IL DIRITTO DIGITALE
Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

Title: LEGAL DESIGN AND DATA SCIENCE FOR EXPLICABLE AI IN LEGAL DOMAIN
Acronym: LEDS 4 XAIL
n. GPA: 101085576
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Fondazione Bologna University Press
Via Saragozza 10, 40123 Bologna
tel. (+39) 051 232 882

www.buponline.com
e-mail: info@buponline.com

ISBN 979-12-5477-771-8
ISBN on line 979-12-5477-772-5
DOI 10.30682/9791254777725

Questo volume è stato realizzato a partire da un impaginato camera-ready in formato pdf fornito dai curatori

In copertina: Summit Art Creations/Shutterstook.com

Prima edizione: marzo 2026

LA PROTEZIONE DEI DATI PERSONALI*

Federico Galli, Giovanni Sartor

SOMMARIO: 1. Privacy e protezione dei dati: origine e sviluppi. 2. Il Regolamento generale sulla protezione dei dati. 2.1. L'ambito di applicazione materiale. 2.2. L'ambito di applicazione territoriale. 3. La definizione di "dato personale". 3.1. Pseudonimizzazione e anonimizzazione. 4. Principi generali sul trattamento. 5. Le condizioni di liceità del trattamento. 5.1. Categorie particolari di dati (dati sensibili). 5.2. Il consenso dell'interessato. 5.3. Il legittimo interesse. 6. I diritti dell'interessato. 6.1. Il diritto alla cancellazione (diritto all'oblio). 7. Gli obblighi del titolare del trattamento. 7.1. Il titolare e il responsabile del trattamento. 7.2. Gli obblighi del titolare del trattamento. 7.3. *Data protection by design* e *by default*. 7.4. Valutazione di impatto sulla protezione dei dati e il *Data Protection Officer*. 8. Il Garante per la protezione dei dati personali. 9. La tutela giurisdizionale. 10. L'applicazione del GDPR nel contesto europeo (cenni).

1. Privacy e protezione dei dati: origine e sviluppi

La protezione dei dati ha origini dalla confluenza di diverse esigenze di protezione giuridica.

Una prima esigenza attiene alla protezione rispetto alla diffusione non autorizzata di informazioni sulla vita privata dei singoli (che include non solo i comportamenti che l'individuo tiene nel proprio domicilio, al di fuori dello sguardo altrui, ma anche quelli che non rilevano per ruoli o funzioni di interesse pubblico). Era questo il tema affrontato nel famoso saggio che aprì il dibattito statunitense sul "diritto alla privacy" alla fine del XIX secolo[1].

La stessa esigenza di tutela è stata affermata dalla nostra Corte di Cassazione nella sentenza n. 2129 del 27 maggio 1975, che riguardava la pubblicazione, da parte di un settimanale, di fotografie e dettagli sulla vita privata della principessa Soraya, ex moglie dello Scià di Persia. Nel sanzionare tale comportamento, la Corte riconosceva l'esistenza di un autonomo diritto alla riservatezza, qualificandolo come un diritto della personalità tutelato dall'ordinamento, ricollegandolo agli articoli 2 e 3 della Costituzione.

Una seconda esigenza di tutela attiene alla garanzia della libertà dell'individuo nella propria vita privata, quale sfera sottratta alle intrusioni dello Stato,

* Il presente contributo è un risultato del progetto ERC-Advanced "CompuLaw" (Grant Agreement No 833647).

[1] S. WARREN, L. BRENDEIS, *The Right to Privacy*, in *Harvard L. Rev.*, 1890, pp. 193-220.

un'esigenza fortemente sentita in Europa dopo l'esperienza dei regimi totalitari (caratterizzati dalla tendenziale negazione di ogni dimensione privata). Questa esigenza è alla base del diritto alla protezione della vita privata, affermato nell'articolo 12 della Dichiarazione Universale dei Diritti Umani:

> Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge, contro tali interferenze o lesioni.

La Convenzione europea dei diritti dell'uomo (1950) ha seguito l'esempio, nell'articolo 8 della Convenzione che recita:

> 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non vi sarà alcuna ingerenza da parte di un'autorità pubblica nell'esercizio di tale diritto, salvo quella prevista dalla legge e necessaria in una società democratica nell'interesse della sicurezza nazionale, della pubblica sicurezza o del benessere economico del Paese, per la prevenzione di disordini o crimini, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Il diritto alla protezione della vita privata comprende due aspetti. Da un lato vi è la così detta "privacy decisionale", cioè la libertà dell'individuo nelle scelte che riguardano la sua sfera intima (per esempio, la dimensione sessuale, affettiva o familiare). Dall'altro lato, vi è la così detta "privacy informazionale", che riguarda invece il diritto a limitare l'accesso alle informazioni che riguardano quella stessa sfera. Questo secondo aspetto è specificamente rilevante ai nostri fini.

Una terza esigenza di tutela emersa più recentemente attiene invece alla protezione dell'individuo dai rischi che derivano dalla raccolta ed elaborazione sistematica dei dati che lo riguardano, in particolare mediante sistemi informatici. Tale esigenza di protezione ha un ambito più esteso rispetto a quello della "privacy informazionale" quale aspetto della tutela della vita privata: riguarda ogni tipo di dato personale, anche al di là degli aspetti "privati" (pensiamo ad esempio, alle informazioni raccolte dai datori di lavoro sui dipendenti, dallo stato sui cittadini a fini fiscali o previdenziali, dalle imprese per l'invio di pubblicità mirata, ecc.).

Nel costruire una disciplina giuridica che risponda a questa così ampia esigenza di protezione bisogna però considerare che vi sono interessi importanti – pubblici e privati – che possono giustificare la raccolta e l'elaborazione dei dati personali. Si pensi a come dati sugli individui siano necessari per la gestione del

personale nelle imprese, per l'erogazione dei servizi da parte degli enti pubblici, per l'erogazione del credito da parte delle banche, per la fornitura di prestazioni sanitarie da parte di strutture pubbliche e private, per pagamenti e consegne nel commercio elettronico, ecc. Per rispondere a tali esigenze è necessario consentire la raccolta e l'elaborazione dei dati personali per scopi legittimi, regolando però tale elaborazione in modo da minimizzare i rischi che ne derivino per gli individui interessati.

Affrontare quei rischi è oggi necessario poiché tecnologie sempre più potenti consentono di sorvegliare le persone e di tracciarne la vita in ogni aspetto (gli spostamenti, gli acquisti, le interazioni sociali, le condizioni di salute, ecc.). I dati raccolti possono essere poi elaborati per inferire caratteristiche, attitudini, interessi e vulnerabilità degli interessati, e quindi per adottare decisioni (possibilmente ingiuste o discriminatorie) che li riguardano, o per cercare di influenzarne il comportamento nella sfera economica o anche in quella politica. In questo contesto non solo la riservatezza o la vita privata, ma le libertà civili e politiche (libertà di espressione, di associazione, di informazione, diritto al lavoro, ecc.) sono minacciate e lo stesso assetto democratico della società è in discussione.

Per affrontare questi rischi si è sviluppata la disciplina della "protezione dei dati", che, ricoprendo ogni elaborazione sistematica di dati personali (non solo di quelli che attengono alla dimensione intima o privata), si affianca e sovrappone alla tutela della riservatezza e alla tutela della vita privata. Lo scopo di tale disciplina non è la protezione dei dati stessi ma piuttosto la protezione degli individui dai rischi che derivano dal trattamento dei loro dati personali, protezione che richiede una regolazione dei processi mediante i quali i dati sono raccolti ed elaborati.

Il diritto alla protezione dei dati si configura quindi come il diritto dell'interessato a controllare il trattamento dei propri dati, e più in generale, ad essere protetto dai rischi che derivano dall'elaborazione di quei dati. La protezione si attua mediante diritti garantiti all'interessato (es., all'informazione, l'accesso, e la rettifica), mediante obblighi imposti a chi effettua i trattamenti e grazie alla supervisione da parte di autorità indipendenti.

Tale diritto è infatti così caratterizzato dall'articolo 8 della Carta dei Diritti Fondamentali dell'Unione europea.

> 1. Ogni persona ha diritto alla protezione dei dati personali che la riguardano.
>
> 2. Tali dati devono essere trattati lealmente per finalità specifiche e sulla base del consenso dell'interessato o di un'altra base legittima prevista dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di queste regole è soggetto al controllo di un'autorità indipendente.

Nell'Unione Europea la protezione dei dati è oggi disciplinata dal Regolamento 679/2016 sulla protezione dei dati, cui si fa spesso riferimento con l'acronimo GDPR (*General Data Protection Regulation*).

Tale regolamento ha abrogato la precedente disciplina rappresentata dalla direttiva 95/46 che costituiva il principale riferimento europeo in materia di tutela dei dati personali, fissando principi comuni per tutti gli Stati membri tesi ad armonizzare le legislazioni nazionali in materia.

In Italia tale direttiva era stata trasposta con la legge 31 dicembre 1996, n. 675 (la prima disciplina organica della protezione dei dati nel nostro Paese), poi riorganizzata all'interno del Codice in materia di protezione dei dati personali, detto anche Codice privacy (d.lgs. 30 giugno 2003, n. 196).

Dopo l'entrata in vigore del Regolamento, il Codice privacy non è stato abrogato (sebbene molte delle sue disposizioni siano state superate dalla nuova normativa europea), ma è stato pesantemente modificato dal d.lgs. 10 agosto 2018, n. 101. Tale decreto ha abrogato le disposizioni incompatibili con il GDPR e ha introdotto norme integrative per le materie lasciate alla competenza degli Stati membri, come il trattamento dei dati in ambito giudiziario, la protezione dei dati dei minori e le sanzioni amministrative.

Il Codice privacy è stato successivamente ulteriormente modificato. Si ricorda in particolare il d.l. 8 ottobre 2021, n. 139 (cosiddetto "decreto Capienze"), che ha inciso in modo significativo su vari articoli del Codice, ridefinendo, tra l'altro, il ruolo delle basi giuridiche per i trattamenti effettuati da soggetti pubblici, chiarendo l'ambito applicativo dell'art. 2-ter e introducendo modifiche anche in materia di trattamento per finalità di interesse pubblico, semplificazioni procedurali e coordinamento con il GDPR.

2. Il Regolamento Generale sulla Protezione dei Dati

Il Regolamento UE 2016/679 è stato adottato nel 2016 ed è entrato in vigore il 25 maggio 2018[2]. Il GDPR è stato concepito per uniformare le leggi sulla protezione dei dati in tutta Europa, per proteggere e potenziare la privacy dei

[2] Si ricorda che il GDPR è stato proposto nel cosiddetto Pacchetto Protezione Dati accanto alla così detta Direttiva Polizia, relativa alla protezione dei dati nel corso delle indagini di polizia e dell'applicazione del diritto penale (Direttiva (UE) 2016/680), che protegge i dati personali nelle forze dell'ordine, e al Regolamento sulla libera circolazione dei dati non personali (Regolamento (UE) 2018/1807). Inoltre, il pacchetto ha proposto il regolamento sulla privacy elettronica, che si sarebbe concentrato sulla riservatezza delle comunicazioni elettroniche e avrebbe sostituito la direttiva sulla privacy elettronica del 2002, che tuttavia non è mai stato approvato.

dati di tutti i cittadini dell'UE e per rimodellare il modo in cui le organizzazioni affrontano la privacy dei dati.

In particolare, l'oggetto è così specificato nell'articolo 1:

> 1. 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.
>
> 2. Il presente regolamento tutela i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
>
> 3. La libera circolazione dei dati personali all'interno dell'Unione non è limitata né vietata per motivi connessi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

2.1. L'ambito di applicazione materiale

L'ambito di applicazione materiale del GDPR è definito dall'articolo 2 del Regolamento e determina i casi in cui le norme sulla protezione dei dati personali si applicano o meno.

In linea generale, il GDPR si applica al trattamento dei dati personali che riguardano persone fisiche identificate o identificabili, effettuato, totalmente o parzialmente, con mezzi automatizzati, nonché al trattamento non automatizzato di dati contenuti in un archivio o destinati a figurarvi.

Ciò significa che il Regolamento copre una vasta gamma di attività, che spaziano dalla gestione di banche dati digitali alle raccolte cartacee strutturate di informazioni personali, purché destinate a essere organizzate o consultate sistematicamente. L'elemento determinante, come vedremo sotto, è dunque l'identificabilità della persona fisica, diretta o indiretta, attraverso elementi come nome, numero di identificazione, dati relativi all'ubicazione, identificatori online o altri fattori specifici relativi all'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale dell'interessato.

L'articolo 2, paragrafo 2, elenca in modo espresso alcune esclusioni dall'ambito di applicazione, tra cui i trattamenti effettuati: a) nell'esercizio di attività non rientranti nell'ambito di applicazione del diritto dell'Unione; b) dagli Stati membri quando esercitano attività rientranti nell'ambito della politica estera e di sicurezza comune; c) da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) dalle autorità competenti per finalità di prevenzione, indagine, accertamento o perseguimento di reati o per l'esecuzione di sanzioni penali, disciplinate dalla Direttiva (UE) 2016/680.

2.2. L'ambito di applicazione territoriale

L'articolo 3 del GDPR definisce l'ambito di applicazione territoriale del Regolamento, stabilendo che esso riguarda le attività di trattamento dei dati personali effettuate da titolari o responsabili stabiliti nell'Unione europea, indipendentemente dal luogo in cui il trattamento viene materialmente svolto[3]. La nozione di "stabilimento" è interpretata in senso funzionale e sostanziale, secondo la giurisprudenza della Corte di giustizia, e richiede la presenza di un'attività reale ed effettiva, anche se minima, esercitata tramite un'organizzazione stabile.

Il GDPR si applica inoltre ai trattamenti effettuati da soggetti non stabiliti nell'UE quando tali trattamenti riguardano l'offerta di beni o servizi a interessati che si trovano nell'Unione, oppure il monitoraggio del loro comportamento, nella misura in cui tale comportamento avvenga all'interno del territorio dell'Unione. Questa clausola, introdotta dall'articolo 3, paragrafo 2, ha un ruolo centrale nel contrastare fenomeni di delocalizzazione opportunistica dei trattamenti (al fine di godere di una disciplina meno rigorosa): non è dunque determinante la sede giuridica del titolare, ma l'effettiva incidenza delle sue attività sugli interessati nell'UE.

L'estensione extraterritoriale del GDPR ha ampliato in modo significativo il numero di soggetti obbligati a conformarsi alla disciplina europea. Una società con sede negli Stati Uniti o in un Paese terzo che offra servizi a utenti europei, oppure che tracci il loro comportamento mediante cookie, identificatori online o altre tecniche di profilazione, è tenuta a rispettare il GDPR e a designare un rappresentante nell'Unione, salvo eccezioni. In questo modo si assicura che i diritti degli interessati nell'UE siano tutelati anche quando il trattamento è effettuato da entità situate al di fuori del territorio europeo.

Questa portata extraterritoriale ha contribuito a ciò che è stato definito "effetto Bruxelles"[4]. Il GDPR, attraverso i suoi standard elevati e la sua capacità di incidere sulle pratiche di attori globali, ha influenzato normative e politiche aziendali in tutto il mondo. Molte imprese multinazionali hanno scelto di adottare modelli di conformità uniformi a livello globale, estendendo le tutele del GDPR a tutti i loro utenti, non solo a quelli residenti nell'UE.

---

[3] Articolo 3, paragrafo 1 del GDPR.

[4] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford: Oxford University Press, 2020.

3. La definizione di "dato personale"

Ai sensi dell'articolo 4, paragrafo 1, del GDPR, per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile, cioè del "soggetto interessato" (in inglese *data subject*). Tali informazioni includono identificatori come il nome, il numero di identificazione, i dati relativi all'ubicazione e gli identificatori online[5], nonché fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale.

Entro la categoria generale di dato personale, il GDPR distingue una sottocategoria di informazioni che, per la loro natura, richiedono una tutela rafforzata: le categorie particolari di dati personali, comunemente dette dati sensibili. Sono quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale e all'orientamento sessuale della persona.

Come vedremo sotto, il trattamento di tali dati è vietato in linea di principio (dunque viene invertita la regola generale rispetto al trattamento dei dati comuni, consentito qualora vi sia una base giuridica), salvo che ricorra una delle eccezioni tassativamente previste dallo stesso articolo 9, paragrafo 2.

Tornando alla definizione generale di dato personale, la questione interpretativa più delicata della definizione di dato personale è la misura in cui le informazioni possono essere considerate relative a una "persona fisica identificabile".

Il GDPR stabilisce che per valutare se una persona è identificabile, si devono considerare tutti i mezzi ragionevolmente utilizzabili, come l'individuazione, da parte del responsabile del trattamento o di un'altra persona. Ciò include la considerazione di fattori quali il costo e la quantità di tempo necessari per l'identificazione, considerando la tecnologia disponibile al momento del trattamento e qualsiasi progresso tecnologico futuro[6].

---

[5] Si ricorda, in questo caso, la sentenza *Breyer* (C-582/14, 19 ottobre 2016), con la quale la Corte di giustizia dell'Unione europea ha stabilito che un indirizzo IP dinamico può costituire un dato personale qualora il titolare del trattamento disponga di mezzi legittimi e ragionevoli per identificare l'interessato mediante informazioni aggiuntive detenute da terzi, come il fornitore di accesso a Internet. La Corte ha chiarito che, per valutare l'identificabilità di una persona, occorre considerare non solo i mezzi effettivamente a disposizione del titolare, ma anche quelli che potrebbero essere utilizzati da altri soggetti, purché l'identificazione non richieda sforzi sproporzionati. Tale pronuncia conferma un'interpretazione ampia e funzionale del concetto di "dato personale", coerente con il considerando 26 del GDPR, e rafforza l'approccio contestuale fondato sul rischio di re-identificazione.

[6] Considerando 26.

Questo aspetto è particolarmente problematico se si considerano le numerose tecnologie che consentono la re-identificazione dei dati. Tecniche come il *data mining*, l'apprendimento automatico e l'analisi dei big data possono incrociare i set di dati anonimizzati con altre fonti di dati, rivelando potenzialmente le identità personali. Anche informazioni apparentemente innocue, se combinate con altri dati, possono portare all'identificazione di individui.

Tale sviluppo ha portato alcuni autori a ritenere che oggi il diritto alla protezione dei dati rischia di diventare un «diritto sull'informazione in quanto tale»[7], cioè che potrebbe estendersi ipoteticamente a qualsiasi informazione che, anche solo potenzialmente, possa contribuire all'identificazione di un individuo, diretta o indiretta. Tale sviluppo, se da un lato estende l'ambito delle garanzie, rischia di sminuire la specificità e la funzione originaria del diritto alla protezione dei dati, trasformandolo in una clausola generale di controllo su qualsiasi flusso informativo.

3.1. Pseudonimizzazione e anonimizzazione

Per comprendere appieno la nozione di dato personale e dunque i confini di applicazione del Regolamento, occorre introdurre anche la distinzione tra pseudonimizzazione e anonimizzazione

La pseudonimizzazione è definita all'articolo 4, paragrafo 5, del GDPR come «il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, purché tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative atte a garantire che non siano attribuite a una persona fisica identificata o identificabile».

In altri termini, la pseudonimizzazione è una tecnica di sicurezza che riduce il rischio di identificazione, ma non elimina il carattere personale del dato: i dati pseudonimizzati restano infatti "dati personali", in quanto l'identità dell'interessato può essere ricostruita tramite informazioni ausiliarie in possesso del titolare o di terzi. Ciò è stato ribadito dal Considerando 26 del GDPR, secondo cui «i dati personali che sono stati sottoposti a pseudonimizzazione, e che potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di informazioni supplementari, devono essere considerati informazioni su una persona fisica identificabile».

La qualificazione dei dati pseudonimizzati come dati personali implica che essi restano soggetti a tutte le disposizioni del Regolamento, inclusi i principi di

[7] N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law, Innovation and Technology*, 2018 (1), pp. 40-81.

liceità, minimizzazione, limitazione della conservazione e sicurezza del trattamento. Tuttavia, la pseudonimizzazione rappresenta una misura di garanzia significativa, in quanto riduce i rischi per gli interessati e può essere considerata un mezzo di conformità ai sensi dell'articolo 25 (protezione dei dati fin dalla progettazione e per impostazione predefinita) e dell'articolo 32 (sicurezza del trattamento).

La giurisprudenza ha confermato questo approccio in più occasioni. In particolare, nella sentenza "Deloitte" del 26 ottobre 2023 (Causa C-319/22), la Corte di giustizia dell'Unione europea (CGUE) ha chiarito che i dati pseudonimizzati restano dati personali anche se il destinatario del trattamento non dispone direttamente delle chiavi di ricodifica, qualora il titolare originario o un altro soggetto abbia i mezzi per risalire all'identità della persona. Secondo la Corte, la valutazione dell'identificabilità deve essere effettuata tenendo conto non solo dei mezzi del soggetto che detiene i dati, ma anche di quelli potenzialmente accessibili ad altri soggetti che collaborano o possono accedere alle informazioni aggiuntive. La decisione Deloitte ha così ristretto l'ambito del "dato personale" escludendone i dati pseudonimizzati qualora trasmessi ad un terzo che non ha la capacità di procedere alla reidentificazione dei soggetti interessati.

L'anonimizzazione, invece, si distingue dalla pseudonimizzazione per il fatto che comporta un trattamento irreversibile, attraverso il quale le informazioni non possono più essere ricondotte, neppure indirettamente o tramite tecniche avanzate, a una persona fisica identificata o identificabile. I dati anonimizzati non rientrano più nell'ambito di applicazione del GDPR, poiché perdono la loro natura di dato personale. Tuttavia, l'anonimizzazione completa è difficile da garantire nella pratica, specialmente, come detto, alla luce delle tecniche moderne di re-identificazione e dell'integrazione di dataset eterogenei.

Un aspetto particolarmente controverso nel dibattito contemporaneo riguarda i dati sintetici, ossia dati generati artificialmente mediante algoritmi (spesso di intelligenza artificiale) che riproducono le caratteristiche statistiche dei dati reali senza corrispondere a persone effettive. La questione centrale è se tali dati possano essere considerati "anonimi" o se, a causa del loro processo di generazione basato su dati personali, possano comunque implicare un rischio di re-identificazione indiretta. L'assenza di una posizione univoca da parte del legislatore o delle autorità di controllo europee rende l'inquadramento dei dati sintetici ancora oggetto di dibattito dottrinale e giurisprudenziale: mentre alcuni ritengono che essi debbano essere esclusi dal campo di applicazione del GDPR, altri sostengono che, se la generazione sintetica consente la ricostruzione o inferenza di dati riferibili a individui reali, tali dati dovrebbero continuare a essere trattati come dati personali.

4. Principi generali sul trattamento

L'articolo 5 del GDPR delinea i principi per il trattamento dei dati personali:

- Liceità, correttezza e trasparenza: i dati devono essere trattati in modo legale, corretto e trasparente, garantendo la conformità alle regole del GDPR, equità nel trattamento e chiara comunicazione sull'uso dei dati agli interessati.
- Limitazione delle finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e non devono essere ulteriormente trattati in modo incompatibile con tali finalità.
- Minimizzazione dei dati: devono essere trattati solo i dati adeguati, pertinenti e limitati a quanto necessario per le finalità previste.
- Esattezza: i dati personali devono essere esatti e aggiornati; devono essere adottate misure per correggere o eliminare informazioni inesatte.
- Limitazione della conservazione: i dati personali non devono essere conservati più a lungo del necessario per le finalità per cui sono trattati.
- Integrità e riservatezza: i dati personali devono essere trattati in modo sicuro, proteggendoli da trattamenti non autorizzati o illeciti, perdita accidentale, distruzione o danni.

Tutti i principi elencati all'articolo 5 costituiscono le fondamenta del regime di protezione dei dati personali, poiché vi delineano i criteri ai quali ogni trattamento deve conformarsi perché sia una lecita e proporzionata interferenza con il diritto fondamentale alla protezione dei dati personali. Essi non sono meri obblighi formali, ma regole di condotta sostanziali che orientano l'intero ciclo di vita del dato personale, dalla raccolta, all'utilizzo, fino alla conservazione e cancellazione.

Secondo il principio di responsabilizzazione (*accountability*, art. 5, par. 2), il titolare del trattamento, cioè colui che stabilisce le finalità e i mezzi del trattamento, non solo è tenuto a rispettare i principi di cui al paragrafo 1, ma deve anche essere in grado di dimostrarne la conformità. Ciò segna un'evoluzione fondamentale rispetto alla disciplina previgente: la protezione dei dati non è più basata su un modello meramente autorizzativo o formale, bensì su un sistema di responsabilità proattiva, in cui il titolare deve adottare misure tecniche, organizzative e documentali idonee a garantire e comprovare la conformità al Regolamento.

Vi sono due principi che rispondono in modo particolarmente diretto ai principi di necessità e proporzionalità, espressione del bilanciamento tra tutela dei diritti fondamentali e libertà economiche: la limitazione della finalità e la minimizzazione dei dati.

Il principio di limitazione della finalità impone che i dati personali siano raccolti per scopi determinati, espliciti e legittimi, e che ogni successivo trattamento sia compatibile con tali scopi originari. Ciò serve a evitare che i dati vengano utilizzati in modo arbitrario o per finalità ulteriori non previste al momento della raccolta. La valutazione di compatibilità deve tener conto, secondo il considerando 50 del GDPR, di elementi quali il nesso tra la finalità originaria e quella del trattamento successivo, il contesto in cui i dati sono stati raccolti, la natura dei dati e le possibili conseguenze per gli interessati.

Il principio di minimizzazione dei dati, invece, rappresenta la traduzione più diretta del principio di necessità: i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario» rispetto alle finalità perseguite. Tale principio impone una valutazione preventiva di proporzionalità del trattamento, in modo da evitare la raccolta e conservazione di informazioni eccedenti o non indispensabili. Esso si collega strettamente anche al principio di protezione dei dati fin dalla progettazione (*privacy by design*, art. 25), che obbliga il titolare a configurare i sistemi informativi e i processi aziendali in modo da limitare per quanto possibile la quantità e la portata dei dati trattati.

Nel complesso, i principi di limitazione della finalità e di minimizzazione dei dati costituiscono l'espressione operativa della proporzionalità nel trattamento dei dati personali: garantiscono che l'azione del titolare sui dati personali dell'interessato sia limitata nella misura strettamente necessaria al raggiungimento di scopi legittimi, preservando al contempo l'essenza del diritto alla protezione dei dati sancito dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

5. Le condizioni di liceità del trattamento

L'articolo 6 del GDPR specifica le condizioni per il trattamento legale dei dati, chiamate anche "basi legali". Queste sono le uniche condizioni che rendono legittimo il trattamento dei dati personali.

Le condizioni sono:

- Consenso: l'interessato ha dato il proprio consenso al trattamento dei propri dati personali per una o più finalità specifiche.
- Necessità contrattuale: il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte, o per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
- Obbligo legale: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.
- Interessi vitali: il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica.

- Esecuzione di un compito di interesse pubblico: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
- Legittimo interesse: il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, salvo che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali.

Per ciascuna delle condizioni sopra, è possibile fornire alcuni esempi ricorrenti nella pratica:

- Consenso: l'interessato acconsente a ricevere una newsletter promozionale iscrivendosi volontariamente tramite un modulo online.
- Necessità contrattuale: un'azienda di e-commerce tratta i dati dell'acquirente per spedire un prodotto acquistato e gestire il pagamento.
- Obbligo legale: un'azienda conserva i dati fiscali delle fatture per il periodo previsto dalla normativa tributaria.
- Interessi vitali: in caso di emergenza medica, i dati sanitari di un paziente vengono comunicati ai soccorritori per salvaguardarne la vita.
- Esecuzione di un compito di interesse pubblico: un ente pubblico tratta i dati dei cittadini per l'emissione della carta d'identità elettronica.
- Legittimo interesse: un'azienda installa un sistema di videosorveglianza per proteggere i propri locali da furti, nel rispetto dei principi di necessità e proporzionalità.

In ogni caso, spetta al titolare stabilire quale base giuridica sia applicabile al trattamento, prima di iniziare a trattare i dati, e documentare tale scelta in modo chiaro e motivato. La scelta della base di liceità non può essere modificata retroattivamente né "selezionata" in maniera opportunistica: il titolare deve individuare quella che rispecchia effettivamente la finalità perseguita e le circostanze del trattamento.

5.1. Categorie particolari di dati (dati sensibili)

Come abbiamo anticipato sopra, i dati sensibili (o, come definiti dall'art. 9 GDPR, categorie particolari di dati personali) sono quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute e i dati relativi alla vita sessuale o all'orientamento sessuale della persona.

La *ratio* di una disciplina rafforzata per queste categorie di dati risponde all'esigenza di graduare la protezione dei dati in base alla sensibilità e al rischio potenziale per i diritti e le libertà fondamentali dell'individuo. I dati sensibili, infatti, possono rivelare aspetti intimi e profondamente identitari della persona e, se divulgati o trattati in modo improprio, possono condurre a forme di discriminazione o stigmatizzazione sociale. La regola generale è che è vietato trattare tali dati (art. 9, par. 1 GDPR), salvo che ricorra una delle eccezioni previste dal paragrafo 2.

L'articolo 9, par. 2, delinea infatti requisiti specifici per il trattamento di categorie particolari di dati. Tali requisiti devono essere considerati come aggiuntivi rispetto all'art. 6(1) GDPR, cioè è necessario che sussista una base giuridica ordinaria per il trattamento (ad es. consenso, obbligo legale, interesse pubblico, interesse legittimo)[8], e in più una delle condizioni speciali che giustificano il trattamento dei dati sensibili.

Queste includono, tra le altre, il consenso esplicito[9] dell'interessato (lett. a); il trattamento di dati manifestamente resi pubblici dall'interessato (lett. e); il trattamento necessario per motivi di interesse pubblico rilevante (lett. g); il trattamento necessario per finalità di assistenza sanitaria o sociale (lett. h); il trattamento necessario per motivi di sanità pubblica (lett. i); e il trattamento necessario per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica, o a fini statistici (lett. j)[10].

5.2. Il consenso dell'interessato

Secondo l'art. 4, par. 11, il consenso dell'interessato è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o

[8] L'interesse legittimo non è applicabile al trattamento di categorie particolari di dati, salvo casi eccezionali nei quali il trattamento ricada in una delle basi dell'art. 9(2).

[9] Secondo il Comitato europeo per la protezione dei dati, il termine "esplicito" si riferisce al modo in cui il consenso viene espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso, come una dichiarazione scritta o, online, compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato. Vedi *European Data Protection Board*, Linee guida 05/2020 sul consenso ai sensi del Regolamento 2016/679 Versione 1.1, adottate il 4 maggio 2020.

[10] Il Comitato europeo per la protezione dei dati ha chiarito che, laddove le basi legali dell'articolo 9(2) siano meno protettive dell'articolo 6 (ad esempio, quando i dati sono manifestamente resi pubblici dall'interessato), l'articolo 6 dovrebbe applicarsi cumulativamente in questo contesto per garantire una protezione completa delle categorie particolari di dati. Ciò significa che anche se i dati sono resi pubblici, dovrebbero comunque essere trattati in modo legale, corretto e trasparente, mantenendo gli elevati standard di protezione dei dati richiesti dal GDPR.

azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Innanzitutto, il consenso deve essere libero; cioè l'individuo deve avere una scelta genuina. Questo significa che, se l'interessato non può scegliere, è obbligato a dare il consenso o subirà conseguenze negative per non averlo dato, allora il consenso non è considerato libero.

In secondo luogo, il consenso deve essere specifico, in linea con il principio della limitazione delle finalità. Ogni finalità del trattamento dei dati deve avere il proprio consenso, permettendo all'interessato di accettare o rifiutare ogni finalità individualmente. Questa specificità può comprendere attività di trattamento separate se condividono la stessa finalità.

Inoltre, il consenso deve essere informato, aderendo al principio della trasparenza e al diritto all'informazione come delineato negli articoli 13 e 14 del GDPR. Gli elementi essenziali che devono essere comunicati includono l'identità del titolare del trattamento, le finalità del trattamento, le categorie di dati coinvolti, i diritti dell'interessato e qualsiasi processo decisionale automatizzato o trasferimento di dati.

Infine, il consenso deve essere affermativo, indicando chiaramente che l'interessato ha acconsentito all'attività di trattamento specifica. Questo può avvenire tramite una dichiarazione scritta o orale o un'altra azione positiva.

Relativamente al consenso, l'articolo 7(3) aggiunge che l'interessato ha sempre il diritto di revocare il consenso.

Il consenso è spesso considerato la condizione di liceità più protettiva. In effetti, esso riflette l'essenza stessa del diritto alla protezione dei dati personali poiché attribuisce all'individuo la possibilità di decidere autonomamente sull'uso dei propri dati personali.

Tuttavia, sono state sollevate crescenti critiche sull'efficacia del consenso, specialmente riguardo al trattamento dei dati in contesti online[11].

È stato osservato che il consenso risulta spesso non pienamente libero, poiché l'accesso a molti servizi online viene subordinato all'accettazione di trattamenti di dati non necessari alla loro effettiva erogazione[12]. Inoltre, il design delle interfacce dei siti web può influenzare o coartare il consenso (ad es. tramite i

---

[11] Vedi, tra gli altri, B. CUSTERS ET AL., *Consent and Privacy*, in P. SCHABER, A MÜLLER (eds.), *The Routledge Handbook of the Ethics of Consent*, Abingdon: Routledge, 2018 e F. ZUIDERVEEN BORGESIUS, *Informed Consent: We Can Do Better to Defend Privacy*, in *IEEE Security & Privacy*, 2015 (2), pp. 103-107.

[12] In tali casi può rilevare l'Articolo 7, paragrafo 4, secondo cui, nel valutare se il consenso è stato liberamente prestato, occorre considerare in particolare se la conclusione o l'esecuzione di un contratto, inclusa la fornitura di un servizio, sia condizionata al consenso a trattamenti di dati personali non indispensabili per tale esecuzione.

cosiddetti "*tracking walls*"), con la pratica dei cosiddetti "*dark patterns*"[13]. Questi ultimi sono strategie di design utilizzate per manipolare gli utenti a fare scelte che potrebbero non essere nel loro miglior interesse o che potrebbero non aver fatto liberamente. Questi possono includere pulsanti ingannevoli, linguaggio confuso o opzioni di opt-out nascoste, che rendono difficile per gli utenti rifiutare o revocare il consenso o capire a cosa stanno acconsentendo.

Il consenso non è spesso specifico. In molti contesti online, agli utenti viene generalmente richiesto di dare un consenso generico, non potendo selettivamente accettare certe attività di trattamento mentre ne rifiutano altre, fornendo così un "consenso aggregato".

Il consenso è anche spesso scarsamente informato. Molti utenti di Internet danno il consenso senza leggere o comprendere le informazioni sul trattamento dei dati, che sono talvolta presentate in modo vago e ambiguo. Gli utenti spesso non sanno chi tratterà i loro dati.

Infine, il consenso non è sempre inequivocabile. Potrebbe essere dato semplicemente cliccando su un banner o spuntando una casella, possibilmente insieme all'accettazione dei termini di servizio, senza chiara evidenza che questa azione rappresenti una scelta vera da parte dell'utente.

Vi è chi sostiene che occorrerebbe rafforzare il modello del consenso attraverso obblighi più stringenti per i titolari: informative più chiare e brevi, interfacce progettate in modo neutrale, divieto di pratiche manipolative, possibilità di negare il consenso senza perdere l'accesso ai servizi e meccanismi facilmente accessibili per revocarlo in qualsiasi momento.

D'altra parte, vi è chi ritiene invece che l'idea di un consenso genuino si debba abbandonare – almeno in molti contesti digitali – a favore di modelli normativi che responsabilizzino maggiormente i titolari del trattamento, spostando l'onere della protezione dei dati dalle spalle dell'individuo a quelle dell'organizzazione, come nel caso del legittimo interesse.

5.3. Il legittimo interesse

Il legittimo interesse rappresenta una delle basi giuridiche più flessibili e, al tempo stesso, più controverse del GDPR. Ai sensi dell'articolo 6, par. 1, lett. f), il trattamento è lecito quando è «necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi», a meno che su tali interessi non prevalgano «gli interessi o i diritti e le libertà fondamentali dell'interessato».

---

[13] J. LUGURI, L.J. STRAHILEVITZ, *Shining a Light on Dark Patterns*, in *Journal of Legal Analysis*, 2021 (13,1), pp. 43-109.

Questa base giuridica non è disponibile per le autorità pubbliche nell'esecuzione dei loro compiti istituzionali e, in generale, richiede l'esistenza di un interesse reale, attuale e sufficientemente concreto, che il titolare deve essere in grado di dimostrare.

Il Comitato europeo per la protezione dei dati ha chiarito che il ricorso al legittimo interesse richiede un'analisi strutturata (spesso definita test di bilanciamento o LIA, cioè *Legitimate Interest Assessment*) composta da tre fasi:

1. Il titolare deve identificare un interesse proprio o di terzi che sia effettivo e non meramente ipotetico. Esempi ricorrenti includono la sicurezza dei sistemi informatici, la prevenzione delle frodi, la protezione del patrimonio aziendale o il miglioramento di servizi già richiesti dagli utenti.
2. Il trattamento deve essere necessario per perseguire tale interesse e non devono esistere modalità alternative, meno invasive rispetto ai diritti dell'interessato, che permettano di ottenere il medesimo risultato.
3. Occorre valutare se i diritti, le aspettative ragionevoli e le libertà fondamentali dell'interessato prevalgano sull'interesse perseguito dal titolare. Per esempio, un trattamento può risultare sproporzionato quando incide significativamente sulla sfera privata dell'interessato o quando avviene in modo inatteso rispetto al contesto della raccolta dei dati.

Il test di bilanciamento deve essere documentato e, quando appropriato, reso disponibile all'interessato, in linea con il principio di trasparenza (art. 5 GDPR). Inoltre, quando si fa affidamento sul legittimo interesse, il titolare deve garantire che l'interessato possa esercitare il diritto di opposizione previsto dall'articolo 21, salvo la presenza di motivi cogenti che prevalgano sui diritti dell'interessato.

Il legittimo interesse, se correttamente applicato, consente un trattamento proporzionato e coerente con finalità legittime del titolare, senza tuttavia indebolire le tutele riconosciute agli individui. Se applicato in modo improprio, rischia invece di diventare una base "di comodo" per il titolare del trattamento, che può sottostimare i rischi del trattamento, in contrasto con i principi del GDPR e con le aspettative degli interessati.

6. I diritti dell'interessato

I diritti dell'interessato costituiscono uno dei pilastri fondamentali del GDPR. Essi rappresentano gli strumenti attraverso i quali la persona fisica può esercitare il controllo sui propri dati personali, verificare che il trattamento avvenga nel rispetto dei principi di liceità, correttezza e trasparenza, e reagire a eventuali violazioni.

Il Regolamento non si limita a elencare tali diritti, ma impone anche al titolare del trattamento obblighi specifici per garantirne l'effettivo esercizio[14], come la predisposizione di canali di comunicazione adeguati, la risposta entro termini certi e la gratuità delle operazioni (salvo richieste manifestamente infondate o eccessive).

I diritti riconosciuti all'interessato dagli articoli 13-22 del GDPR sono:

- Il diritto di essere informato (articoli 13 e 14): il diritto di ricevere informazioni chiare, comprensibili e facilmente accessibili sul trattamento, sia quando i dati sono raccolti presso il soggetto interessato, sia quando provengono da terzi. Tale diritto, nella pratica, porta alla redazione delle cosiddette "informative privacy" che, secondo i contenuti del GDPR, devono contenere, tra gli altri, l'identità del titolare del trattamento, le finalità del trattamento dei dati, le categorie di dati personali trattati, i destinatari o le categorie di destinatari dei dati, il periodo per il quale i dati saranno conservati, l'esistenza dei diritti dell'interessato e qualsiasi processo decisionale automatizzato coinvolto nel trattamento dei dati.
- Il diritto di accesso (articolo 15): il diritto di ottenere una conferma sul trattamento dei dati personali e di ottenere informazioni su come vengono trattati, inclusa una copia dei dati stessi.
- Il diritto di rettifica (articolo 16): il diritto di far correggere dati personali inesatti o completare dati incompleti.
- Il diritto alla cancellazione (articolo 17): conosciuto anche come diritto all'oblio (si veda nel dettaglio sotto), consente agli interessati di richiedere la cancellazione dei propri dati personali in determinate condizioni.
- Il diritto di limitazione del trattamento (articolo 18): il diritto di limitare il trattamento dei propri dati personali in determinate circostanze.
- Il diritto alla portabilità dei dati (articolo 20): il diritto di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e di trasmetterli a un altro titolare del trattamento.
- Il diritto di opposizione (articolo 21): il diritto di opporsi al trattamento dei propri dati personali per determinate finalità, inclusi i fini di marketing diretto.
- Il diritto a non essere soggetto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione (articolo 22): il di-

[14] Articolo 12 del Regolamento.

ritto a non essere soggetto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici o incida significativamente sulla persona.

6.1. Il diritto alla cancellazione (diritto all'oblio)

Il diritto all'oblio, disciplinato dall'articolo 17 del GDPR, rappresenta una delle innovazioni più rilevanti introdotte dal Regolamento. Esso riconosce all'interessato la possibilità di ottenere la cancellazione dei propri dati personali quando ricorrono determinate condizioni, riflettendo l'idea che i dati non debbano essere conservati o resi disponibili oltre il tempo necessario rispetto alle finalità per le quali sono stati raccolti.

Le principali situazioni in cui l'interessato può chiedere la cancellazione sono:

- i dati non sono più necessari rispetto alle finalità originarie del trattamento;
- l'interessato revoca il consenso e non sussiste altra base giuridica per il trattamento;
- l'interessato si oppone al trattamento basato sul legittimo interesse del titolare e non prevalgono motivi legittimi per proseguire;
- i dati sono stati trattati illecitamente;
- i dati devono essere cancellati per adempiere a un obbligo legale;
- i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Il diritto all'oblio non è tuttavia assoluto. L'art. 17, par. 3, individua una serie di eccezioni, tra cui l'esercizio del diritto alla libertà di espressione e di informazione; l'adempimento di obblighi legali o l'esecuzione di compiti di interesse pubblico; motivi di interesse pubblico nel settore della sanità pubblica; finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica, o a fini statistici; l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto all'oblio è divenuto particolarmente rilevante nel contesto online, dove la persistenza delle informazioni può avere effetti duraturi sulla reputazione personale. La giurisprudenza della Corte di giustizia, a partire dalla sentenza *Google Spain* del 2014[15], ha riconosciuto che gli interessati possono richiedere ai motori di ricerca la deindicizzazione dei risultati che li riguardano, quando le informazioni siano inadeguate, non pertinenti, non più pertinenti o eccessive rispetto alle finalità della pubblicazione.

[15] CGUE, C-131/12, *Google Spain v AEPD and Mario Costeja González*.

È importante distinguere tra cancellazione dei dati alla fonte e deindicizzazione: nel primo caso si tratta dell'eliminazione dei dati presso il titolare del trattamento; nel secondo, invece, i dati rimangono disponibili sul sito originario, ma non sono più facilmente reperibili tramite ricerche nominative.

Il diritto all'oblio, pur essendo uno strumento potente di tutela, richiede un equilibrio con altri diritti fondamentali, primo tra tutti la libertà di informazione. Per questo motivo, la valutazione delle richieste di cancellazione o deindicizzazione deve essere svolta caso per caso, alla luce del contesto, del ruolo pubblico dell'interessato e della rilevanza sociale dell'informazione.

7. Gli obblighi del titolare del trattamento

7.1. Il titolare e il responsabile del trattamento

Il titolare del trattamento è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali (articolo 4, par. 7). In quanto tale, il titolare ha la responsabilità primaria di garantire che le attività di trattamento dei dati siano conformi ai principi del GDPR. Ciò include la definizione dei motivi per cui i dati personali vengono raccolti, le modalità di utilizzo e la garanzia che vengano adottate misure adeguate per la protezione dei dati.

Per contro, un responsabile del trattamento, ai sensi dell'articolo 4, paragrafo 8, è la persona fisica o giuridica che tratta i dati per conto del titolare del trattamento. Il ruolo del responsabile dunque è più operativo, in quanto gestisce le attività di trattamento dei dati sulla base delle istruzioni fornite dal titolare del trattamento.

L'articolo 28 del GDPR prevede che il titolare e il responsabile del trattamento formalizzino il loro rapporto attraverso un contratto. Questo contratto deve stabilire le istruzioni specifiche per il trattamento dei dati, la natura e lo scopo del trattamento, il tipo di dati personali coinvolti e gli obblighi di entrambe le parti.

Una sfida significativa si presenta quando i titolari del trattamento hanno più potere contrattuale e influenza dei titolari del trattamento. In tali scenari, i responsabili potrebbero dettare condizioni che limitano la capacità del titolare del trattamento di applicare pienamente la conformità al GDPR, creando uno squilibrio di potere che potrebbe compromettere gli sforzi di protezione dei dati.

L'articolo 26 affronta anche il caso di contitolarità, cioè quando due o più entità determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali. In tal caso entrambe tali entità sono titolari del trattamento e dovranno, attraverso l'accordo di contitolarità, definire chiaramente le rispettive responsabilità in relazione al trattamento.

L'attuazione pratica del controllo congiunto può essere complessa[16]. Determinare l'esatta natura del controllo e della responsabilità può essere impegnativo, con conseguenti difficoltà nel classificare se un'entità è un contitolare del trattamento o un semplice responsabile del trattamento. Questa ambiguità può complicare la responsabilità e la conformità, rendendo essenziale per le entità coinvolte in attività di trattamento congiunto documentare accuratamente i propri ruoli e responsabilità.

7.2. Gli obblighi del titolare del trattamento

Il GDPR enfatizza la responsabilità del titolare del trattamento richiedendo implementare misure tecniche e organizzative adeguate a garantire e dimostrare la conformità in base al rischio del trattamento per i diritti e le libertà dei soggetti interessati.

Questo è il nucleo del "principio di responsabilizzazione" alla base della filosofia del GDPR[17]. Il Regolamento riconosce la complessità e la varietà delle attività di trattamento dei dati e la difficoltà di definire misure universali applicabili a tutte le situazioni. Inoltre, il titolare del trattamento è considerato la persona più competente per valutare i rischi e implementare misure preventive. Questo cambiamento sottolinea il ruolo dei titolari del trattamento e la responsabilità proattiva, spostandosi da prescrizioni dettagliate a un "impegno per la conformità".

La misura chiave di responsabilità è il rischio delle operazioni di trattamento dei dati rispetto al diritto alla protezione dei dati[18]. Ciò significa che i titolari del trattamento devono valutare i rischi specifici posti dalle loro attività di trattamento, considerando sia la probabilità di occorrenza sia l'impatto potenziale sugli interessati. Devono quindi implementare misure tecniche e organizzative proporzionate a questi rischi, garantendo che il trattamento dei dati sia effettuato in conformità ai principi del GDPR.

7.3. Data protection by design e *by default*

Il principio di responsabilizzazione è accompagnato dall'idea di favorire una "privacy by design".

---

[16] C. MILLARD, *At This Rate, Everyone Will Be a [Joint] Controller of Personal Data*!, in *International Data Privacy Law*, 2019 (4), pp. 217-219.

[17] T. KARJALAINEN, *All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm*, in *Eur. Data Prot. L. Rev.*, 2022 (1).

[18] In questo senso, si può dire che il GDPR adotti un "approccio basato sul rischio" alla protezione dei dati.

Il concetto di protezione dei dati *by design* e *by default* può essere fatto risalire all'idea di "*privacy by design*", introdotta negli anni '90 da Ann Cavoukian, allora Commissario per l'informazione e la privacy dell'Ontario, Canada.

I principi alla base di questo concetto includono la prevenzione dei problemi piuttosto che la loro correzione, il che significa che i problemi dovrebbero essere valutati durante la fase di progettazione e l'applicazione dovrebbe prevenire il verificarsi dei rischi. La privacy dovrebbe essere l'impostazione predefinita, quindi non dovrebbe essere obbligatorio compilare un campo del modulo quando la fornitura dei dati è facoltativa. La privacy dovrebbe anche essere incorporata nel design, ad esempio utilizzando tecniche come la pseudonimizzazione o la minimizzazione dei dati. È essenziale mantenere la piena funzionalità, rispettando tutte le esigenze e respingendo false dicotomie come più privacy equivale a meno sicurezza. La sicurezza deve essere garantita per tutto il ciclo di vita del prodotto o servizio. La visibilità e la trasparenza del trattamento sono cruciali; tutte le fasi operative dovrebbero essere trasparenti per verificare la protezione dei dati. Infine, l'utente deve essere al centro, con i suoi diritti rispettati e risposte tempestive e chiare fornite alle sue richieste di controllo sui dati personali.

Ispirandosi a questi criteri, il principio della data protection by design e by default previsto all'art. 25 del GDPR richiede ai titoli del trattamento di implementare misure tecniche e organizzative adeguate sia al momento di determinare i mezzi per il trattamento (letteralmente "*by design*") sia durante il trattamento stesso. Queste misure, come la pseudonimizzazione, dovrebbero integrare efficacemente i principi di protezione dei dati come la minimizzazione dei dati e garantire le necessarie salvaguardie per soddisfare i requisiti del GDPR e proteggere i diritti degli interessati.

7.4. Valutazione di impatto sulla protezione dei dati e il Data Protection Officer

L'articolo 35 richiede ai titolari del trattamento di condurre una Valutazione di Impatto sulla Protezione dei Dati (*Data Protection Impact Assessment* o DPIA) quando il trattamento è probabilmente destinato a comportare un rischio elevato per i diritti e le libertà degli individui[19].

[19] Secondo il Gruppo di lavoro Articolo 29 (ovvero l'odierno Comitato europeo per la protezione dei dati), il rischio elevato può essere indicato, tra l'altro, da uno o più di questi fattori: trattamento valutativo o di scoring, compresa la profilazione per valutare aspetti come la performance professionale e la situazione economica, come un'azienda biotecnologica che offre test genetici direttamente ai consumatori; decisioni automatizzate che producono effetti giuridici significativi, come assunzioni, concessione di prestiti o sottoscrizione di polizze assicurative; monitoraggio si-

Una DPIA è una procedura strutturata per valutare i rischi connessi al trattamento dei dati. Deve includere: a) una descrizione sistematica delle operazioni di trattamento previste e delle finalità del trattamento; b) una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati; e d) le misure previste per affrontare i rischi.

Gli articoli 37-39 richiedono la designazione di un Responsabile della Protezione dei Dati (*Data Protection Officer,* abbreviato DPO) in condizioni specifiche. Il DPO ha il compito di supervisionare la strategia di protezione dei dati e garantire la conformità ai requisiti del GDPR. Il ruolo del DPO include informare e consigliare il titolare o il responsabile del trattamento e i loro dipendenti sui loro obblighi in materia di protezione dei dati, monitorare la conformità al GDPR e cooperare con l'autorità di controllo.

8. Il Garante per la protezione dei dati personali

Il GDPR stabilisce un sistema di controllo incentrato sul ruolo delle autorità di controllo nazionali. Queste sono incaricate di monitorare i titolari e i responsabili del trattamento e di far rispettare la conformità al Regolamento.

Come noto, nel nostro ordinamento tale ruolo è esercitato dall'Autorità Garante per la protezione dei dati personali, istituita con la legge n. 675/1996 e oggi disciplinata dal Codice della privacy come modificato dal d.lgs. 101/2018.

L'Autorità, con sede a Roma, è composta da quattro membri, nominati per sette anni non rinnovabili: due eletti dalla Camera dei deputati e due dal Senato della Repubblica, con maggioranze qualificate. Il Collegio elegge al proprio interno il Presidente, che ha la rappresentanza dell'Autorità e ne coordina l'attività. La struttura operativa è supportata da un Ufficio composto da dirigenti, funzionari e personale tecnico-amministrativo.

Al fine di monitorare l'applicazione del Regolamento il Garante dispone di ampi poteri investigativi, correttivi, autorizzativi e consultivi, come previsto dagli articoli 57 e 58 del GDPR. In particolare, l'Autorità può condurre indagini e ispezioni, anche avvalendosi della Guardia di Finanza; effettuare audit e richiedere informazioni e documenti a titolari e responsabili; ottenere accesso a qualsiasi sede in cui avvenga il trattamento dei dati; adottare avvertimenti, ammonimenti e reprimende; ingiungere al titolare di conformarsi al GDPR, compresa

---

stematico, come la videosorveglianza in luoghi pubblici; trattamento di dati sensibili, giudiziari o altamente personali, come opinioni politiche, dati di geolocalizzazione o dati finanziari, ecc. Vedi Art. 29 WP, Linee guida sulla Valutazione di Impatto sulla Protezione dei Dati (DPIA) e Determinazione di quando il trattamento è «probabilmente destinato a comportare un rischio elevato» ai sensi del Regolamento 2016/679, 9-11.

la limitazione o il divieto del trattamento; autorizzare determinati trattamenti quando previsto dalla legge; emettere pareri su atti normativi e schemi di regolamento che incidono sulla protezione dei dati personali.

In caso di non conformità, il Garante può imporre sanzioni amministrative pecuniarie, che possono essere particolarmente rilevanti. Il GDPR prevede un sistema sanzionatorio graduato, con importi che possono raggiungere fino a 20 milioni di euro o il 4% del fatturato annuo mondiale del gruppo nel precedente esercizio, scegliendo il valore più elevato. La determinazione dell'importo dipende da una serie di fattori, tra cui natura, gravità e durata della violazione; grado di responsabilità del titolare o del responsabile; eventuali precedenti violazioni; modalità con cui l'Autorità è venuta a conoscenza dell'illecito; misure correttive adottate dal titolare; qualunque fattore aggravante o attenuante pertinente.

9. La tutela giurisdizionale

Il GDPR prevede un sistema di tutela giurisdizionale articolato e coerente con i principi di effettività e accessibilità della protezione. L'interessato può attivare diversi rimedi quando ritenga che il trattamento dei suoi dati personali violi il Regolamento, sia nei confronti dei titolari o responsabili del trattamento, sia nei confronti dell'autorità di controllo.

In primo luogo, il soggetto interessato può presentare un reclamo al Garante in funzione dell'articolo 77, che riconosce il diritto di presentare un reclamo all'Autorità di controllo competente. Il reclamo rappresenta un rimedio amministrativo attraverso il quale l'interessato può denunciare eventuali violazioni e sollecitare l'intervento correttivo o sanzionatorio dell'Autorità.

L'articolo 78 del GDPR prevede inoltre la possibilità di proporre ricorso contro le decisioni dell'autorità di controllo o contro la sua inerzia, nel caso in cui non si sia pronunciata sul reclamo entro i termini dovuti. In Italia, la competenza a conoscere tali ricorsi è attribuita al tribunale ordinario del luogo in cui risiede l'interessato, secondo quanto stabilito dagli articoli 152 e seguenti del Codice della privacy. Le pronunce del tribunale sono impugnabili dinanzi alla Corte d'Appello e, in ultima istanza, alla Corte di Cassazione.

Accanto alla tutela di fronte al Garante, l'articolo 79 GDPR attribuisce all'interessato la possibilità di proporre un ricorso giurisdizionale nei confronti del titolare o del responsabile del trattamento dinanzi al giudice competente, qualora ritenga che il trattamento violi le disposizioni del Regolamento. Nel nostro ordinamento, tale ricorso va effettuato dinnanzi al giudice civile ed è finalizzato sia ad accertare l'illiceità del trattamento sia, eventualmente, ad adottare misure

idonee a rimuovere la violazione, incluse, ad esempio, l'interruzione del trattamento o la cancellazione dei dati.

In questo caso è sempre ammessa la possibilità di richiedere il risarcimento del danno patito dal soggetto interessato.

Tale ipotesi è confermata dall'articolo 82 del GDPR che introduce un regime particolarmente ampio, volto a garantire un risarcimento effettivo a chiunque abbia subito un danno – materiale o immateriale – causato da una violazione del Regolamento. Il titolare o il responsabile del trattamento rispondono del danno, salvo che riescano a dimostrare che l'evento non è loro imputabile. Il danno risarcibile può consistere non solo in una perdita economica, ma anche in un pregiudizio morale, come la lesione della reputazione, lo stress, l'ansia o altre forme di sofferenza derivanti dall'illecito trattamento.

Ove più titolari o responsabili siano coinvolti nel medesimo trattamento, il GDPR prevede un regime di responsabilità solidale, che assicura all'interessato la possibilità di ottenere l'integrale ristoro del danno da uno qualsiasi dei soggetti coinvolti, lasciando poi a questi ultimi l'onere di rivalersi tra loro in funzione del grado di responsabilità.

Il rapporto tra i rimedi giurisdizionali e quelli amministrativi è caratterizzato da complementarità: il reclamo al Garante consente un intervento rapido e specializzato sul piano amministrativo, mentre il ricorso al giudice permette di ottenere una valutazione piena della responsabilità e un eventuale risarcimento del danno. L'interessato, pertanto, dispone di un ventaglio di strumenti che possono essere attivati parallelamente o in alternativa, in funzione della natura della violazione e del tipo di tutela ricercata.

10. L'applicazione del GDPR nel contesto europeo (cenni)

L'applicazione del GDPR avviene in un quadro europeo complesso caratterizzato da una combinazione di norme direttamente applicabili, competenze condivise tra Stati membri e meccanismi di cooperazione istituzionale. Sebbene il Regolamento abbia l'obiettivo di garantire un livello uniforme di protezione dei dati personali in tutta l'Unione, la sua attuazione pratica mostra significative differenze tra i vari ordinamenti, dovute sia alle norme nazionali di integrazione sia alle prassi delle singole autorità di controllo.

Un ruolo centrale è svolto dal Comitato europeo per la protezione dei dati (*European Data Protection Board*), l'organismo che riunisce le autorità di controllo degli Stati membri e il Garante europeo della protezione dei dati. Il Comitato adotta linee guida, raccomandazioni e pareri che contribuiscono all'interpretazione uniforme del Regolamento e assicura il funzionamento del meccanismo di coerenza previsto dal Capo VII del GDPR. Attraverso questo meccanismo,

l'EDPB interviene per garantire che le autorità nazionali applichino il Regolamento in modo convergente, in particolare nei casi transfrontalieri.

Nei trattamenti che coinvolgono più Stati membri, trova applicazione il principio del *one-stop-shop*, che individua un'unica autorità capofila (*lead supervisory authority*) competente a coordinare il procedimento, riducendo la frammentazione e assicurando una risposta più efficiente nei confronti delle grandi piattaforme digitali e dei soggetti che operano su scala europea.

Nonostante questi strumenti di armonizzazione, persistono differenze rilevanti nelle modalità con cui gli Stati membri applicano il GDPR. Ciò riguarda tanto la struttura e le risorse delle singole autorità di controllo, quanto la disciplina nazionale relativa alle materie rimesse alla competenza statale, come il trattamento dei dati in ambito lavorativo, la sanità, la ricerca scientifica o i trattamenti effettuati per finalità di sicurezza pubblica. Queste differenze possono incidere sull'effettiva uniformità della protezione offerta dal Regolamento.

Un tentativo di ridurre le divergenze nelle modalità applicative, almeno nei procedimenti transfrontalieri, è stato fatto con il Regolamento (EU) 2025/2518 del 26 novembre 2025 che stabilisce norme procedurali supplementari relative all'applicazione del GDPR. Questo nuovo strumento mira a rafforzare il funzionamento del meccanismo dello *one-stop-shop*, a migliorare la cooperazione tra autorità di controllo e a rendere più prevedibili e tempestivi i procedimenti, contribuendo così a una più omogenea e coerente applicazione del Regolamento all'interno dell'Unione.