Parere 28/2024 su taluni aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di IA

Adottato il 17 dicembre 2024

Sintesi

Le tecnologie dell'intelligenza artificiale offrono numerose opportunità e vantaggi in un'ampia gamma di settori e attività sociali.

Tutelando il diritto fondamentale alla protezione dei dati, il RGPD sostiene tali opportunità e promuove altri diritti fondamentali dell'UE, tra cui il diritto alla libertà di pensiero, di espressione e di informazione, il diritto all'istruzione e alla libertà d'impresa. In tal modo, il RGPD rappresenta un quadro giuridico che incoraggia l'innovazione responsabile.

In tale contesto, tenendo conto delle questioni di protezione dei dati sollevate da queste tecnologie, l'Autorità di controllo irlandese ha chiesto all'EDPB un parere su aspetti di applicazione generale ai sensi dell'articolo 64, paragrafo 2 del RGPD. La richiesta riguarda il trattamento dei dati personali nelle fasi di sviluppo e diffusione dei modelli di intelligenza artificiale («**IA**»). Nello specifico, la richiesta poneva i seguenti quesiti: 1) quando e in che modo un modello di IA può essere considerato «anonimo»; 2) in che modo i titolari del trattamento possono dimostrare l'adeguatezza dell'interesse legittimo come base giuridica nelle fasi di sviluppo e 3) diffusione; e 4) quali sono le conseguenze del trattamento illecito di dati personali nella fase di sviluppo di un modello di IA sul successivo trattamento o funzionamento del modello stesso.

Relativamente al primo quesito, il Parere ravvisa che dichiarazioni di anonimità di un modello di IA dovrebbero essere valutate caso per caso dalle AC competenti, in quanto l'EDPB ritiene che i modelli di IA addestrati con i dati personali non possano, in ogni caso, essere considerati anonimi. Affinché un modello di IA sia considerato anonimo, sia (1) la probabilità di estrazione diretta (anche probabilistica) di dati personali relativi a persone i cui dati personali sono stati utilizzati per sviluppare il modello, che (2) la probabilità di ottenere, intenzionalmente o meno, tali dati personali dalle interrogazioni, dovrebbero essere insignificanti, considerando «*tutti i mezzi di cui può ragionevolmente avvalersi*» il titolare del trattamento o altra persona.

Per effettuare la loro valutazione, le AC dovrebbero esaminare la documentazione prodotta dal titolare del trattamento per dimostrare l'anonimità del modello. A tale riguardo, il Parere fornisce un elenco non prescrittivo e non esaustivo di metodi di cui i titolari del trattamento possono avvalersi per dimostrare l'anonimità e possono essere presi in considerazione dalle AC per valutare la dichiarazione di anonimità da parte di un titolare del trattamento. Ciò riguarda, ad esempio, gli approcci che i titolari del trattamento adottano durante la fase di sviluppo per prevenire o limitare la raccolta di dati personali utilizzati per l'addestramento, ridurne l'identificabilità, impedirne l'estrazione o fornire garanzie in merito alla resistenza agli attacchi di stato dell'arte.

Per quanto riguarda il secondo e il terzo quesito, il Parere fornisce considerazioni generali di cui le AC devono tenere conto nel valutare se i titolari del trattamento possano invocare il legittimo interesse come base giuridica adeguata per il trattamento effettuato nelle fasi di sviluppo e diffusione dei modelli di IA.

Il Parere rammenta che non esiste una gerarchia tra le basi giuridiche previste dal RGPD e che spetta ai titolari del trattamento individuare la base giuridica adeguata per le loro attività di trattamento. Il Parere richiama, quindi, il test in tre fasi che dovrebbe essere condotto quando si valuta il ricorso all'interesse legittimo come base giuridica, vale a dire (1) identificazione dell'interesse legittimo perseguito dal titolare del trattamento o da terzi; (2) analisi della necessità del trattamento ai fini dell'interesse legittimo (o degli interessi legittimi) perseguito/i (detto anche «test di necessità»); e (3)

verifica che sull'interesse legittimo (o interessi legittimi) non prevalgano gli interessi o i diritti e le libertà fondamentali degli interessati (detto anche «test di bilanciamento»).

Per quanto riguarda la prima fase, il Parere ricorda che un interesse può essere considerato legittimo qualora siano soddisfatti i seguenti tre criteri cumulativi: l'interesse (1) è lecito; (2) è articolato in modo chiaro e preciso; e (3) è reale e presente (ossia non speculativo). Tale interesse può riguardare, ad esempio, nell'ambito dello sviluppo di un modello di IA – la realizzazione di un servizio di agente conversazionale per l'assistenza agli utenti o, in fase di diffusione – il miglioramento del rilevamento delle minacce in un sistema informatico.

Per quanto riguarda la seconda fase, il Parere ricorda che quando si valuta la necessità occorre considerare i seguenti aspetti: 1) se l'attività di trattamento consente il perseguimento dell'interesse legittimo e 2) se non esiste un modo meno invasivo per perseguire tale interesse. Nel valutare se la condizione di necessità sia soddisfatta, le AC dovrebbero prestare particolare attenzione alla quantità di dati personali trattati e se questi siano proporzionati al perseguimento dell'interesse legittimo in questione, anche alla luce del principio di minimizzazione dei dati.

Per quanto riguarda la terza fase, il Parere ricorda che la verifica del bilanciamento deve essere effettuata tenendo conto delle circostanze specifiche di ciascun caso. Fornisce poi una panoramica degli elementi di cui le AC possono tenere conto nel valutare se sull'interesse di un titolare del trattamento o di terzi prevalgano gli interessi, i diritti fondamentali e le libertà degli interessati.

Nell'ambito della terza fase, il Parere evidenzia i rischi specifici per i diritti fondamentali che possono emergere nella fase di sviluppo e di diffusione dei modelli di IA. Chiarisce inoltre che il trattamento dei dati personali che avviene durante le fasi di sviluppo e diffusione dei modelli di IA può avere un impatto positivo o negativo sugli interessati. Per valutare tale impatto, le AC possono prendere in considerazione la natura dei dati trattati dai modelli, il contesto del trattamento e le possibili ulteriori conseguenze del trattamento.

Il Parere sottolinea, inoltre, il ruolo delle ragionevoli aspettative degli interessati nel test di bilanciamento. Ciò è importante per via della complessità delle tecnologie utilizzate nei modelli di IA e perché può essere difficile per gli interessati comprendere la varietà dei loro potenziali utilizzi e delle diverse attività di trattamento coinvolte. A questo proposito, tra gli elementi da considerare per valutare se gli interessati possono ragionevolmente aspettarsi che i loro dati personali vengano trattati, possono rientrare sia le informazioni fornite agli interessati che il contesto del trattamento. Per quanto riguarda il contesto, questo può includere: il fatto che i dati personali siano pubblicamente disponibili, la natura del rapporto tra l'interessato e il titolare del trattamento (e se esista un collegamento tra i due), la natura del servizio, il contesto in cui i dati personali sono stati raccolti, la fonte da cui i dati sono stati raccolti (ossia il sito web o il servizio in cui i dati personali sono stati raccolti e le impostazioni di *privacy* previste), i potenziali ulteriori utilizzi del modello e se gli interessati siano effettivamente consapevoli del fatto che i loro dati personali sono disponibili *online*.

Il Parere ricorda inoltre che, quando gli interessi, i diritti e le libertà degli interessati sembrano prevalere sul legittimo interesse o sui legittimi interessi perseguiti dal titolare del trattamento o da terzi, il titolare del trattamento può prendere in considerazione l'introduzione di misure di attenuazione per limitare l'impatto del trattamento su tali interessati. Le misure di attenuazione non dovrebbero essere confuse con le misure che il titolare del trattamento è tenuto per legge ad adottare, in ogni caso, per garantire il rispetto del RGPD. Inoltre, le misure dovrebbero essere adattate alle circostanze del caso e alle caratteristiche del modello di IA, compreso l'utilizzo che se ne intende fare. Al riguardo, il Parere fornisce un elenco non esaustivo di esempi di misure di attenuazione per la fase di sviluppo (anche in relazione al *web scraping*) e la fase di diffusione. Le misure di attenuazione

possono essere soggette a una rapida evoluzione e dovrebbero essere adattate alle circostanze del caso. Spetta pertanto alle AC valutare l'adeguatezza delle misure di attenuazione adottate caso per caso.

Relativamente al quarto quesito, il Parere, in generale, rammenta che le AC dispongono di poteri discrezionali per valutare le possibili violazioni e scegliere misure appropriate, necessarie e proporzionate, tenendo conto delle circostanze di ogni singolo caso. Il Parere prende quindi in considerazione tre scenari.

Nello scenario 1, i dati personali sono conservati nel modello di IA (il che significa che il modello non può essere considerato anonimo, come specificato nel primo quesito) e sono successivamente trattati dallo stesso titolare del trattamento (ad esempio nel contesto della diffusione del modello). Il Parere ribadisce che occorre valutare caso per caso, a seconda del contesto di riferimento, se le fasi di sviluppo e diffusione comportino finalità distinte (costituendo, così, attività di trattamento separate) e la misura in cui l'assenza di una base giuridica per l'attività di trattamento iniziale incida sulla liceità del trattamento successivo.

Nello scenario 2 i dati personali sono conservati nel modello e sono trattati da un altro titolare del trattamento nella fase di diffusione del modello. A tale riguardo, il Parere afferma che le AC dovrebbero valutare se il titolare del trattamento che utilizza il modello abbia condotto un'adeguata valutazione, nell'ambito dei suoi obblighi di responsabilità, per dimostrare la conformità all'articolo 5, paragrafo 1, lettera a), e all'articolo 6 del RGPD, al fine di accertare che il modello di IA non sia stato sviluppato mediante il trattamento illecito di dati personali. Questa valutazione dovrebbe tenere conto, ad esempio, della fonte dei dati personali e del fatto che il trattamento nella fase di sviluppo sia stato oggetto di una constatazione di violazione, soprattutto se sia stata accertata da un'autorità di controllo o giurisdizionale, e dovrebbe essere più o meno dettagliata a seconda dei rischi derivanti dal trattamento nella fase di diffusione.

Nello scenario 3, un titolare del trattamento tratta illecitamente i dati personali per sviluppare il modello di IA, quindi si assicura che sia anonimizzato, prima che lo stesso, o un altro titolare del trattamento, avvii un altro trattamento di dati personali in fase di diffusione. A questo proposito, il Parere chiarisce che, qualora possa essere dimostrato che il successivo funzionamento del modello di IA non comporta il trattamento di dati personali, l'EDPB ritiene che il RGPD non troverebbe applicazione. Pertanto, l'illiceità del trattamento iniziale non dovrebbe incidere sul successivo funzionamento del modello. Inoltre, l'EDPB ritiene che, successivamente, quando i titolari del trattamento effettuano il trattamento dei dati personali raccolti durante la fase di diffusione, dopo l'anonimizzazione del modello, il RGPD si applicherebbe in relazione a tali trattamenti. In questi casi, il Parere ritiene che, per quanto riguarda il RGPD, sulla liceità del trattamento effettuato nella fase di diffusione non dovrebbe incidere l'illiceità del trattamento iniziale.

Indice

Il Comitato europeo per la protezione dei dati

Visti gli articoli 63 e 64, paragrafo 2, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito denominato «RGPD»),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018, del 6 luglio 2018[1],

Visti gli articoli 10 e 22 del proprio Regolamento interno,

considerando quanto segue:

(1) Il ruolo principale del Comitato europeo per la protezione dei dati (di seguito denominato **«Comitato»** o **«EDPB»**) è assicurare l'applicazione coerente del RGPD in tutto lo Spazio economico europeo (**«SEE»**). L'articolo 64, paragrafo 2 del RGPD stabilisce che qualsiasi Autorità di controllo (**«AC»**), il Presidente del Comitato o la Commissione possono richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro del SEE siano esaminate dal Comitato al fine di ottenere un parere. Il presente parere ha lo scopo di esaminare una questione di applicazione generale o che produce effetti in più di uno Stato membro del SEE.

(2) Il parere del Comitato è adottato ai sensi dell'articolo 64, paragrafo 3 del RGPD in combinato disposto con l'articolo 10, paragrafo 2, del Regolamento interno dell'EDPB entro otto settimane dalla data in cui il Presidente e l'AC competente avranno ritenuto completo il fascicolo. Su decisione del Presidente, tale termine può essere prorogato di ulteriori sei settimane, a seconda della complessità della questione.

HA ADOTTATO IL SEGUENTE PARERE:

1 Introduzione

1.1 Sintesi dei fatti

1. Il 4 settembre 2024, l'AC irlandese (l'«**AC IE**» o «**AC richiedente**») ha chiesto all'EDPB di emettere un parere ai sensi dell'articolo 64, paragrafo 2 del RGPD in relazione ai modelli di IA e al trattamento dei dati personali («**la Richiesta**»).

2. La Presidente del Comitato e l'AC IE hanno ritenuto il fascicolo completo il 13 settembre 2024. Il giorno lavorativo seguente, ossia il 16 settembre 2024, il fascicolo è stato trasmesso dal Segretariato dell'EDPB. La Presidente, considerata la complessità della questione, ha deciso di prorogare il termine legale ai sensi dell'articolo 64, paragrafo 3 de RGPD e dell'articolo 10, paragrafo 4, del Regolamento interno.

3. La Richiesta riguarda alcuni aspetti relativi all'addestramento, aggiornamento, sviluppo e funzionamento dei modelli di IA in cui i dati personali fanno parte del relativo insieme di dati. L'AC IE

[1] Nel presente Parere, con il termine «Stati membri» si intendono gli «Stati membri del SEE». I riferimenti all'«Unione» in tutto il Parere sono da intendersi come riferimenti al «SEE».

sottolinea che la Richiesta riguarda questioni fondamentali che producono un forte impatto sugli interessati e sui titolari del trattamento nel SEE e che, in questo momento, non esiste una posizione armonizzata tra le AC nazionali[2]. La terminologia utilizzata ai fini del presente parere è riportata nelle sezioni 2.2 e 2.3 di seguito.

4. L'AC IE ha posto i seguenti quesiti.

Quesito n. 1: si ritiene che il modello finale di IA, addestrato utilizzando dati personali non rientri, in ogni caso, nella definizione di dati personali (di cui all'4, paragrafo 1 del RGPD)?

In caso di risposta affermativa al primo quesito:

i. In quale fase delle operazioni di trattamento finalizzate alla creazione di un modello di IA, i dati personali non vengono più trattati?
   a) Come è possibile dimostrare che il modello di IA non tratta dati personali?

ii. Vi sono fattori che potrebbero far sì che il funzionamento del modello di IA finale non sia più considerato anonimo?
   a) In caso affermativo, come si possono dimostrare le misure adottate per attenuare, prevenire o tutelarsi da tali fattori (in modo da garantire che il modello di IA non tratti dati personali)?

In caso di risposta negativa al primo quesito:

i. Quali sono le circostanze in cui ciò potrebbe verificarsi?
   a) In tal caso, come si possono dimostrare le misure adottate per garantire che il modello di IA non tratti dati personali?

Quesito n. 2: qualora un titolare del trattamento invochi gli interessi legittimi come base giuridica per il trattamento dei dati personali al fine di creare, aggiornare e/o sviluppare un modello di IA, in che modo detto titolare dovrebbe dimostrare l'adeguatezza degli interessi legittimi come base giuridica, sia in relazione al trattamento dei dati di terza parte che di quelli di prima parte?

i. Di quali considerazioni dovrebbe tener conto tale titolare per garantire che gli interessi degli interessati, i cui dati personali costituiscono oggetto di trattamento, siano adeguatamente bilanciati rispetto agli interessi del titolare del trattamento nel contesto di:
   a) Dati di terza parte

   b) Dati di prima parte

Quesito n. 3: successivamente alla fase di addestramento, qualora un titolare del trattamento utilizzi gli interessi legittimi come base giuridica per il trattamento dei dati personali nell'ambito di un modello di IA o di un sistema di IA di cui fa parte un modello di IA, in che modo dovrebbe dimostrare l'adeguatezza degli interessi legittimi come base giuridica?

Quesito n. 4: se si accerta che un modello di IA è stato creato, aggiornato o sviluppato utilizzando dati personali trattati illecitamente, quali sono le eventuali conseguenze di ciò sulla liceità del trattamento continuato o successivo e sul funzionamento del modello di IA, sia come modello autonomo che integrato in un sistema di IA, nei casi in cui:

[2] Richiesta, pag. 1.

i. Il modello di IA, autonomo o integrato in un sistema di IA, tratta dati personali?
ii. Né il modello di IA, né il modello di IA integrato in un sistema di IA, trattano dati personali?

1.2 Ammissibilità della richiesta di parere ai sensi dell'articolo 64, paragrafo 2 del RGPD

5. L'articolo 64, paragrafo 2 del RGPD stabilisce, in particolare, che qualsiasi AC può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal Comitato al fine di ottenere un parere.

6. L'AC richiedente ha posto all'EDPB quesiti sugli aspetti relativi alla protezione dei dati nel contesto dei modelli di IA. Nella Richiesta ha specificato che, sebbene molte organizzazioni utilizzino attualmente modelli di IA, tra cui i *Large Language Models* («**LLM**»), il loro funzionamento, addestramento e utilizzo sollevano «*numerose e estese preoccupazioni in materia di protezione dei dati*»[3] che «*hanno un impatto sugli interessati in tutta l'UE/il SEE*»[4].

7. La Richiesta solleva, in sostanza, questioni relative (i) all'applicazione del concetto di dati personali; (ii) al principio di liceità, con specifico riguardo alla base giuridica del legittimo interesse nel contesto dei modelli di IA; nonché, (iii) alle conseguenze del trattamento illecito dei dati personali nella fase di sviluppo dei modelli di IA, sul successivo trattamento e sul funzionamento del modello.

8. Il Comitato ritiene che la Richiesta riguardi «*questioni di applicazione generale*» ai sensi dell'articolo 64, paragrafo 2 del RGPD. In particolare, la questione riguarda l'interpretazione e l'applicazione dell'articolo 4, paragrafo 1, dell'articolo 5, paragrafo 1, lettera a), e dell'articolo 6 del RGPD in relazione al trattamento dei dati personali nello sviluppo e nella diffusione dei modelli di IA. Come sottolineato dall'AC richiedente, l'applicazione di tali disposizioni ai modelli di IA solleva questioni nuove, astratte e sistemiche[5]. Il rapido sviluppo e la diffusione dei modelli di IA da parte di un numero crescente di organizzazioni sollevano questioni specifiche e, come sottolineato nella Richiesta, «*il Comitato potrà beneficiare del raggiungimento di una posizione comune sulle questioni sollevate dalla presente Richiesta, che sono al centro del lavoro che l'EDPB ha in programma di realizzare nel breve e medio termine*»[6]. Inoltre, le tecnologie di IA offrono numerose opportunità e vantaggi in un'ampia gamma di settori e attività sociali e il RGPD rappresenta un quadro giuridico che incoraggia l'innovazione responsabile. Ne consegue che esiste un interesse generale a effettuare questa valutazione attraverso un parere dell'EDPB, al fine di garantire l'applicazione coerente di alcune disposizioni del RGPD nel contesto dei modelli di IA.

9. La condizione alternativa di cui all'articolo 64, paragrafo 2 del RGPD si riferisce a questioni che «*producono effetti in più di uno Stato membro*». L'EDPB rammenta che il termine «effetti» deve essere interpretato *lato sensu* e, pertanto, non si limita semplicemente agli effetti giuridici[7]. Poiché sempre più modelli di IA sono addestrati e utilizzati da un numero crescente di organizzazioni all'interno del SEE essi producono un impatto su un gran numero di interessati in tutto il SEE, alcuni dei quali hanno

[3] Richiesta, pag. 1.
[4] Ibidem.
[5] Richiesta, pag. 2.
[6] Richiesta, pag. 1. Come indicato nel programma di lavoro dell'EDPB per il periodo 2024-2025, adottato l'8 ottobre 2024, disponibile all'indirizzo https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, l'EDPB prevede di emanare, tra l'altro, linee guida in materia di anonimizzazione, pseudonimizzazione e *data scraping* nel contesto dell'IA generativa.
[7] EDPB, Documento interno 3/2019 recante indicazioni relative all'articolo 64, paragrafo 2 del RGPD, adottato l'8 ottobre 2019, paragrafo 15, disponibile all'indirizzo https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.

già sollevato perplessità presso le AC competenti[8]. Pertanto, l'EDPB ritiene che la questione sollevata dall'AC richiedente soddisfi anche questa condizione.

10. La Richiesta illustra per iscritto il contesto e le motivazioni alla base dei quesiti sottoposti al Comitato, compreso il quadro giuridico di riferimento. Pertanto, il Comitato ritiene che la Richiesta sia motivata in conformità con l'articolo 10, paragrafo 3 del Regolamento interno dell'EDPB.

11. Ai sensi dell'articolo 64, paragrafo 3 del RGPD[9], l'EDPB non emette un parere qualora ne abbia già reso uno sulla medesima questione. L'EDPB non ha emesso un parere sulla medesima questione e non ha ancora fornito risposte ai quesiti contenuti nella Richiesta.

12. Per tali motivi, il Comitato ritiene che la Richiesta sia ammissibile e che i quesiti in essa formulati debbano essere analizzati nel presente parere (il «**Parere**») adottato ai sensi dell'articolo 64, paragrafo 2 del RGPD.

2 Ambito di applicazione e nozioni fondamentali

2.1 Ambito di applicazione del Parere

13. Il Comitato concorda con l'AC richiedente sul fatto che, dal punto di vista della protezione dei dati, lo sviluppo e la diffusione di modelli di IA pongono questioni fondamentali relative alla protezione dei dati. Le questioni riguardano in particolare: i) quando e come un modello di IA può essere considerato «anonimo» (Quesito n. 1 della Richiesta); ii) in che modo i titolari del trattamento possono dimostrare l'adeguatezza dell'interesse legittimo come base giuridica nelle fasi di sviluppo (Quesito n. 2 della Richiesta) e di diffusione (Quesito n. 3 della Richiesta); e iii) se il trattamento illecito di dati personali nella fase di sviluppo abbia conseguenze sulla liceità del successivo trattamento o funzionamento del modello di IA (Quesito n. 4 della Richiesta).

14. L'EDPB ricorda che le AC sono responsabili del monitoraggio dell'applicazione del RGPD e dovrebbero contribuire alla sua coerente applicazione in tutta l'Unione[10]. Pertanto, spetta alle AC approfondire gli specifici modelli di IA e, in tale contesto, effettuare valutazioni sui singoli casi.

15. Il presente Parere fornisce alle AC competenti un quadro di riferimento per valutare casi specifici in cui potrebbero sorgere (alcune delle) questioni sollevate nella Richiesta. Il presente Parere non ambisce a essere esaustivo, ma intende offrire considerazioni generali sull'interpretazione delle disposizioni vigenti, di cui le AC competenti dovrebbero tenere conto nell'esercizio dei loro poteri di indagine. Sebbene il presente Parere sia rivolto alle AC competenti e riguardi le loro attività e i loro poteri, esso non pregiudica gli obblighi dei titolari e dei responsabili del trattamento ai sensi del RGPD. In particolare, conformemente al principio di responsabilizzazione sancito dall'articolo 5, paragrafo 2 del RGPD, i titolari del trattamento sono competenti per il rispetto di tutti i principi relativi al trattamento dei dati personali e sono in grado di comprovarlo.

16. In alcuni casi, il Parere può fornire degli esempi. Tuttavia, tenuto conto dell'ampia portata dei quesiti presenti nella Richiesta, nonché dei diversi tipi di modelli di IA ivi contemplati, il presente Parere non potrà prendere in considerazione tutti gli scenari possibili. Le tecnologie associate ai modelli di IA sono

[8] Richiesta, pagg. 1-2.
[9] Articolo 64, paragrafo 3 del RGPD e articolo 10, paragrafo 4 del Regolamento interno dell'EDPB.
[10] Articolo 51, paragrafo 1 del RGPD e articolo 51, paragrafo 2 del RGPD.

soggette a una rapida evoluzione; di conseguenza, le considerazioni dell'EDPB nel presente Parere dovrebbero essere interpretate tenendo conto di questo aspetto.

17. **Il presente Parere non analizza le disposizioni seguenti, che possono comunque svolgere un ruolo importante nella valutazione dei requisiti di protezione dei dati applicabili ai modelli di IA.**

- **Trattamenti riguardanti categorie particolari di dati:** l'EDPB rammenta il divieto di cui all'articolo 9, paragrafo 1 del RGPD riguardante il trattamento di categorie particolari di dati e le limitate eccezioni di cui all'articolo 9, paragrafo 2 del RGPD[11]. A questo proposito, la Corte di giustizia dell'Unione europea (**«CGUE»**) ha ulteriormente chiarito che «*nel caso in cui un insieme di dati contenente al contempo dati sensibili e dati non sensibili sia oggetto di siffatte operazioni e segnatamente sia raccolto in blocco senza che i dati possano essere dissociati gli uni dagli altri al momento di tale raccolta, il trattamento di tale insieme di dati deve essere considerato vietato, ai sensi dell'articolo 9, paragrafo 1 del RGPD, nella misura in cui contenga almeno un dato sensibile e non sia applicabile nessuna delle deroghe di cui all'articolo 9, paragrafo 2, del medesimo regolamento.*»[12]. Inoltre, la CGUE ha anche evidenziato che «*ai fini dell'applicazione dell'eccezione prevista all'articolo 9, paragrafo 2, lettera e) del RGPD, si deve verificare se l'interessato abbia inteso, in modo esplicito e con un atto positivo chiaro, rendere accessibili al pubblico i dati personali in questione*»[13]. Occorre tener conto di tali considerazioni quando il trattamento dei dati personali nel contesto dei modelli di IA riguarda particolari categorie di dati.

- **Processo decisionale automatizzato, compresa la profilazione**: le operazioni di trattamento effettuate nel contesto dei modelli di IA possono rientrare nell'ambito di applicazione dell'articolo 22 del RGPD, che impone obblighi aggiuntivi ai titolari del trattamento e fornisce garanzie supplementari agli interessati. L'EDPB richiama, a tale riguardo, le sue Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento (UE) 2016/679[14].

- **Compatibilità delle finalità**: l'articolo 6, paragrafo 4 del RGPD fornisce, per alcune basi giuridiche, i criteri di cui un titolare del trattamento deve tener conto al fine di verificare se il trattamento per una finalità diversa sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti. Tale disposizione può rilevare nell'ambito dello sviluppo e della diffusione dei modelli di IA e spetta alle AC valutarne la sua applicabilità.

- **Valutazioni d'impatto sulla protezione dei dati** («**DPIA**») (articolo 35 del RGPD): le valutazioni d'impatto sulla protezione dei dati sono un importante elemento di responsabilizzazione, in

[11] Cfr. anche il rapporto dell'EDPB sul lavoro svolto dalla *task force* ChatGPT, adottato il 23 maggio 2024, paragrafo 18: «Per quanto riguarda il trattamento di categorie particolari di dati personali deve, inoltre, essere applicabile una delle eccezioni di cui all'articolo 9, paragrafo 2 affinché il trattamento sia lecito. *In linea di principio, una di queste eccezioni può essere l'articolo 9, paragrafo 2, lettera e) del RGPD. Tuttavia, il semplice fatto che i dati personali siano accessibili al pubblico non implica che «l'interessato abbia manifestamente reso pubblici tali dati» [...]*».

[12] CGUE, Sentenza del 4 luglio 2023, causa C-252/21, *Meta contro Bundeskartellamt* (ECLI:EU:C:2023:537), punto 89.

[13] CGUE, Sentenza del 4 luglio 2023, causa C-252/21, *Meta contro Bundeskartellamt* (ECLI:EU:C:2023:537), punto 77.

[14] Linee guida del Gruppo Articolo 29 **(«WP29»**) sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento (CE) n. 2016/679, come modificate e adottate da ultimo il 6 febbraio 2018, approvate dal Comitato europeo per la protezione dei dati il 25 maggio 2018. Si veda anche la sentenza della CGUE del 7 dicembre 2023, causa C-634/21, *SCHUFA Holding e altri* (ECLI:EU:C:2023:957).

quanto il trattamento potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche nel contesto dei modelli di IA[15].

- **Principio della protezione dei dati fin dalla progettazione** (articolo 25, paragrafo 1 del RGPD): la protezione dei dati fin dalla progettazione è una garanzia essenziale che le AC devono valutare nell'ambito dello sviluppo e della diffusione di un modello di IA.

2.2 Nozioni fondamentali

18. In via preliminare, l'EDPB desidera chiarire la terminologia e i concetti utilizzati nel presente Parere, ed esclusivamente ai fini del medesimo:

- «**Dati di prima parte**» indica i dati personali che il titolare del trattamento ha raccolto presso gli interessati.
- «**Dati di terza parte**» indica i dati personali che i titolari del trattamento non hanno ottenuto dagli interessati, ma che hanno raccolto o ricevuto da terzi, ad esempio da un *broker* di dati o attraverso il *web scraping*.
- Il «**web scraping**» è una tecnica comunemente utilizzata per raccogliere informazioni da fonti *online* pubbliche. Ad esempio, possono contenere dati personali le informazioni estratte da servizi quali testate giornalistiche, *social media*, discussioni nei *forum* e siti web personali.
- La Richiesta fa riferimento al **«ciclo di vita» dei modelli di IA**, nonché a varie fasi che riguardano, tra l'altro, la «creazione», lo «sviluppo», l'«addestramento», l'«aggiornamento», la «messa a punto», il «funzionamento» e il «post-addestramento» dei modelli di IA. L'EDPB riconosce che, a seconda delle circostanze, tali fasi possono avere luogo durante lo sviluppo e nella diffusione dei modelli di IA e possono comportare il trattamento di dati personali per finalità di trattamento diverse. Tuttavia, ai fini del presente Parere, l'EDPB ritiene importante semplificare la categorizzazione delle fasi che potrebbero verificarsi. Pertanto, ai fini del presente Parere, l'EDPB farà riferimento alla «**fase di sviluppo**» e alla «**fase di diffusione**». Lo sviluppo di un modello di IA comprende tutte le fasi che precedono la diffusione del modello stesso e comprende, tra l'altro, lo sviluppo del codice, la raccolta dei dati personali di addestramento, la pre-elaborazione dei dati di addestramento e l'addestramento. La diffusione di un modello di IA riguarda tutte le fasi relative all'utilizzo di un modello di IA e comprende tutte le operazioni condotte dopo la fase di sviluppo. L'EDPB è consapevole della varietà di casi di utilizzo e delle potenziali ricadute in termini di trattamento dei dati personali; pertanto, spetta alle AC valutare se le osservazioni fornite nel presente Parere siano pertinenti ai fini del trattamento preso in esame.
- L'EDPB sottolinea inoltre che, ove necessario, il termine «**addestramento**» indica il momento della fase di sviluppo in cui i modelli di IA apprendono dai dati per eseguire i compiti previsti (come illustrato nella prossima sezione del presente Parere).
- La nozione e l'ambito di applicazione dei **modelli di IA**, così come intesi dall'EDPB ai fini del presente Parere, sono ulteriormente specificati nella successiva sezione dedicata.

2.3 Modelli di IA nel contesto del Parere

[15] Linee guida WP29 in materia di valutazione d'impatto sulla protezione dei dati (DPIA) e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679, riviste e adottate il 4 aprile 2017, approvate dall'EDPB il 25 maggio 2018.

19. Il Regolamento sull'intelligenza artificiale dell'UE («**regolamento sull'IA**»)[16] definisce un «sistema di IA» come «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare risultati quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*» [17]. Il considerando 12 del regolamento sull'IA chiarisce ulteriormente la nozione di «sistema di IA». Quindi, una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono *il machine learning* e gli approcci basati sulla logica e sulla conoscenza.

20. I «modelli di IA», d'altro canto, sono definiti solo indirettamente nel regolamento sull'IA: «*Sebbene i modelli di IA siano componenti essenziali dei sistemi di IA, essi non costituiscono di per sé sistemi di IA. I modelli di IA necessitano dell'aggiunta di altri componenti, ad esempio un'interfaccia utente, per diventare sistemi di IA. I modelli di IA sono generalmente integrati nei sistemi di IA e ne fanno parte*»[18].

21. L'EDPB ritiene che la definizione di modello di IA contenuta nella Richiesta sia più circoscritta rispetto a quella presente nel regolamento sull'IA, in quanto considera un «modello di IA» come «*il prodotto risultante dai meccanismi di addestramento applicati a un insieme di addestramento, nel contesto dell'intelligenza artificiale, del machine learning, del deep learning o di altri contesti di trattamento correlati*» e specifica inoltre che «*Il termine si applica ai modelli di IA destinati ad essere ulteriormente addestrati, perfezionati e/o sviluppati, nonché ai modelli di IA che non lo saranno*»19.

22. Su tale base, l'EDPB ha adottato il presente Parere, ritenendo che un sistema di IA si basi su un modello di IA per conseguire l'obiettivo previsto, integrando il modello in un quadro più ampio (ad esempio, un sistema di IA per il servizio clienti potrebbe utilizzare un modello di IA addestrato sui dati dello storico delle conversazioni per generare le risposte alle interrogazioni degli utenti).

23. Inoltre, i modelli di IA (o «**modelli**») rilevanti ai fini del presente Parere sono quelli sviluppati attraverso un processo di addestramento. Tale processo di addestramento fa parte della fase di sviluppo in cui i modelli imparano dai dati a svolgere il compito previsto. Pertanto, il processo di addestramento richiede un insieme di dati dal quale il modello individua e «apprende» gli schemi ricorrenti. In questi casi, il modello utilizza diverse tecniche per costruire una rappresentazione della conoscenza estratta dall'insieme di addestramento. Questo è esattamente ciò che accade nel *machine learning*.

24. In pratica, qualsiasi modello di IA è un algoritmo il cui funzionamento è determinato da una serie di elementi. Ad esempio, i modelli di *deep learning* assumono spesso la forma di una rete neurale con molteplici strati costituiti da nodi collegati da archi a cui vengono assegnati dei pesi, che vengono regolati durante l'addestramento per apprendere le relazioni tra gli *input* e gli *output*. Le caratteristiche di un semplice modello di *deep learning* sono le seguenti: (i) tipo e dimensione degli strati, (ii) peso attribuito a ogni arco (anche detti «parametri»), (iii) funzioni di attivazione [20] tra gli strati ed eventualmente (iv) altre operazioni che possono avvenire tra gli strati. Ad esempio, durante l'addestramento di un semplice modello di *deep learning* per la classificazione delle immagini, gli *input*

[16] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

[17] Cfr. l'articolo 3, paragrafo 1 del regolamento sull'IA.

[18] Considerando 97 del regolamento sull'IA.

[19] Richiesta, pag. 3.

[20] Ossia funzioni che calcolano, sulla base di *input* e pesi, l'*output* di un nodo neurale che sarà poi inviato al livello successivo della rete neurale.

(i «**pixel delle immagini**») vengono associati agli *output* e i pesi possono essere regolati in modo da produrre il giusto *output* nella maggior parte dei casi.

25. Altri esempi di modelli di *deep learning* includono i modelli LLM e l'IA generativa, che vengono utilizzati, ad esempio, per generare contenuti di tipo umano e creare nuovi dati.

26. **Sulla base delle considerazioni sopra esposte, in linea con la Richiesta, l'ambito di applicazione del presente Parere riguarda esclusivamente il sottoinsieme di modelli di IA sviluppati attraverso l'addestramento con dati personali.**

3 Sul merito della Richiesta

3.1 Sulla natura dei modelli di IA in relazione alla definizione di dati personali

27. L'articolo 4, paragrafo 1 del RGPD definisce i dati personali come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile*» (cioè l'interessato). Inoltre, il considerando 26 del RGPD stabilisce che i principi di protezione dei dati non dovrebbero applicarsi alle informazioni anonime, vale a dire le informazioni che non si riferiscono a una persona fisica identificata o identificabile, tenendo conto di «*tutti i mezzi di cui può ragionevolmente avvalersi*» il titolare del trattamento o un terzo. Ciò comprende: (i) i dati che non sono mai stati riferiti a una persona fisica identificata o identificabile e (ii) i dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

28. Di conseguenza, il Quesito n. 1[21] della Richiesta può essere risolto verificando se un modello di IA sviluppato tramite un addestramento che comporta il trattamento di dati personali debba essere considerato anonimo in ogni caso. Coerentemente con la formulazione del Quesito, in questa sezione l'EDPB farà riferimento al processo di «addestramento» di un modello di IA.

29. Innanzitutto, l'EDPB desidera esprimere le seguenti considerazioni generali. I modelli di IA, indipendentemente dal fatto che siano addestrati o meno con dati personali, sono solitamente progettati per fare previsioni o trarre conclusioni, cioè sono progettati per dedurre. Inoltre, i modelli di IA addestrati con dati personali sono spesso progettati per fare inferenze su individui diversi da quelli i cui dati personali sono stati utilizzati per addestrare il modello di IA. Tuttavia, alcuni modelli di IA sono specificamente progettati per fornire dati personali relativi alle persone i cui dati personali sono stati utilizzati per addestrare il modello, o in qualche modo, per rendere disponibili tali dati. In questi casi, tali modelli di IA comprendono intrinsecamente (e in genere necessariamente) informazioni riferite a una persona fisica identificata o identificabile, e quindi comportano il trattamento di dati personali. Pertanto, i modelli di IA che rientrano in questa tipologia non possono essere considerati anonimi. Questo si verificherebbe, ad esempio, nel caso di (i) un modello generativo affinato attraverso le registrazioni vocali di una persona per imitare la sua voce; o (ii) qualsiasi modello progettato per rispondere attingendo ai dati personali usati per l'addestramento quando vengono richieste informazioni su una persona specifica.

30. Sulla base delle considerazioni sopra esposte, nel rispondere al Quesito n. 1 della Richiesta, l'EDPB analizza nello specifico la situazione dei modelli di IA che non sono progettati per fornire dati personali relativi ai dati di addestramento.

[21] «*Si ritiene che il modello di intelligenza artificiale finale, addestrato utilizzando dati personali non rientri, in ogni caso, nella definizione di dati personali (di cui all'articolo 4, paragrafo 1, del RGPD)?*»

31. L'EDPB ritiene che, anche quando un modello di IA non sia stato progettato intenzionalmente per produrre informazioni riferite a una persona fisica identificata o identificabile dai dati di addestramento, le informazioni tratte dal *set* di addestramento, compresi i dati personali, possono essere «incorporate» nei parametri del modello, vale a dire rappresentate mediante oggetti matematici. Possono differire dai dati originali di addestramento, pur tuttavia trattenendo le informazioni originali di tali dati, che possono eventualmente essere estratte o altrimenti ottenute, direttamente o indirettamente, dal modello. Ogniqualvolta sia possibile ottenere da un modello di IA attraverso mezzi di cui ci si può ragionevolmente avvalere, le informazioni riferite a persone identificate o identificabili i cui dati personali sono stati utilizzati per addestrare il modello, si può concludere che tale modello non è anonimo.

32. A questo proposito, la Richiesta ribadisce che «*Ricerche scientifiche attualmente disponibili mettono in evidenza alcune potenziali vulnerabilità dei modelli di IA che potrebbero comportare il trattamento di dati personali*[22]*, nonché il trattamento di dati personali che può verificarsi quando la diffusione dei modelli prevede l'utilizzo congiunto di altri dati, attraverso le interfacce API (**«API»**) o interfacce «di prompt*»[23].

33. Analogamente, l'attività di ricerca sull'estrazione dei dati di addestramento è particolarmente dinamica[24]. Dimostra che, in alcuni casi, è possibile utilizzare mezzi ragionevolmente idonei a estrarre dati personali da alcuni modelli di IA o semplicemente a ottenere dati personali casualmente interagendo con un modello di IA (ad esempio nell'ambito di un sistema di IA). La costante attività di ricerca in questo campo contribuirà a valutare ulteriormente i rischi residui di rigurgito[25] e di estrazione di dati personali in ciascun caso specifico.

34. **Sulla base delle considerazioni sopra esposte, l'EDPB ritiene che i modelli di IA addestrati con dati personali non possano, in ogni caso, essere considerati anonimi. Al contrario, la determinazione dell'anonimità di un modello di IA dovrebbe essere valutata caso per caso, sulla base di criteri specifici.**

3.2 Sulle circostanze in cui i modelli di IA potrebbero essere considerati anonimi e relativa dimostrazione

[22] Come i cd. *Membership Inference Attacks* (OWASP) e i cd. *Model Inversion Attacks* (OWASP e Veale et al, 2018).
[23] Richiesta, pagg. 1-2.
[24] Cfr., al riguardo, ad esempio: (i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, disponibile all'indirizzo: http://dx.doi.org/10.1098/rsta.2018.0083; (ii) Brown H., Lee K., Mireshghallah F., Shokri R., and Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, 20/06/ 2022, Seoul, Repubblica di Corea, disponibile all'indirizzo https://dl.acm.org/doi/abs/10.1145/3531146.3534642; (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, gennaio 2024, National Institute of Standards and Technology, disponibile all'indirizzo: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf; (iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15/06/2021, disponibile all'indirizzo: https://arxiv.org/pdf/2012.07805; (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12/10/2015, disponibile all'indirizzo: https://dl.acm.org/doi/abs/10.1145/2810103.2813677; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18/04/2020, disponibile all'indirizzo: https://arxiv.org/pdf/1911.07135.
[25] Per un sistema di IA basato sull'IA generativa, il rigurgito corrisponde alla situazione in cui i risultati sarebbero direttamente correlati ai dati di addestramento.

35. Per quanto riguarda il Quesito n. 1 della Richiesta[26], si chiede all'EDPB di chiarire le circostanze in cui un modello di IA, che è stato addestrato utilizzando dati personali, possa essere considerato anonimo. Per quanto riguarda il Quesito n. 1, punto i), lettera a), della Richiesta[27], l'EDPB è invitato a illustrare quali evidenze e/o documentazione dovrebbero prendere in considerazione le AC per verificare se un modello di IA è anonimo.

3.2.1 Considerazione generale sull'anonimizzazione nel contesto in esame

36. L'uso dell'espressione «*qualsiasi informazione*» nella definizione di «*dati personali*» di cui all'articolo 4, paragrafo 1 del RGPD riflette l'obiettivo di associare a tale concetto un ambito di applicazione ampio, che comprende tutti i tipi di informazioni a condizione che «*riguardino*» l'interessato, che si identifica o possa essere identificato direttamente o indirettamente.

37. Le informazioni possono riguardare una persona fisica anche quando sono tecnicamente organizzate o codificate (ad esempio in un formato esclusivamente *machine readable*, sia esso proprietario o aperto) secondo una modalità che non rende immediatamente evidente la relazione con tale persona fisica. In questi casi, è possibile utilizzare le applicazioni software per identificare, riconoscere ed estrarre facilmente dati specifici. Ciò accade soprattutto nei modelli di IA in cui i parametri rappresentano relazioni statistiche tra i dati di addestramento e in cui può essere possibile estrarre dati personali accurati o non accurati (perché dedotti statisticamente), sia direttamente dalle relazioni tra i dati inclusi nel modello, sia interrogando il modello stesso.

38. Poiché i modelli di IA solitamente non contengono *record* che possono essere direttamente isolati o collegati, ma parametri che rappresentano relazioni probabilistiche tra i dati contenuti nel modello, è possibile, in scenari realistici, inferire[28] informazioni dal modello, come l'inferenza di appartenenza.

[26] «*Quali sono le circostanze in cui ciò potrebbe verificarsi?*»

[27] «*In tal caso, come si possono dimostrare le misure adottate per garantire che il modello di IA non tratti dati personali?*»

[28] (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles,* arXiv:2112.03570, disponibile all'indirizzo: https://arxiv.org/abs/2112.03570;
(ii) Creţu A.M, Guépin F., and De Montjoye Y.A, *Correlation inference attacks against machine learning models*. Sci. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 disponibile all'indirizzo: https://www.science.org/doi/10.1126/sciadv.adj9260;
(iii) Dana L., Pydi M. S., Chevaleyre Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15 /11/2024, disponibile all'indirizzo: https://arxiv.org/abs/2411.10115;
(iv) Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13/06/2024, disponibile all'indirizzo: https://doi.org/10.1007/s13218-024-00851-y;
(v) HU H., *Membership Inference Attacks and defenses on Machine Learning Models Literature*, disponibile all'indirizzo: https://github.com/HongshengHu/membership-inference-machine-learning-literature;
(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., and Lee K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28/11/2023, disponibile all'indirizzo: https://arxiv.org/abs/2311.17035;
(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31/03/2017, disponibile all'indirizzo https://arxiv.org/abs/1610.05820;
(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond memorisation: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6/05/2024, disponibile all'indirizzo https://arxiv.org/abs/2310.07298;
(ix) Wu F., Cui L., Yao S., Yu S., *InferenceAttacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* arXiv: 2406.02027v1 [cs.LG], 27/06/2024, disponibile all'indirizzo https://arxiv.org/abs/2406.02027v1:

Pertanto, affinché le AC possano convalidare l'anonimità di un determinato modello di IA come dichiarato dal titolare del trattamento, esse dovrebbero almeno verificare che il titolare abbia raccolto sufficienti evidenze secondo cui, avvalendosi di mezzi ragionevoli: i) i dati personali relativi ai dati di addestramento non possono essere estratti [29] dal modello e ii) qualsiasi *output* risultante dall'interrogazione del modello non riguarda gli interessati i cui dati personali sono stati utilizzati per addestrare il modello.

39. Nel valutare se tali condizioni siano soddisfatte, le AC dovrebbero prendere in considerazione tre elementi.

40. In primo luogo, le AC dovrebbero prendere in considerazione gli elementi individuati nei più recenti pareri del WP29 e/o nelle Linee guida dell'EDPB in materia. Per quanto riguarda l'anonimizzazione, alla data del presente Parere, le AC dovrebbero prendere in considerazione gli elementi di cui al parere 05/2014 del WP29 sulle tecniche di anonimizzazione (**«parere 05/2014 del WP29»**), in cui si afferma che, ove non sia possibile individuare, correlare e trarre inferenze dall'insieme di dati presumibilmente anonimo, i dati possono essere considerati anonimi[30]. Esso afferma inoltre che «*ogniqualvolta che una proposta non soddisfa uno dei criteri, occorre effettuare una valutazione approfondita dei rischi di identificazione*»[31]. **Data la probabilità di estrazione e di inferenza di cui sopra, l'EDPB ritiene che sia altamente probabile che i modelli di IA richiedano tale valutazione approfondita dei rischi di identificazione.**

41. In secondo luogo, tale valutazione dovrebbe essere effettuata tenendo conto «*di tutti i mezzi di cui può ragionevolmente avvalersi*» il titolare del trattamento o un terzo per identificare le persone[32] e la determinazione di tali mezzi dovrebbe basarsi su fattori oggettivi, come illustrato nel considerando 26 del RGPD, tra cui:
    a. le caratteristiche dei dati di addestramento, il modello di IA e la procedura di addestramento[33];
    b. il contesto in cui il modello di IA viene rilasciato e/o elaborato[34];
    c. le informazioni supplementari che consentirebbero l'identificazione e che potrebbero risultare accessibili ad una determinata persona;
    d. i costi e il tempo necessario alla persona per ottenere tali informazioni aggiuntive (nel caso in cui non siano già a sua disposizione[35]); e,

(x) Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your Data* arXiv:2409.19798v1, [cs.LG], 29/09/2024, disponibile all'indirizzo https://arxiv.org/abs/2409.19798;
(xi) Zhou Z., Xiang J., Chen C., and Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models*, arXiv:2308.15727v2 [cs.CL] 5/11/2023, disponibile all'indirizzo: https://arxiv.org/abs/2308.15727.

[29] L'estrazione comprende in particolare il caso in cui i dati personali sono dedotti dal modello di IA stesso, con un uso limitato o nullo delle interfacce di interrogazione.
[30] Parere 05/2014 del WP29, pag. 24.
[31] Parere 05/2014 del WP29, pag. 24.
[32] CGUE, sentenza del 19 ottobre 2016, causa C-582/14, *Breyer contro Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), punto 43.
[33] Ciò include caratteristiche quali l'unicità dei *record* dei dati di addestramento, la precisione delle informazioni, l'aggregazione, la randomizzazione e, in particolare, il modo in cui queste influiscono sulla vulnerabilità all'identificazione.
[34] Ciò comprende elementi contestuali, come la limitazione dell'accesso solo ad alcune persone e le tutele giuridiche.
[35] CGUE, sentenza del 7 marzo 2024, causa C-479/22 P, *OC/Commissione europea* (ECLI:EU:C:2024:215), punto 50.

e. la tecnologia disponibile al momento del trattamento, nonché gli sviluppi tecnologici[36].

42. In terzo luogo, le AC dovrebbero verificare se i titolari del trattamento abbiano valutato il rischio di identificazione da parte del titolare del trattamento e di diverse tipologie di *«altre persone»*, compresi i terzi non intenzionali che accedono al modello di IA, anche valutando se si possa ragionevolmente ritenere che siano in grado di accedere ai dati in questione o di trattarli.

43. **In sintesi, l'EDPB ritiene che, affinché un modello di IA sia considerato anonimo, utilizzando mezzi ragionevoli, sia (i) la probabilità di estrazione diretta (anche probabilistica) di dati personali relativi a persone i cui dati personali sono stati utilizzati per addestrare il modello, sia (ii) la probabilità di ottenere, intenzionalmente o meno, tali dati personali dalle interrogazioni, dovrebbero risultare insignificanti[37] per qualsiasi interessato. Di norma, le AC dovrebbero considerare il fatto che è probabile che i modelli di IA richiedano una valutazione approfondita della probabilità di identificazione al fine di giungere a una conclusione sulla loro possibile natura anonima. Tale probabilità dovrebbe essere valutata tenendo conto di «*tutti i mezzi di cui può ragionevolmente avvalersi*» il titolare del trattamento o un terzo, e dovrebbe anche prendere in considerazione il (ri)uso o la divulgazione non intenzionali del modello.**

3.2.2 Elementi per valutare la probabilità residua di identificazione

44. Sebbene sia possibile adottare misure per ridurre la probabilità di ricavare dati personali da un modello di IA, sia nella fase di sviluppo che in quella di diffusione, nel valutare l'anonimità di un modello di IA si dovrebbe prendere in considerazione anche l'accesso diretto al modello.

45. Inoltre, le AC dovrebbero valutare, caso per caso, l'adeguatezza e l'efficacia delle misure adottate dal titolare del trattamento per garantire e dimostrare l'anonimità di un modello di IA.

46. In particolare, l'esito della valutazione di un'AC potrebbe differire a seconda che si tratti di un modello di IA pubblico, accessibile a un numero imprecisato di persone con una gamma imprecisata di metodi per l'estrazione dei dati personali, o un modello interno di IA accessibile solo ai dipendenti. Sebbene in entrambi i casi le AC debbano verificare che i titolari del trattamento abbiano adempiuto all'obbligo di responsabilizzazione di cui all'articolo 5, paragrafo 2, e all'articolo 24 del RGPD, i «*mezzi di cui possono ragionevolmente avvalersi*» altre persone possono avere un impatto sul numero e sulla natura dei possibili scenari da prendere in considerazione. Pertanto, a seconda del contesto di sviluppo o diffusione del modello, le AC possono prendere in considerazione diversi livelli di *testing* e resistenza agli attacchi.

47. A tale riguardo, l'EDPB fornisce di seguito un elenco non prescrittivo e non esaustivo dei possibili elementi che le AC possono prendere in considerazione nel valutare la dichiarazione di anonimità resa da un titolare del trattamento. Sono possibili altri approcci purché offrano un livello di tutela equivalente, in particolare tenendo conto dello stato dell'arte.

48. La presenza o l'assenza degli elementi elencati di seguito non costituisce un criterio decisivo per valutare l'anonimità di un modello di IA.

[36] CGUE, sentenza del 7 marzo 2024, causa C-479/22 P, *OC/Commissione europea* (ECLI:EU:C:2024:215), punto 50.

[37] CGUE, sentenza del 19 ottobre 2016, causa C-582/14, *Breyer c. Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), punto 46, e sentenza della CGUE del 7 marzo 2024, causa C-479/22 P, *OC c. Commissione europea* (ECLI:EU:C:2024:215), punto 51.

3.2.2.1 Progettazione del modello di IA

49. Per quanto riguarda la progettazione del modello di IA, le AC dovrebbero valutare gli approcci adottati dai titolari del trattamento durante la fase di sviluppo. A questo proposito, dovrebbero essere prese in considerazione l'applicazione e l'efficacia di quattro aree chiave (individuate di seguito).

Selezione delle fonti

50. La prima area di valutazione consiste nell'esaminare la selezione delle fonti utilizzate per addestrare il modello di IA. Ciò include una valutazione, da parte delle AC, di tutte le misure adottate per evitare o limitare la raccolta di dati personali, tra cui, tra l'altro, (i) l'adeguatezza dei criteri di selezione; (ii) la pertinenza e l'adeguatezza delle fonti scelte in funzione della finalità o delle finalità previste; e (iii) l'eventuale esclusione di fonti inappropriate.

Preparazione e minimizzazione dei dati

51. La seconda area di valutazione riguarda la preparazione dei dati per la fase di addestramento. Le AC dovrebbero esaminare in particolare: i) se sia stato preso in considerazione l'uso di dati anonimi e/o personali sottoposti a pseudonimizzazione; e ii) qualora sia stato deciso di non ricorrere a tali misure, i motivi di tale decisione, tenendo conto della finalità prevista; iii) le strategie e le tecniche di minimizzazione dei dati utilizzate per limitare il volume di dati personali coinvolti nel processo di addestramento; e iv) eventuali processi di filtraggio dei dati attuati prima dell'addestramento del modello volti a rimuovere dati personali non pertinenti.

Scelte metodologiche riguardanti l'addestramento

52. La terza area di valutazione riguarda la selezione di metodi robusti per lo sviluppo dei modelli di IA. Le AC dovrebbero valutare scelte metodologiche in grado di ridurre significativamente l'identificabilità o eliminarla, tra cui, tra l'altro: i) se tale metodologia utilizza metodi di regolarizzazione per migliorare la generalizzazione del modello e ridurre l'eccesso di adattamento; e, soprattutto, ii) se il titolare del trattamento ha attuato tecniche adeguate ed efficaci di tutela della *privacy* (ad esempio la *privacy* differenziale).

Misure relative agli output del modello

53. L'ultima area di valutazione riguarda tutte le misure o i metodi integrati nel modello di IA che possono non avere un impatto sul rischio di estrazione diretta di dati personali per il modello da parte di chiunque vi acceda direttamente, ma che potrebbero ridurre la probabilità di ricavare dati personali per l'addestramento dalle interrogazioni.

3.2.2.2 Analisi del modello di IA

54. Affinché le AC valutino la robustezza del modello di IA sviluppato, dal punto di vista dell'anonimizzazione, è necessario, innanzitutto, assicurarsi che il progetto sia stato sviluppato così come era stato programmato e che sia soggetto a un'efficace *governance* tecnica. Le AC dovrebbero approfondire se i titolari abbiano condotto verifiche documentali (interne o esterne) per valutare le misure adottate e la loro efficacia nel limitare la probabilità di identificazione. In questo potrebbe rientrare l'analisi dei rapporti di revisione del codice, nonché un'analisi teorica che documenti l'adeguatezza delle misure adottate per ridurre la probabilità di re-identificazione del modello in questione.

3.2.2.3 Test dei modelli di IA e resistenza agli attacchi

55. Infine, le AC dovrebbero prendere in considerazione l'ambito, la frequenza, la quantità e la qualità dei test che il titolare del trattamento ha effettuato sul modello. In particolare, le AC dovrebbero tenere conto del fatto che il successo dei test relativi ad attacchi ampiamente noti e di stato dell'arte, può soltanto dimostrare una resistenza a tali attacchi. Alla data del presente Parere, ciò potrebbe comprendere, tra l'altro, test strutturati contro: i) inferenza degli attributi e inferenza di appartenenza;

ii) esfiltrazione; iii) rigurgito dei dati di addestramento; iv) inversione del modello; o v) attacchi di ricostruzione.

3.2.2.4 Documentazione

56. Gli articoli 5, 24, 25 e 30 del RGPD e, nei casi in cui vi possa essere un rischio elevato per i diritti e le libertà degli interessati, l'articolo 35 del RGPD, prevedono che i titolari del trattamento sono tenuti a documentare adeguatamente le operazioni di trattamento. Ciò vale anche per qualsiasi trattamento che preveda l'addestramento di un modello di IA, anche se l'obiettivo del trattamento è l'anonimizzazione. Le AC dovrebbero prendere in considerazione tale documentazione e qualsiasi valutazione periodica dei rischi consequenziali per il trattamento effettuato dai titolari del trattamento, in quanto si tratta di passaggi fondamentali per dimostrare che non vi è trattamento di dati personali.

57. **L'EDPB ritiene che le AC dovrebbero tener conto della documentazione ogniqualvolta occorra valutare una dichiarazione di anonimità relativa a un determinato modello di IA. L'EDPB osserva che qualora un'AC non sia in grado di confermare, dopo aver valutato la attestazione di anonimità, anche alla luce della documentazione, che sono state adottate misure efficaci per anonimizzare il modello di IA, l'AC potrebbe ritenere che il titolare del trattamento non abbia adempiuto ai propri obblighi di responsabilizzazione ai sensi dell'articolo 5, paragrafo 2 del RGPD. Pertanto, andrebbe valutata anche la conformità con altre disposizioni del RGPD.**

58. Idealmente, le AC dovrebbero verificare se la documentazione del titolare del trattamento comprende:

    a. Eventuali informazioni relative alle valutazioni d'impatto sulla protezione dei dati, comprese le valutazioni e le decisioni in base alle quali non è stata ritenuta necessaria una valutazione d'impatto sulla protezione dei dati;

    b. Eventuali indicazioni o riscontri forniti dal responsabile della protezione dei dati («**RPD**») (nel caso in cui sia stato nominato un RPD o avrebbe dovuto esserlo);

    c. Informazioni sulle misure tecniche e organizzative adottate durante la progettazione del modello di IA per ridurre la probabilità di identificazione, compreso il modello di minaccia e le valutazioni del rischio alla base di tali misure. Questo dovrebbe includere le misure specifiche per ogni fonte dei dati di addestramento, compresi gli URL delle fonti pertinenti e le descrizioni delle misure adottate (o già adottate dai fornitori di insiemi di dati di terza parte);

    d. Le misure tecniche e organizzative adottate in tutte le fasi del ciclo di vita del modello che hanno contribuito o verificato l'assenza di dati personali al suo interno;

    e. La documentazione comprovante la resistenza teorica del modello di IA alle tecniche di re-identificazione, nonché i controlli volti a limitare o valutare il successo e l'impatto dei principali attacchi (rigurgito, attacchi di inferenza di appartenenza, esfiltrazione, ecc.). Ciò può includere, in particolare: (i) il rapporto tra la quantità di dati di addestramento e il numero di parametri del modello, compresa l'analisi del suo impatto sul modello[38]; (ii) le metriche sulla

[38] Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data*, Privacy in Statistical Databases conference (PSD 2024), Antibes, Francia, settembre 2024, slide disponibili all'indirizzo: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf e Belkin M., Hsu D., Ma S., & Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias-variance trade-off*. Proceedings of the National Academy of Sciences, 24/07/2019, 116(32) 15849-15854, disponibile all'indirizzo: https://www.pnas.org/doi/10.1073/pnas.1903070116

probabilità di re-identificazione sulla base dell'attuale stato dell'arte; (iii) i rapporti sui test effettuati sul modello (chi, quando, come e in che misura) e (iv) i risultati dei test;

f. La documentazione fornita al titolare o ai titolari del trattamento che utilizzano il modello e/o agli interessati, in particolare la documentazione relativa alle misure adottate per ridurre la probabilità di identificazione e i possibili rischi residui.

3.3 Sull'adeguatezza dell'interesse legittimo come base giuridica per il trattamento dei dati personali nel contesto dello sviluppo e della diffusione dei modelli di IA.

59. Per rispondere ai Quesiti n. 2 e n. 3 della Richiesta, l'EDPB fornirà innanzitutto osservazioni generali su alcuni aspetti importanti di cui le AC dovrebbero tenere conto, indipendentemente dalla base giuridica del trattamento, nel valutare in che modo i titolari del trattamento possano dimostrare il rispetto del RGPD nel contesto dei modelli di IA. L'EDPB, sulla base delle Linee guida 1/2024 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD [39], prenderà quindi in considerazione le tre fasi previste per la valutazione dell'interesse legittimo nel contesto dello sviluppo e della diffusione dei modelli di IA.

3.3.1 Osservazioni generali

60. L'EDPB rammenta che il RGPD non stabilisce alcuna gerarchia tra le diverse basi giuridiche di cui all'articolo 6, paragrafo 1 del Regolamento stesso[40].

61. L'articolo 5 del RGPD enuncia i principi relativi al trattamento dei dati personali. L'EDPB evidenzia quelli rilevanti ai fini del presente Parere e che dovrebbero essere almeno presi in considerazione dalle AC nella valutazione di specifici modelli di IA, insieme ai requisiti più rilevanti previsti da altre disposizioni del RGPD, tenendo conto dell'ambito di applicazione del presente Parere.

62. **Principio di responsabilizzazione** (articolo 5, paragrafo 2 del RGPD) – Tale principio prevede che il titolare del trattamento sia competente per il rispetto del RGPD e in grado di comprovarlo. A tale riguardo, i ruoli e le responsabilità delle parti che trattano i dati personali nel contesto dello sviluppo o della diffusione di un modello di IA dovrebbero essere valutati prima che il trattamento abbia luogo, al fine di definire, sin dall'inizio, gli obblighi dei titolari o contitolari del trattamento e degli eventuali responsabili del trattamento.

63. **Principi di liceità, correttezza e trasparenza** (articolo 5, paragrafo 1, lettera a) del RGPD) - Nel valutare la liceità del trattamento nel contesto dei modelli di IA, alla luce dell'articolo 6, paragrafo 1 del RGPD, l'EDPB ritiene utile distinguere le diverse fasi del trattamento dei dati personali [41]. Il principio di correttezza, strettamente connesso al principio di trasparenza, prevede che i dati personali non siano trattati con metodi sleali, o con l'inganno, o in un modo che sia «*ingiustificatamente dannoso, illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato*»[42]. In considerazione della complessità delle tecnologie coinvolte, le informazioni sul trattamento dei dati personali all'interno

[39] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024.
[40] Ibidem, paragrafo 1.
[41] Rapporto dell'EDPB sul lavoro svolto dalla *task force* ChatGPT, adottato il 23 maggio 2024, punto 14.
[42] Rapporto dell'EDPB sul lavoro svolto dalla *task force* ChatGPT, adottato il 23 maggio 2024, punto 23; Linee guida 4/2019 dell'EDPB sull'articolo 25 «Protezione dei dati fin dalla progettazione e per impostazione predefinita», versione 2.0, adottate il 20 ottobre 2020, punto 69; Linee guida del gruppo di lavoro «Articolo 29» sulla trasparenza ai sensi del regolamento (UE) 2016/679, riviste e adottate l'11 aprile 2018, approvate dall'EDPB il 25 maggio 2018, punto 2.

dei modelli di IA dovrebbero pertanto essere fornite in modo accessibile, comprensibile e di facile utilizzo[43]. La trasparenza in merito al trattamento dei dati personali comprende, in particolare, il rispetto degli obblighi di informazione di cui agli articoli 12-14 del RGPD[44], che richiedono anche, in caso di processo decisionale automatizzato, compresa la profilazione, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato[45]. Tenuto conto del fatto che le fasi di sviluppo dei modelli di IA possono comportare la raccolta di grandi quantità di dati da fonti pubblicamente accessibili (ad esempio tramite tecniche di *web scraping*), il ricorso all'eccezione prevista all'articolo 14, paragrafo 5, lettera b) del RGPD è strettamente limitato ai casi in cui i requisiti di tale disposizione siano pienamente soddisfatti[46].

64. **Principi di limitazione delle finalità e minimizzazione dei dati** (articolo 5, paragrafo 1, lettere b) e c) del RGPD) – Conformemente al principio di minimizzazione dei dati, nello sviluppo e nella diffusione di modelli di IA, occorre che i dati personali siano adeguati, pertinenti e necessari in relazione alla finalità. Ciò può includere il trattamento di dati personali al fine di evitare rischi di potenziali distorsioni ed errori quando ciò sia chiaramente e specificamente individuato nelle finalità e quando i dati personali siano necessari per tale finalità (ad esempio, l'obiettivo non può essere efficacemente raggiunto attraverso il trattamento di altri dati, compresi dati sintetici o anonimizzati)[47]. Il Gruppo di lavoro «Articolo 29» ha già sottolineato che la «*finalità della raccolta deve essere chiaramente e specificamente individuata* [...]»[48]. Nel valutare se la finalità perseguita sia legittima, specifica ed esplicita e se il trattamento sia conforme al principio di minimizzazione dei dati, si dovrebbe innanzitutto individuare l'attività di trattamento in questione. In particolare, i diversi momenti delle fasi di sviluppo o di diffusione possono costituire medesime o diverse attività di trattamento e possono comportare il coinvolgimento di successivi titolari o contitolari del trattamento. In alcuni casi, è possibile determinare la finalità perseguita durante la diffusione del modello di IA ad una fase iniziale di sviluppo. Anche in caso contrario, dovrebbe essere già chiaro il contesto di tale diffusione e, pertanto, si dovrebbe considerare il modo in cui tale contesto determina la finalità dello sviluppo. Nel riesaminare la finalità del trattamento in una specifica fase di sviluppo, le AC dovrebbero aspettarsi dal titolare, o dai titolari del trattamento, un certo grado di dettaglio e un chiarimento su come tali informazioni determinano la finalità del trattamento. Ciò può includere, ad esempio, informazioni sul tipo di modello di IA sviluppato, sulle funzionalità previste e qualsiasi altra informazione pertinente già nota in quella fase. Relativamente alla fase di diffusione, si può precisare, ad esempio, se un modello sia sviluppato per la diffusione interna, se il titolare del trattamento intenda venderlo o distribuirlo a terzi dopo il suo sviluppo, e se il modello sia destinato principalmente ad un uso per fini commerciali o di ricerca.

65. **Diritti degli interessati** (Capo III del RGPD) – Nonostante le AC debbano garantire il rispetto di tutti i diritti degli interessati quando i titolari del trattamento procedono allo sviluppo e diffusione di modelli

[43] Linee guida del gruppo di lavoro «Articolo 29» sulla trasparenza ai sensi del regolamento 2016/679, riviste e adottate l'11 aprile 2018, approvate dall'EDBP il 25 maggio 2018, punto 5.

[44] Cfr. anche il considerando 39 del RGPD, che statuisce che «*dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati [...]*».

[45] Articolo 13, paragrafo 2, lettera f) e articolo 14, paragrafo 2, lettera g) del RGPD.

[46] Rapporto dell'EDPB sul lavoro svolto dalla *task force* ChatGPT, adottato il 23 maggio 2024, punto 27.

[47] Inoltre, l'articolo 10, paragrafo 5 del regolamento sull'IA prevede norme specifiche per il trattamento di categorie particolari di dati personali in relazione ai sistemi di IA ad alto rischio al fine di garantire il rilevamento e la correzione delle distorsioni.

[48] Parere 03/2013 del WP29 sulla limitazione delle finalità (WP203), pagg. 15 e 16.

di IA, l'EDPB ricorda che ogniqualvolta un titolare del trattamento invoca l'interesse legittimo come base giuridica, si applica, e dovrebbe essere garantito, il diritto di opposizione ai sensi dell'articolo 21 del RGPD[49].

3.3.2 Considerazioni sulle tre fasi della valutazione dell'interesse legittimo nel contesto dello sviluppo e della diffusione dei modelli di IA

66. Al fine di stabilire se un determinato trattamento di dati personali si basi sull'articolo 6, paragrafo 1, lettera f) del RGPD, le AC dovrebbero verificare che i titolari del trattamento abbiano attentamente valutato e documentato la sussistenza delle seguenti tre condizioni cumulative: (i) il perseguimento del legittimo interesse del titolare del trattamento o di terzi; (ii) la necessità del trattamento per il perseguimento del legittimo interesse; e (iii) se sul legittimo interesse non prevalgono gli interessi o i diritti e le libertà fondamentali degli interessati[50].

3.3.2.1 Prima fase – Perseguimento di un interesse legittimo da parte del titolare del trattamento o di terzi

67. Un interesse è il vantaggio o beneficio più ampio che un titolare del trattamento o un terzo possono ricavare dallo svolgimento di una specifica attività di trattamento[51]. Sebbene il RGPD e la Corte di giustizia dell'Unione europea abbiano riconosciuto diversi interessi come legittimi[52], la valutazione della legittimità di un determinato interesse dovrebbe essere il risultato di un'analisi effettuata sui singoli casi.

68. Come ricordato dall'EDPB nelle sue Linee guida sull'interesse legittimo[53], un interesse può essere considerato legittimo quando sono soddisfatti i seguenti tre criteri cumulativi:

    a. l'interesse è lecito[54];

---

[49] Ai sensi dell'articolo 21 del RGPD, se un interessato si oppone, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, il titolare del trattamento si astiene dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Pertanto, i due aspetti di cui le AC devono tenere conto sono se il titolare del trattamento sia in grado di dimostrare tali motivi legittimi, cogenti e prevalenti e se possa essere esercitato il diritto di opposizione.

[50] CGUE, sentenza del 4 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punto 106; CGUE, sentenza dell'11 dicembre 2019, causa C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), punto 40. Cfr. anche le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 12 e segg. Come ricordato nelle Linee guida, questa «*valutazione dovrebbe essere effettuata all'inizio del trattamento, con il coinvolgimento del responsabile della protezione dei dati (RPD) (se designato), e dovrebbe essere documentata dal titolare del trattamento in linea con il principio di responsabilità di cui all'articolo 5, paragrafo 2 del RGPD*».

[51] Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 14.

[52] Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 16.

[53] Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 17.

[54] CGUE, sentenza del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punto 49, in cui la CGUE ha sottolineato che un interesse legittimo non può essere contrario alla legge. A tale riguardo, l'EDPB sottolinea che, a seconda dei casi, nel valutare la legittimità di un determinato interesse occorre tener conto dei quadri normativi. Cfr. ad esempio: Articolo 26, paragrafo 3, e articolo 28 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022,

b. l'interesse è articolato in modo chiaro e preciso; e,

c. l'interesse è reale e presente, non speculativo.

69. Subordinatamente alle altre due fasi richieste per la valutazione dell'interesse legittimo, gli esempi riportati di seguito possono costituire un interesse legittimo nel contesto dei modelli di IA: (i) sviluppare un servizio di un agente conversazionale per l'assistenza agli utenti; (ii) sviluppare un sistema di IA per il riconoscimento di contenuti o comportamenti fraudolenti; e (iii) migliorare il rilevamento delle minacce in un sistema informatico.

3.3.2.2 Seconda fase – Analisi della necessità del trattamento per il perseguimento dell'interesse legittimo

70. La seconda fase della valutazione consiste nel determinare se il trattamento dei dati personali sia necessario ai fini del legittimo interesse o dei legittimi interessi perseguiti[55] («test di necessità»).

71. Il considerando 39 del RGPD, chiarisce che *«I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.»* Secondo la CGUE e le precedenti indicazioni dell'EDPB, la condizione relativa alla necessità del trattamento dovrebbe essere esaminata alla luce dei diritti e delle libertà fondamentali degli interessati e in relazione al principio di minimizzazione dei dati sancito dall'articolo 5, paragrafo 1, lettera c) del RGPD[56].

72. La metodologia a cui fa riferimento la CGUE tiene conto del contesto del trattamento, nonché degli effetti sul titolare del trattamento e sugli interessati. La valutazione della necessità comporta,

relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) per quanto riguarda il divieto di pubblicità mirata rivolta ai minori; articolo 5, paragrafi 1 e 2 del regolamento sull'IA sulle pratiche di IA vietate (pratiche di manipolazione e al di sotto della soglia di consapevolezza); trattamento in violazione dei diritti di proprietà intellettuale e delle disposizioni della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale.

[55] Linee guida EDPB 1/2024 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punti 28-30.

[56] CGUE, sentenza del 4 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punti 108 e 109, con riferimento anche a CGUE, sentenza dell'11 dicembre 2019, causa C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), punto 48; CGUE, sentenza del 9 novembre 2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke (ECLI:UE:C:2010:662), punti 85 e 86; CGUE, sentenza del 22 giugno 2021, causa C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), punti 98, 109, 110, 113. Cfr. anche ad esempio: Linee guida 3/2019 dell'EDPB sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, adottate il 29 gennaio 2020, punti 24-26 e 73; Linee guida 2/2019 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera b) del RGPD nel contesto della fornitura di servizi *online* agli interessati, versione 2.0, adottate l'8 ottobre 2019, punti 23-25; Parere dell'EDPB 11/2024 sull'uso del riconoscimento facciale per snellire il flusso dei passeggeri in aeroporto, versione 1.1, adottato il 23 maggio 2024, punto 27.

pertanto, due elementi: i) se l'attività di trattamento consenta il perseguimento della finalità[57]; e ii) se non vi sia un modo meno invasivo per perseguire tale finalità[58].

73. Ad esempio, e a seconda dei casi, occorre valutare il volume previsto di dati personali coinvolti nel modello di IA alla luce di alternative meno invasive che possono essere ragionevolmente disponibili per conseguire, con la stessa efficacia, la finalità dell'interesse legittimo perseguito. Se il perseguimento della finalità è possibile anche attraverso un modello di IA che non comporta il trattamento di dati personali, il trattamento dei dati personali dovrebbe essere considerato non necessario. Ciò è particolarmente importante ai fini dello sviluppo dei modelli di IA. Nel valutare se la condizione di necessità sia soddisfatta, le AC dovrebbero prestare particolare attenzione alla quantità di dati personali trattati e alla proporzionalità del perseguimento dell'interesse legittimo in questione, anche alla luce del principio di minimizzazione dei dati.

74. La valutazione della necessità dovrebbe anche tener conto del contesto più ampio del trattamento dei dati personali che si intende effettuare. L'esistenza di mezzi meno invasivi per i diritti e le libertà fondamentali degli interessati può variare a seconda che il titolare del trattamento abbia un rapporto diretto con gli interessati (dati di prima parte) o meno (dati di terza parte). La CGUE ha offerto alcune considerazioni di cui tener conto nell'analizzare la necessità del trattamento dei dati di prima parte ai fini del legittimo interesse o dei legittimi interessi perseguiti (sebbene nell'ambito della comunicazione di tali dati a terzi)[59].

75. Anche l'attuazione di garanzie tecniche per la protezione dei dati personali può contribuire a soddisfare la condizione di necessità. Ciò potrebbe includere, ad esempio, misure attuative come quelle di cui alla sezione 3.2.2 che comportano l'anonimizzazione, ma che limitano comunque la facilità con cui gli interessati possono essere identificati. L'EDPB osserva che alcune di queste misure, ove non siano necessarie per conformarsi al RGPD, possono costituire garanzie supplementari, come ulteriormente analizzato nella sottosezione «misure di attenuazione» della sezione 3.3.2.3[60].

---

[57] Cfr. CGUE, sentenza del 16 dicembre 2008, causa C-524/06, *Heinz Huber c. Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), punto 66. Anche nella stessa causa, cfr. le conclusioni dell'avvocato generale Poiares Maduro nella causa C-524/06, *Heinz Huber/Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), punto 16, secondo cui: «*Il criterio adeguato [è] quello dell'efficacia e spetta al giudice nazionale applicarlo. La domanda che esso deve porsi è se le autorità competenti in materia di immigrazione possano dare attuazione alle norme relative al diritto di soggiorno con altre modalità di trattamento dei dati. In caso di soluzione affermativa, la registrazione e il trattamento centralizzato dei dati relativi ai cittadini dell'Unione andrebbero dichiarati illegittimi. Non occorre che il sistema alternativo sia il più efficace o appropriato; è sufficiente che esso funzioni adeguatamente. In altre parole, anche se un registro centrale è più efficace, funzionale o maneggevole dei sistemi alternativi (come i registri decentralizzati, locali), devono essere preferiti i secondi se sono sufficienti per conoscere lo status di residenza dei cittadini dell'Unione.*»

[58] Cfr. CGUE, sentenza del 27 settembre 2017, causa C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), punto 113: «*Spetta al giudice del rinvio verificare se la redazione dell'elenco controverso e l'iscrizione in quest'ultimo del nome delle persone interessate siano atte a conseguire gli obiettivi perseguiti dalle stesse e se non sussistano altri mezzi meno restrittivi per raggiungere tali obiettivi.*»; cfr. anche, ad esempio, le conclusioni dell'avvocato generale Rantos nella causa C-252/21, *Meta c. Bundeskartellamt*, ECLI:EU:C:2022:704, punto 61, in cui si afferma che: «*[...] È quindi necessario che sussista uno stretto collegamento tra il trattamento e l'interesse perseguito, in assenza di alternative più rispettose della protezione dei dati personali, poiché non è sufficiente che il trattamento sia di mera utilità per il titolare del trattamento.*»

[59] CGUE, sentenza del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punti 51-53.

[60] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali 00ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 57.

3.3.2.3 Terza fase - Test di bilanciamento

76. La terza fase della valutazione dell'interesse legittimo è l'«**esercizio di bilanciamento**» (denominato anche «**test di bilanciamento**» nel presente documento)[61]. Questa fase prevede l'individuazione e la descrizione dei diversi diritti e interessi contrapposti in gioco[62], vale a dire, da un lato, gli interessi, i diritti e le libertà fondamentali degli interessati e, dall'altro, gli interessi del titolare del trattamento o di terzi. Pertanto, per dimostrare che l'interesse legittimo costituisce una base giuridica adeguata per le attività di trattamento in questione, bisognerebbe considerare le circostanze specifiche del caso [63].

Interessi, diritti e libertà fondamentali degli interessati

77. L'articolo 6, paragrafo 1, lettera f) del RGPD stabilisce che, nel valutare le diverse componenti nell'ambito della verifica del bilanciamento, il titolare del trattamento deve tenere conto degli interessi, dei diritti e delle libertà fondamentali degli interessati. Gli interessi degli interessati sono quelli sui quali può incidere il trattamento in questione. Durante la fase di sviluppo di un modello di IA, questi possono includere, a titolo esemplificativo ma non esaustivo, l'interesse all'autodeterminazione e alla conservazione del controllo sui propri dati personali (ad esempio, i dati raccolti per lo sviluppo del modello). Nella fase di diffusione di un modello di IA, gli interessi degli interessati possono includere, tra l'altro, l'interesse a mantenere il controllo sui propri dati personali (ad esempio, i dati trattati dopo la diffusione del modello), gli interessi finanziari (ad esempio, quando un modello di IA è utilizzato dall'interessato per generare introiti, oppure viene utilizzato da una persona nell'ambito della sua attività professionale), i vantaggi personali (ad esempio, quando un modello di IA è utilizzato per migliorare l'accessibilità a determinati servizi) o gli interessi socioeconomici (ad esempio, quando un modello di IA consente l'accesso ad una migliore assistenza sanitaria o facilita l'esercizio di un diritto fondamentale come l'accesso all'istruzione)[64].

78. Quanto più precisamente un interesse è definito in base alla finalità prevista del trattamento, tanto più esso consentirà di comprendere chiaramente la realtà dei vantaggi e dei rischi di cui tener conto durante il test di bilanciamento.

79. In relazione ai diritti e alle libertà fondamentali degli interessati, lo sviluppo e la diffusione di modelli di IA possono comportare gravi rischi per i diritti tutelati dalla Carta dei diritti fondamentali dell'Unione europea (la «**Carta dell'UE**»), tra cui, a titolo esemplificativo ma non esaustivo, il diritto al rispetto della vita privata e familiare (articolo 7 della Carta dell'UE) e il diritto alla protezione dei dati personali (articolo 8 della Carta dell'UE). Questi rischi possono verificarsi durante la fase di sviluppo, ad esempio nel caso in cui i dati personali vengano estratti contro la volontà degli interessati o a loro insaputa. I rischi possono verificarsi anche nella fase di diffusione, ad esempio quando i dati personali vengono trattati dal modello (o nell'ambito dello stesso) secondo una modalità che viola i diritti degli interessati, o quando è possibile inferire, accidentalmente o tramite attacchi (ad esempio, inferenza di appartenenza, estrazione o inversione del modello), i dati personali contenuti nel *database* di apprendimento. Tali situazioni comportano un rischio per la *privacy* degli interessati i cui dati

[61] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punti 31-60.
[62] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 32.
[63] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 32, che fanno riferimento anche alla sentenza CGUE del 4 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punto 110.
[64] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 38.

potrebbero comparire nella fase di diffusione del sistema di IA (ad esempio, rischio reputazionale, furto di identità o frode, rischio per la sicurezza a seconda della natura dei dati).

80. A seconda del caso in esame, possono sussistere rischi anche per altri diritti fondamentali. Ad esempio, la raccolta indiscriminata di dati su larga scala da parte di modelli di IA nella fase di sviluppo può generare una sensazione di sorveglianza negli interessati, soprattutto in considerazione delle difficoltà per impedire lo *scraping* dei dati pubblici. Ciò può indurre le persone ad autocensurarsi con il rischio di compromettere la loro libertà di espressione (articolo 11 della Carta dell'UE). Nella fase di diffusione, sono presenti rischi per la libertà di espressione anche quando i modelli di IA vengono utilizzati per bloccare la pubblicazione di contenuti da parte degli interessati. Inoltre, un modello di IA che suggerisce contenuti inappropriati a persone vulnerabili può comportare rischi per la loro salute mentale (articolo 3, paragrafo 1 della Carta dell'UE). In altri casi, la diffusione di modelli di IA può anche portare a conseguenze negative sul diritto dell'individuo di lavorare (articolo 15 della Carta dell'UE), ad esempio quando si affida ad un modello di IA la preselezione delle domande per un posto di lavoro. Analogamente, un modello di IA potrebbe comportare rischi per il diritto alla non discriminazione (articolo 21 della Carta dell'UE), ove discriminasse gli individui sulla base di determinate caratteristiche personali (come la nazionalità o il genere). Inoltre, l'impiego di modelli di IA può presentare rischi per la sicurezza e l'incolumità dell'individuo (ad esempio, se il modello di IA viene utilizzato con intenzioni malevole), nonché rischi per la sua integrità fisica e mentale[65].

81. La diffusione dei modelli di IA può anche avere un impatto positivo su alcuni diritti fondamentali, ad esempio il modello può sostenere il diritto all'integrità psichica della persona (articolo 3 della Carta), come nel caso di un modello di IA utilizzato per individuare contenuti dannosi *online*; o quando il modello facilita l'accesso a determinati servizi essenziali o agevola l'esercizio di diritti fondamentali, come l'accesso alle informazioni (articolo 11 della Carta UE) o l'accesso all'istruzione (articolo 14 della Carta dell'UE).

Impatto del trattamento sugli interessati

82. Il trattamento dei dati personali che avviene durante lo sviluppo e la diffusione dei modelli di IA può avere un impatto diverso sugli interessati, sia positivo che negativo[66]. Ad esempio, se un'attività di trattamento comporta vantaggi per l'interessato, tali vantaggi possono essere considerati nella verifica del bilanciamento. Anche se l'esistenza di tali vantaggi può portare un'AC a concludere che sugli interessi del titolare del trattamento o di un terzo non prevalgono gli interessi, i diritti e le libertà fondamentali degli interessati, tale conclusione può essere tratta solo a seguito di un'analisi effettuata caso per caso che tenga conto di tutti i fattori rilevanti.

83. L'impatto del trattamento sugli interessati può essere influenzato (i) dalla natura dei dati trattati dai modelli, (ii) dal contesto del trattamento e (iii) dalle ulteriori conseguenze che il trattamento può avere[67].

84. Relativamente alla **natura dei dati trattati**, è opportuno rammentare che – a parte le categorie particolari di dati personali e i dati relativi a condanne penali e reati che godono rispettivamente di una ulteriore protezione ai sensi degli articoli 9 e 10 del RGPD – il trattamento di alcune altre categorie di dati personali può determinare conseguenze significative sugli interessati. In tale contesto, il

[65] Linee guida 1/2024 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 46.
[66] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 39.
[67] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 32.

trattamento di alcuni tipi di dati personali che rivelano informazioni altamente private (ad esempio dati finanziari o dati di localizzazione) per lo sviluppo e la diffusione di un modello di IA, dovrebbe essere considerato potenzialmente in grado di produrre un impatto significativo sugli interessati. Nella fase di diffusione, le conseguenze di tale trattamento sugli interessati possono essere di natura economica (ad esempio, discriminazione nel contesto lavorativo) e/o reputazionale (ad esempio, diffamazione).

85. In relazione al **contesto del trattamento,** occorre innanzitutto individuare gli elementi che potrebbero far insorgere rischi per gli interessati (ad esempio, le modalità di sviluppo e diffusione del modello, e/o se le misure di sicurezza utilizzate per proteggere i dati personali sono adeguate). La natura del modello e gli utilizzi operativi a cui è destinato svolgono un ruolo fondamentale nell'identificazione di queste potenziali cause.

86. Occorre inoltre valutare la gravità di tali rischi per gli interessati. Si può considerare, tra l'altro, il modo in cui i dati personali sono trattati (ad esempio, se sono combinati con altri insiemi di dati), la portata del trattamento e la quantità di dati personali trattati[68] (il volume complessivo dei dati, il volume dei dati per interessato, il numero di interessati)[69], lo status dell'interessato (bambini o altri interessati vulnerabili) e il rapporto con il titolare del trattamento (se l'interessato è un cliente). Ad esempio, l'uso del *web scraping* nella fase di sviluppo può portare – in assenza di sufficienti garanzie – a conseguenze significative sulle persone, per via dell'ingente volume di dati raccolti, dell'elevato numero di interessati e della raccolta indiscriminata di dati personali.

87. Nel valutare l'impatto del trattamento sugli interessati occorre prendere in considerazione anche le **ulteriori conseguenze** che il trattamento può avere. Esse dovrebbero essere valutate dalle AC caso per caso, tenendo conto degli specifici fatti in esame.

88. Tra le conseguenze figurano (a titolo esemplificativo ma non esaustivo) i rischi di violazione dei diritti fondamentali degli interessati, come descritto nella sottosezione precedente[70]. I rischi possono variare in termini di verosimiglianza e gravità e possono derivare da un trattamento dei dati personali che potrebbe causare danni fisici, materiali o immateriali, in particolare qualora il trattamento possa dar luogo a discriminazione[71].

89. Quando la diffusione di un modello di IA comporta il trattamento dei dati personali sia di (i) soggetti i cui dati personali sono inclusi nel set di dati utilizzati nella fase di sviluppo; sia di (ii) soggetti i cui dati personali sono trattati nella fase di diffusione, le AC, nel verificare il bilanciamento effettuato da un titolare del trattamento, devono distinguere e considerare i rischi che incidono sugli interessi, i diritti e le libertà di ciascuna di queste categorie di soggetti.

90. **Infine, l'analisi delle possibili ulteriori conseguenze del trattamento dovrebbe anche prendere in considerazione la probabilità che queste ulteriori conseguenze si concretizzino**. La valutazione di tale probabilità deve essere effettuata tenendo conto delle misure tecniche e organizzative in atto e delle circostanze specifiche del caso. Ad esempio, le AC possono valutare se siano state adottate misure per evitare un potenziale uso improprio del modello di IA. Per i modelli di IA destinati ad una varietà di scopi, come l'IA generativa, ciò può includere controlli volti a limitare il più possibile il loro utilizzo per

[68] Cfr. le Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 43.
[69] CGUE, sentenza del 4 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punto 116.
[70] Cfr. la precedente sottosezione «Interessi, diritti e libertà fondamentali degli interessati».
[71] Cfr. la sezione 2.3 delle Linee guida 1/2024 dell'EDPB sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024. Cfr. anche il considerando 75 del RGPD per ulteriori esempi.

pratiche dannose, ad esempio: la creazione di *deepfake*; *chatbot* utilizzati per la disinformazione, *phishing* e altri tipi di frode; e IA manipolativa/agenti IA (in particolare quando sono antropomorfi o forniscono informazioni fuorvianti).

Ragionevoli aspettative degli interessati

91. Sulla base del considerando 47 del RGPD, *«In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali.»*[72]

92. Le ragionevoli aspettative svolgono un ruolo fondamentale nella valutazione del bilanciamento, non da ultimo per via della complessità della tecnologia utilizzata nei modelli di IA e per il fatto che può essere difficile per gli interessati comprendere la varietà dei potenziali utilizzi di un modello di IA e il trattamento dei dati che ne consegue[73]. A tal fine, è possibile prendere in considerazione le informazioni fornite agli interessati per valutare se questi possano ragionevolmente aspettarsi che vi sia un trattamento dei loro dati personali. Tuttavia, sebbene l'omissione di informazioni possa contribuire a far sì che gli interessati non si aspettino un determinato trattamento, il mero adempimento degli obblighi di trasparenza di cui al RGPD non è di per sé sufficiente a ritenere che gli interessati possano ragionevolmente aspettarsi un determinato trattamento[74]. Inoltre, il semplice fatto che le informazioni relative alla fase di sviluppo di un modello di IA siano riportate nell'informativa *privacy* del titolare del trattamento, non significa necessariamente che gli interessati possano ragionevolmente aspettarsi che ciò avvenga; piuttosto, questo dovrebbe essere analizzato dalle AC in base alle circostanze specifiche del caso e tenendo conto di tutti i fattori rilevanti.

93. Nel valutare le ragionevoli aspettative degli interessati in relazione al trattamento che ha luogo nella fase di sviluppo, è importante fare riferimento agli elementi citati nelle Linee guida dell'EDPB sul legittimo interesse[75]. Inoltre, con riferimento all'oggetto del presente Parere, è importante considerare il contesto più ampio del trattamento. Ciò può comprendere, ma non solo, il fatto che i dati personali siano pubblicamente disponibili o meno, la natura del rapporto tra l'interessato e il titolare del trattamento (e se esista un collegamento tra i due), la natura del servizio, il contesto in cui i dati personali sono stati raccolti, la fonte da cui i dati sono stati ottenuti (ad esempio, il sito web o il servizio in cui i dati personali sono stati raccolti e le relative impostazioni sulla *privacy*), i potenziali

[72] Cfr. anche CGUE, sentenza del 4 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punto 112; CGUE, sentenza dell'11 dicembre 2019, causa C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), punto 58; CGUE, sentenza del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punto 55.

[73] Ad esempio, nella sentenza del 4 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt* (ECLI:EU:C:2023:537), punto 123, la Corte di giustizia dell'Unione europea ha rilevato che, sebbene il «miglioramento del prodotto» non possa, in linea di principio, essere escluso come legittimo interesse, osserva altresì che «*appare dubbio che [...] l'obiettivo diretto al miglioramento del prodotto possa – tenuto conto della portata di tale trattamento e del suo notevole impatto sull'utente, nonché della circostanza che quest'ultimo non possa ragionevolmente attendersi che tali dati siano trattati [...] – prevalere sui diritti fondamentali e sugli interessi di detto utente, tanto più nel caso in cui quest'ultimo sia minorenne*».

[74] Linee guida 1/2024 sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 53.

[75] Linee guida 1/2024 sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punti 50-54.

ulteriori utilizzi del modello e il fatto che gli interessati siano effettivamente consapevoli che i loro dati personali sono accessibili *online*.

94. Nella fase di sviluppo del modello, le ragionevoli aspettative degli interessati possono variare a seconda che i dati trattati per sviluppare il modello siano resi pubblici o meno dagli interessati. Inoltre, le ragionevoli aspettative possono variare anche a seconda che essi abbiano fornito direttamente i dati al titolare del trattamento (ad esempio nel contesto di fruizione del servizio) o se il titolare del trattamento li abbia ottenuti da un'altra fonte (ad esempio tramite terzi o attività di *scraping*). In entrambi i casi, al momento di valutare le ragionevoli aspettative, occorre tener conto delle misure adottate per informare gli interessati delle attività di trattamento.

95. Nella fase di diffusione del modello di IA, è altrettanto importante considerare le ragionevoli aspettative degli interessati in relazione alle capacità specifiche del modello. Ad esempio, per i modelli di IA in grado di adattarsi in base agli *input* forniti, può essere importante considerare se gli interessati siano consapevoli di aver fornito dati personali in modo che il modello di IA possa adattare le risposte alle loro esigenze e, in tal modo, ottenere servizi personalizzati. Inoltre, può essere importante considerare se questa attività di trattamento produce un impatto solo sul servizio fornito agli interessati (ad esempio, la personalizzazione dei contenuti per un utente specifico) o se possa essere utilizzata per modificare il servizio erogato a tutti i clienti (ad esempio, per migliorare il modello in generale). Come per la fase di sviluppo, può essere particolarmente importante valutare se vi sia un legame diretto tra gli interessati e il titolare del trattamento. Tale collegamento diretto può, ad esempio, consentire al titolare del trattamento di fornire facilmente agli interessati informazioni sull'attività di trattamento e sul modello, cosa che potrebbe influenzare le ragionevoli aspettative degli interessati.

Misure di attenuazione

96. Quando gli interessi, i diritti e le libertà degli interessati sembrano prevalere sull'interesse o sugli interessi legittimi perseguiti dal titolare del trattamento o da terzi, il titolare del trattamento può prendere in considerazione l'introduzione di misure di attenuazione per limitare l'impatto del trattamento sugli interessati. Le misure di attenuazione sono garanzie che dovrebbero essere adattate alle circostanze del caso e dipendono da diversi fattori, tra cui l'utilizzo a cui è destinato il modello di IA. Tali misure di attenuazione mirano a garantire che possano continuare a prevalere gli interessi del titolare del trattamento o di terzi, in modo tale che il titolare del trattamento possa avvalersi di tale base giuridica.

97. Come ricordato nelle Linee guida dell'EDPB sul legittimo interesse, le misure di attenuazione non devono essere confuse con le misure che il titolare del trattamento è comunque tenuto ad adottare per legge per garantire il rispetto del RGPD, indipendentemente dal fatto che il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del RGPD[76]. Ciò è particolarmente importante per le misure che, ad esempio, prevedono il rispetto dei principi del RGPD, come il principio di minimizzazione dei dati.

98. L'elenco delle misure riportato di seguito non è esaustivo né prescrittivo e la loro attuazione dovrebbe essere considerata valutando i singoli casi. Sebbene, a seconda delle circostanze, alcune delle misure riportate di seguito siano necessarie per adempiere a specifici obblighi del RGPD, qualora ciò non avvenga, possono essere prese in considerazione come ulteriori garanzie. Inoltre, alcune delle misure menzionate di seguito si riferiscono a settori soggetti a rapida evoluzione e in continuo sviluppo e dovrebbero essere valutate dalle AC nell'esame di un caso specifico.

[76] Linee guida 1/2024 sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f) del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 57.

99. **In relazione alla fase di sviluppo dei modelli di IA**, possono essere adottate diverse misure per attenuare i rischi derivanti dal trattamento dei dati di prima e di terza parte (anche per ridurre i rischi legati alle pratiche di *web scraping*). Sulla base di quanto sopra, l'EDPB fornisce alcuni esempi di misure che possono essere adottate per mitigare i rischi identificati attraverso il test di bilanciamento e che dovrebbero essere prese in considerazione dalle AC nella valutazione di specifici modelli di IA in base al singolo caso.

100. **Misure tecniche**

a. Le misure di cui alla sezione 3.2.2, idonee a mitigare i rischi in questione, laddove tali misure non comportino l'anonimizzazione del modello e non siano richieste per ottemperare ad altri obblighi del RGPD o tenendo conto del test di necessità (seconda fase della valutazione del legittimo interesse).

101. Oltre a queste misure, si possono valutare altre misure pertinenti, quali:

b. misure di pseudonimizzazione: tra cui, ad esempio, misure atte a prevenire qualsiasi combinazione di dati basati su identificativi individuali. Queste misure possono non risultare appropriate ove l'AC ritenga che il titolare del trattamento abbia dimostrato la ragionevole necessità di raccogliere dati diversi su un determinato soggetto per lo sviluppo del sistema o del modello di IA in questione.

c. misure per mascherare i dati personali o sostituirli con dati personali falsi all'interno del *dataset* di addestramento (ad esempio la sostituzione di nomi e indirizzi di posta elettronica con nomi e indirizzi di posta elettronica falsi). Questa misura può rivelarsi particolarmente appropriata quando l'effettivo contenuto sostanziale dei dati non è rilevante ai fini del trattamento complessivo (ad esempio nell'addestramento dei modelli LLM).

102. **Misure che facilitano l'esercizio dei diritti individuali**

a. Osservare un periodo di tempo ragionevole tra la raccolta di un insieme di addestramento e il suo utilizzo. Questa ulteriore garanzia supplementare può consentire agli interessati di esercitare i propri diritti durante detto periodo che viene valutato in base alle circostanze di ciascun caso.

b. Proporre, fin dall'inizio, la possibilità di «opposizione» incondizionata, ad esempio prevedendo per gli interessati un diritto discrezionale di opposizione prima che il trattamento abbia luogo, al fine di rafforzare il controllo che le persone hanno sui propri dati, che va al di là delle condizioni di cui all'articolo 21 del RGPD[77].

c. Consentire agli interessati di esercitare il diritto alla cancellazione anche quando non si applicano le circostanze specifiche di cui all'articolo 17, paragrafo 1 del RGPD[78].

d. Consentire agli interessati di presentare segnalazioni di rigurgito o memorizzazione dei dati personali e le circostanze e i mezzi con i quali tali segnalazioni possono essere riprodotte, consentendo ai titolari del trattamento di riprodurre e valutare adeguate tecniche di disapprendimento per farvi fronte.

103. **Misure di trasparenza:** in alcuni casi, le misure di attenuazione potrebbero includere misure che garantiscono maggiore trasparenza nello sviluppo del modello di IA. Alcune misure, oltre al rispetto

[77] Ibidem.
[78] Ibidem.

degli obblighi previsti dal RGPD, possono contribuire a superare l'asimmetria informativa consentendo agli interessati di comprendere meglio il trattamento effettuato nella fase di sviluppo:

a. Diffusione di comunicazioni pubbliche e facilmente accessibili che vanno oltre le informazioni richieste dall'articolo 13 e 14 del RGPD, ad esempio dettagli ulteriori sui criteri di raccolta e su tutti i *dataset* utilizzati, tenendo conto della speciale protezione riservata a minori e persone vulnerabili;

b. Forme alternative di informazione degli interessati, ad esempio: campagne mediatiche per informare gli interessati attraverso mezzi di comunicazione diversi, campagne informative via e-mail, uso di visualizzazioni grafiche, FAQ, etichette di trasparenza e *model cards* la cui sistematizzazione potrebbe strutturare la presentazione delle informazioni sui modelli di IA, oltre a rapporti annuali volontari sulla trasparenza.

104. **Misure di attenuazione specifiche nel contesto del *web scraping*:** poiché, come già detto, il *web scraping* comporta rischi specifici[79], potrebbero essere individuate, in questo contesto, misure di attuazione specifiche. Ove opportuno, tali misure possono essere prese in considerazione dalle AC, in aggiunta alle misure di attenuazione di cui sopra, nel caso di attività di indagine nei confronti di titolari del trattamento che effettuano *web scraping*.

105. Ove non necessarie ai fini della seconda fase della valutazione del legittimo interesse, alcune misure specifiche possono rivelarsi utili per l'attenuazione del rischio associato al *web scraping*. Tra queste misure possono rientrare **misure tecniche**, quali:

a. Escludere dai contenuti pubblicati i dati che potrebbero contenere informazioni personali che comportano rischi per determinate persone o gruppi di persone (ad esempio persone che potrebbero essere vittime di abusi, pregiudizi o addirittura danni fisici in caso di divulgazione pubblica delle informazioni);

b. Assicurare che non siano raccolte determinate categorie di dati e che siano escluse dalla raccolta dei dati determinate fonti; ad esempio, alcuni siti web ritenuti particolarmente invasivi a causa della sensibilità del contenuto trattato;

c. Escludere la raccolta da siti web (o sezioni di siti web) che si oppongono chiaramente al *web scraping* e al riuso dei contenuti per la creazione di *database* per l'addestramento dell'IA (ad esempio, rispettando i file robots.txt o ai.txt o qualsiasi altro meccanismo riconosciuto per esprimere l'esclusione dal *crawling* e dallo *scraping* automatizzato);

d. Imporre altre opportune limitazioni alla raccolta, eventualmente includendo criteri basati su tempo e durata.

106. Nel contesto del *web scraping*, tra gli esempi di misure specifiche **che favoriscono l'esercizio dei diritti delle persone e la trasparenza** possono rientrare: la creazione di una lista di opposizione, gestita dal titolare del trattamento, che consente agli interessati di opporsi alla raccolta dei loro dati su

[79] Queste pratiche possono anche sollevare ulteriori questioni che non sono trattate nel presente Parere, cfr. ad esempio Pagallo U., Ciani Sciolla J., *Anatomia of web data scraping: ethics, standards, and the trouble of the law*. European Journal of Privacy Law & Technologies, (2023) 2, pagg. 1-19, disponibile all'indirizzo: https://doi.org/10.57230/EJPLT232PS.

determinati siti web o piattaforme *online* che forniscono informazioni che li identificano sugli stessi siti web, anche prima che la raccolta dei dati abbia luogo[80].

107. **Considerazioni specifiche sulle misure di attenuazione nella fase di diffusione:** sebbene alcune delle misure precedenti possano essere valide anche per la fase di diffusione, l'EDPB fornisce di seguito un elenco non esaustivo di ulteriori misure di sostegno che possono essere adottate e che dovrebbero essere valutate dalle AC caso per caso a seconda delle circostanze.

    a. **Misure tecniche** che possono essere messe in atto, ad esempio, per impedire la memorizzazione, il rigurgito o la generazione di dati personali, in particolare nell'ambito dei modelli di IA generativa (come i filtri in uscita), e/o per mitigare il rischio di riuso illecito da parte di modelli di IA generici (ad esempio, la filigrana digitale dei risultati generati dall'IA).

    b. **Misure che facilitano o accelerano l'esercizio dei diritti degli individui** nella fase di diffusione del modello, al di là di quanto previsto per legge, e relativamente, in particolare, ma non solo, all'esercizio del diritto alla cancellazione dei dati personali dai dati di *output* del modello, la deduplicazione e le tecniche post-addestramento che tentano di rimuovere o eliminare i dati personali.

108. Quando le AC analizzano la diffusione di uno specifico modello di IA, queste dovrebbero verificare se il titolare del trattamento ha pubblicato il test di bilanciamento condotto, dal momento che ciò potrebbe aumentare la trasparenza e l'equità. Come indicato nelle Linee guida dell'EDPB sul legittimo interesse, si possono prendere in considerazione altre misure per fornire agli interessati, prima di qualsiasi raccolta di dati personali, informazioni sulla verifica del bilanciamento[81]. L'EDPB ribadisce[82], inoltre, che un elemento da considerare è se il titolare del trattamento abbia coinvolto, ove possibile, il RPD.

3.4 Sul possibile impatto di un trattamento illecito nello sviluppo di un modello di IA sulla liceità del successivo trattamento o funzionamento del modello di IA

109. La presente sezione del Parere tratta il Quesito n. 4 della Richiesta. Il Quesito chiede chiarimenti sul possibile impatto di un trattamento illecito effettuato nella fase di sviluppo sul trattamento successivo (ad esempio nella fase di diffusione del modello di IA) o sul funzionamento del modello. Il Quesito intende esaminare sia la situazione in cui il modello di IA tratta dati personali conservati nel modello (Quesito n. 4, punto i), della Richiesta), sia la situazione in cui non viene effettuato alcun trattamento di dati personali nella fase di diffusione del modello di IA (ossia il modello è anonimo) (Quesito n. 4, punto ii), della Richiesta).

110. Prima di affrontare alcuni scenari specifici, l'EDPB esprime le seguenti considerazioni generali.

111. In primo luogo, i chiarimenti forniti in questa sezione si concentreranno sul trattamento dei dati personali effettuato nella fase di sviluppo in violazione del principio di liceità di cui all'articolo 5,

[80] Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
[81] Linee guida EDPB 1/2024 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 68.
[82] Linee guida EDPB 1/2024 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0, adottate l'8 ottobre 2024, punto 12.

paragrafo 1, lettera a) del RGPD e, più specificamente, articolo 6 RGPD (di seguito «**illiceità**»)[83]. Analogamente, le considerazioni dell'EDPB si concentreranno sull'impatto dell'illiceità del trattamento nella fase di sviluppo sulla liceità del successivo trattamento o funzionamento del modello (ossia il rispetto dell'articolo 5, paragrafo 1, lettera a) e dell'articolo 6 del RGPD). Tuttavia, l'EDPB evidenzia che il trattamento effettuato nella fase di sviluppo può anche comportare violazioni di altre disposizioni del RGPD, quali la mancanza di trasparenza nei confronti degli interessati o la protezione dei dati fin dalla progettazione e/o la protezione per impostazione predefinita, aspetti non analizzati nel presente Parere.

112. In secondo luogo, nell'affrontare tale questione, assume un ruolo fondamentale il principio di responsabilizzazione in base al quale i titolari del trattamento sono competenti per il rispetto, tra l'altro, dell'articolo 5, paragrafo 1 e dell'articolo 6 del RGPD[84], e in grado di comprovarlo. Ciò vale anche per la necessità di appurare quale organizzazione sia titolare del trattamento in essere e se si verifichino situazioni di contitolarità del trattamento (in quanto potrebbero essere strettamente collegate)[85]. Tenuto conto della rilevanza delle circostanze fattuali di ciascun caso, anche per quanto riguarda il ruolo svolto da ciascuna delle parti coinvolte nel trattamento, le considerazioni dell'EDPB vanno intese come osservazioni generali e valutate caso per caso dalle AC.

113. In terzo luogo, l'EDPB sottolinea che, ai sensi dell'articolo 51, paragrafo 1 del RGPD, le AC sono «*incaricate di controllare l'applicazione del [RGPD] al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione*». Rientra pertanto nella loro competenza valutare la liceità del trattamento ed esercitare i poteri loro conferiti dal RGPD in conformità con il rispettivo ordinamento nazionale[86]. In tali casi, le AC dispongono di poteri discrezionali per valutare le possibili violazioni e scegliere misure appropriate, necessarie e proporzionate, tra quelle di cui all'articolo 58 del RGPD, tenendo conto delle circostanze di ogni singolo caso[87].

114. **In caso di accertamento di una violazione, le AC possono imporre misure correttive, ad esempio ordinare ai titolari del trattamento, tenendo conto delle circostanze di ciascun caso, di adottare misure per porre rimedio all'illiceità del trattamento iniziale.** Tali misure possono includere, ad esempio, l'irrogazione di una sanzione amministrativa pecuniaria, l'imposizione di una limitazione provvisoria al trattamento, la cancellazione di parte dell'insieme di dati trattati illecitamente o, qualora ciò non sia possibile, a seconda delle circostanze, tenuto conto della proporzionalità della misura, l'ordine di cancellazione dell'intero *dataset* utilizzato per sviluppare il modello di IA e/o del modello di IA stesso. Nel valutare la proporzionalità della misura prevista, le AC possono prendere in

[83] CGUE, sentenza del 4 maggio 2023, causa C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), punti 55-57.

[84] CGUE, sentenza del 4 maggio 2023, causa C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), punto 53.

[85] Linee guida 07/2020 dell'EDPB sui concetti di titolare del trattamento e responsabile del trattamento di cui al RGPD, versione 2.1, adottate il 7 luglio 2021.

[86] Potrebbe essere necessario tenere conto di specifiche norme nazionali. Cfr. ad esempio l'Articolo 2-*decies* del Codice italiano in materia di protezione dei dati personali (Decreto Legislativo 196/2003) che stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati. Ciò non pregiudica altri ordinamenti giuridici nazionali, come le leggi penali.

[87] Cfr. a questo proposito il considerando 129 del RGPD, nonché CGUE, sentenza del 26 settembre 2024, causa C-768-21, T*R c. Land Hessen* (ECLI:EU:C:2024:785), punto 37; CGUE, sentenza del 7 dicembre 2023, nelle cause riunite C-26/22 e C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958), punto 57; e CGUE, sentenza del 14 marzo 2024, causa C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), punto 34.

considerazione le misure che il titolare del trattamento può adottare per porre rimedio all'illiceità del trattamento iniziale (ad esempio, effettuando un riaddestramento).

115. L'EDPB evidenzia inoltre che, quando i dati personali sono oggetto di trattamento illecito, gli interessati possono chiedere la cancellazione dei propri dati personali, fatte salve le condizioni di cui all'articolo 17 del RGPD, e le AC possono ordinare la cancellazione *ex officio* dei dati personali[88].

116. Nel valutare se una misura sia appropriata, necessaria e proporzionata, le AC possono prendere in considerazione, tra gli altri elementi, i rischi per gli interessati, la gravità della violazione, la fattibilità tecnica e finanziaria della misura, nonché il volume dei dati personali coinvolti.

117. Infine, l'EDPB ricorda che le misure adottate dalle AC a norma del RGPD non pregiudicano quelle adottate dalle autorità competenti in virtù del regolamento sull'IA e/o di altri quadri giuridici applicabili (ad esempio la disciplina sulla responsabilità civile).

118. Nelle sezioni successive, l'EDPB affronterà tre scenari evocati nel Quesito n. 4 della Richiesta, che si differenziano in base alla possibilità che i dati personali trattati per sviluppare il modello siano conservati nel modello e/o che il successivo trattamento sia effettuato dallo stesso titolare del trattamento o da un altro titolare del trattamento.

3.4.1 Scenario 1. Un titolare del trattamento effettua un trattamento illecito dei dati personali per sviluppare il modello, i dati personali sono conservati nel modello e sono successivamente trattati dallo stesso titolare del trattamento (ad esempio nella fase di diffusione del modello)

119. Questo scenario si riferisce al Quesito n. 4, punto i) della Richiesta, nella situazione in cui un titolare del trattamento tratta illecitamente dati personali (cioè in violazione dell'articolo 5, paragrafo 1, lettera a) e dell'articolo 6 del RGPD) per sviluppare un modello di IA, il modello di IA conserva informazioni relative a una persona fisica identificata o identificabile e quindi non è anonimo. I dati personali sono successivamente trattati dallo stesso titolare del trattamento (ad esempio nella fase di diffusione del modello). In relazione a questo scenario, l'EDPB formula le seguenti considerazioni.

120. Il potere dell'AC di imporre misure correttive al trattamento iniziale (come illustrato nei precedenti punti 113, 114 e 115) avrebbe, in linea di principio, un impatto sul successivo trattamento (ad esempio, se l'AC ordinasse al titolare del trattamento la cancellazione dei dati personali oggetto di trattamento illecito, tali misure correttive non consentirebbero a quest'ultimo di trattare successivamente i dati personali oggetto delle misure).

121. Con specifico riguardo all'impatto del trattamento illecito effettuato nella fase di sviluppo sul successivo trattamento (ad esempio nella fase di diffusione), l'EDPB rammenta che spetta alle AC condurre un'analisi caso per caso che tenga conto delle circostanze specifiche di ciascun caso.

122. **Occorre valutare di volta in volta, a seconda del contesto del caso, se le fasi di sviluppo e di diffusione comportino finalità distinte (costituendo così attività di trattamento separate) e la misura in cui l'assenza di una base giuridica per l'attività di trattamento iniziale incide sulla liceità del successivo trattamento.**

[88] A questo proposito, il parere 39/2021 dell'EDPB sull'eventualità che l'articolo 58, paragrafo 2, lettera g), del RGPD possa fungere da base giuridica per un'AC che ordini d'ufficio la cancellazione di dati personali in una situazione in cui tale richiesta non sia stata presentata dall'interessato, punto 28. Si veda anche, a questo proposito, CGUE, sentenza del 14 marzo 2024, causa C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), punto 42.

123. Ad esempio, con specifico riguardo alla base giuridica di cui all'articolo 6, paragrafo 1, lettera f) del RGPD, quando il trattamento successivo è basato su un interesse legittimo, il fatto che il trattamento iniziale fosse illecito dovrebbe essere preso in considerazione nella valutazione dell'interesse legittimo (ad esempio, in relazione ai rischi per gli interessati o al fatto che gli interessati potrebbero non aspettarsi tale trattamento successivo). In questi casi, l'illiceità del trattamento nella fase di sviluppo può incidere sulla liceità del trattamento successivo.

3.4.2 Scenario 2. Un titolare del trattamento effettua un trattamento illecito dei dati personali per sviluppare il modello, i dati personali sono conservati nel modello e sono trattati da un altro titolare del trattamento nella fase di diffusione del modello

124. Questo scenario si riferisce al Quesito n. 4, punto i) della Richiesta. Si differenzia dallo scenario 1 (di cui alla Sezione 3.4.1 del presente Parere) in quanto i dati personali vengono successivamente trattati da un altro titolare del trattamento in fase di diffusione del modello di IA.

125. L'EDPB rammenta che l'accertamento dei ruoli assegnati a questi diversi attori nell'ambito della disciplina della protezione dei dati costituisce un'attività imprescindibile per individuare quali siano gli obblighi derivanti dal RGPD e chi ne sia responsabile, e che occorre anche considerare le situazioni di contitolarità del trattamento nel valutare le responsabilità di ciascuna parte ai sensi del RGPD. Pertanto, le osservazioni che seguono devono essere considerate come elementi generali di cui le AC dovrebbero tener conto, ove pertinenti. In relazione a questo scenario 2, l'EDPB formula le seguenti considerazioni.

126. Innanzitutto, va ricordato che, ai sensi dell'articolo 5, paragrafo 1, lettera a) del RGPD, letto alla luce dell'articolo 5, paragrafo 2 dello stesso Regolamento, ogni titolare del trattamento deve garantire la liceità del trattamento che effettua ed essere in grado di comprovarla. Pertanto, le AC dovrebbero valutare la liceità del trattamento effettuato i) dal titolare del trattamento che ha originariamente sviluppato il modello di IA e ii) dal titolare del trattamento che ha acquisito il modello di IA e tratta i dati personali in autonomia.

127. In secondo luogo, le considerazione effettuate nei precedenti punti 113, 114, 115 assumono rilevanza nel caso di specie, per quanto riguarda il potere di intervento delle AC sul trattamento iniziale. L'articolo 17, paragrafo 1, lettera d) del RGPD (cancellazione dei dati trattati illecitamente) e l'articolo 19 del RGPD (obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento) possono, a seconda delle circostanze del caso, essere rilevanti anche in questo contesto, ad esempio relativamente alla notifica che il titolare del trattamento che sviluppa il modello deve effettuare nei confronti del titolare del trattamento che utilizza il modello.

128. In terzo luogo, per quanto riguarda il possibile impatto dell'illiceità del trattamento iniziale su quello successivo effettuato da un altro titolare del trattamento, tale valutazione dovrebbe essere effettuata dalle AC sui singoli casi.

129. **Al fine di accertare che il modello di IA non sia stato sviluppato attraverso un trattamento illecito di dati personali le AC dovrebbero verificare se il titolare del trattamento che utilizza il modello abbia effettuato una valutazione adeguata, nell'ambito dei suoi obblighi di responsabilizzazione[89], per dimostrare il rispetto dell'articolo 5, paragrafo 1, lettera a), e dell'articolo 6 del RGPD.** Attraverso tale valutazione le AC dovrebbero verificare se il titolare del trattamento ha valutato alcuni criteri non esaustivi, quali la fonte dei dati, e se il modello di IA comporta una violazione del RGPD, in particolare

[89] Articolo 5, paragrafo 2 del RGPD e articolo 24 del RGPD.

quando questa sia stata accertata da un'AC o in sede giurisdizionale, in modo che il titolare del trattamento che utilizza il modello non possa ignorare che il trattamento iniziale fosse illecito.

130. Il titolare del trattamento dovrebbe verificare, ad esempio, se i dati sono frutto di una violazione di dati personali o se sia stata rilevata una violazione nel trattamento da parte di un'AC o in sede giurisdizionale. **Il grado della valutazione del titolare del trattamento e il livello di dettaglio atteso dalle AC possono variare in base a diversi fattori, tra cui il tipo e il grado dei rischi associati al trattamento effettuato durante la fase di diffusione del modello di IA in relazione agli interessati i cui dati sono stati utilizzati per sviluppare il modello.**

131. L'EDPB osserva che il regolamento sull'IA impone ai fornitori di sistemi di IA ad alto rischio di redigere una dichiarazione di conformità UE[90] e che tale dichiarazione deve attestare che il sistema di IA in questione è conforme alla normativa UE in materia di protezione dei dati[91]. L'EDPB osserva che tale autodichiarazione non può costituire un accertamento definitivo di conformità al RGPD. Tuttavia, può essere presa in considerazione dalle AC nell'esame di uno specifico modello di IA.

132. Le stesse considerazioni di cui al precedente punto 123 sono rilevanti anche in questo caso. Quando le AC verificano se e in che modo il titolare del trattamento ha valutato l'adeguatezza dell'interesse legittimo come base giuridica per il trattamento effettuato dallo stesso, nella valutazione dell'interesse legittimo occorre prendere in considerazione l'illiceità del trattamento iniziale, ad esempio considerando i potenziali rischi a carico degli interessati i cui dati personali sono stati oggetto di trattamento illecito per lo sviluppo del modello. Nell'ambito del test di bilanciamento, occorre tenere in debita considerazione diversi aspetti, sia di natura tecnica (ad esempio, l'esistenza di filtri o limitazioni di accesso posti durante lo sviluppo del modello, che il successivo titolare del trattamento non può eludere o influenzare, e che potrebbero impedire l'accesso o la divulgazione dei dati personali), sia di natura giuridica (ad esempio, la natura e la gravità dell'illiceità del trattamento iniziale).

3.4.3 Scenario 3. Un titolare del trattamento effettua un trattamento illecito dei dati personali per sviluppare il modello, successivamente garantisce che il modello è anonimizzato, prima che lo stesso titolare, o un altro titolare del trattamento, avvii un ulteriore trattamento dei dati personali nella fase di diffusione

133. Questo scenario riguarda il Quesito n. 4, punto ii), della Richiesta e si riferisce al caso in cui un titolare del trattamento effettua un trattamento illecito dei dati personali per sviluppare il modello di IA, ma lo fa in modo da garantire che i dati personali siano resi anonimi, prima che lo stesso titolare del trattamento, o un altro titolare del trattamento, avvii un ulteriore trattamento di dati personali nella fase di diffusione. In primo luogo, l'EDPB ricorda che le AC hanno competenza e facoltà di intervenire in merito al trattamento correlato all'anonimizzazione del modello, nonché al trattamento effettuato durante la fase di sviluppo. Pertanto, le AC possono, a seconda delle circostanze specifiche del caso, imporre misure correttive sul trattamento iniziale (come illustrato nei precedenti punti 113, 114 e 115).

134. Ove sia possibile dimostrare che il successivo funzionamento del modello di IA non comporta un trattamento di dati personali, l'EDPB ritiene che non troverebbe applicazione il RGPD[92]. Pertanto, l'illiceità del trattamento iniziale non dovrebbe influire sul successivo funzionamento del modello. Tuttavia, l'EDPB sottolinea che una semplice affermazione di anonimità del modello non sia sufficiente

[90] Articolo 16, lettera g) e articolo 47 del regolamento sull'IA.
[91] Allegato V, punto 5 del regolamento sull'IA.
[92] Considerando 26 del RGPD.

per sottrarlo all'applicazione del RGPD e osserva che le AC dovrebbero valutarla tenendo conto, di volta in volta, delle considerazioni formulate dall'EDPB in risposta al Quesito n. 1 della Richiesta.

135. **Quando, in una fase successiva, i titolari del trattamento effettuano un trattamento dei dati personali raccolti durante la fase di diffusione, una volta anonimizzato il modello, a tali trattamenti si applicherebbe il RGPD. In questi casi, per quanto riguarda il RGPD, sulla liceità del trattamento effettuato nella fase di diffusione non dovrebbe incidere l'illiceità del trattamento iniziale.**

4 Osservazioni finali

136. Tutte le AC sono destinatarie del presente Parere che sarà reso pubblico ai sensi dell'articolo 64, paragrafo 5, lettera b) del RGPD.

Per il Comitato europeo per la protezione dei dati

La Presidente

Anu Talus