolare il loro diritto alla privacy, per quanto riguarda il trattamento dei dati personali. Tuttavia, a causa dell'ampia definizione di dati personali contenuta nel GDPR, il gruppo di lavoro dell'articolo 29 sulla protezione dei dati, le autorità nazionali di controllo della protezione dei dati e la giurisprudenza della Corte di giustizia europea (di seguito, CGCE) approvano la definizione di dati personali.

L'analisi del Gruppo dell'articolo 29 per la protezione dei dati sul concetto di dati personali nel parere 4/2007 si è basata sui seguenti quattro principali "elementi costitutivi" che possono essere distinti nella definizione di "dati[55] personali":

- *"Qualsiasi informazione"* - Questo termine segnala chiaramente la volontà del legislatore di disegnare un concetto ampio di dati personali. Questa formulazione richiede un'ampia interpretazione. Copre informazioni "oggettive", come la presenza di una certa sostanza nel sangue. Include anche informazioni "soggettive", opinioni o valutazioni. Inoltre, perché un'informazione sia un "dato personale", non è necessario che sia vera o provata.

54 Articolo 4(1) GDPR.

55 Vedi, Gruppo di lavoro per la protezione dei dati dell'articolo 29: Parere 4/2007 sul concetto di dati personali. Adottato il 20 giugno, 01248/07/EN WP 136, pp.9-12, 21. Disponibile all'indirizzo: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Bisogna dire che il concetto di dati personali include una gamma molto ampia di informazioni, "non solo oggettive ma anche soggettive", sotto forma di opinioni e valutazioni, purché "si riferiscano" alla persona interessata[56].

- *"Relativo a"* - In termini generali, le informazioni possono essere considerate "relative" a un individuo quando riguardano quell'individuo. Si potrebbe sottolineare che, per considerare che i dati "si riferiscono" a un individuo, dovrebbe essere presente un elemento "contenuto" o un elemento "scopo" o un elemento "risultato". Questi tre elementi (contenuto, scopo, risultato) devono essere considerati come condizioni alternative, e non cumulative, per cui è sufficiente la presenza di uno di questi elementi per essere considerati "relativi" a un individuo.

Nelle parole della CGCE i criteri di contenuto, scopo o effetto fungono da parametro per classificare alcune informazioni come dati personali. Se il contenuto, lo scopo o l'effetto sono collegati a una persona particolare, allora l'informazione è un dato personale. L'uso di uno di questi criteri è sufficiente per esistere per classificare qualsiasi informazione come dati[57] personali.

- *"Una persona identificata o identificabile"* - In termini generali, una persona fisica può essere considerata "identificata" quando, all'interno di un gruppo di persone, è "distinta" da tutti gli altri membri del gruppo. Di conseguenza, la persona fisica è "identificabile" quando, sebbene la persona non sia stata ancora identificata, è possibile farlo (questo è il significato del suffisso "-abile").

Il GDPR menziona questi "identificatori" nella definizione di "dati personali" nell'articolo 4(1) citato in precedenza. Inoltre, per quanto riguarda la determinazione se una persona fisica è identificabile, si dovrebbe tener conto di tutti i mezzi che possono essere ragionevolmente utilizzati, come l'individuazione, sia da parte del titolare del trattamento o da un'altra persona per identificare la persona fisica direttamente o indirettamente[58]. Tuttavia, se la persona è "identificabile", è ancora al centro delle recenti discussioni[59] degli studiosi.

- *"Persona fisica"* - La protezione si applica alle persone fisiche, cioè agli esseri umani. Il diritto alla protezione dei dati personali è, in questo senso, un diritto universale che non è limitato ai cittadini o residenti in un certo paese.

Il GDPR stabilisce che le persone fisiche possono essere associate a identificatori online forniti dai loro dispositivi, applicazioni, strumenti e protocolli, come indirizzi di protocollo internet, identificatori di cookie o altri identificatori come tag di identificazione a radio frequenza. Ciò può lasciare tracce che, in particolare se combinate con identificatori unici e

---

56 Sentenza della Corte di giustizia dell'Unione europea (seconda sezione), causa C-43 4/16, *Peter Nowak contro Commissario per la protezione dei dati*, 20 dicembre 2017, §34.

57 Sentenza della Corte di giustizia dell'Unione europea (seconda sezione), causa C-43 4/16, *Peter Nowak contro Commissario per la protezione dei dati*, 20 dicembre 2017, §35.

58 Considerando (26) GDPR.

59 Vedi, per esempio; Purtova, N. (2018). La legge del tutto. Concetto ampio di dati personali e futuro della legge europea sulla protezione dei dati. *Diritto, innovazione e tecnologia*. DOI:https://doi.org/10.1080/17579961.2018.1452176.

altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle[60]. Inoltre, i principi e le norme sulla protezione delle persone fisiche in relazione al trattamento dei loro dati personali dovrebbero, indipendentemente dalla loro nazionalità o residenza, rispettare i loro diritti e libertà fondamentali, in particolare il diritto alla protezione dei dati personali. Il presente regolamento intende contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone[61] fisiche.

Si potrebbe affermare che il gruppo di lavoro dell'articolo 29 sulla protezione dei dati afferma che questi quattro elementi forniti nella prima frase della definizione dei dati personali *(qualsiasi informazione relativa a una persona fisica identificata o identificabile)* sono strettamente intrecciati e si alimentano a vicenda, ma insieme determinano se un'informazione deve essere considerata come "dati personali".

2.1.2 Quali informazioni possono essere considerate come dati personali?

Le autorità nazionali di controllo della protezione dei dati e la giurisprudenza della Corte di giustizia europea giocano un ruolo essenziale nel fornire un'interpretazione delle disposizioni legali e una guida concreta ai titolari del trattamento e agli interessati, sostenendo una definizione di dati personali che sia abbastanza ampia. La definizione dei dati personali è un elemento centrale per l'applicazione e l'interpretazione delle norme sulla protezione dei dati che hanno un profondo impatto su una serie di questioni e argomenti importanti. Considerando il formato o il mezzo su cui l'informazione è contenuta, il concetto di dati personali include informazioni disponibili in qualsiasi forma, sia alfabetica, numerica, grafica, fotografica o acustica, per esempio[62]. La CGCE fornisce una classificazione delle informazioni come dati personali in diverse sentenze. In questa misura, il termine dati personali comprende senza dubbio il nome di una persona insieme alle sue coordinate telefoniche o informazioni sulle sue condizioni di lavoro o hobby. Anche le informazioni contenute in un testo libero in un documento elettronico possono qualificarsi come dati personali, a condizione che gli altri criteri della definizione di dati personali siano soddisfatti. La posta elettronica, per esempio, conterrà "dati personali". La CGCE si è espressa in questo senso quando ha considerato che "fare riferimento, in una pagina Internet, a varie persone e identificarle per nome o con altri mezzi, ad esempio fornendo il loro numero di telefono o informazioni relative alle loro condizioni di lavoro e hobby, costituisce il trattamento di dati personali [...][63].

Il 20 dicembre 2017 la CGCE con la sentenza sul "caso *Nowak*"[64] stabilisce la classificazione delle risposte e dei commenti soggettivi dell'esaminatore all'interno delle risposte scritte

60 Considerando (30) GDPR.
61 Considerando (2) GDPR.
62 Gruppo di lavoro per la protezione dei dati dell'articolo 29: Parere 4/2007 sul concetto di dati personali. Adottato il 20 giugno, 01248/07/EN WP 136, p.7. Disponibile su: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
63 Sentenza della Corte di giustizia europea, C-101/2001, *Lindqvist*, §27, 06.11.2003.
64 Sentenza della Corte di giustizia dell'Unione europea (seconda sezione), causa C-43 4/16, *Peter Nowak contro Commissario per la protezione dei dati*, 20 dicembre 2017.

presentate da un candidato in un esame professionale come dati personali, stabilendo una serie di criteri che permettono di capire quali dati sono di natura[65] personale. La sentenza affronta la potenziale applicazione del GDPR per costituire dati[66] personali. Bisogna sottolineare che la classificazione di questi dati come dati personali comporta, per il candidato, la possibilità di utilizzare i suoi diritti di accesso, rettifica e opposizione. In questo senso, la classificazione come dati personali prevede il diritto di accesso, ma anche gli altri poteri concessi al proprietario di questo tipo di dati, che sono: diritti di rettifica, cancellazione e opposizione, così come tutte le garanzie incluse nella legislazione[67] sulla protezione dei dati.

La sentenza analizza anche l'applicabilità del diritto di accesso ai dati con più di un proprietario e interessi opposti (in questo caso l'esaminatore e il candidato). La CGCE ha riaffermato l'idea che il fatto che l'informazione sia nelle mani di una o più persone è irrilevante per quanto riguarda la sua classificazione come dati personali. L'attribuzione della condizione di dati personali non deriva da questo fatto, ma dalla natura stessa dell'informazione. Per quanto riguarda la definizione di dati personali, la CGCE aggiunge un'altra caratteristica: la pluralità di persone interessate, o la possibilità che un'informazione sia dati personali di più di una persona[68].

A causa della classificazione di un'informazione come dato personale, nel caso *YS e altri*[69]*,* si ritiene che l'analisi giuridica di un verbale prodotto nell'ambito di una richiesta di permesso di soggiorno, non sia un dato personale in quanto si riferisce a "informazioni sulla valutazione e applicazione da parte dell'autorità competente della legge alla situazione del richiedente". Questa interpretazione ha fatto sì che, nel caso *YS e altri, il* diritto di accesso non fosse riconosciuto per quelle informazioni, ritenendo che tale accesso si sarebbe basato su un diritto di accesso ai documenti pubblici che non è coperto dalla legislazione[70] GDPR. Tuttavia, se l'analisi avesse incluso qualsiasi valutazione del soggetto, o che potesse avere uno sforzo su di esso, allora questo sarebbe stato considerato come dati personali che, come tali, sarebbero stati soggetti al GDPR[71].

Si potrebbe affermare che la definizione del GDPR, come ricordato dalla Corte di giustizia europea, si basa sull'ampia definizione di dati personali che riflette l'intenzione del legislatore di assegnare una vasta portata al concetto, comprendendo informazioni soggettive e oggettive sul soggetto dei dati. Poiché la classificazione delle informazioni come dati personali le porta nell'ambito dell'architettura di protezione dei diritti fondamentali dell'UE, stabilisce anche sia

65 Jove, D. (2019). Peter Nowak contro il commissario per la protezione dei dati: Potenziali postumi per quanto riguarda le annotazioni soggettive nelle cartelle cliniche. *European Data Protection Law Review*, Volume 5, Issue 2, p. 175. DOI: https://doi.org/10.21552/edpl/2019/2/7

66 Sentenza della Corte di giustizia dell'Unione europea (seconda sezione), causa C-43 4/16, *Peter Nowak contro Commissario per la protezione dei dati*, 20 dicembre 2017, §27.

67 Jove, D. (2019). Peter Nowak contro il commissario per la protezione dei dati: Potenziali postumi per quanto riguarda le annotazioni soggettive nelle cartelle cliniche. *European Data Protection Law Review*, Volume 5, Issue 2, p. 177. DOI: https://doi.org/10.21552/edpl/2019/2/7

68 Ibídem, p. 176, 178.

69 Sentenza della Corte, cause riunite C-141/12 e C-372/12, *YS e altri*, 17 luglio 2014.

70 Sentenza della Corte, cause riunite C-141/12 e C-372/12, *YS e altri*, 17 luglio 2014, §40.

71 Jove, D. (2019). Peter Nowak contro il commissario per la protezione dei dati: Potenziali postumi per quanto riguarda le annotazioni soggettive nelle cartelle cliniche. *European Data Protection Law Review*, Volume 5, Issue 2, p. 179. DOI: https://doi.org/10.21552/edpl/2019/2/7

i diritti degli interessati che le circostanze in cui lo standard di protezione può essere diminuito a causa di obiettivi giustificabili[72].

2.2 Elaborazione dei dati

Iñigo de Miguel Beriain (UPV/EHU)

Questa parte delle Linee guida è stata rivista da Daniel Jove Villares, Universidade Da Coruna, Spagna

Questa parte delle Linee guida è stata rivista e convalidata da Marko Sijan, Senior Advisor Specialist, (HR DPA)

2.2.1 Definizione

Secondo l'articolo 4(2) del GDPR, il trattamento "qualsiasi operazione o insieme di operazioni eseguite su dati personali o su insiemi di dati personali, con o senza l'ausilio di mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Pertanto, il concetto di trattamento è ampio. Esso copre una vasta gamma di operazioni eseguite su dati personali, anche con mezzi manuali o automatizzati, se fa parte di un archivio strutturato, cioè un insieme strutturato di dati personali che sono accessibili secondo criteri specifici, sia centralizzato, decentralizzato o disperso su base funzionale o geografica (art. 4(6)).

Chiaramente, l'elenco incluso nell'articolo 4(2) non è esaustivo, il che significa che anche altre operazioni con dati personali che funzionano bene con la definizione generale dovrebbero essere considerate trattamento secondo il GDPR. Alcuni esempi di trattamento includono: gestione del personale e amministrazione del libro paga; accesso/consultazione di un database di contatti contenente dati personali; invio di e-mail promozionali; triturazione di documenti contenenti dati personali; pubblicazione/inserimento di una foto di una persona su un sito web; memorizzazione di indirizzi IP o indirizzi MAC; registrazione video (CCTV), ecc. [73]

2.2.2 Il trattamento come concetto chiave nel GDPR

Il trattamento è un elemento essenziale in termini di diritti di protezione dei dati. Ciò che il GDPR regola veramente non sono i dati in sé, ma il trattamento dei dati personali. Questo uso

72 Podstawa, K. (2018). Peter Nowak Commissario per la protezione dei dati: Puoi accedere al tuo copione d'esame, perché è un dato personale. *European Data Protection Law Review (EDPL),* 4(2), pp. 254, 256. DOI: https://doi.org/10.21552/edpl/2018/2/17.

73 Commissione UE, Cosa costituisce il trattamento dei dati, all'indirizzo: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en.

dei dati fa scattare l'applicazione delle norme sulla protezione dei dati. Infatti, l'articolo 1(1) del GDPR afferma che "Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con **riguardo al trattamento dei dati personali** e norme relative alla libera circolazione dei dati personali."

Le circostanze del trattamento definiscono gli elementi normativi essenziali: la necessità (o meno) di trovare un motivo per trattare i dati, se si tratta di una categoria speciale; la base di legittimità appropriata; se si tratta di un trattamento uno ad uno o di un trattamento su larga scala; il livello di rischio specifico; le garanzie da attuare; e così via. Ogni trattamento sarà, insomma, un evento separato e indipendente, con caratteristiche e dimensioni proprie. Quindi, è sempre necessario pensare che le norme di protezione dei dati si applicano a ciascuno di essi.

2.3 Protezione dei dati per progettazione e per impostazione predefinita

Bud P. Bruegger (ULD)

Ringraziamenti: L'autore ringrazia l'aiuto di Kirsten Bock per l'interpretazione giuridica, il feedback e la revisione di Harald Zwingelberg e una revisione dettagliata e i suggerimenti di Hans Graux

Questa parte delle Linee guida è stata infine convalidata da Hans Graux, docente ospite sul diritto delle TIC e della protezione della privacy al Tilburg Institute for Law, Technology, and Society (TILT) e alla AP Hogeschool Antwerpen. Presidente del Vlaamse Toezichtscommissie (Comitato di vigilanza fiammingo), che controlla la conformità della protezione dei dati negli enti pubblici fiamminghi

La presente sezione cerca di fornire ai professionisti una comprensione più dettagliata di come attuare praticamente i requisiti dell'Art. 25 GDPR *Protezione dei dati per progettazione e per impostazione predefinita (**DPbDD**)*.

La presente sezione sul DPbDD è strutturata come segue:

Una prima sottosezione discute le Linee guida sull'argomento pubblicate dall'EDPB. Sottolinea le differenze con l'approccio adottato qui.

Una seconda sottosezione descrive la portata degli obblighi derivanti dall'art. 25 GDPR. Soprattutto, chiarisce in che modo i fornitori di tecnologia sono interessati da esso.

Una terza sottosezione analizza l'art. 25 GDPR. Poiché l'art. 25(1) obbliga i titolari del trattamento ad attuare misure sia al *momento della determinazione dei mezzi* che al *momento del trattamento stesso*, viene discusso il significato preciso della ***determinazione dei mezzi*** e del ***trattamento stesso.*** Questo si basa su un'analisi di ciò che il GDPR afferma sulla struttura del trattamento. L'analisi dell'art. 25(1) mette anche l'accento sul significato di ***efficacia*** delle misure. La discussione dell'art. 25(2) spiega cosa si intende esattamente con il termine ***default*** e analizza gli obblighi del titolare del trattamento.

Una quarta sottosezione si concentra sui processi effettivi che implementano la protezione dei dati per progettazione. In particolare, descrive i processi per implementare il DPbDD nelle tre fasi principali di *determinazione degli scopi*, *determinazione dei mezzi* e l'*elaborazione stessa*. Questi processi mirano a un'implementazione sistematica dei principi di protezione dei dati in ogni compito di lavoro di ogni fase. Questo porta poi all'identificazione e all'implementazione di misure tecniche e organizzative.

2.3.1 Linee guida del Comitato europeo per la protezione dei dati

L'European Data Protection Board (EDPB) ha pubblicato delle Linee guida sulla protezione dei dati per progettazione e per difetto[74]. Sottolinea l'importanza di comprendere e applicare i **principi di protezione dei dati** (vedi la sezione "Principi fondamentali" nella parte generale di queste Linee guida) e di implementare i **diritti degli interessati** (vedi la sezione "Diritti degli interessati" nella parte generale di queste Linee guida).

L'importanza dei principi di protezione dei dati è per esempio espressa nel paragrafo 61: "I titolari del trattamento devono attuare i principi per realizzare il DPbDD. Questi principi includono: trasparenza, legittimità, equità, limitazione delle finalità, minimizzazione dei dati, accuratezza, limitazione della conservazione, integrità e riservatezza, e responsabilità. Questi principi sono delineati nell'articolo 5 e nel considerando 39 del GDPR. Per avere una comprensione completa di come implementare il DPbDD, si sottolinea l'importanza di comprendere il significato di ciascuno dei principi."

L'importanza dei diritti degli interessati è dichiarata nel paragrafo 63: "Mentre questa sezione si concentra sull'attuazione dei principi, il titolare del trattamento dovrebbe anche attuare modi appropriati ed efficaci per proteggere i diritti degli interessati, anche secondo il capo III del GDPR dove ciò non è già previsto dai principi stessi."

La linea guida EDPB dedica la sua sezione 3 all'attuazione dei principi di protezione dei dati. Le Linee guida PANELFIT vanno oltre, fornendo una descrizione più dettagliata di ogni principio insieme a molti esempi di misure tecniche e organizzative adatte a implementare quei principi.

Come le Linee guida EDPB, anche il seguente testo analizza il significato dell'articolo 25 GDPR. Tuttavia, il presente testo cerca di fornire ulteriori indicazioni concrete. Per raggiungere questo obiettivo, non solo fornisce un'analisi legale delle fasi del trattamento secondo il GDPR, ma anche un'analisi tecnica di quali compiti sono necessari per ogni fase. In particolare, questo viene fatto per *determinare i mezzi di trattamento* e per il *trattamento stesso*. In ognuno dei compiti che sono identificati, i principi di protezione dei dati possono essere applicati e le misure tecniche e organizzative identificate e implementate.

Una seconda grande differenza tra il presente testo e le Linee guida dell'EDPB è che il primo discute l'effettivo processo necessario per applicare il DPbDD nelle varie fasi.

Una differenza minore è che il presente testo entra in ulteriori dettagli su come i titolari del trattamento possono trasmettere i requisiti ai produttori di software e servizi. Il testo non entra nel merito della certificazione, comunque; se questo dovesse essere rilevante per i lettori, sono rimandati alle Linee guida EDBP.

74 Comitato europeo per la protezione dei dati, Linee guida 4/2019 sull'articolo 25 sulla protezione dei dati per progettazione e per impostazione predefinita, versione 2.0, adottata il 20 ottobre 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (ultima visita 30/11/2021).

2.3.2 La portata del DPbDD

Questa sezione discute come il GDPR contenga solo obblighi per i titolari del trattamento (e responsabili del trattamento) e come questo possa influenzare indirettamente i fornitori di tecnologia.

La protezione dei dati per progettazione può essere vista come la presa in considerazione della protezione dei dati non solo per le operazioni di *trattamento* che hanno luogo nella fase operativa, ma anche prima nelle fasi di pianificazione e attuazione. Più in generale, si potrebbe vedere la protezione dei dati per progettazione come una metodologia che prende in considerazione la protezione dei dati in tutte le fasi del ciclo di vita di un'*attività di trattamento*[75], che va dalla concezione, alla progettazione e all'implementazione, all'uso operativo e allo smantellamento finale.

L'intero ciclo di vita coinvolge generalmente attività di attori diversi dal titolare e dal responsabile del trattamento. Soprattutto, molte decisioni che riguardano gli aspetti di protezione dei dati di un'attività di trattamento sono prese da fornitori di tecnologia, che spesso progettano e implementano software e sistemi. Quando i fornitori di tecnologia investono nello sviluppo di prodotti e servizi che vengono poi offerti sul mercato, contribuiscono anche a definire il livello di sviluppo di un certo tipo di trattamento dei dati personali.

Al contrario, il GDPR esprime obblighi per i titolari del trattamento e i responsabili del trattamento. Manca qualsiasi obbligo diretto per i fornitori di tecnologia. Nel suo *parere preliminare sulla privacy by design*[76], il GEPD sottolinea questo fatto affermando quanto segue: [77]

"Una grave limitazione degli obblighi dell'articolo 25 è che si applicano solo per imporre un obbligo ai titolari del trattamento e non agli sviluppatori di quei prodotti e tecnologie utilizzati per trattare i dati personali. L'obbligo per i fornitori di prodotti e tecnologie non è incluso nelle disposizioni sostanziali del GDPR."

Poiché il GDPR nel suo complesso, e l'art. 25 in particolare, esprimono solo obblighi per i titolari del trattamento (e responsabili del trattamento), la portata della presente sezione è limitata di conseguenza.

Mentre non ci sono obblighi legali per i fornitori di tecnologia, l'art. 25 GDPR li influenza comunque indirettamente. Il considerando 78 del GDPR accenna a questo affermando quanto segue[78]: *"I principi della protezione dei dati by design e by default dovrebbero essere presi in considerazione anche nel contesto degli appalti pubblici."* Come avviene l'influenza sui fornitori di tecnologia è descritto più in dettaglio nel seguito.

L'argomento si concentra sul software creato da un fornitore di tecnologia. Ci sono due opzioni per come un titolare del trattamento può ottenere tale software:

- Come risultato di uno sviluppo personalizzato, o
- Acquisendo il software sul mercato.

---

75 Il termine *attività di trattamento* è qui utilizzato nel senso dell'art. 30 GDPR *record di attività di trattamento* e 4(16)(b) GDPR. In entrambi i casi, un'*attività di trattamento* è l'unità di base dell'impresa di un responsabile del trattamento che comporta il trattamento di dati personali.

76 Il Garante europeo della protezione dei dati (GEPD), parere 5/2018, parere preliminare sulla privacy by design, 31 maggio 2018, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (ultima visita 29/6/2020).

77 Pagine 7 e 8, lato numero 37.

78 Vedi la frase 5.

Nel primo caso, la progettazione e lo sviluppo della software house è attivata dal titolare del trattamento e il fornitore di tecnologia può essere sia interno che esterno; nel secondo caso, c'è una moltitudine di titolari del trattamento con esigenze simili che creano una domanda di mercato per certi tipi di software. La progettazione e lo sviluppo del software sono quindi innescati dal fornitore di tecnologia con l'obiettivo di raggiungere una posizione competitiva sul mercato.

I dettagli tecnici inerenti allo sviluppo del software sono di solito inaccessibili ai titolari del trattamento e ai loro rappresentanti. Pertanto, in entrambi i casi, l'interazione tra titolari del trattamento e fornitori di tecnologia è limitata alla comunicazione sui requisiti. In particolare, il ruolo dei requisiti nei due casi è il seguente:

- Nel caso dello sviluppo personalizzato, i requisiti sono lo strumento principale dei titolari del trattamento per esprimere gli obiettivi del processo di sviluppo. I requisiti sono anche usati per determinare se il processo di sviluppo è terminato con successo. Questo accade durante il test di accettazione.
- Nel caso di titolari del trattamento che acquistano software, hanno bisogno di requisiti per guidare la loro selezione di un software adeguato dall'offerta del mercato. Nelle gare d'appalto, tali requisiti possono essere comunicati ai fornitori di tecnologia al fine di sollecitare offerte adeguate alle esigenze; quando il software viene acquistato senza gara, i titolari del trattamento devono verificare se le varie offerte di software candidate soddisfano i requisiti. In entrambi i casi, la convalida delle offerte rispetto ai requisiti è un fattore importante nella decisione di acquisto da parte del titolare del trattamento.

Così, mentre gli obblighi per i fornitori di tecnologia sono fuori dal campo di applicazione dell'Art. 25, i titolari del trattamento sono obbligati a determinare adeguati requisiti di protezione dei dati e hanno la piena responsabilità del software che utilizzano. La convalida del software rispetto ai requisiti può prendere in considerazione il livello di sviluppo e il costo di implementazione (vedi art. 25 GDPR e la discussione successiva). L'assenza o il costo eccessivo di un software adeguato sul mercato non può tuttavia essere considerato una valida giustificazione per l'utilizzo di un software inadeguato.

2.3.3 Analisi dell'articolo 25. Protezione dei dati per progettazione

La presente sezione analizza la lettera della legge con l'**obiettivo** di trovare **un approccio strutturato e sistematico** per discutere le misure che i titolari del trattamento sono tenuti ad attuare dall'Art. 25 GDPR. La sistematica e la struttura risultante sono poi **utilizzate nella sezione 2.3.3.1 sulle misure** che costituisce la guida più concreta per i professionisti.

Per favorire una chiara comprensione del testo, il seguente riquadro definisce due termini spesso usati.

Definizione: ***attività di elaborazione***

Il termine *attività di trattamento* è qui utilizzato nel senso dell'art. 30 GDPR *record di attività di trattamento* e 4(16)(b) GDPR. In entrambi i casi, un'attività di trattamento è l'unità di base autonoma dell'impresa di un titolare del trattamento che comporta il trattamento di dati personali. Un'attività di trattamento subisce un ciclo di vita che comprende la concezione, la progettazione, l'attuazione, il funzionamento e lo smantellamento.

Definizione ***operazione di elaborazione***

Il termine *operazione di trattamento* si riferisce solo alla fase operativa di un'*attività di trattamento* in cui un sistema di trattamento viene utilizzato per trattare effettivamente i dati personali. Esso comporta l'esecuzione delle *operazioni di trattamento* come sono definite nell'art. 4(2) GDPR. Altri aspetti delle attività di trattamento, come la concezione e la progettazione, non eseguono tali operazioni di trattamento e non sono quindi considerati parte delle operazioni di trattamento.

2.3.3.1 Panoramica e obbligo principale per i titolari del trattamento

L'art. 25 GDPR comprende quanto segue:

Art. 25(1):

Tenendo conto [..], ***il titolare del trattamento deve****, sia al momento della determinazione dei mezzi di trattamento che al momento del trattamento stesso,* ***mettere in atto misure tecniche e organizzative adeguate*** *[...] volte ad attuare in modo efficace i principi di protezione dei dati [...] e ad integrare nel trattamento le garanzie necessarie [...].*

L'obbligo principale per i titolari del trattamento di cui all'art. 25(1) GDPR è quindi che essi "***devono*** *[.....]* ***attuare misure tecniche e organizzative adeguate*** *[...] che sono destinate* ***ad attuare i principi di protezione dei dati***" (vedi la sezione "Principi fondamentali" nella parte generale di queste Linee guida).

In tutto il GDPR[79], si afferma che l'implementazione di misure tecniche e organizzative è il modo per rispettare i principi di protezione dei dati. Ciò implica che tutto ciò che un titolare del trattamento fa a sostegno dei principi di protezione dei dati deve essere considerato come una misura. Di conseguenza, il **concetto di misura** deve essere **inteso in un senso molto ampio**. Ciò significa che non si limita agli artefatti fisici (come i firewall), o azioni specifiche (come la formazione del personale). Piuttosto, deve comprendere anche tutte le considerazioni e decisioni che sono necessarie per determinare i mezzi di trattamento in un modo che sia conforme ai principi e agli obblighi della protezione dei dati.

L'art. 25(1) GDPR afferma anche che queste misure devono essere attuate "***in modo efficace***". L'efficienza sarà quindi analizzata di seguito.

Inoltre, l'art. 25(1) afferma che le misure sono attuate "***per integrare le garanzie necessarie nel trattamento***". In altre parole, l'attuazione delle misure è il modo per raggiungere l'obiettivo di integrare le garanzie necessarie nel trattamento. Grammaticalmente, questa interpretazione diventa ancora più chiara quando si espande "*integrare*" nella sua forma completa di "*per integrare*". Il "per" esclude l'interpretazione che, oltre all'*implementazione delle misure*, sia richiesta anche l'*integrazione delle garanzie.*

Probabilmente, l'essenza dell'Art. 25(1) sta nella formulazione "*sia* ***al momento della determinazione dei mezzi*** *per il trattamento che* ***al momento del trattamento stesso****".* Ciò significa che l'attuazione delle misure deve avvenire in **due periodi di tempo distinti**. Implica quindi un **modello a fasi per un'attività di trattamento**. Ciò è compatibile con l'interpretazione della protezione dei dati fin dalla progettazione, che considera la protezione dei dati in ogni fase di un'attività di trattamento. L'interpretazione giuridica delle fasi del trattamento di cui all'art. 25(1) è fornita nella seguente sottosezione.

79 Questo include tra gli altri l'art. 24, 25 e 32 GDPR.

2.3.3.2 Le fasi del trattamento nel GDPR

L'art. 25(1) GDPR parla di due fasi in relazione a un'attività di trattamento, cioè "**il *momento della determinazione dei mezzi* per il trattamento**" e "**il *momento del trattamento stesso***". È evidente che entrambi questi *tempi* devono essere periodi di tempo di una certa durata molto più che punti nel tempo. È anche evidente che il momento della determinazione dei mezzi deve precedere il momento della elaborazione stessa. Chiamiamo quindi questi periodi di tempo anche ***fasi***.

L'art. 4(7) afferma che oltre ai mezzi, il titolare del trattamento "**determina** anche **gli scopi**". Anche questo evidentemente richiede tempo e precede la determinazione dei mezzi. Sembra utile includere la determinazione delle finalità per completezza e nel caso in cui ci siano misure che possono essere attuate in quella fase.

Di conseguenza, il GDPR implica il seguente **modello di fase di un'attività di trattamento**:

- Fase 1: Determinazione degli scopi
- Fase 2: Determinazione dei mezzi
- Fase 3: Elaborazione stessa

Per capire meglio cosa succede esattamente in ogni fase, è necessario analizzare più in dettaglio la concezione che il GDPR ha di un'operazione di trattamento.

2.3.3.3 Operazioni di trattamento nel GDPR

Di seguito si analizza la concezione che il GDPR ha di un'operazione di trattamento.

L'art. 5(1)(f) GDPR afferma la necessità di "protezione contro il trattamento non autorizzato"... Ciò implica che il trattamento ordinario deve essere **autorizzato**. È anche chiaro dal contesto che tale autorizzazione deve provenire dal titolare del trattamento che ha la piena responsabilità del trattamento. Ma come può un titolare del trattamento limitare il trattamento a ciò che è autorizzato?

Una risposta parziale a questa domanda può essere trovata nell'art. 29 GDPR: "Il responsabile del trattamento e chiunque **agisca sotto l'autorità del titolare del trattamento** o del responsabile del trattamento, che abbia accesso ai dati personali, non deve trattare tali dati se non **su *istruzioni* del titolare del trattamento**, [..]". Anche l'art. 32(4) GDPR usa una formulazione molto simile. L'art. 29 GDPR implica la seguente concezione:

- L'operazione di trattamento è eseguita da "una **persona fisica che agisce sotto l'autorità del titolare del trattamento o del responsabile del trattamento**". Tali persone sono il più delle volte *dipendenti* del titolare del trattamento, ma potrebbero anche lavorare per un responsabile o lavorare senza un effettivo impiego[80]. Sono chiamate ***risorse umane*** nel seguito. Si noti che queste persone controllano a loro volta i mezzi tecnici che supportano o automatizzano parzialmente il trattamento[81].
- Il **mezzo** con cui un **titolare del trattamento assicura che solo il trattamento autorizzato abbia luogo** è attraverso l'emissione di ***istruzioni***.

80 Vedi anche le Linee guida EDPB sui concetti di titolare e responsabile del trattamento nel GDPR, paragrafo 88 per una discussione sul significato di "persone che, sotto l'autorità diretta del titolare o del responsabile del trattamento, sono autorizzate a trattare dati personali".

81 Si noti che anche nel caso di "elaborazione completamente automatica", è sempre una persona che controlla tale elaborazione avviandola e fermandola. Il controllo da parte di una persona è ancora più evidente quando si guardano gli "strumenti" computerizzati che sono utilizzati da esseri umani attraverso un'interfaccia uomo-macchina.

Per assicurare che solo il trattamento autorizzato abbia luogo, le istruzioni devono specificare tutti gli aspetti rilevanti dell'attività di trattamento: **chi, quando, cosa** e **come**. In altre parole, le risorse umane devono agire solo **su istruzione** (chi, quando) e **secondo le istruzioni** (cosa, come).

Anche se con meno chiarezza, il GDPR afferma anche che le **risorse tecniche** sono necessarie. Questo è molto chiaro nel considerando 39 (frase 12) che parla delle "**attrezzature utilizzate per il trattamento**". Altri termini relativi alle risorse tecniche che vengono utilizzati nel GDPR sono "attrezzature per il trattamento dei dati" nell'Art. 58(1)(f) e "sistemi di trattamento" nell'Art. 32(1)(b).

Mentre il GDPR usa il termine *istruzione* solo nel contesto delle risorse umane, è chiaro che **anche le risorse tecniche richiedono istruzioni** per eseguire solo il trattamento autorizzato. Nel dominio tecnico, il termine *istruzioni macchina* è usato qui. Un tipo importante di tali istruzioni è il ***software***.

In sintesi, quando si guarda a una **risorsa individuale** (umana o tecnica), il GDPR ha la seguente concezione di un'operazione di trattamento:

operazione di elaborazione individuale
=
esecuzione delle istruzioni del titolare del trattamento **da parte di una** singola **risorsa**

Nella maggior parte dei casi, le **operazioni complessive di elaborazione** coinvolgono un sistema di una moltitudine di risorse umane e tecniche che interagiscono. Questo si esprime nel seguente modo:

operazioni complessive di trattamento

moltitudine di singole **operazioni di trattamento**
eseguite **da singole risorse** umane e tecniche

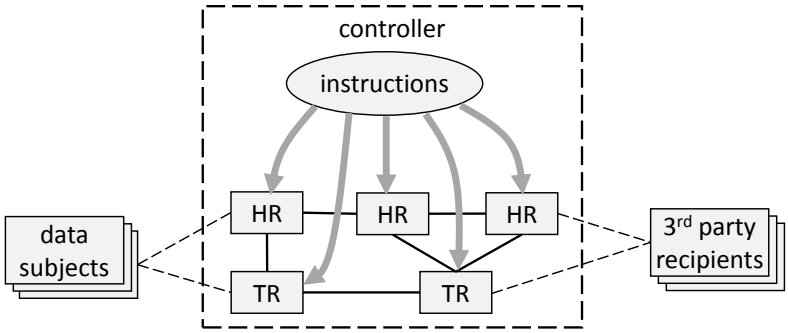

Figura 5: La concezione del GDPR di un trattamento.

Figura 5 illustra il concetto di trattamento del GDPR in un contesto più ampio. Illustra il dominio di responsabilità del titolare del trattamento con un riquadro tratteggiato. Il titolare del trattamento determina le operazioni di trattamento autorizzate emettendo o selezionando/approvando[82] istruzioni sia alle risorse umane (HR) che agiscono sotto la sua autorità (vedi art. 29 GDPR) sia alle risorse tecniche (TR) sotto il suo controllo. Tutte le

82 La selezione e l'approvazione delle istruzioni da parte di un titolare avviene, per esempio, quando si acquista un software di serie o quando un titolare sceglie il servizio di un determinato responsabile del trattamento.

risorse interagiscono per formare il sistema complessivo di trattamento. Il contesto di questo sistema di trattamento è definito dagli *interessati che* interagiscono con le risorse umane e/o tecniche e, facoltativamente, con i *destinatari terzi* (cfr. art. 4(9) e (10) GDPR) ai quali le risorse comunicano i dati personali.

Questo modello di elaborazione rappresenta l'elaborazione autorizzata dal titolare del trattamento. Viene utilizzato nella prossima sezione per capire meglio cosa comporta effettivamente la *determinazione dei mezzi.*

2.3.3.4 Determinazione dei mezzi

Nelle sue Linee guida sui concetti di titolare del trattamento e responsabile del trattamento nel GDPR[83], il Comitato europeo per la protezione dei dati fornisce un'analisi giuridica di ciò che significa *determinare i mezzi di* trattamento. La discussione qui è più orientata tecnicamente. Il Comitato distingue tra mezzi "essenziali" e "non essenziali"; questi ultimi possono essere determinati anche dai responsabili del trattamento. Il presente testo non fa tale distinzione e si limita a fornire un'interpretazione tecnica delle decisioni che la determinazione dei mezzi comporta.

La determinazione dei mezzi è una fase che precede l'uso operativo di un sistema di elaborazione e prepara e allestisce tutto ciò che è necessario per le operazioni di elaborazione vere e proprie. Ciò significa che, guidato dagli *scopi*, un titolare del trattamento deve pianificare, progettare e implementare tutto ciò che è necessario per consentire l'*elaborazione stessa*. Questo include almeno i seguenti compiti:

- **Determinare** le **risorse** umane e tecniche necessarie per l'elaborazione;
- **Determinare** le **istruzioni** che **definiscono l'elaborazione autorizzata** e che sono adatte alle risorse;

Ciò che questo comporta in modo più dettagliato è descritto qui di seguito.

La determinazione delle risorse umane comporta almeno quanto segue:

- Pianificazione che determina quali risorse umane sono necessarie, selezionando le risorse umane adatte e portandole sotto l'autorità del titolare del trattamento o responsabile del trattamento. Questo è generalmente fatto attraverso l'assunzione che stabilisce una relazione contrattuale tra il dipendente e il titolare del trattamento.
- Mettere le risorse umane in una condizione in cui possano tradurre le istruzioni in un modo che costituisca un trattamento autorizzato. Questo può comportare:
    - la sottoscrizione di un accordo di astensione dalla divulgazione dei dati personali
    - l'impegno della risorsa umana a certe politiche generali o codici di condotta
    - formazione della risorsa umana per acquisire le conoscenze e le competenze necessarie per eseguire le istruzioni nel modo desiderato

La determinazione delle risorse tecniche comporta almeno quanto segue:

- Pianificazione, selezione e acquisizione delle risorse tecniche necessarie.
- Portare le risorse tecniche in una condizione tale che possano eseguire le operazioni di elaborazione necessarie. Questo può comportare cose come

83 Comitato europeo per la protezione dei dati, Linee guida 07/2020 sui concetti di titolare e responsabile del trattamento nel GDPR, versione 2.0, adottate il 07 luglio 2021, https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (ultima visita 2/12/2021).

- installazione fisica
- configurazione
- integrazione nell'infrastruttura usata
- installando il software necessario

Determinazione delle istruzioni per le risorse in generale: Dopo aver discusso la determinazione delle risorse, di seguito si analizza la determinazione delle istruzioni. Guardando Figura 5è chiaro che esistono i seguenti tipi di istruzioni:

- Istruzioni che determinano il comportamento di una **singola risorsa**
- istruzioni che determinano l'**interazione tra** più **risorse**
- istruzioni che determinano l'**interazione** tra le risorse e gli **interessati**
- istruzioni che determinano la divulgazione dei dati personali a **terzi destinatari**

Questi diversi tipi di istruzioni sono discussi più in dettaglio nel seguito, mentre si distingue tra risorse umane e tecniche.

La determinazione delle istruzioni per le risorse umane viene discussa di seguito:

- **Le istruzioni per le risorse umane individuali** possono essere espresse in due stili diversi:
  - Definire gli output richiesti, i prodotti e gli effetti che l'attività della risorsa umana deve produrre. Questo costituisce ***istruzioni dichiarative*** che si concentrano sull'aspetto "***cosa***" e si affidano alla capacità della risorsa per riempire l'aspetto "***come***" delle istruzioni.
  - Descrizioni dettagliate del modo in cui un'attività deve essere eseguita. Si tratta di ***istruzioni imperative*** che si concentrano sul ***come***, richiedono meno intelligenza e autonomia da parte della risorsa che esegue e spesso definiscono l'aspetto del "***cosa***" in modo più implicito.
- **Istruzioni su come le risorse umane interagiscono tra loro**: Questo include la progettazione e la specificazione di *processi di business*, *flussi di lavoro* e *flussi di dati*. Ci sono vari linguaggi[84] formali e notazioni[85] grafiche per supportare tali attività.
- **Istruzioni su come le risorse umane interagiscono con le risorse tecniche**: Le risorse tecniche non sono autonome. Piuttosto, sono controllate da esseri umani (cioè, risorse umane). Anche la risorsa tecnica più autonoma ha bisogno di essere accesa. Di solito, le risorse umane esercitano un ulteriore controllo sulla risorsa tecnica attraverso ***interfacce utente*** e tramite l'*interazione uomo-macchina* (HMI). Un modo comune per modellare tali interazioni sono i ***diagrammi dei casi d'uso***. Questi sono spesso usati anche per la *specifica* dei *requisiti funzionali* del software. Le istruzioni su come gli esseri umani interagiscono con le risorse tecniche definiscono anche quali risorse umane sono **autorizzate ad accedere a** quali risorse tecniche per quali scopi. Questi tipi di istruzioni determinano quindi anche la **responsabilità** che le risorse umane hanno per il funzionamento di certe risorse tecniche.

84 Questi linguaggi formali includono per esempio l'*XML Process Definition Language* (XPDL) e il *Business Process Execution* Language (BPEL).

85 Queste visualizzazioni grafiche includono per esempio il *Business Process Model and Notation* (BPMN), *Activity Diagrams*, *diagrammi di flusso* e *Petri Nets*.

- **Le istruzioni su come le risorse umane interagiscono con gli interessati** determinano quali interazioni gli interessati possono avere con il titolare del trattamento. Ciò include il trattamento manuale delle invocazioni dei diritti degli interessati (cfr. Capitolo 3 GDPR) e le interazioni previste con il responsabile della protezione dei dati (DPO) (cfr. Art. 38(4) GDPR).
- **Le istruzioni su come le risorse umane interagiscono con i terzi destinatari** determinano quali dati personali sono comunicati manualmente ai terzi destinatari.

La determinazione delle istruzioni per le risorse tecniche comporta quanto segue:

- **Le istruzioni per le risorse tecniche individuali** comprendono potenzialmente i seguenti aspetti:
    - Acquisto[86] di ***software*** che di solito costituisce istruzioni macchina che sono espresse in qualche linguaggio di programmazione formale (imperativo o dichiarativo). Il comportamento del software può dipendere da parametri che possono essere determinati in un momento successivo; tali parametri sono generalmente chiamati *configurazione*. La decisione se la configurazione è possibile e quali parametri comporta è incorporata nel software. Ci sono due tipi di configurazione,
        - quello determinato dal titolare del trattamento
        - quello controllato dall'interessato (per esempio *preferenze* e *impostazioni* supportate da un'interfaccia utente appropriata)
    - ***Configurazione*** del software **da parte del titolare del trattamento**.
    - **Specificazione dei *valori predefiniti*** per le configurazioni eseguite dall'interessato. Questo è ovviamente l'oggetto della ***protezione dei dati per difetto*** che è regolata nell'art. 25(2) GDPR (vedi sezione 2.3.4 sotto).
- **Istruzioni su come le risorse tecniche interagiscono tra loro:** Le risorse tecniche possono interagire tra loro quando hanno ***interfacce*** che sono collegate da ***canali di*** comunicazione. Le comunicazioni che possono avvenire sono generalmente determinate da ***protocolli***. Le comunicazioni possono essere rappresentate, per esempio, da ***diagrammi di interazione*** come i *diagrammi di sequenza UML* e i *diagrammi di comunicazione UML*. Tali comunicazioni comportano generalmente lo scambio di dati (personali). Questi possono essere rappresentati graficamente in ***diagrammi di flusso di dati***. Questo tipo di istruzioni determina anche quali risorse tecniche sono **autorizzate** a interagire con quali altre per quali scopi. Gli aspetti determinati da questo tipo di istruzioni sono spesso legati al concetto di ***architettura tecnica (componente)***.
- **Le istruzioni su come le risorse tecniche interagiscono con gli interessati** sono generalmente utilizzate per la **configurazione da parte degli interessati** (cfr. art. 25(2) GDPR e la sua discussione più avanti) e per il supporto automatizzato dei ***diritti degli interessati*** (cfr. capitolo 3 GDPR). Entrambi richiedono ***interfacce utente appropriate***. Anche in questo caso, i *diagrammi dei casi d'uso* possono essere utilizzati per rappresentarli. Ancora una volta, l'***autenticazione*** e il ***controllo***

86 L'approvvigionamento è qui usato come un termine collettivo che comprende sia lo sviluppo personalizzato che l'acquisizione di software dal mercato. In entrambi i casi, i titolari sono responsabili di un'adeguata analisi dei requisiti e delle specifiche.

dell'accesso sono necessari per la risorsa tecnica per determinare se l'utente è effettivamente l'interessato legittimo.

- **Le istruzioni sul trasferimento automatico di dati a terzi destinatari** determinano quali dati (personali) vengono divulgati, a quali condizioni e come. Questo generalmente richiede interfacce per esseri umani o macchine e canali di comunicazione appropriati. I dati possono essere spinti ai destinatari o rivelati su richiesta. L'autenticazione (di persone o macchine) e il controllo dell'accesso sono generalmente rilevanti anche qui.

Identificare le misure tecniche e organizzative appropriate: Come è stato discusso nella sezione 2.3.3.1 sopra, l'art. 25(1) obbliga i titolari del trattamento a mettere in atto *misure tecniche e organizzative adeguate, volte ad attuare i principi di protezione dei dati* anche al momento della *determinazione dei mezzi*. È stato argomentato sopra, che la determinazione dei mezzi consiste nel determinare le risorse e le istruzioni. Inoltre, insieme, risorse e istruzioni costituiscono un sistema di trattamento in grado di eseguire le istruzioni autorizzate sui dati personali reali.

È chiaro che le misure richieste devono essere integrate con questo sistema di trattamento. Vale a dire, devono essere integrate nelle sue istruzioni e applicate alle sue risorse. In altre parole, tali misure non possono essere determinate indipendentemente. Piuttosto, devono essere determinate insieme alla determinazione delle istruzioni e delle risorse. In ogni fase della determinazione di una parte o di un aspetto del sistema di trattamento, i principi della protezione dei dati devono essere presi in considerazione per identificare e integrare misure adeguate.

Per questo motivo, gli aspetti di un sistema di elaborazione che sono stati distinti nella discussione precedente identificano direttamente le aree in cui devono essere trovate e implementate misure appropriate. Questa sezione è quindi strumentale nel fornire una struttura per la discussione dettagliata delle misure nella sezione seguente**2.3.3.1**. Serve anche a raggiungere una certa completezza considerando sistematicamente tutti gli aspetti e ogni principio.

2.3.3.5 Elaborazione stessa

L'elaborazione stessa è **avviata** dal **via libera** del titolare del trattamento alle risorse per iniziare l'esecuzione delle istruzioni emesse. Da questo punto in poi, il **trattamento dei dati personali effettivi** inizia ad avere luogo. Vale a dire, viene eseguito dalle risorse designate che seguono le istruzioni del titolare del trattamento.

Il *trattamento stesso* **termina** quando non vengono più trattati dati personali. Considerando che secondo l'Art. 4(2) GDPR la *memorizzazione* dei dati personali costituisce un trattamento, la cessazione del *trattamento stesso* va oltre il semplice dire alle risorse di smettere di eseguire le istruzioni emesse. Piuttosto, richiede anche **ulteriori istruzioni** per accertare che i dati personali non vengano più memorizzati. Chiamiamo questo ***smantellamento*** delle operazioni di trattamento. Lo smantellamento comprende la ***cancellazione*** e la ***distruzione*** dei dati personali, entrambi i quali costituiscono ancora un *trattamento* ai sensi dell'art. 4(2). 4(2).

L'art. 25(1) richiede ai titolari del trattamento di attuare anche misure tecniche e organizzative appropriate durante il trattamento stesso. In analogia alla *determinazione dei mezzi*, la struttura trovata per il trattamento stesso sarà usata per guidare la discussione delle misure.

2.3.3.6 Rideterminazione dei mezzi durante l'elaborazione operativa

Considerando che il risultato della determinazione dei mezzi sono le risorse e le istruzioni, è comune rideterminare i mezzi anche durante l'elaborazione operativa. I seguenti esempi lo illustrano:

- **Sostituzione di risorse** tecniche carenti e di risorse umane non disponibili. La sostituzione delle risorse può essere temporanea o permanente.
- **Aggiunta, sottrazione o sostituzione di risorse** per adattarsi a un **volume di elaborazione che cambia**. Questo potrebbe per esempio includere l'aggiunta di risorse umane a un'unità di lavoro sovraccarica o la sostituzione di una risorsa tecnica con una più potente.
- **Cambio di istruzioni** per migliorare l'**efficienza e l'efficacia**. Questo può includere per esempio gli aggiornamenti di routine del software all'ultima versione. Altri esempi sono il miglioramento evolutivo delle istruzioni o la riprogettazione dei processi organizzativi.
- Oltre a questo, è possibile anche un'estensione dei **mezzi** per supportare un'**estensione degli scopi.** Questo generalmente va di pari passo con una funzionalità aggiuntiva supportata dall'elaborazione.

Poiché tale rideterminazione dei mezzi è ancora determinazione dei mezzi, anche qui, misure appropriate devono essere attuate dal titolare del trattamento. L'analisi di cui sopra sarà quindi utilizzata anche per strutturare la discussione sui mezzi nel seguito2.3.3.1.

2.3.3.7 Efficacia delle misure

Di seguito si analizza il requisito dell'art. 25(1) GDPR che le misure devono essere attuate "***in modo efficace***". Lo fa nel contesto dell'altra formulazione dell'art. 25(1) GDPR.

A differenza dell'analisi precedente, la presente non sarà usata per identificare le aree per le quali si devono trovare misure. Piuttosto, sarà usata come un aspetto importante che deve essere considerato per ciascuna delle misure proposte.

L'art. 25(1) GDPR incarica i titolari del trattamento di attuare misure appropriate "*che sono destinate ad attuare i **principi di protezione dei dati***" al fine di "*integrare le **garanzie** necessarie nel trattamento*". In questo contesto, il requisito dell'efficacia esprime che non è un obiettivo in sé l'attuazione di misure. Piuttosto, le misure hanno valore solo in base alla loro **efficacia per attuare i principi di protezione dei dati** e **per integrare le garanzie**. Di conseguenza, implementare semplicemente le misure senza considerare la loro efficacia sarebbe un esercizio inutile.

I contesti relativi a cui l'efficacia deve essere analizzata sono forniti nell'Art. 25(1) GDPR sotto forma di aspetti che i titolari del trattamento devono prendere in considerazione. Vale a dire, questi aspetti sono i seguenti [elencati in un ordine diverso da quello utilizzato nel testo del GDPR]:

- "*i rischi di diversa probabilità e gravità per i diritti e le libertà delle persone fisiche posti dal trattamento*"
- "*il costo dell'implementazione*"
- "*il livello di sviluppo*"
- "*la natura, la portata, il contesto e le finalità del trattamento*"

Quando si considera l'efficacia nel **contesto dei rischi** per le persone fisiche colpite, è evidente che la misura deve essere efficace per mitigare i rischi. Implica anche una certa proporzionalità rispetto alla grandezza dei rischi. Quando si considera un **insieme di misure attuate**, la loro efficacia è **sufficiente** se è adatta a **mitigare il rischio a un livello accettabile**.

Quando si considera l'efficacia nel **contesto dei costi**, il GDPR sembra riconoscere che le risorse disponibili per attuare le misure sono limitate e dovrebbero essere utilizzate in modo efficace. Questo permette ai titolari del trattamento di usare misure meno costose ed efficaci in termini di costi al posto di quelle costose con un effetto simile. In altre parole, il criterio è l'efficacia, non l'accessibilità o il costo per i titolari del trattamento in quanto tali. Mentre la considerazione del costo lascia la possibilità che un costo possa essere considerato eccessivo, un costo elevato non può essere usato come giustificazione per trascurare l'efficacia richiesta in contesti diversi. Se i costi richiesti per assicurare un adeguato livello di garanzie sono troppo alti per un titolare del trattamento, quest'ultimo dovrebbe astenersi dalle attività di trattamento.

Quando si considera l'efficacia nel **contesto del livello di sviluppo**, le conseguenze sono duplici. Da un lato, impedisce ai titolari del trattamento di ignorare le nuove misure e di astenersi dall'aggiornare il livello di protezione a quello offerto del livello di sviluppo. D'altra parte, un titolare del trattamento non può essere obbligato a implementare misure che sono state delineate in qualche documento di ricerca senza essere state testate o rese utilizzabili in un ambiente operativo. In situazioni in cui i titolari del trattamento fanno affidamento sul mercato per fornire certi tipi di software, i titolari del trattamento possono essere giustificati a limitare le misure implementate a quelle effettivamente disponibili sul mercato, se queste sono sufficienti a fornire protezioni efficaci. Come nel contesto dei costi, questo non può tuttavia rinunciare ai requisiti di efficacia in altri contesti.

Nel contesto delle misure di sicurezza, il livello di sviluppo ha un significato particolare. La sicurezza informatica può essere vista come una corsa agli armamenti tra attaccanti e difensori. Nel panorama delle minacce in continua evoluzione, ogni volta che i difensori pensano a mezzi più efficaci per contrastare gli attacchi, gli attaccanti trovano mezzi di attacco più sofisticati. Questo rende evidente che il concetto di "difesa efficace" è in costante movimento. In questo contesto, le informazioni attuali sulle minacce e sulle difese disponibili sono importanti quando si valuta l'efficacia delle misure implementate. Inoltre, una mancata implementazione di nuove misure, per esempio sotto forma di aggiornamenti o patch critiche per la sicurezza, non può essere giustificata dai titolari del trattamento (tranne nel raro caso in cui le nuove misure siano irrilevanti per le attività di trattamento e i rischi correlati).

Si noti che l'EDPB sottolinea nelle sue Linee guida sul DPbDD che il livello di sviluppo non è definito solo da misure tecniche, ma include anche misure organizzative come quadri, standard, certificazione e codici di condotta[87].

Quando si considera l'efficacia relativa alla **natura, all'ambito, al contesto e agli scopi dell'elaborazione**, si riconosce che le misure devono essere abbinate all'elaborazione in questione. Una misura che è efficace per un sistema informativo tradizionale che supporta gli esseri umani che prendono decisioni può non essere efficace se applicata a un'applicazione di apprendimento automatico che prende decisioni automatiche; una misura che funziona bene per l'elaborazione a basso volume in un piccolo ambiente può non scalare fino all'elaborazione ad alto volume; e una misura che funziona efficacemente quando si utilizzano responsabili del trattamento affidabili (che sono essi stessi soggetti al GDPR) può non essere

87 Vedi il paragrafo 22 delle Linee guida EDPB sul DPbDD.

efficace e sufficiente quando si utilizzano responsabili del trattamento meno affidabili (come quelli situati in 3rd paesi e non vincolati dal GDPR).

L'art. 5(2) richiede che i titolari del trattamento siano in grado di dimostrare la conformità con il GDPR. Un aspetto importante di questo è quello di essere in grado di dimostrare che le misure attuate sono effettivamente efficaci. Dovrebbe essere parte integrante del processo di prendere decisioni su quali misure attuare. Le dimensioni dell'efficacia sono date nell'art. 25(1) e sono state discusse sopra.

2.3.4 Analisi della protezione dei dati per difetto nell'art. 25(2) GDPR

Di seguito analizzeremo i requisiti dell'art. 25(2) GDPR. Utilizza la definizione di default fornita nella sezione "*determinare le istruzioni per le risorse tecniche*" di questo documento (1.3.3).

Come è chiaro dalla definizione di cui sopra, le impostazioni predefinite riguardano le impostazioni (a volte disposte come *preferenze* o *profilo utente*) che sono sotto il controllo della persona interessata. I titolari del trattamento decidono le **impostazioni di default**, cioè le **impostazioni** che sono attive **in assenza di qualsiasi intervento da parte dell'interessato**.

Queste impostazioni influenzano l'elaborazione che avviene, compresi i seguenti aspetti:

- i dati personali che vengono trattati,
- l'entità dell'elaborazione che viene eseguita,
- il periodo per il quale i dati sono conservati, e
- le persone fisiche a cui sono resi accessibili i dati personali.

Il seguente esempio di impostazioni lo illustra:

- Gli interessati possono opzionalmente fornire un **indirizzo e-mail** per **essere informati sullo stato di elaborazione di un ordine**. Evidentemente, questo influisce sulla quantità di dati personali trattati dal titolare del trattamento. Influisce anche sulla portata del trattamento.
- Per l'elaborazione di un ordine, gli interessati devono sempre fornire un **indirizzo di spedizione e le informazioni di pagamento**. Opzionalmente, possono cliccare su una casella per **ricordare** queste informazioni per **evitare di digitarle ripetutamente** per ordini futuri. Mentre la quantità di dati trattati dal titolare del trattamento è sempre la stessa, l'opzione controllata dall'utente influisce ovviamente sul periodo di conservazione di tali dati.
- Un fornitore di **social media** può presentare ai suoi utenti delle **impostazioni di privacy** che controllano la **visibilità dei loro post**, che vanno dai *soli amici stretti* a *tutti*. Evidentemente, queste impostazioni di privacy controllano le persone fisiche che hanno accesso ai post, che rappresentano dati personali.

Il GDPR include quanto segue:

> Art. 25(2):
>
> *Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che, di default, siano trattati solo i dati personali necessari per ogni scopo specifico del trattamento. Tale obbligo riguarda la quantità di dati personali raccolti, la portata del loro trattamento, la durata della loro conservazione e la loro accessibilità. In particolare, tali misure devono garantire che di default i dati personali non siano resi accessibili, senza l'intervento dell'interessato, a un numero indefinito di persone fisiche.*

L'art. 25(2) prevede quindi che, **per difetto, il** trattamento sia **limitato** a quanto **necessario per le finalità**. Chiarisce inoltre che ciò deve essere inteso per quanto riguarda la **quantità di dati**, la **portata del trattamento** e il **periodo di conservazione dei dati**. La terza frase afferma che ciò è applicabile[88] anche al numero di persone a cui i dati sono resi accessibili. Questo sembra quindi riferirsi al numero di destinatari (come definito nell'art. 4(9) GDPR).

La formulazione dell'art. 25(2) implica che ci devono essere alcuni tipi di scopi aggiuntivi: per default, il trattamento deve essere limitato a un certo insieme di scopi; ma dopo l'intervento della persona interessata, evidentemente il trattamento va oltre questa limitazione. Ciò implica che il trattamento persegue poi finalità aggiuntive.

Gli esempi di cui sopra aiutano a capire meglio. Nel primo esempio, lo scopo aggiuntivo è quello di **tenere la persona interessata informata sullo stato di elaborazione** degli ordini. Nel secondo esempio, lo scopo aggiuntivo è quello di migliorare la **comodità dell'utente** per gli interessati che prevedono di effettuare nuovamente ordini in futuro. Nel terzo esempio, non viene perseguito alcuno scopo aggiuntivo. Piuttosto, è sempre presente lo scopo di limitare la visibilità dei post sui social media alla **gamma prevista dall'utente.** Si noti che la terza frase dell'art. 25(2) che si adatta a questo esempio si astiene anche dal fare riferimento agli scopi.

Questi esempi illustrano che gli **scopi aggiuntivi** e gli scopi sottostanti la situazione affrontata nella terza frase sono sempre **scopi che vanno a beneficio delle persone interessate**.

Sulla base di questa analisi, l'art. 25(2) sembra affermare che **per difetto**:

- **gli scopi aggiuntivi** che possono andare a beneficio degli interessati sono **disabilitati**, almeno nella misura in cui richiedono la raccolta di dati aggiuntivi, aumentano l'estensione del trattamento, causano un prolungamento del periodo di conservazione o aumentano il numero di destinatari;
- se una finalità nell'interesse della persona interessata è sempre perseguita dal trattamento (cioè non può essere disattivata), il suo **impatto sulla protezione dei dati deve essere ridotto al minimo per quanto riguarda i** dati raccolti, la portata del trattamento, il periodo di conservazione e il numero di destinatari.

L'art. 25(2) può essere visto come una sorta di **protezione contro le "porte di servizio"** in cui i titolari del trattamento raccolgono ulteriori dati, li conservano per periodi più lunghi, aumentano l'estensione del trattamento o i destinatari, con la giustificazione che era il desiderio della persona interessata. Evidentemente, gli interessati che non sono intervenuti in alcun modo, possono anche non essere consapevoli dei "loro desideri", possono non aver letto l'espressione dei loro desideri in dettaglio, o sono almeno influenzati dai valori predefiniti per esprimere più probabilmente "desideri" favoriti dal titolare del trattamento.

Questa salvaguardia che richiede esplicitamente l'intervento esplicito della persona interessata impone quindi l'uso di dialoghi di opt-in e vieta i dialoghi di opt-out. È lo stesso concetto che viene chiamato "azione di affermazione chiara" nel contesto del consenso (vedi Art. 4(11) GDPR). È direttamente paragonabile ad affermare che senza una chiara azione affermativa, cioè "***senza l'intervento dell'individuo"***, *un* trattamento aggiuntivo in termini di quantità e periodo di conservazione dei dati, estensione del trattamento, o numero di destinatari è illegittimo. È importante notare che questo requisito di soluzioni opt-in è indipendente dal fatto che il *consenso* sia scelto come base giuridica o meno.

Sulla base dell'analisi di cui sopra, le misure di cui all'art. 25(2) potrebbero includere quanto segue:

88 "In particolare" indica che il resto della frase è un'applicazione dell'espressione della frase precedente.

- Misure che accertano che le impostazioni predefinite riducono al minimo l'impatto del trattamento sulla protezione dei dati.
- Misure che accertano che gli interessati siano informati delle conseguenze delle impostazioni che sono sotto il loro controllo.
- Misure che accertano che le decisioni espresse dalle impostazioni siano specifiche. Per esempio, gli scopi aggiuntivi non possono essere abilitati tutti con una sola casella di controllo, ma deve essere possibile abilitarli singolarmente.
- Misure che verificano l'assenza di qualsiasi tipo di nudging nel dialogo in cui gli utenti scelgono le loro impostazioni, al fine di assicurarsi che l'interessato possa scegliere liberamente le sue preferenze.

2.3.5 Applicazione dei principi di protezione dei dati nelle diverse fasi del trattamento

L'obiettivo della protezione dei dati per progettazione è quello di integrare (o implementare) in tutte le fasi di un'attività di trattamento misure tecniche e organizzative appropriate che implementino i principi di protezione dei dati.

Le Linee guida dell'EDPB sul DPbDD contengono un'importante sezione sull'"attuazione dei principi di protezione dei dati nel trattamento dei dati personali utilizzando la protezione dei dati per progettazione e per impostazione predefinita". È strutturata in base ai principi di protezione dei dati che devono essere applicati. Le Linee guida dell'EDPB non affrontano la questione di come applicare il DPbDD nelle diverse fasi.

Questa sezione su come applicare i principi di protezione dei dati non si concentra su una descrizione dei principi stessi come fanno le Linee guida EDPB (indipendentemente dalle fasi); una descrizione dettagliata delle Linee guida è già stata fornita nel capitolo corrispondente delle Linee guida PANELFIT (vedi Parte II di queste Linee guida, sezione "Principi"). Piuttosto, questa sezione discute i processi che possono essere utilizzati per applicare questi principi in ciascuna delle tre fasi identificate nell'analisi dell'Art. 25(1) di cui sopra.

Ciò che è quindi comune a tutte e tre le fasi è che utilizzano i ***principi* della *protezione* dei dati** *in* ogni fase di lavoro (o decisione) al fine di

- **identificare i rischi** che portano alla violazione o all'attuazione inadeguata di un principio, e
- **identificare le misure** tecniche e organizzative appropriate che mitigano questi rischi.

Le misure effettive da attuare dipendono in gran parte dalla natura, dalla portata, dal contesto e dagli scopi del trattamento. Non è quindi possibile fornire una lista completa di misure appropriate per ogni tupla di fase (o compito all'interno di una fase) e principio. Questa sezione descrive quindi il processo di identificazione delle misure appropriate. Una discussione dettagliata (con esempi) delle misure per implementare i vari principi è stata fornita nella seconda sezione delle Linee guida.

Di seguito vengono discusse più dettagliatamente le fasi di *determinazione degli scopi*, *determinazione dei mezzi* e l'*elaborazione stessa.*

2.3.5.1 Determinazione degli scopi

Un'attività di trattamento è concepita determinando i suoi scopi. Questo stabilisce l'obiettivo di ciò che l'attività di trattamento deve raggiungere. Questa specificazione di "cosa" deve essere fatto è ancora relativamente astratta e manca qualsiasi dettaglio di "come" questo obiettivo è raggiunto. Il "come" è soggetto alla determinazione dei mezzi.

Gli scopi sono generalmente determinati dal top management che rappresenta ed è responsabile di un'organizzazione (o unità organizzativa). Gli scopi sono generalmente espressi nella stessa lingua in cui sono espressi la missione o il mandato dell'organizzazione. Ciò significa che provengono dal "dominio applicativo" e non hanno alcun contenuto tecnico. Una specifica di scopo non è in grado di determinare decisioni tecniche come quali risorse (cioè, mezzi) sono necessari per raggiungere gli obiettivi, quali dati devono essere raccolti, ecc. Piuttosto, una specifica di scopo può essere implementata in molti modi diversi. L'obiettivo della determinazione dei mezzi è quindi quello di trovare la migliore implementazione dal punto di vista della protezione dei dati.

Secondo l'art. 5(1)(a) GDPR, gli scopi devono essere "specificati [ed] espliciti". Ciò significa che devono essere registrati in una forma scritta precisa.

La determinazione degli scopi del trattamento è generalmente un processo iterativo. Iniziando con la/e finalità principale/i, la specifica viene continuamente completata e perfezionata fino ad arrivare a una versione finale. Ogni versione deve essere valutata, prendendo in considerazione i principi di protezione dei dati, le ragionevoli aspettative degli interessati e il rischio complessivo che il trattamento potrebbe comportare. Sulla base di questa valutazione, vengono apportati miglioramenti alla specifica delle finalità che migliorano il rispetto dei principi, sono più equilibrati con le aspettative degli interessati e mantengono la necessità/beneficio del trattamento in equilibrio con il rischio che esso comporta per gli interessati. Le iterazioni possono essere viste come un processo per trovare il minimo impatto sui diritti e le libertà degli interessati mentre si raggiungono gli obiettivi essenziali dell'organizzazione. Tipicamente, in ogni integrazione, la specifica dello scopo diventa più focalizzata, più stretta e specifica e impone un impatto minore sugli interessati.

Questo processo è visualizzato in Figura 6.

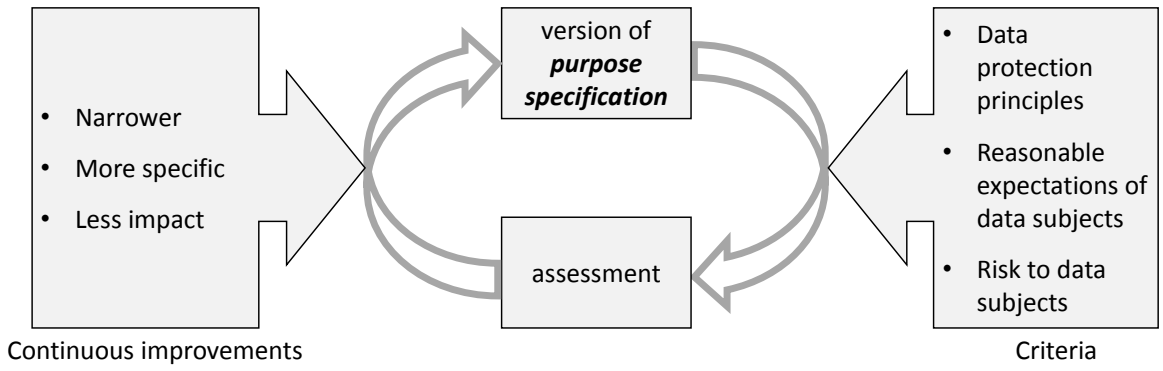

Figura 6: Il processo di specificazione dello scopo.

La protezione dei dati per progettazione applica i principi della protezione dei dati ad ogni passo della determinazione. Mentre alcuni dei principi di protezione dei dati sono meglio applicabili ai mezzi di trattamento, la *legittimità*, la *liceità* e l'*equità* sono direttamente applicabili alle finalità. Indirettamente, anche la *minimizzazione dei dati* è applicabile nel senso che l'impatto del trattamento sulle persone interessate dovrebbe essere ridotto al

minimo. Questo poi si traduce generalmente in una minimizzazione dei dati che vengono raccolti sugli interessati. Si noti inoltre che la limitazione delle finalità durante la determinazione dei mezzi ha senso solo se le finalità sono specificate in modo ristretto; solo allora si può determinare con precisione se i dati o le fasi del trattamento sono effettivamente necessari per le finalità. I principi principali sono discussi più in dettaglio nel seguito.

Legalità (vedi "Legalità, equità e trasparenza" nella sezione "Principi" nella parte II di queste Linee guida):

Secondo l'art. 6 GDPR, il trattamento è lecito se si applica una delle **basi giuridiche** descritte nel suo paragrafo 1. L'art. 9 GDPR aggiunge ulteriori requisiti per categorie speciali di dati. Per rispettare il principio di *liceità*, il titolare del trattamento deve scegliere una base giuridica dall'art. 6 ed eventualmente 9 GDPR per ogni singola finalità che viene perseguita dall'attività di trattamento.

Si noti che è comune che un'attività di trattamento persegua una moltitudine di scopi che utilizzano diverse basi giuridiche. Un'illustrazione di questo usando l'esempio dello shopping online è stato descritto da Bruegger et. al[89].

Legittimità (vedi "Legalità, equità e trasparenza" nella sezione "Principi" nella parte II di queste Linee guida):

Mentre la liceità riguarda gli artt. 6 e 9 del GDPR, la legittimità richiede di seguire la legge nel senso più ampio. Non è quindi limitato al GDPR ma si estende a qualsiasi altra legge applicabile. Probabilmente, le leggi non dovrebbero essere seguite solo alla lettera ma anche nello spirito. In molte situazioni, la legittimità può anche essere interpretata per includere la *soft law* come i requisiti etici comunemente usati e gli standard professionali. Può anche estendersi a proteggere i valori della società in generale.

La valutazione della legittimità degli scopi dipende in gran parte dalla natura, dalla portata e dal contesto del trattamento. In alcuni casi, il rispetto della legittimità può richiedere passaggi formali. Questo è per esempio tipico nelle organizzazioni di ricerca dove un'attività di trattamento deve essere preventivamente approvata da un comitato etico di ricerca.

Equità (vedi "Legalità, equità e trasparenza" nella sezione "Principi" nella parte II di queste Linee guida):

Un elemento chiave dell'equità è prendere in considerazione le ragionevoli aspettative e situazioni degli interessati. Gli interessi del titolare del trattamento, come espressi nella specificazione dello scopo, sono poi bilanciati con quelli degli interessati. L'impatto sui diritti e le libertà degli interessati dovrebbe essere giustificato con un livello adeguato di necessità e benefici potenziali per il titolare del trattamento.

La valutazione dell'equità delle finalità richiede generalmente la valutazione delle aspettative degli interessati. Ci sono vari modi per farlo, compreso il semplice "mettersi nella posizione degli interessati" fino a coinvolgere le organizzazioni dei consumatori o realizzare indagini.

Per valutare le aspettative degli interessati, è spesso utile distinguere diverse persone che rappresentano diversi tipi e situazioni di interessati. Questi dovrebbero anche includere

89 Bud P. Bruegger, Eva Schlehahn e Harald Zwingelberg, Data Protection Aspects of Online Shopping - A Use Case, W3C Data Privacy Vocabularies and Controls Community Group, 12 dicembre 2019, https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/ (ultima visita 15/7/2021).

soggetti particolarmente vulnerabili (come i minori o i pazienti), o gruppi di soggetti che possono essere colpiti molto più significativamente dal trattamento rispetto alla media.

Il bilanciamento deve considerare i rischi che l'attività di trattamento rappresenta per i diritti e le libertà degli interessati. Una rapida valutazione globale del rischio è fornita dai 9 criteri[90] del Gruppo di lavoro per la protezione dei dati dell'articolo 29 se un'attività di trattamento comporta un rischio elevato (e quindi richiede una valutazione d'impatto sulla protezione dei dati). Questo dovrebbe essere integrato da un'analisi di come le categorie speciali di interessati e gli interessati vulnerabili sono interessati dall'attività di trattamento prevista.

Si noti che un test di bilanciamento è formalmente richiesto quando la base giuridica dell'*interesse legittimo* (cfr. art. 6(1)(f) GDPR) è stato scelto per un determinato scopo. Orientamenti su come realizzare un test comparativo in questo contesto sono stati forniti dal Gruppo di lavoro "Articolo 29" sulla protezione dei dati[91] (cfr. "Interesse legittimo e test comparativo", Parte II sezione "Strumenti e azioni principali"). In un contesto più generale, il GEPD ha fornito orientamenti sulla proporzionalità[92].

2.3.5.2 Determinazione dei mezzi

La seguente sottosezione descrive come identificare le misure tecniche e organizzative appropriate quando si determinano i mezzi.

Mentre la determinazione degli scopi del trattamento specifica il "cosa" deve essere raggiunto dal trattamento, la determinazione dei mezzi specifica il "come" questo obiettivo è raggiunto. In ogni passo della determinazione di questo "come", i principi e i requisiti della protezione dei dati devono essere presi in considerazione.

La determinazione dei mezzi può essere vista come il risultato di un *piano di attuazione* dell'attività di trattamento. Comporta risorse, istruzioni e misure tecniche e organizzative. Queste ultime sono destinate ad attuare i principi di protezione dei dati. Per una discussione dettagliata delle misure che attuano i vari principi, si veda la sezione delle Linee guida sui principi (si veda la sezione "Principi" nella parte II di queste Linee guida).

2.3.5.2.1 *Gestire il processo di determinazione dei mezzi*

La determinazione dei mezzi è spesso un processo sostanziale che generalmente coinvolge una moltitudine di persone, campi di competenza, unità organizzative o dipartimenti, e può anche coinvolgere consulenti ed esperti esterni.

La **prima misura** (meta-) **organizzativa** consiste quindi nell'impostare il **processo di determinazione dei mezzi** in modo che sia conforme alla protezione dei dati per progettazione. Questa misura viene chiamata "metamisura", poiché è destinata a identificare le misure che attuano effettivamente i principi della protezione dei dati. La metamisura deve assegnare chiare responsabilità alla direzione superiore:

---

90 Vedi le pagine 9 - 11 in Article 29 Data Protection Working Party, WP 248rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017,As last Revised and Adopted on 4 October2017, https://ec.europa.eu/newsroom/article29/items/611236 (last visited 15/7/2021).

91 in Article 29 Data Protection Working Party, WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last visited 15/7/2021).

92 Garante europeo della protezione dei dati, Linee guida del GEPD sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali alla privacy e alla protezione dei dati personali, 19 dicembre 2019, https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en (ultima visita 15/7/2021).

- La direzione superiore che rappresenta legalmente il titolare del trattamento deve avere il controllo di questo processo e incaricare che la protezione dei dati sia adeguatamente presa in considerazione in ogni passo e decisione.
- La direzione superiore deve essere in grado di progettare se i mezzi determinati (cioè il risultato di questo processo) sono effettivamente conformi ai requisiti della protezione dei dati.
- Alla fine di questo processo, spetta alla direzione superiore approvare i mezzi determinati e dare il via libera alle operazioni di trattamento vere e proprie (il trattamento stesso).

Ci sono diverse **possibili misure** (meta-) **organizzative** su come raggiungere questo obiettivo. Alcuni esempi sono elencati di seguito:

- Ogni passo o decisione presa come parte della determinazione dei mezzi deve descrivere i requisiti di protezione dei dati pertinenti e come sono stati applicati o altrimenti soddisfatti.
- Se si sceglie[9394] un approccio a tappe, qualsiasi transizione dei cancelli di tappa deve essere soggetta all'approvazione degli aspetti di protezione dei dati.
- Una chiara designazione delle persone responsabili di determinare se i requisiti di protezione dei dati sono stati soddisfatti nelle singole fasi dovrebbe essere fatta.
- Se disponibile, il responsabile della protezione dei dati (DPO)[95] dovrebbe essere coinvolto nel processo.
- (Continua) la documentazione (cioè, la dimostrazione) di considerare e incorporare la protezione dei dati dovrebbe essere parte integrante del processo. Questo serve sia per soddisfare il principio di *responsabilità* (vedi Art. 5(2) GDPR) sia come base per la determinazione da parte della direzione superiore per la loro decisione di proteggere i dati. 5(2) GDPR) e come base per la determinazione da parte della direzione superiore per la loro decisione di approvare formalmente il risultato da utilizzare operativamente (cioè, un via libera al *trattamento stesso*).

Il processo di determinazione dei mezzi ha inevitabilmente bisogno di **valutare l'efficacia** delle varie misure (vedere la discussione sull'efficacia nella sezione 2.3.3.7 sopra). Questo generalmente richiede di eseguire:

- valutazioni del rischio
- indagini sul livello di sviluppo o del mercato

Si noti che lo strumento formale previsto dal GDPR per valutare l'efficacia delle misure di protezione dei dati è la *valutazione d'impatto sulla protezione dei dati* (DPIA, vedi art. 35 GDPR) (vedi "DPIA", Parte II, sezione "Strumenti e azioni principali"). Sia la valutazione del rischio che la descrizione delle misure sono contenute nelle sue parti obbligatorie. Una DPIA è formalmente richiesta dal GDPR solo in presenza di un rischio elevato, ma può essere utilizzata informalmente nel processo interno. Una DPIA è anche uno strumento primario per documentare la conformità con la protezione dei dati attraverso la progettazione.

---

93 Vedi per esempio, https://en.wikipedia.org/wiki/Phase-gate_process (ultima visita 13/7/2021).

94 Si noti che le tappe non sono limitate alla gestione "waterfall", ma esistono anche nei metodi agili, come l'Agile Unified Process, vedi http://www.ambysoft.com/unifiedprocess/aup11/html/phases.html (ultima visita 13/7/2021).

95 Si noti che il responsabile della protezione dei dati non ha la responsabilità diretta della conformità, ma è l'esperto interno che probabilmente ha più familiarità con i requisiti del GDPR (si veda anche l'art. 39(1)(a) a (c) GDPR).

Almeno le organizzazioni più grandi con diverse attività di elaborazione distinte possono beneficiare dell'uso di un **approccio** più **sistematico** di determinazione dei mezzi. Questo può includere quanto segue:

- L'uso di ***politiche di protezione dei dati*** che sono applicabili a più attività di trattamento e possono quindi portare economia di scala (vedi art. 24(2) GDPR).
- L'identificazione e l'applicazione di codici di condotta applicabili a livello di settore possono risparmiare sforzi e migliorare la qualità dell'attuazione (cfr. art. 24(3) del GDPR). 24(3) GDPR).

Il **risultato finale** di un processo riuscito di determinazione dei mezzi è un'approvazione chiara e documentata dei mezzi e un **via libera** da parte della direzione superiore che rappresenta il titolare del trattamento. Il via libera è necessario affinché il titolare del trattamento si assuma la piena responsabilità del trattamento (vedi art. 29 GDPR). Come base aggiuntiva per la decisione dell'autorizzazione, i titolari del trattamento possono chiedere una **certificazione formale** secondo l'Art. 42 GDPR (cfr. Art. 24(3) GDPR). La certificazione rappresenta un'attestazione formale di conformità al GDPR. Un'autorizzazione documentata è un prerequisito per l'inizio della fase operativa del trattamento (il *trattamento stesso*).

2.3.5.2.2 *Valutare l'efficacia delle misure relative ai principi di protezione dei dati*

Il processo di cui sopra dovrebbe adottare un approccio sistematico per applicare tutti i principi di protezione dei dati in modo sistematico a tutte le decisioni sui mezzi. In particolare, ogni principio deve essere applicato con misure tecniche e organizzative. Si deve dimostrare che queste misure sono efficaci per quanto riguarda

- "*i rischi di diversa probabilità e gravità per i diritti e le libertà delle persone fisiche posti dal trattamento*",
- "*il costo dell'implementazione*",
- "*il livello di sviluppo*", e
- "*la natura, la portata, il contesto e le finalità del trattamento*"

(vedere la sezione 2.3.3.7 sopra).

Quando si valuta il rischio (vedi primo punto), un rischio fondamentale è che il principio sia violato o insufficientemente garantito. Questo potrebbe essere il caso per tutti gli interessati o per gruppi speciali o minoranze. Gli interessati vulnerabili che sono stati eventualmente identificati durante la determinazione delle finalità dovrebbero essere presi in considerazione (vedi sezione 2.3.5.1).

Per valutare il terzo aspetto dell'efficacia, può essere necessario realizzare indagini sul livello di sviluppo.

Un modo per valutare l'efficacia delle misure è quello di utilizzare un approccio iterativo che è molto simile a quello utilizzato per determinare gli scopi (vedi Figura 6). Invece di una versione della *specifica degli scopi*, si valuta un *piano di implementazione* concreto. Questo piano comporta sia risorse, istruzioni e misure tecniche e organizzative già previste (si veda la sezione "Principi" nella parte II di queste Linee guida). In ogni iterazione, si valuta l'efficacia delle misure e si migliora il piano in base alle carenze individuate. Il processo iterativo termina quando è stato trovato un piano di implementazione con misure efficaci.

Per rendere sistematico questo processo, ogni compito che risulta in una decisione sui mezzi deve essere valutato rispetto a tutti i principi. La sezione 2.3.3.4 sopra ha fornito una panoramica dei possibili compiti. La suddivisione precisa della determinazione globale in

compiti dipende però dalla natura, dalla portata, dal contesto e dagli scopi dell'attività di trattamento. È quindi necessario adattare la suddivisione in compiti alla situazione concreta.

2.3.5.3 Elaborazione stessa

Qui di seguito si esamina l'applicazione dei principi di protezione dei dati durante la fase operativa, vale a dire l'elaborazione stessa.

La trasparenza e l'**equità** sono probabilmente i principi più rilevanti in questa fase (vedi "Legalità, equità e trasparenza" nella Parte II, sezione "Principi"). Richiedono tra l'altro le seguenti misure tecniche e organizzative:

- Il trattamento efficiente delle invocazioni dei diritti degli interessati.
- La gestione delle violazioni dei dati personali.

Alla fine di un'attività di trattamento, (l'aspetto temporale della) **minimizzazione dei dati** (vedi la "minimizzazione dei dati" nella Parte II, sezione "Principi fondamentali" di queste Linee guida): richiede che i dati personali che non sono più necessari per gli scopi siano cancellati. Sono disponibili diverse misure per accertare che i dati siano cancellati in modo irreversibile e che tutti i dispositivi tecnici di archiviazione siano considerati prima del loro smantellamento. Queste misure sostengono anche il principio della **limitazione delle finalità** (vedi "Limitazione delle finalità" nella parte II di queste Linee guida, sezione "Principi"): poiché la mancata cancellazione dei dati aprirebbe la possibilità che essi siano utilizzati per altri scopi. L'efficacia delle misure utilizzate per lo smantellamento dovrebbe essere verificata e documentata come descritto nella sezione 2.3.5.2.2 precedente.

L'art. 5(1)(b) GDPR prevede la possibilità di un **ulteriore trattamento per scopi compatibili**. Il principio della **limitazione delle finalità** richiede un'attenta valutazione (secondo l'art. 6(4) GDPR) se queste finalità sono effettivamente compatibili. Tale ulteriore trattamento richiede anche l'attuazione di misure aggiuntive come ulteriore **minimizzazione dei dati**, pseudonimizzazione o anonimizzazione (cioè **limitazione della memorizzazione**) al fine di garantire le **garanzie** richieste nell'Art. 89(1) GDPR.

Mentre l'**efficacia delle misure** è stata inizialmente verificata durante la determinazione dei mezzi, la 2ª frase dell'Art. 24(1) GDPR richiede che questo sia **regolarmente rivisto** e che le misure siano aggiornate se necessario. Tali revisioni e aggiornamenti sono misure a sé stanti.

Esempi di dove tali revisioni sono elencate di seguito:

- I diritti di accesso per il personale che garantiscono la **riservatezza** e la **limitazione dello scopo** potrebbero dover essere aggiornati per riflettere i cambiamenti del personale e la fine degli incarichi temporanei e delle sostituzioni.
- Un software che è stato trovato per garantire la **riservatezza** potrebbe non farlo più, a meno che non vengano installati aggiornamenti critici di sicurezza.
- **La riservatezza** che è stata ritenuta sufficiente potrebbe non esserlo più se il **panorama delle minacce** si evolve e **nuovi tipi di attacchi** diventano possibili. Di solito questo richiede l'implementazione di misure aggiuntive o più sofisticate.
- Si può presumere che i dati siano **anonimi** o che impediscano l'identificazione diretta (come parte della pseudonimizzazione), ma i **nuovi metodi di re-identificazione mettono** in discussione queste presunzioni. Per sostenere ancora la **limitazione della conservazione**, è necessaria un'ulteriore riduzione del potenziale di identificazione dei dati interessati o una nuova progettazione del trattamento.

Una situazione simile si presenta durante la **sostituzione di routine delle risorse** (umane e tecniche). Quando, per esempio, si è constatato che una persona ha una formazione e competenze sufficienti per eseguire una serie di istruzioni, lo stesso tipo di valutazione è necessario per i successori di questa persona. Allo stesso modo, le nuove risorse tecniche devono mostrare le stesse proprietà che hanno garantito l'efficacia del componente originale.

Le istruzioni generalmente si evolvono durante il tempo di vita di un'attività di elaborazione. Le istruzioni per le risorse umane e i flussi di lavoro possono per esempio essere ridisegnati o resi più efficienti in base all'esperienza. Le istruzioni per le risorse tecniche cambiano generalmente con ogni versione del software e spesso vengono installate automaticamente (per esempio, da un servizio di aggiornamento). Con ogni nuova versione di istruzioni, deve essere verificato quanto segue:

- Che la nuova versione comporti ancora le misure necessarie per garantire l'effettiva applicazione dei principi; e
- che non ci sia un "function creep" che estende il trattamento al di là di ciò che è necessario per gli scopi.

Quando il cambiamento delle risorse o delle istruzioni è più sostanziale, può essere necessaria una nuova iterazione completa del processo iterativo di determinazione dei mezzi (vedi sezione 2.3.5.2.2) può essere necessaria.

(IDETIFICAZIONE; ANONIMIZZAZIONE...)

2.4 Protezione dei dati e ricerca scientifica

Pilar Nicolás Jiménez[96] *(UPV/EHU), Mikel Recuero Linares (UPV/EHU)*

Questa parte delle Linee guida è stata rivista da Rossana Ducato

Questa parte delle Linee guida è stata rivista e convalidata da Marko Sijan, Senior Advisor Specialist, (HR DPA)

2.4.1 Punti chiave

- Il GDPR è attento all'importanza fondamentale che possono avere le operazioni di trattamento con finalità di archiviazione nel pubblico interesse, finalità di ricerca scientifica o storica, o finalità statistiche.
- Pertanto, il Regolamento prevede un regime speciale e favorevole nel tentativo di garantire che le norme sulla protezione dei dati non costituiscano un grosso ostacolo alle operazioni di trattamento per le finalità indicate.
- A questo proposito, è espressamente previsto come condizione per il trattamento di categorie speciali di dati personali, la sua necessità per finalità di archiviazione nel pubblico interesse, scopi di ricerca scientifica o storica, o finalità statistiche.

96 Questa sezione incorpora alcuni riferimenti estratti da un capitolo del libro dell'autore, originariamente pubblicato in spagnolo: *Comentarios al Reglamento General de Protección de Datos y a Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (Antonio Troncoso Reigada, Dir.), Thomson Reuters Aranzadi, 2020.

- Il testo stabilisce anche un regime flessibile per la conservazione dei dati a lungo termine e una presunzione di compatibilità per scopi secondari o ulteriori.
- Inoltre, sono previste limitazioni, eccezioni o deroghe, *tra l'altro,* ai diritti di informazione, accesso, rettifica, restrizione del trattamento, opposizione e, per quanto riguarda le finalità di archiviazione nel pubblico interesse, al diritto di notifica e portabilità.
- Al fine di trovare il giusto equilibrio con i diritti e gli interessi delle persone interessate, il regolamento richiede l'adozione di garanzie adeguate in conformità con l'articolo 89 e, in alcune situazioni, anche un ulteriore sviluppo da parte del diritto dell'Unione o degli Stati membri.

2.4.2 **Introduzione**

Come ha evidenziato il Garante europeo della protezione dei dati (GEPD), "la Commissione europea ha definito gli obiettivi delle politiche di ricerca e innovazione dell'UE come "l'apertura del processo di innovazione a persone con esperienza in campi diversi da quello accademico e scientifico", "la diffusione della conoscenza non appena è disponibile utilizzando la tecnologia digitale e collaborativa" e "la promozione della cooperazione internazionale nella comunità di ricerca".[97] Questi scopi non sono in conflitto con la protezione dei dati. Infatti, le norme sulla protezione dei dati non dovrebbero essere un ostacolo alla libertà della scienza ai sensi dell'articolo 13 della Carta dei diritti fondamentali dell'UE (CFREU). Piuttosto, questi diritti e libertà devono essere attentamente valutati e bilanciati, portando a un risultato che rispetti l'essenza di entrambi.[98]

In effetti, l'intenzione dietro la nostra attuale legislazione sulla protezione dei dati è di armonizzare il trattamento dei dati con gli scopi della ricerca scientifica.[99] Questa intenzione è chiaramente legata all'articolo 179, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE) per realizzare uno spazio europeo della ricerca. In linea con questo, il regolamento generale sulla protezione dei dati (GDPR) ha introdotto un nuovo quadro volto a consentire il trattamento dei dati per scopi di archiviazione nell'interesse pubblico, scopi di ricerca storica e scientifica o scopi statistici che va oltre quello previsto dalla direttiva 95/46/CE.[100] Il nucleo di questo nuovo regolamento è l'articolo 89 del GDPR, che è accompagnato da molti altri riferimenti in tutto il testo che lo completano. Questi si trovano sia nella parte del GDPR che include i criteri decisivi per la sua interpretazione (considerando), sia in alcune disposizioni[101] specifiche. Sulla base di questi considerando, è opportuno evidenziare alcune idee preliminari.

---

97 GEPD, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 2020, pag. 10. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Accesso: 15 gennaio 2020.

98 EDPB, Linee guida 03/2020 sul trattamento dei dati relativi alla salute ai fini della ricerca scientifica nel contesto dell'epidemia COVID-19. Adottato il 21 aprile 2020, p. 5. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Accesso 23 aprile 2020.

99 Considerando 159 GDPR.

100 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

101 Vedi, *tra l'altro*: l'articolo 5, paragrafo 1, lettera b), per le finalità compatibili; l'articolo 5, paragrafo 1, lettera e), relativo alla limitazione della conservazione; l'articolo 9, paragrafo 2, lettera j), come deroga per il trattamento di categorie particolari di dati; l'articolo 14, paragrafo 5, lettera b), relativo alla trasparenza e all'informazione; l'articolo 17, paragrafo 3, lettera d), relativo al diritto alla cancellazione; o l'articolo 21, paragrafo 6, per il diritto di opposizione.

In primo luogo, il considerando 157 afferma che accoppiando le informazioni dei registri, compresi diversi tipi di dati corrispondenti a molti individui, i ricercatori possono ottenere "nuove conoscenze di grande valore per quanto riguarda condizioni mediche diffuse come le malattie cardiovascolari, il cancro e la depressione". Di conseguenza, "i risultati della ricerca possono essere migliorati, poiché attingono a una popolazione più ampia". Questi strumenti possono contribuire a migliorare le politiche di ricerca e, di conseguenza, la qualità della vita della popolazione. Questi vantaggi fanno sì che il trattamento dei dati a questi fini da parte dei ricercatori sia ragionevole, a condizione che i diritti dei soggetti siano garantiti. Questo stabilisce una concezione della ricerca come un processo che persegue un beneficio sociale, a breve, medio o lungo termine, considerato in modo molto ampio (miglioramento della qualità della vita) ma, allo stesso tempo, limitando tale attività a questo scopo specifico. Inoltre, il considerando 159 precisa che "per rispondere alle specificità del trattamento dei dati personali a fini di ricerca scientifica, si dovrebbero applicare condizioni specifiche, in particolare per quanto riguarda la pubblicazione o altrimenti la divulgazione di dati personali nel contesto di finalità di ricerca scientifica".

La seconda questione da affrontare è la natura specifica del consenso come requisito per la sua validità, che ha alcune particolarità quando lo scopo del trattamento è la ricerca scientifica. Infatti, l'articolo 4 del GDPR stabilisce che per consenso "si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale questi, mediante una dichiarazione o un'azione positiva e chiara, manifesta il proprio consenso al trattamento dei dati personali che lo riguardano". Tuttavia, il considerando 33 afferma che "spesso non è possibile identificare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati".

Tuttavia, è comune che durante un progetto, possano emergere approcci non previsti inizialmente, o che, al completamento del progetto, le conclusioni aprano le porte ad altri progetti correlati. Inoltre, i ricercatori e i team sono spesso specializzati in un'area o linea di ricerca sviluppata da progetti specifici, e i dati possono rimanere utili o necessari per lunghi periodi di tempo[102]. Come risposta, sono emersi modelli istituzionali - come le biobanche - che funzionano come intermediari tra soggetti e ricercatori. Lo scopo della raccolta di questi dati è quello di conservarli per quando potrebbero essere necessari, senza sapere, in linea di principio, quale progetto di ricerca, o quali progetti, li elaboreranno. Alla luce di questa realtà, il considerando 33 afferma che "gli interessati dovrebbero essere autorizzati a dare il loro consenso a certe aree della ricerca scientifica" anche se "gli interessati dovrebbero avere la possibilità di dare il loro consenso solo a certe aree di ricerca o parti di progetti di ricerca nella misura consentita dallo scopo previsto". Le diverse opzioni e il consenso sono quindi consentiti in varia misura a condizione che siano, come ricorda il considerando, "in linea con gli standard etici riconosciuti per la ricerca scientifica".

Un terzo punto che merita attenzione è quello contenuto nel considerando 50, che si riferisce alla cosiddetta compatibilità delle finalità[103], cioè "il trattamento dei dati personali per finalità diverse da quelle per cui i dati personali sono stati inizialmente raccolti". Si tratta di un termine utilizzato nei casi in cui i dati personali, destinati ad essere utilizzati per scopi di ricerca, sono stati inizialmente raccolti o trattati per uno scopo diverso, ma possono essere legittimamente trattati per ulteriori nuovi scopi (compatibili). Inoltre, l'ulteriore trattamento per scopi di archiviazione nel pubblico interesse, scopi di ricerca scientifica o storica o scopi statistici sono *ex lege* considerati trattamenti legittimi compatibili. Ciò significa che non sono necessari né il consenso della persona interessata né altre basi legali per questo ulteriore

102 A questo proposito, si veda anche l'articolo 5(1)(e) del GDPR che permette di conservare i dati personali per periodi più lunghi nella misura in cui sono trattati esclusivamente "a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89(1).

103 A questo proposito, si veda anche l'articolo 5(1)(b) del GDPR.

scopo, alle condizioni che saranno descritte in seguito. Questa opzione è di estrema importanza per la ricerca scientifica perché può facilitare l'accesso a un'enorme quantità di dati senza la necessità di ricontattare gli interessati.

Infine, è necessario menzionare il considerando 53, che riprende lo scopo del GDPR relativo alla definizione di condizioni armonizzate per il trattamento di categorie speciali di dati personali a fini sanitari (in particolare, nel contesto della gestione di servizi e sistemi di assistenza sanitaria o sociale). Inoltre, afferma che "il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e adeguate per proteggere i diritti fondamentali e i dati personali delle persone fisiche", mentre dichiara che "gli Stati membri dovrebbero essere autorizzati a mantenere o introdurre ulteriori condizioni, comprese le limitazioni, per quanto riguarda il trattamento di dati genetici, dati biometrici o dati relativi alla salute." Tuttavia, le misure introdotte "non dovrebbero ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero di tali dati".

2.4.3 Nozioni nel contesto del quadro normativo dell'UE

A. Nozione di "scopi di archiviazione nell'interesse pubblico"

Per archivi di interesse pubblico si intendono quelli di enti pubblici o privati che detengono documenti di interesse pubblico e che, ai sensi del diritto dell'Unione o degli Stati membri, hanno l'obbligo giuridico di acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire l'accesso a documenti di valore durevole per l'interesse[104] pubblico generale. Tuttavia, non si applica ai dati delle persone decedute (cfr. "Dati personali", parte II delle presenti Linee guida, sezione "Concetti principali").

B. Nozione di "ricerca scientifica

La ricerca scientifica è un termine troppo ampio che si riferisce generalmente alla ricerca della conoscenza, attraverso una certa metodologia, in qualsiasi area del sapere umano. Il GDPR non include una definizione di "ricerca scientifica" in quanto tale, ma introduce una serie di considerazioni che ci permettono di definirne le caratteristiche principali. In primo luogo, la ricerca "scientifica" è diversa dagli "scopi di ricerca storica" e dagli "scopi statistici". Inoltre, copre diversi campi, ad esempio la ricerca nelle scienze della vita legate alla salute umana, ma anche le scienze sociali (considerando 157 e 159). Deve portare "benefici", almeno potenzialmente. Questa aspettativa giustifica un regime unico che permette eccezioni e deroghe a certi diritti (art. 89.2).[105]

In questo quadro, il GDPR intraprende un'interpretazione ampia dell'attività scientifica, includendo "lo sviluppo tecnologico e la dimostrazione, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata privatamente" (considerando 159). Questa concezione ampia include progetti di ricerca con risultati pubblicabili e altri studi analitici, senza escludere la ricerca finanziata privatamente o quella finanziata da aziende commerciali a scopo di lucro. Tuttavia, contiene anche alcuni limiti, alcuni criteri che permettono di determinare la misura in cui le eccezioni previste in tutto il GDPR possono essere applicate in uno scenario di aumento delle procedure di analisi dei dati. Tuttavia, il regolamento rimane ambiguo su quali parametri un'attività o un trattamento deve soddisfare per essere considerato "ricerca

104 Considerando 158 del GDPR.
105 Considerando 157 GDPR.

scientifica". Il GEPD, nel tentativo di far luce su questo, ha alluso ai seguenti parametri nel suo parere preliminare sulla protezione dei dati e la ricerca scientifica[106]:

- L'attività deve contribuire all'aumento della conoscenza (ricerca scientifica in senso stretto) o all'uso della conoscenza per la produzione di dispositivi, materiali, servizi, processi o prodotti (sviluppo tecnologico e dimostrazione).
- L'attività deve essere sviluppata sotto certi standard di qualità (professionali, metodologici e istituzionali), "compresa la nozione di consenso informato, responsabilità e supervisione"[107].
- "La ricerca è condotta con l'obiettivo di far crescere la conoscenza e il benessere collettivo della società, invece di servire principalmente uno o più interessi privati".[108]

Secondo questa prospettiva, la ricerca scientifica, ai fini del GDPR, copre l'attività di generazione e applicazione della conoscenza ed esclude l'attività che non presenta una garanzia di rigore nel suo sviluppo. Pertanto, la ricerca scientifica richiede che i progetti di ricerca siano "impostati secondo le norme metodologiche ed etiche pertinenti al settore, in conformità con le buone pratiche".[109] Le procedure che permettono l'adeguata valutazione di questi parametri, che possono variare da caso a caso, rappresenteranno per il trattamento dei dati nel senso dell'articolo 89.1.

È importante sottolineare che l'insegnamento[110] non può essere considerato un'attività scientifica, anche se è finalizzato alla formazione di professionisti in questo settore. Di conseguenza, dato che il GDPR non ne fa menzione, il trattamento dei dati per questo scopo è soggetto al regime generale, il che può portare a molte disfunzioni nella pratica.[111]

C. Nozione di "ricerca storica"

Il GDPR applica questa descrizione ai dati trattati per scopi di ricerca storica. Questa è una nozione ampia che include sia la ricerca storica stessa che la ricerca per scopi genealogici[112]. Tuttavia, non si applica alla ricerca effettuata con i dati di persone decedute.

D. Nozione di "trattamento a fini statistici"

Per scopi statistici si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari per indagini statistiche o per la produzione di risultati statistici[113]. Tuttavia, i dati risultanti devono essere dati non personali (dati aggregati), ed è inoltre richiesto che né questo risultato né i dati personali siano utilizzati a sostegno di misure o decisioni riguardanti una particolare persona fisica.

Inoltre, ancora una volta, il diritto dell'Unione o degli Stati membri, nei limiti del GDPR, dovrebbe determinare la maggior parte degli aspetti pratici e particolari del trattamento (quali dati sono considerati come contenuto statistico, controllo dell'accesso, e misure appropriate

---

106 GEPD, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 2020, pag. 12. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Accesso: 15 gennaio 2020.

107 Ibidem.

108 Ibidem.

109 EDPB, Linee guida 05/2020 sul consenso ai sensi del regolamento 2016/679, adottate il 4 maggio 2020, v1.1 .,p. 30. Disponibile all'indirizzo: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf Acceduto il 16 settembre 2021.

110 "Insegnamento" non deve essere identificato con "espressione accademica" nel contesto dell'art. 85 GDPR.

111 Vedi, a proposito di "espressione accademica", GEPD, p. 10.

112 Considerando 160 GDPR.

113 Considerando 162 GDPR.

per salvaguardare i diritti e le libertà della persona interessata e per garantire la riservatezza statistica, ecc.)

2.4.4 Quali dati copre l'articolo 89?

Un altro punto rilevante di discussione è la natura dei dati per i quali il trattamento richiede garanzie adeguate e può giustificare eccezioni e deroghe ai diritti dei soggetti.

Non c'è dubbio che l'articolo 89 comprende tutte le categorie di dati personali, il che include anche il trattamento di categorie speciali di dati personali, a condizione che le condizioni per il trattamento di questi ultimi siano soddisfatte.

Così, l'uso secondario dei dati a fini di archiviazione, di ricerca scientifica o storica, o a fini statistici (art. 5), deve essere sostenuto dalle garanzie di cui all'art. 89 quando, ad esempio, l'analisi o il controllo incrociato con altri dati evidenzia informazioni di natura sensibile. Pertanto, nell'applicare il regime dell'art. 89, il contesto del trattamento, le sue implicazioni e la natura dei dati sono di fondamentale importanza.

2.4.5 Compatibilità di scopo

Secondo l'articolo 5, paragrafo 1, lettera b), l'ulteriore trattamento a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici è compatibile anche se i dati sono stati inizialmente raccolti per altre finalità diverse (a condizione che siano in atto misure tecniche e organizzative che garantiscano il rispetto dei diritti e delle libertà dell'interessato). Tuttavia, rimane in discussione se altre disposizioni possono essere applicate, ad esempio, il test di compatibilità ai sensi dell'articolo 6, paragrafo 4, del GDPR.

Tuttavia, in relazione a categorie speciali di dati, l'articolo 9 (2) (j) menziona esplicitamente che il trattamento deve essere "basato sul 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 adeguate e specifiche per salvaguardare i diritti fondamentali e gli interessi della persona interessata".

Questo apparente problema giuridico richiede uno sforzo interpretativo che potrebbe risolvere la questione in due modi. In primo luogo, poiché l'articolo 5 non fa riferimento a categorie speciali di dati personali, potrebbe essere inteso come limitato ai casi in cui non vengono utilizzate tali informazioni. Se si dovesse parlare di dati personali di queste categorie, si applicherebbe l'articolo 9, che è più specifico.

La seconda soluzione si basa su un'interpretazione dell'articolo 5 come semplice principio generale e alla luce del considerando 50, che delinea una serie di condizioni per l'uso secondario, che rappresentano il requisito di un maggiore autocontrollo da parte del titolare del trattamento, nonché una "ragionevole aspettativa" da parte della persona interessata che questo trattamento secondario possa avere luogo. Inoltre, l'art. 6(4) stabilisce una serie di criteri per determinare la compatibilità di un trattamento con la (diversa) finalità per cui i dati personali sono stati raccolti, che dovrebbero essere presi in considerazione anche in questi casi: "a) l'eventuale nesso tra le finalità per le quali i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) il contesto in cui i dati personali sono stati raccolti, in particolare per quanto riguarda la relazione tra gli interessati e il titolare del trattamento; c) la natura dei dati personali, in particolare se sono trattate categorie particolari di dati personali, ai sensi dell'articolo 9, o se sono trattati dati personali relativi a condanne penali e reati, ai sensi dell'articolo 10; d) le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) l'esistenza di garanzie adeguate, che possono includere la cifratura o la pseudonimizzazione" (vedi "Identificazione", "Pseudonimizzazione" e

"Anonimizzazione" nella Parte II di queste Linee guida, sezione "Concetti principali"). Pertanto, sembra che gli articoli 5, 6 e 9 debbano essere letti e interpretati insieme[114].

2.4.6 Questioni concettuali: base giuridica del trattamento.

Per quanto riguarda la base giuridica del trattamento, è importante distinguere tra categorie di dati:

- Trattamento di dati personali ("non sensibili"). Le basi giuridiche del trattamento sono quelle indicate nell'articolo 6 del GDPR (vedi "Liceità, correttezza e trasparenza" nella Parte II sezione "Principi" di queste Linee guida). Ciò significa che ogni trattamento di dati personali deve necessariamente basarsi su una delle basi giuridiche di cui all'articolo 6(1):
  a) Consenso dell'interessato (art. 6.1 a).
  b) Contratto (art. 6.1 b).
  c) Obbligo legale (art. 6.1 c).
  d) Interessi vitali (art. 6.1 d).
  e) Compito pubblico o interesse pubblico (art. 6.1 e).
  f) Interessi legittimi (art. 6.1 f).
- Trattamento di categorie speciali di dati personali ("dati personali sensibili"). Il trattamento di quelle categorie di dati incluse nell'articolo 9 è vietato a meno che non venga identificata una base legittima specifica tra quelle dell'articolo 9, paragrafo 2.[115] L'articolo 9 richiede un'ulteriore legittimazione, aggiunta a quelle dell'articolo 6. Tra queste basi giuridiche, il trattamento non è vietato, se, tra le altre cose:
  a) "la persona interessata ha dato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità determinate, tranne nei casi in cui il diritto dell'Unione o degli Stati membri preveda che il divieto di cui al paragrafo 1 non possa essere revocato dalla persona interessata". Articolo 9, paragrafo 2, lettera a).
  b) è "necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o di uno Stato membro che sia proporzionato alla finalità perseguita, rispetti il contenuto essenziale del diritto alla protezione dei dati e preveda misure adeguate e specifiche per la salvaguardia dei diritti fondamentali e degli interessi della persona interessata". [116]

---

114 GEPD, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 2020, pag. 23. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Accesso: 15 gennaio 2020.

115 EDPB, parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulle sperimentazioni cliniche (CTR) e il regolamento generale sulla protezione dei dati (GDPR) (art. 70.1.b)) Adottato il 23 gennaio 2019, pp. 8-9. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf Accesso: 20 maggio 2020.
Questo documento descrive diverse possibilità che combinano gli articoli 6 e 9: I motivi legittimi del trattamento possono derivare da obblighi legali del responsabile del trattamento e che rientrano nella base giuridica dell'articolo 6, paragrafo 1, lettera c), in combinato disposto con l'articolo 9, paragrafo 1, lettera i); o l'interesse pubblico ai sensi dell'articolo 6, paragrafo 1, lettera e), in combinato disposto con l'articolo 9, paragrafo 2, i) o j); o i legittimi interessi del responsabile del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f), in combinato disposto con l'articolo 9, paragrafo 2, lettera j); o in circostanze specifiche, quando tutte le condizioni sono soddisfatte, il consenso esplicito dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera a), e dell'articolo 9, paragrafo 2, lettera a).

116 Articolo 9, paragrafo 2, lettera j).

Inoltre, l'articolo 9 (4) recita: "Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese le limitazioni, per quanto riguarda il trattamento dei dati genetici, dei dati biometrici o dei dati relativi alla salute." Questa possibilità non implica, tuttavia, che il contenuto del paragrafo (2)(j) dell'articolo 9 debba essere reso inefficace. Ancora una volta, i ricercatori dovrebbero sempre chiedere consiglio ai loro DPO sul quadro normativo nazionale applicabile.

2.4.7 Trattamento a fini di archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici e il diritto all'informazione

Qualora i dati personali non siano stati ottenuti dall'interessato e il trattamento sia effettuato a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici, sono previste dal regolamento deroghe al diritto all'informazione. In stretta relazione ai due punti precedenti, e per facilitare la disponibilità dei dati per tali finalità, l'articolo 14, paragrafo 5, lettera b), del GDPR prevede che le disposizioni dei paragrafi da 1 a 4 (che descrivono le informazioni che il titolare del trattamento deve trasferire all'interessato) non si applicano quando "la fornitura di tali informazioni si rivela impossibile o comporterebbe uno sforzo sproporzionato, in particolare per i trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo possa rendere impossibile o compromettere gravemente il conseguimento degli obiettivi di tale trattamento. In tali casi il titolare del trattamento adotta misure adeguate per proteggere i diritti e le libertà e gli interessi legittimi dell'interessato, anche rendendo pubbliche le informazioni."

Pertanto, come si può dedurre dalla lettera della disposizione, non è necessario un ulteriore sviluppo del diritto dell'Unione o degli Stati membri per applicare questa deroga.

2.4.8 Deroghe a certi diritti delle persone interessate ai sensi dell'articolo 89

L'articolo 89, paragrafo 2, del GDPR afferma che: "Qualora i dati personali siano trattati per finalità di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti possano rendere impossibile o compromettere gravemente il conseguimento delle finalità specifiche, e tali deroghe siano necessarie per il raggiungimento di tali finalità. "Insieme all'articolo 14(5)(b), questa clausola introduce diverse deroghe relative ai diritti degli interessati (si veda la sezione "Diritti degli interessati" nella parte II delle presenti Linee guida), ossia:

- *Diritto di accesso (articolo 15 GDPR):* Secondo l'articolo 89, è possibile limitare il diritto di accesso agli interessati. Questa limitazione riguarda sia i dati personali che sono stati trattati per la ricerca, sia i dati personali che sono stati ottenuti come risultato delle analisi o delle procedure sviluppate. Nel campo biomedico, per esempio, questo riguarda qualsiasi risultato ottenuto da esami o procedure corporali, analisi dei loro campioni o dati, ecc.

- *Diritto alla rettifica (articolo 16 GDPR):* Il diritto di far rettificare o completare i dati inesatti non è di grande importanza nella ricerca scientifica (può essere più rilevante, per esempio, nella ricerca storica). Né lo è la sua limitazione. La metodologia della ricerca scientifica richiede l'accuratezza e l'affidabilità delle informazioni trattate per ottenere conclusioni solide, quindi sarà nel suo stesso interesse esigere tale accuratezza;

- *Limitazione del trattamento (art. 18 GDPR):* Per restrizione del trattamento "si intende la marcatura dei dati personali memorizzati allo scopo di limitarne il trattamento in futuro" (art. 4(3) GDPR). I dati personali il cui trattamento è limitato non vengono cancellati e vengono conservati per scopi diversi, ma non possono essere utilizzati o trasferiti oltre tale ambito. Nel quadro di un'indagine, l'esercizio di questo diritto potrebbe ostacolare la continuità dell'indagine o la pubblicazione dei risultati nella sua prima fase (limitazione della continuità del suo utilizzo). Ecco perché questa deroga ha senso.

- *Diritto di opposizione (art. 21 GDPR): Il* diritto di opposizione consente all'interessato i cui dati personali vengono trattati in base a qualsiasi motivo giuridico diverso dal consenso di opporsi al trattamento. Questa possibilità è alla base dei cosiddetti sistemi di opt-out (in cui si presume il consenso all'uso dei dati per scopi di ricerca), e fondamentale per i casi in cui il consenso al trattamento non è richiesto (articoli 5 e 9 GDPR). Sollevare eccezioni a questo diritto ha conseguenze importanti per l'autonomia degli interessati, poiché può implicare che i dati siano utilizzati contro la loro volontà. Giustificare queste eccezioni come ostacolo che possono rappresentare per la ricerca, sarebbe abbastanza semplice in ogni caso in cui tali dati sono rilevanti per la ricerca.

Esempio: Ricerca sulle malattie rare

La ricerca sulle malattie rare spesso si basa su dati personali ottenuti da un numero abbastanza ridotto di soggetti (a causa della natura pura delle malattie rare). Pertanto, se un numero significativo di individui che partecipano alla ricerca decide di esercitare i propri diritti di restrizione e/o obiezione, la rappresentatività e l'affidabilità dei dati della ricerca potrebbero essere significativamente compromesse come conseguenza. Inoltre, i ricercatori potrebbero affrontare seri problemi in termini di pubblicazione, dal momento che non potrebbero fornire quei dati all'editore. Pertanto, in tali circostanze, il Responsabile del trattamento potrebbe ricorrere alle deroghe a tali diritti stabilite dall'articolo 89.

I titolari del trattamento devono sempre tenere presente che "qualsiasi deroga a questi diritti essenziali dell'interessato deve essere oggetto di un esame particolarmente elevato in linea con le norme richieste dall'articolo 52, paragrafo 1, della Carta". Di conseguenza, le deroghe ai sensi dell'articolo 89, paragrafo 2, del GDPR sono possibili solo se le condizioni e le garanzie richieste dall'articolo 89, paragrafo 1, sono soddisfatte.

Inoltre, ai sensi dell'articolo 89, paragrafo 2, le deroghe possono essere applicate solo "nella misura in cui" i diritti a cui si intende derogare "possano rendere impossibile o compromettere gravemente il conseguimento delle finalità specifiche e tali deroghe siano necessarie per il raggiungimento di tali finalità".[117] Infine, i titolari del trattamento devono considerare che "il fatto che mettere in atto misure tecniche e organizzative per fornire l'accesso e altri diritti agli individui possa richiedere risorse finanziarie e umane non è di per sé una valida giustificazione per derogare ai diritti degli individui ai sensi del GDPR".[118]

117 GEPD, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 2020, pag. 21. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Accesso: 15 gennaio 2020.

118 Parere del GEPD sulle garanzie e le deroghe ai sensi dell'articolo 89 del GDPR nel contesto di una proposta di regolamento sulle statistiche agricole integrate, 2017. p.3. All'indirizzo: https://edps.europa.eu/sites/edp/files/publication/17-11-20_opinion_farm_statistics_en.pdf. Accessibile: 17 gennaio 2020.

Infine, per quanto riguarda solo i dati trattati a fini di archiviazione nell'interesse pubblico, il diritto dell'Unione o degli Stati membri può prevedere, oltre a quelli summenzionati, deroghe al diritto di notifica in materia di rettifica, cancellazione o limitazione del trattamento (articolo 19) e al diritto di portabilità (articolo 20)[119]. Ancora una volta, ciò richiede che l'esercizio di questi diritti possa rendere impossibile o compromettere gravemente il raggiungimento delle finalità specifiche e che tali deroghe possano essere, di conseguenza, necessarie per il raggiungimento di tali finalità.

Deroghe al diritto alla cancellazione o al diritto all'oblio

Ai sensi dell'articolo 17, paragrafo 3, lettera d), questo diritto non si applica nella misura in cui il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui può rendere impossibile o compromettere gravemente il conseguimento degli obiettivi di tale trattamento.

Allo stesso modo, le deroghe al diritto alla cancellazione si applicheranno direttamente, senza bisogno di ulteriori sviluppi da parte degli Stati membri.

2.4.9 Limitazione della conservazione

Secondo l'articolo 5(1)(e) del GDPR, i dati personali dovrebbero essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario" (vedi "Principio di limitazione della conservazione" nella Parte II sezione "Principi" di queste Linee guida). Tuttavia, il GDPR permette la conservazione per periodi più lunghi se l'unico scopo è la ricerca scientifica (o l'archiviazione nel pubblico interesse, la ricerca storica o scopi statistici), a condizione che i titolari del trattamento siano autorizzati a procedere a tale trattamento in base a una base giuridica adeguata (la conservazione comporta il trattamento dei dati). L "intenzione del legislatore sembra essere stata quella di dissuadere la conservazione illimitata anche in questo regime speciale e di evitare che la ricerca scientifica sia un pretesto per una conservazione più lunga per altri scopi privati. In caso di dubbio, il titolare del trattamento dovrebbe considerare se una nuova base legale è appropriata".[120]

Pertanto, i periodi di conservazione dovrebbero essere proporzionati agli scopi del trattamento. "Per definire i periodi di conservazione (scadenze), si dovrebbero prendere in considerazione criteri come la durata e lo scopo della ricerca. Va notato che le disposizioni nazionali possono anche stabilire delle regole relative al periodo di conservazione".[121]

2.4.10 Garanzie appropriate da adottare ai sensi dell'articolo 89, paragrafo 1

L'articolo 89(1) richiede l'applicazione di "garanzie adeguate" al trattamento dei dati personali per scopi di ricerca scientifica o storica o statistica, indipendentemente dalla base giuridica del trattamento. Lo scopo di queste garanzie è quello di assicurare il rispetto del principio di minimizzazione dei dati personali (vedi sottosezione "Principio di minimizzazione" nella sezione "Principi" all'interno della Parte II di queste Linee Guida). Quindi, il primo parametro

119 Vedi l'articolo 89, paragrafo 3, del regolamento.

120 EDPB, Linee guida 03/2020 sul trattamento dei dati relativi alla salute ai fini della ricerca scientifica nel contesto dell'epidemia COVID-19. Adottato il 21 aprile 2020, pag. 10. Su: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf Accesso: 23 aprile 2020.

121 Ibidem, p. 10.

da analizzare è se le condizioni stesse per il trattamento dei dati personali sono soddisfatte, vale a dire, il trattamento dei dati personali deve essere necessario per svolgere quella particolare ricerca. L'articolo 89, paragrafo 1, prevede che le garanzie appropriate "devono tradursi in misure tecniche e organizzative", come la pseudonimizzazione. La pseudonimizzazione deve essere accompagnata da altre disposizioni, a seconda dei rischi coinvolti in ogni progetto. I titolari del trattamento devono sempre garantire l'attuazione di misure tecniche e organizzative adeguate per assicurare la protezione dei diritti e delle libertà degli interessati. I seguenti sono alcuni possibili esempi di tali misure o salvaguardie:

- Controllo dell'accesso alle banche dati in modo che tale accesso sia consentito solo alle persone autorizzate, per ricerche approvate, con giustificato interesse scientifico, e soluzione software implementata che permetta un controllo verificabile dei file di log di accesso.

- Firma di un impegno giuridicamente vincolante tra le parti, che include le condizioni del trattamento: impegno alla riservatezza e alla non identificazione degli interessati, e utilizzo dei dati per lo scopo specifico autorizzato.

- Attuare misure di sicurezza per garantire la protezione del trasferimento e dell'archiviazione dei dati presso il destinatario.

- Garantire la trasparenza delle informazioni fornite ai partecipanti.

- Monitoraggio continuo delle condizioni di trattamento nel tempo, che potrebbe assumere la forma di misure di trasparenza (pubblicazione e accessibilità delle politiche di gestione dei dati) e previsioni a lungo termine (identificazione degli obblighi del titolare del trattamento). In relazione a quest'ultimo punto, va sottolineata la necessità di stabilire impegni chiari per monitorare la gestione/il trattamento dei dati personali da parte dell'istituzione che conduce la ricerca e che potrebbero essere più specificamente affidati al corrispondente Comitato di Etica della Ricerca (REC).

- Istituzione di un sistema di controllo esterno allo sperimentatore che potrebbe essere di competenza del REC corrispondente o della direzione del centro di ricerca, che dovrebbe essere coinvolto nel suddetto accordo.

Inoltre, i ricercatori dovrebbero tenere a mente che ci sono altri meccanismi previsti nel regime generale del GDPR che introducono anche misure adeguate al trattamento dei dati a fini di ricerca nel senso dell'articolo 89, paragrafo 1, come le DPIA o l'intervento dei DPO. Infine, è interessante menzionare che ci sono iniziative per promuovere codici di condotta internazionali e meccanismi di certificazione che possono armonizzare queste garanzie.

2.4.11 **Ulteriori letture**

- GEPD, Parere sulle garanzie e le deroghe ai sensi dell'articolo 89 del GDPR nel contesto di una proposta di regolamento sulle statistiche agricole integrate, 2017. All'indirizzo: https://edps.europa.eu/sites/edp/files/publication/17-11-20_opinion_farm_statistics_en.pdf
- GEPD, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 2020. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.
- EDPB, parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulle sperimentazioni cliniche (CTR) e il regolamento generale sulla protezione dei dati

(GDPR) (art. 70.1.b). Adottato il 23 gennaio 2019. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf

- EDPB, Linee guida 03/2020 sul trattamento dei dati relativi alla salute ai fini della ricerca scientifica nel contesto dell'epidemia COVID-19. Adottato il 21 aprile 2020. All'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf