



17/IT

WP 251 rev.01

**Linee guida sul processo decisionale automatizzato relativo alle persone fisiche
e sulla profilazione
ai fini del regolamento 2016/679**

adottate il 3 ottobre 2017

Versione emendata e adottata in data 6 febbraio 2018

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito web: http://ec.europa.eu/justice/data-protection/index_en.htm

**IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL
TRATTAMENTO DEI DATI PERSONALI**

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

INDICE

I. INTRODUZIONE.....	5
II. DEFINIZIONI	6
A. PROFILAZIONE.....	7
B. PROCESSO DECISIONALE AUTOMATIZZATO	8
C. APPROCCIO DEL REGOLAMENTO A QUESTI CONCETTI	9
III. DISPOSIZIONI GENERALI SULLA PROFILAZIONE E SUL PROCESSO DECISIONALE AUTOMATIZZATO	10
A. PRINCIPI IN MATERIA DI PROTEZIONE DEI DATI.....	10
1. <i>Articolo 5, paragrafo 1, lettera a) - liceità, correttezza e trasparenza</i>	<i>10</i>
2. <i>Articolo 5, paragrafo 1, lettera b) - ulteriore trattamento e limitazione della finalità.....</i>	<i>12</i>
3. <i>Articolo 5, paragrafo 1, lettera c) - minimizzazione dei dati.....</i>	<i>12</i>
4. <i>Articolo 5, paragrafo 1, lettera d) - esattezza.....</i>	<i>13</i>
5. <i>Articolo 5, paragrafo 1, lettera e) - limitazione della conservazione.....</i>	<i>13</i>
B. BASI LEGITTIME PER IL TRATTAMENTO	14
1. <i>Articolo 6, paragrafo 1, lettera a) - consenso.....</i>	<i>14</i>
2. <i>Articolo 6, paragrafo 1, lettera b) – necessario all’esecuzione di un contratto.....</i>	<i>14</i>
3. <i>Articolo 6, paragrafo 1, lettera c) – necessario per adempiere un obbligo legale.....</i>	<i>15</i>
4. <i>Articolo 6, paragrafo 1, lettera d) – necessario per la salvaguardia di interessi vitali</i>	<i>15</i>
5. <i>Articolo 6, paragrafo 1, lettera e) – necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri.....</i>	<i>15</i>
6. <i>Articolo 6, paragrafo 1, lettera f) – necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi</i>	<i>16</i>
C. ARTICOLO 9 – CATEGORIE PARTICOLARI DI DATI	16
D. DIRITTI DELL’INTERESSATO.....	17
1. <i>Articoli 13 e 14 – diritto di essere informato</i>	<i>18</i>
2. <i>Articolo 15 – diritto di accesso.....</i>	<i>19</i>
3. <i>Articolo 16 – diritto di rettifica; articolo 17 – diritto alla cancellazione; articolo 18 – diritto di limitazione di trattamento</i>	<i>19</i>
4. <i>Articolo 21 – diritto di opposizione</i>	<i>20</i>
IV. DISPOSIZIONI SPECIFICHE RELATIVE A DECISIONI BASATE UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO DI CUI ALL’ARTICOLO 22	21
A. “DECISIONE BASATA UNICAMENTE SUL TRATTAMENTO AUTOMATIZZATO”	23
B. EFFETTI “GIURIDICI” O “IN MODO ANALOGO SIGNIFICATIVI”	23
C. ECCEZIONI AL DIVIETO.....	25
1. <i>Esecuzione di un contratto.....</i>	<i>26</i>

2.	<i>Autorizzato dal diritto dell'Unione o dello Stato membro</i>	26
3.	<i>Consenso esplicito</i>	27
D.	CATEGORIE PARTICOLARI DI DATI PERSONALI – ARTICOLO 22, PARAGRAFO 4.....	27
E.	DIRITTI DELL'INTERESSATO.....	27
1.	<i>Articolo 13, paragrafo 2, lettera f), e articolo 14, paragrafo 2, lettera g) - diritto di essere informato</i>	27
2.	<i>Articolo 15, paragrafo 1, lettera h) - diritto di accesso</i>	30
F.	STABILIRE GARANZIE ADEGUATE.....	30
V.	MINORI E PROFILAZIONE	31
VI.	VALUTAZIONI D'IMPATTO SULLA PROTEZIONE DEI DATI E RESPONSABILE DELLA PROTEZIONE DEI DATI	33
	ALLEGATO 1 - RACCOMANDAZIONI SULLE BUONE PRASSI	35
	ALLEGATO 2 – PRINCIPALI DISPOSIZIONI DEL REGOLAMENTO	37
	PRINCIPALI DISPOSIZIONI DEL REGOLAMENTO CHE FANNO RIFERIMENTO ALLA PROFILAZIONE E AL PROCESSO DECISIONALE AUTOMATIZZATO IN GENERALE	37
	PRINCIPALI DISPOSIZIONI DEL REGOLAMENTO CHE FANNO RIFERIMENTO AL PROCESSO DECISIONALE AUTOMATIZZATO DI CUI ALL'ARTICOLO 22.....	39
	ALLEGATO 3 - APPROFONDIMENTI	41

I. Introduzione

Il regolamento generale sulla protezione dei dati tratta in maniera specifica la profilazione e il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione¹.

La profilazione e il processo decisionale automatizzato sono utilizzati in un numero crescente di settori, tanto privati quanto pubblici. Banche e finanza, assistenza sanitaria, fiscalità, assicurazioni, marketing e pubblicità sono soltanto alcuni esempi dei settori nei quali la profilazione viene effettuata con maggiore regolarità a sostegno del processo decisionale.

I progressi tecnologici e le capacità in materia di analisi dei megadati (*big data*), intelligenza artificiale e apprendimento automatico hanno reso più facile la creazione di profili e l'adozione di decisioni automatizzate, con potenziali ripercussioni significative sui diritti e sulle libertà delle persone fisiche.

La diffusa disponibilità di dati personali su Internet e di quelli ricavabili dai dispositivi di Internet delle cose, associata alla capacità di trovare correlazioni e creare collegamenti, può consentire la determinazione, l'analisi e la previsione di aspetti della personalità, del comportamento, degli interessi e delle abitudini di una persona.

La profilazione e il processo decisionale automatizzato possono essere utili per le persone fisiche e le organizzazioni, offrendo loro vantaggi quali:

- miglioramenti dell'efficienza;
- risparmi di risorse.

Presentano inoltre numerose applicazioni commerciali: ad esempio, possono essere utilizzati per segmentare meglio i mercati e personalizzare i servizi e i prodotti allineandoli alle singole esigenze. Anche la medicina, l'istruzione, l'assistenza sanitaria e i trasporti possono beneficiare di questi processi.

Tuttavia, la profilazione e il processo decisionale automatizzato possono comportare rischi significativi per i diritti e le libertà delle persone fisiche, che richiedono garanzie adeguate.

Questi processi possono essere poco trasparenti. Le persone fisiche potrebbero non sapere di essere profilate o non comprenderne le conseguenze.

¹ 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. La profilazione e il processo decisionale automatizzato relativo alle persone fisiche sono disciplinati anche dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Sebbene si concentrino sulla profilazione e sul processo decisionale automatizzato relativo alle persone fisiche ai sensi del regolamento generale sulla protezione dei dati, le presenti linee guida sono rilevanti anche per quanto riguarda le disposizioni analoghe su questi due temi contenute nella direttiva 2016/680. Le caratteristiche specifiche della profilazione e del processo decisionale automatizzato relativo alle persone fisiche ai sensi della direttiva 2016/680 sono analizzate nel parere WP 258 "*Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*" [Parere su alcune questioni chiave della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie], adottato dal Gruppo di lavoro il 29 novembre 2017, che tratta tali aspetti alle pagine 11-14. Tale parere è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178

La profilazione può perpetuare stereotipi e la segregazione sociale. Può anche confinare una persona in una categoria specifica e limitarla alle preferenze suggerite per tale categoria. Ciò può minare la libertà delle persone di scegliere, ad esempio, determinati prodotti o servizi quali libri, musica o *newsfeed*. In taluni casi, la profilazione può portare a previsioni imprecise, in altri al diniego di servizi e beni e a discriminazioni ingiustificate.

Il regolamento introduce nuove disposizioni per far fronte ai rischi derivanti dalla profilazione e dal processo decisionale automatizzato, in particolare, ma non solo, in relazione alla tutela della vita privata. Le presenti linee guida mirano a chiarire tali disposizioni.

Il presente documento tratta i seguenti temi:

- definizioni di profilazione e processo decisionale automatizzato e approccio del regolamento a tali aspetti in generale – [capitolo II](#);
- disposizioni generali sulla profilazione e sul processo decisionale automatizzato – [capitolo III](#);
- disposizioni specifiche sulle decisioni basate unicamente sul trattamento automatizzato di cui all'articolo 22 - [capitolo IV](#);
- minori e profilazione – [capitolo V](#);
- valutazioni d'impatto sulla protezione dei dati e responsabili della protezione dei dati – [capitolo VI](#).

Gli allegati contengono alcune raccomandazioni sulle migliori prassi, basate sull'esperienza accumulata negli Stati membri.

Il Gruppo di lavoro articolo 29 per la protezione dei dati (Gruppo di lavoro) monitorerà l'attuazione delle presenti linee guida e provvederà alle integrazioni che si riveleranno opportune.

II. Definizioni

Il regolamento introduce disposizioni per garantire che la profilazione e il processo decisionale automatizzato relativo alle persone fisiche (comprensivo o meno di profilazione) non siano utilizzati in maniera tale da avere un impatto ingiustificato sui diritti delle persone. Esso prevede ad esempio:

- requisiti specifici di trasparenza e correttezza;
- maggiori obblighi in termini di responsabilizzazione;
- basi giuridiche specifiche per il trattamento;
- il diritto delle persone fisiche di opporsi alla profilazione, segnatamente alla profilazione per finalità di marketing;
- qualora siano soddisfatte determinate condizioni, la necessità di effettuare una valutazione d'impatto sulla protezione dei dati.

Il regolamento non si concentra soltanto sulle decisioni prese a seguito di un trattamento automatizzato o della profilazione. Si applica anche alla raccolta di dati per la creazione di profili e all'applicazione di tali profili alle persone fisiche.

A. Profilazione

Il regolamento definisce la profilazione all'articolo 4, punto 4, come:

qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

La profilazione è costituita da tre elementi:

- deve essere una forma di trattamento *automatizzato*;
- deve essere effettuata su *dati personali*;
- il suo obiettivo deve essere quello di *valutare aspetti personali* relativi a una persona fisica.

L'articolo 4, punto 4, fa riferimento a “qualsiasi forma di trattamento automatizzato” e non al trattamento “unicamente” automatizzato (di cui all'articolo 22). La profilazione deve implicare una qualche forma di trattamento automatizzato, sebbene il coinvolgimento umano non comporti necessariamente l'esclusione dell'attività dalla definizione.

La profilazione è una procedura che può implicare una serie di deduzioni statistiche. Spesso viene impiegata per effettuare previsioni su persone usando dati provenienti da varie fonti per dedurre qualcosa su una persona in base alle qualità di altre persone che sembrano statisticamente simili.

Il regolamento afferma che la profilazione è il trattamento automatizzato di dati personali per valutare determinati aspetti personali, in particolare per analizzare o prevedere aspetti riguardanti persone fisiche. L'uso del verbo “valutare” suggerisce che la profilazione implichi una qualche forma di valutazione o giudizio in merito a una persona.

La semplice classificazione di persone basata su caratteristiche note quali età, sesso e altezza non determina necessariamente una profilazione. Quest'ultima dipende infatti dalla finalità della classificazione.

Ad esempio, un'azienda potrebbe voler classificare i propri clienti in base all'età o al sesso per finalità statistiche e per acquisire una panoramica aggregata dei propri clienti senza effettuare previsioni o trarre conclusioni in merito a una persona specifica. In questo caso, la finalità non è la valutazione delle caratteristiche individuali e quindi non si tratta di profilazione.

Il regolamento si ispira alla definizione di profilazione di cui alla raccomandazione CM/Rec (2010)13² del Consiglio d'Europa ma non la riprende tale e quale, infatti la raccomandazione *esclude* il trattamento che non include la deduzione. Tuttavia, la raccomandazione spiega in maniera utile che la profilazione può comportare tre fasi distinte:

- raccolta dei dati;
- analisi automatizzata per individuare correlazioni;

² Consiglio d'Europa. La protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione. Raccomandazione CM/Rec (2010)13 e relazione. Consiglio d'Europa, 23 novembre 2010.
[https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec\(2010\)13E_Profiling.pdf](https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf).
Accesso effettuato il 24 aprile 2017;

- applicazione della correlazione a una persona fisica per individuare caratteristiche di comportamento presenti o future.

Il titolare del trattamento che effettua la profilazione dovrà assicurarsi di soddisfare le prescrizioni del regolamento in relazione a tutte le fasi di cui sopra.

In generale, la profilazione consiste nella raccolta di informazioni su una persona (o un gruppo di persone) e nella valutazione delle loro caratteristiche o dei loro modelli di comportamento al fine di includerli in una determinata categoria o gruppo, in particolare per analizzare e/o fare previsioni, ad esempio, in merito a:

- capacità di eseguire un compito;
- interessi, o
- comportamento probabile.

Esempio

Un intermediario di dati raccoglie dati da diverse fonti pubbliche e private, per conto dei suoi clienti o per finalità proprie. Raccoglie i dati per sviluppare profili sulle persone e inserirle in segmenti e poi vende queste informazioni alle imprese che desiderano migliorare l'orientamento dei loro beni e servizi. L'intermediario di dati esegue la profilazione inserendo una persona in una determinata categoria in base ai suoi interessi.

L'esistenza o meno di un processo decisionale automatizzato, così come definito nell'articolo 22, paragrafo 1, dipenderà dalle circostanze.

B. Processo decisionale automatizzato

Il processo decisionale automatizzato ha una portata diversa da quella della profilazione, a cui può sovrapporsi parzialmente o da cui può derivare. Il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano. Le decisioni automatizzate possono essere basate su qualsiasi tipo di dati, ad esempio:

- dati forniti direttamente dall'interessato (come le risposte a un questionario);
- dati osservati riguardo a una persona (come i dati relativi all'ubicazione raccolti tramite un'applicazione);
- dati derivati o desunti, come un profilo della persona che è già stato creato (ad esempio un punteggio sull'affidabilità creditizia).

Le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate. Tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Qualcosa che inizia come un semplice processo decisionale automatizzato potrebbe diventare un processo basato sulla profilazione, a seconda delle modalità di utilizzo dei dati.

Esempio

Infliggere una multa per eccesso di velocità esclusivamente sulla base delle prove fornite dall'autovelox è un processo decisionale automatizzato che non implica necessariamente la profilazione.

Tuttavia la decisione di infliggere la multa sarebbe basata sulla profilazione se le abitudini di guida della persona in questione fossero state monitorate nel tempo e, ad esempio, l'ammontare della multa fosse il risultato di una valutazione che coinvolge altri fattori quali l'eventuale recidiva di eccesso di velocità o l'eventuale recente violazione di altre disposizioni del codice della strada.

Le decisioni che non sono unicamente automatizzate potrebbero includere anche la profilazione. Ad esempio, prima di concedere un mutuo, un istituto bancario può prendere in considerazione il punteggio sull'affidabilità creditizia del mutuatario, associandolo a ulteriori interventi significativi svolti da esseri umani prima che venga adottata qualsiasi decisione relativa alla persona in questione.

C. Approccio del regolamento a questi concetti

Esistono potenzialmente tre modalità d'uso della profilazione:

- i) profilazione generale;
- ii) processo decisionale basato sulla profilazione;
- iii) decisione basata *unicamente* sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici o incide in modo analogo significativamente sull'interessato (articolo 22, paragrafo 1).

La differenza tra i punti ii) e iii) è dimostrata più chiaramente dai due esempi che seguono, nei quali una persona chiede un prestito online:

- un essere umano decide se accordare il prestito sulla base di un profilo prodotto con mezzi unicamente automatizzati - punto ii);
- un algoritmo decide se il prestito viene accordato e la decisione viene trasmessa automaticamente alla persona, senza alcuna previa valutazione significativa da parte di un essere umano - punto iii).

Il titolare del trattamento può svolgere attività di profilazione e processi decisionali automatizzati purché sia in grado di soddisfare tutti i principi e disponga di una base legittima per il trattamento. Garanzie supplementari e limitazioni si applicano nel caso di decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafo 1.

Il capitolo III delle presenti linee guida spiega le disposizioni del regolamento per *tutti* i processi decisionali automatizzati relativi alle persone fisiche e di profilazione. Ciò include i processi decisionali che *non* sono unicamente automatizzati.

Il capitolo IV delle presenti linee guida spiega le disposizioni specifiche che si applicano *esclusivamente* al processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione³. Esiste un divieto generale relativamente a questo tipo di trattamento al fine di riflettere i potenziali rischi per i diritti e le libertà delle persone fisiche.

³ Come stabilito all'articolo 22, paragrafo 1, del regolamento generale sulla protezione dei dati.

III. Disposizioni generali sulla profilazione e sul processo decisionale automatizzato

La presente panoramica delle disposizioni si applica a tutte le profilazioni e a tutti i processi decisionali automatizzati. Qualora il trattamento soddisfi la definizione di cui all'articolo 22, paragrafo 1, si applicano le disposizioni specifiche supplementari di cui al capitolo IV.

A. Principi in materia di protezione dei dati

I principi in materia di protezione dei dati sono pertinenti per tutte le attività di profilazione e tutti i processi decisionali automatizzati che comportano l'uso di dati personali⁴. Al fine di agevolare il rispetto delle norme, il titolare del trattamento dovrebbe considerare i seguenti elementi fondamentali:

1. Articolo 5, paragrafo 1, lettera a) - liceità, correttezza e trasparenza

La trasparenza del trattamento⁵ è una prescrizione fondamentale sancita dal regolamento.

Spesso il processo di profilazione è invisibile all'interessato. Funziona creando dati derivati o desunti in merito a persone fisiche, ossia dati personali "nuovi" che non sono stati forniti direttamente dagli interessati. Le persone fisiche hanno gradi diversi di comprensione e per alcune potrebbe essere difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati.

Ai sensi dell'articolo 12, paragrafo 1, il titolare del trattamento deve fornire agli interessati informazioni concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei loro dati personali⁶.

Per i dati raccolti direttamente dall'interessato, tali informazioni devono essere fornite al momento della raccolta (articolo 13); per i dati ottenuti indirettamente, le informazioni devono essere fornite entro i termini stabiliti all'articolo 14, paragrafo 3.

⁴ Regolamento generale sulla protezione dei dati, considerando 72: "la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati".

⁵ Le linee guida del Gruppo di lavoro in materia di trasparenza trattano della trasparenza in modo più approfondito; cfr. "Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)" [Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679], 11 aprile 2018 (in inglese) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

⁶ Ufficio del commissario australiano per l'informazione. Bozza di consultazione: *Guide to big data and the Australian Privacy Principles* [Guida ai megadati e ai principi australiani in materia di tutela della vita privata], 05/2016. In tale documento si afferma che: "le informative sulla protezione dei dati personali devono comunicare le informazioni relative alle prassi applicate in maniera chiara e semplice, nonché esaustiva e con sufficiente specificità da poter essere significative. *La stessa tecnologia che porta a una maggiore raccolta di informazioni personali offre anche l'opportunità di realizzare informative sulla protezione dei dati più dinamiche, a più livelli e incentrate sull'utente*". <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles>. Accesso effettuato il 24 aprile 2017.

Esempio

Alcuni assicuratori offrono tariffe e servizi assicurativi in base al comportamento di guida delle persone. Gli elementi presi in considerazione in questi casi potrebbero includere la distanza percorsa, il tempo trascorso alla guida e l'itinerario percorso, nonché previsioni basate su altri dati raccolti dai sensori dell'auto (intelligente). I dati raccolti vengono utilizzati per fini di profilazione con l'obiettivo di individuare comportamenti di guida errati (come accelerazione rapida, frenata improvvisa ed eccesso di velocità). Queste informazioni possono essere incrociate con altre fonti (ad esempio il clima, il traffico, il tipo di strada) in maniera da comprendere meglio il comportamento del conducente.

Il titolare del trattamento deve assicurarsi di disporre di una base legittima per tale tipo di trattamento. Il titolare del trattamento deve inoltre fornire all'interessato informazioni sui dati raccolti e, se del caso, sull'esistenza di processi decisionali automatizzati di cui all'articolo 22, paragrafi 1 e 4, sulla logica applicata, nonché sulla rilevanza e sulle conseguenze previste di tale trattamento.

I requisiti specifici riguardanti le informazioni e l'accesso ai dati personali sono esaminati nei capitoli III (sezione D) e IV (sezione E).

Il trattamento deve inoltre essere corretto e trasparente.

La profilazione può essere iniqua e creare discriminazioni, ad esempio negando l'accesso a opportunità di lavoro, credito o assicurazione oppure offrendo prodotti finanziari eccessivamente rischiosi o costosi. L'esempio seguente, che non rispetta le prescrizioni di cui all'articolo 5, paragrafo 1, lettera a), illustra come una profilazione iniqua può portare a proporre ad alcuni consumatori offerte meno interessanti rispetto ad altri.

Esempio

Un intermediario di dati vende profili di consumatori a società finanziarie senza il consenso dei consumatori o senza che essi conoscano i dati sottostanti. I profili classificano i consumatori in categorie (con diciture quali "popolazione rurale e che ce la fa a malapena", "membro di una minoranza etnica che vive in povertà in una realtà urbana secondaria", "inizi difficili: giovani genitori single") oppure assegnano loro dei punteggi, concentrandosi sulla vulnerabilità finanziaria dei consumatori. Le società finanziarie offrono a questi consumatori prestiti a breve termine (*payday loan*) e altri servizi finanziari "non tradizionali" (prestiti a costo elevato e altri prodotti finanziariamente rischiosi)⁷.

⁷ Questo esempio è tratto da: Senato degli Stati Uniti, Comitato per il commercio, la scienza e i trasporti. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* [Rassegna del settore degli intermediari: raccolta, utilizzo e vendita di dati sui consumatori per finalità di marketing], rapporto informativo per il presidente Rockefeller, 18 dicembre 2013 (in inglese). https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf. Cfr. pagina ii della sintesi e pagina 12 del corpo principale del documento. Accesso effettuato il 21 luglio 2017.

2. Articolo 5, paragrafo 1, lettera b) - ulteriore trattamento e limitazione della finalità

La profilazione può comportare l'utilizzo di dati personali originariamente raccolti per una finalità diversa.

Esempio

Alcune applicazioni mobili forniscono servizi di localizzazione che consentono all'utente di trovare ristoranti nelle vicinanze che offrono sconti. Tuttavia, i dati raccolti vengono utilizzati anche per creare un profilo dell'interessato per finalità di marketing, ossia per individuare le sue preferenze alimentari o il suo stile di vita in generale. L'interessato si aspetta che i suoi dati vengano utilizzati per trovare ristoranti, ma non per ricevere pubblicità relative alla consegna di pizza a domicilio soltanto perché l'applicazione ha stabilito che arriva a casa tardi. Questo ulteriore utilizzo dei dati relativi all'ubicazione potrebbe non essere compatibile con le finalità per le quali tali dati sono stati originariamente raccolti e può quindi richiedere il consenso dell'interessato⁸.

La compatibilità di tale ulteriore trattamento con le finalità originarie per le quali i dati sono stati raccolti dipenderà da una serie di fattori⁹, tra gli altri, le informazioni che il titolare del trattamento ha inizialmente fornito all'interessato. Tali fattori si riflettono nel regolamento¹⁰ e sono così riassunti:

- il rapporto tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento;
- il contesto in cui i dati personali sono stati raccolti e le ragionevoli aspettative dell'interessato in merito al loro uso futuro;
- la natura dei dati;
- l'impatto dell'ulteriore trattamento sull'interessato;
- le garanzie applicate dal titolare del trattamento per assicurare un trattamento corretto e prevenire qualsiasi impatto indebito sull'interessato.

3. Articolo 5, paragrafo 1, lettera c) - minimizzazione dei dati

Le opportunità commerciali create dalla profilazione, da costi di memorizzazione più economici e dalla capacità di trattare grandi quantità di informazioni possono incoraggiare le organizzazioni a raccogliere più dati personali di quelli di cui hanno effettivamente bisogno, poiché tali dati potrebbero rivelarsi utili in futuro. Il titolare del trattamento deve assicurarsi di rispettare il principio di minimizzazione dei dati e le prescrizioni dei principi di limitazione della finalità e limitazione della conservazione.

⁸ Si noti che possono trovare applicazione anche le disposizioni del futuro regolamento sulla vita privata e le comunicazioni elettroniche.

⁹ Evidenziati nel documento del Gruppo di lavoro "*Opinion 03/2013 on purpose limitation*" [Parere 03/2013 sulla limitazione della finalità], 2 aprile 2013 (in inglese). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Accesso effettuato il 24 aprile 2017;

¹⁰ Articolo 6, paragrafo 4, del regolamento generale sulla protezione dei dati.

Il titolare del trattamento dovrebbe essere in grado di spiegare in maniera chiara e giustificare la necessità della raccolta e della conservazione dei dati personali oppure prendere in considerazione l'utilizzo di dati aggregati, anonimizzati o (laddove ciò consenta una protezione sufficiente) pseudonimizzati per la profilazione.

4. Articolo 5, paragrafo 1, lettera d) - esattezza

Il titolare del trattamento dovrebbe esaminare l'esattezza in tutte le fasi del processo di profilazione, in particolare quando:

- raccoglie i dati;
- analizza i dati;
- crea un profilo per una persona o
- applica un profilo per prendere una decisione su una persona.

Se i dati utilizzati nel contesto di un processo decisionale automatizzato o di profilazione non sono esatti, qualsiasi decisione o profilo che ne deriverà sarà viziato. Le decisioni possono essere prese sulla base di dati obsoleti o di un'interpretazione errata di dati esterni. Eventuali inesattezze possono portare a previsioni o affermazioni inappropriate in merito, ad esempio, alla salute, al rischio di credito o al rischio assicurativo di una data persona.

Anche qualora i dati grezzi siano registrati in maniera esatta, l'insieme dei dati potrebbe non essere pienamente rappresentativo oppure l'analisi potrebbe contenere distorsioni nascoste.

Il titolare del trattamento deve introdurre misure efficaci per verificare e assicurare su base continuativa che i dati riutilizzati od ottenuti indirettamente siano esatti e aggiornati. Ciò sottolinea ulteriormente l'importanza di fornire informazioni chiare sui dati personali trattati, in maniera da consentire all'interessato di correggere eventuali inesattezze e migliorare la qualità dei dati.

5. Articolo 5, paragrafo 1, lettera e) - limitazione della conservazione

Gli algoritmi di apprendimento automatico sono progettati per trattare grandi volumi di informazioni e creare correlazioni che consentano alle organizzazioni di creare profili estremamente esaustivi e personali delle persone fisiche. Sebbene possano esservi vantaggi nel conservare i dati in caso di profilazione, dal momento che sarà disponibile una quantità maggiore di dati dai quali l'algoritmo può apprendere, il titolare del trattamento deve rispettare il principio di minimizzazione dei dati all'atto della raccolta e assicurare che i dati non siano conservati per un periodo superiore a quello necessario e proporzionato alle finalità per le quali i dati vengono trattati.

La politica di conservazione del titolare del trattamento dovrebbe tenere conto dei diritti e delle libertà delle persone fisiche in linea con le prescrizioni di cui all'articolo 5, paragrafo 1, lettera e).

Il titolare del trattamento dovrebbe inoltre assicurarsi che i dati rimangano aggiornati durante il periodo di conservazione in maniera da ridurre il rischio di inesattezze¹¹.

¹¹ Autorità norvegese di protezione dei dati. *"The Great Data Race – How commercial utilisation of personal data challenges privacy"* [La corsa ai dati eccezionali – Quali sono le sfide in termini di tutela della vita privata poste dall'utilizzo commerciale di dati personali], relazione, novembre 2015. Datatilsynet <https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/>. Accesso effettuato il 24 aprile 2017.

B. Basi legittime per il trattamento

Il processo decisionale automatizzato di cui all'articolo 22, paragrafo 1, è consentito soltanto qualora si applichi una delle eccezioni di cui al capitolo IV (sezioni C e D). Le seguenti basi legittime per il trattamento sono pertinenti per tutti i processi decisionali automatizzati relativi alle persone fisiche e di profilazione.

1. Articolo 6, paragrafo 1, lettera a) - consenso

Il consenso come base per il trattamento in generale è trattato nelle Linee guida del Gruppo di lavoro sul consenso¹². Il consenso esplicito è una delle eccezioni al divieto di processo decisionale automatizzato e profilazione di cui all'articolo 22, paragrafo 1.

La profilazione può non essere trasparente. Spesso si basa su dati derivati o desunti da altri dati, anziché su dati forniti direttamente dall'interessato.

Il titolare del trattamento che intende fare affidamento sul consenso come base per la profilazione dovrà dimostrare che gli interessati comprendono esattamente a cosa stanno acconsentendo e dovrà ricordare che il consenso non è sempre una base appropriata per il trattamento¹³. In tutti i casi, gli interessati dovrebbero disporre di sufficienti informazioni pertinenti sull'uso previsto e sulle conseguenze del trattamento in maniera da assicurare che il consenso fornito sia frutto di una scelta informata.

2. Articolo 6, paragrafo 1, lettera b) – necessario all'esecuzione di un contratto

Il titolare del trattamento potrebbe voler utilizzare la profilazione e i processi decisionali automatizzati perché tali processi:

- consentono potenzialmente una maggiore coerenza o correttezza nel processo decisionale (ad esempio riducendo le possibilità di errore umano, discriminazione e abuso di potere);
- riducono il rischio che i clienti non riescano a soddisfare i pagamenti per beni o servizi (ad esempio utilizzando referenze per il credito), o
- consentono di prendere decisioni in tempi più brevi e migliorare l'efficienza.

Indipendentemente da quanto sopra, queste considerazioni da sole non sono sufficienti a dimostrare che questo tipo di trattamento è *necessario* ai sensi dell'articolo 6, paragrafo 1, lettera b), per l'esecuzione di un contratto. Come descritto nel parere del Gruppo di lavoro sull'interesse legittimo¹⁴, la nozione di necessità deve essere interpretata in maniera restrittiva.

Quello che segue è un esempio di profilazione che *non* soddisfa le condizioni di cui all'articolo 6, paragrafo 1, lettera b).

¹² Gruppo di lavoro articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso effettuato il 18 dicembre 2017.

¹³ Ibidem.

¹⁴ Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017;

Esempio

Un utente acquista alcuni articoli da un rivenditore al dettaglio online. Per soddisfare il contratto, il rivenditore deve trattare le informazioni della carta di credito dell'utente per finalità di pagamento e l'indirizzo dell'utente per consegnare la merce. Il completamento del contratto non dipende dalla creazione di un profilo dei gusti e delle scelte in termini di stile di vita dell'utente, basato sulle sue visite sul sito web. Anche se la profilazione è espressamente menzionata in caratteri minuscoli nel contratto, questo fatto, da solo, non la rende "necessaria" all'esecuzione del contratto.

3. Articolo 6, paragrafo 1, lettera c) – necessario per adempiere un obbligo legale

Vi possono essere casi in cui sussiste un obbligo legale¹⁵ all'esecuzione della profilazione, ad esempio in relazione alla prevenzione delle frodi o al riciclaggio di denaro. Il parere del Gruppo di lavoro sugli interessi legittimi¹⁶ fornisce informazioni utili su questa base per il trattamento e sulle garanzie da applicare.

4. Articolo 6, paragrafo 1, lettera d) – necessario per la salvaguardia di interessi vitali

Tale base si applica nelle circostanze in cui il trattamento è necessario per la salvaguardia di un interesse essenziale per la vita dell'interessato o di un'altra persona fisica.

Determinati tipi di trattamento possono essere necessari per importanti motivi di interesse pubblico e per proteggere gli interessi vitali dell'interessato, come la profilazione per sviluppare modelli che individuino in anticipo la diffusione di malattie potenzialmente letali o in situazioni di emergenza umanitaria. In questi casi, tuttavia, e in linea di principio, il titolare del trattamento può basarsi su motivi di interesse vitale unicamente se non sono disponibili altre basi giuridiche per il trattamento¹⁷. Se il trattamento comprende dati personali appartenenti a categorie particolari, il titolare del trattamento deve altresì assicurarsi di soddisfare le prescrizioni di cui all'articolo 9, paragrafo 2, lettera c).

5. Articolo 6, paragrafo 1, lettera e) – necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri

L'articolo 6, paragrafo 1, lettera e), potrebbe costituire una base adeguata per la profilazione nel settore pubblico in determinate circostanze. Il compito o la funzione devono avere una base giuridica chiara.

¹⁵ Considerando 41 e 45 del regolamento generale sulla protezione dei dati.

¹⁶ Pagina 22 Gruppo di lavoro articolo 29, Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf . Accesso effettuato il 24 aprile 2017;

¹⁷ Considerando 46 del regolamento generale sulla protezione dei dati.

6. Articolo 6, paragrafo 1, lettera f) – necessario per il perseguimento del legittimo interesse¹⁸ del titolare del trattamento o di terzi

La profilazione è consentita se è necessaria ai fini degli interessi legittimi¹⁹ perseguiti dal titolare del trattamento o da un terzo. Tuttavia, l'articolo 6, paragrafo 1, lettera f), non si applica automaticamente soltanto perché il titolare del trattamento o il terzo ha un legittimo interesse. Il titolare del trattamento deve procedere a una ponderazione per valutare se gli interessi o i diritti e le libertà fondamentali dell'interessato non prevalgano sui propri interessi.

I seguenti aspetti sono particolarmente rilevanti:

- il livello di dettaglio del profilo (un interessato profilato in un gruppo descritto in maniera ampia come “persone interessate alla letteratura inglese” o segmentato e mirato a livello granulare);
- la completezza del profilo (il profilo descrive solo un aspetto minore dell'interessato oppure dipinge un quadro più completo);
- l'impatto della profilazione (gli effetti sull'interessato);
- le garanzie destinate ad assicurare la correttezza, la non discriminazione e l'esattezza nel processo di profilazione.

Sebbene si basi sull'articolo 7 della direttiva 95/46/CE sulla protezione dei dati, il parere del Gruppo di lavoro sui legittimi interessi²⁰ contiene esempi che sono comunque utili e pertinenti per il titolare del trattamento che svolge attività di profilazione. Tale parere suggerisce inoltre che sarebbe difficile per il titolare del trattamento giustificare il ricorso al legittimo interesse come base legittima per pratiche intrusive di profilazione e tracciamento per finalità di marketing o pubblicità, ad esempio quelle che comportano il tracciamento di persone fisiche su più siti web, ubicazioni, dispositivi, servizi o l'intermediazione di dati.

Nel valutare la validità del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f), il titolare del trattamento dovrebbe altresì considerare l'uso futuro o la combinazione di profili.

C. Articolo 9 – categorie particolari di dati

Il titolare del trattamento può trattare dati personali appartenenti a categorie particolari soltanto se ricorrono una delle condizioni di cui all'articolo 9, paragrafo 2, e una condizione di cui all'articolo 6. Questo vale anche per i dati appartenenti a categorie particolari derivati o desunti da attività di profilazione.

La profilazione può creare dati appartenenti a categorie particolari desumendoli da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati. Ad esempio, può essere possibile desumere lo stato di salute di una persona associando le registrazioni dei suoi acquisti di alimenti a dati sulla qualità e sul contenuto energetico di tali alimenti.

¹⁸ I legittimi interessi elencati nel considerando 47 del regolamento comprendono il trattamento per finalità di marketing diretto e il trattamento strettamente necessario a fini di prevenzione delle frodi.

¹⁹ Il “legittimo interesse” del titolare del trattamento non può rendere lecita la profilazione se il trattamento rientra nella definizione di cui all'articolo 22, paragrafo 1.

²⁰ Gruppo di lavoro articolo 29, Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE. Commissione europea, 9 aprile 2014, pagina 55, esempi alle pagine 70 e 71. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017.

Possono essere scoperte correlazioni che forniscono indicazioni sulla salute, sulle convinzioni politiche o religiose oppure sull'orientamento sessuale delle persone, come dimostrato dal seguente esempio:

Esempio

Uno studio²¹ ha combinato i “Mi Piace” di Facebook con informazioni limitate tratte da sondaggi e ha rilevato che i ricercatori hanno predetto con precisione l'orientamento sessuale di un utente maschile nell'88 % dei casi, l'origine etnica di un utente nel 95 % dei casi e se un utente era cristiano o musulmano nell'82 % dei casi.

Se dalla profilazione sono dedotte preferenze e caratteristiche sensibili, il titolare del trattamento dovrebbe assicurarsi:

- che il trattamento non sia incompatibile con la finalità originaria;
- di aver individuato una base legittima per il trattamento di dati appartenenti a categorie particolari;
- di informare l'interessato sul trattamento.

Il processo decisionale automatizzato, così come descritto dall'articolo 22, paragrafo 1, basato su categorie particolari di dati, è trattato nel capitolo IV (sezione D).

D. Diritti dell'interessato²²

Il regolamento introduce maggiori diritti per gli interessati e crea nuovi obblighi per i titolari del trattamento.

Nel contesto della profilazione questi diritti possono essere esercitati nei confronti del titolare del trattamento che crea il profilo e del titolare del trattamento che prende una decisione automatizzata su un interessato (con o senza intervento umano), qualora tali soggetti non siano il medesimo.

Esempio

Un intermediario di dati effettua la profilazione di dati personali. In linea con gli obblighi di cui agli articoli 13 e 14, deve informare l'interessato in merito al trattamento e al fatto che intende condividere il profilo con altre organizzazioni. Deve inoltre indicare separatamente anche i dettagli relativi al diritto di opposizione di cui all'articolo 21, paragrafo 1.

L'intermediario di dati condivide il profilo con un'altra impresa. Tale impresa utilizza il profilo per inviare alla persona in questione comunicazioni di marketing diretto.

²¹ Michael Kosinski, David Stilwell e Thore Graepel. Private traits and attributes are predictable from digital records of human behaviour [Tratti e attributi privati sono prevedibili dalle registrazioni digitali del comportamento umano]. Atti della National Academy of Sciences degli Stati Uniti d'America, <http://www.pnas.org/content/110/15/5802.full.pdf>. Accesso effettuato il 29 marzo 2017.

²² La presente sezione è pertinente tanto per la profilazione quanto per il processo decisionale automatizzato. Per il processo decisionale automatizzato ai sensi dell'articolo 22, si ricorda che esistono anche requisiti aggiuntivi come descritto nel capitolo IV.

L'impresa deve informare l'interessato [articolo 14, paragrafo 1, lettera c)] in merito alle finalità dell'utilizzo del profilo e alla fonte da cui ha ottenuto l'informazione [articolo 14, paragrafo 2, lettera f)] nonché al diritto dell'interessato di opporsi al trattamento, compresa la profilazione, per finalità di marketing diretto (articolo 21, paragrafo 2).

L'intermediario di dati e l'impresa devono consentire all'interessato di accedere alle informazioni utilizzate (articolo 15) per correggere eventuali informazioni errate (articolo 16) e, in determinate circostanze, di cancellare il profilo o i dati personali utilizzati per crearlo (articolo 17). L'interessato deve inoltre ricevere informazioni sul proprio profilo, ad esempio, in merito ai "segmenti" o alle "categorie" nei quali viene collocato²³.

Se utilizza il profilo per prendere una decisione basata unicamente sul trattamento automatizzato che produce effetti giuridici o che incide in modo analogo significativamente sull'interessato, l'impresa è soggetta alle disposizioni dell'articolo 22. (Ciò non esclude l'intermediario di dati dall'articolo 22 se il trattamento soddisfa la soglia pertinente).

1. Articoli 13 e 14 – diritto di essere informato

In considerazione del principio fondamentale della trasparenza che sta alla base del regolamento, il titolare del trattamento deve spiegare in maniera chiara e semplice alle persone interessate come funziona la profilazione o il processo decisionale automatizzato.

In particolare, quando il trattamento implica un processo decisionale basato sulla profilazione (indipendentemente dal fatto che rientri nell'applicazione delle disposizioni di cui all'articolo 22), deve essere chiarito all'interessato²⁴ il fatto che il trattamento avviene per finalità di a) profilazione e di b) adozione di decisioni basate sul profilo generato.

Il considerando 60 afferma che fornire informazioni sulla profilazione fa parte degli obblighi di trasparenza del titolare del trattamento ai sensi dell'articolo 5, paragrafo 1, lettera a). L'interessato ha diritto di *essere informato* dal titolare del trattamento e, in alcune circostanze, gode di un diritto di *opposizione alla "profilazione"*, *indipendentemente* dal fatto che abbia luogo un processo decisionale unicamente automatizzato relativo alle persone fisiche.

Ulteriori orientamenti sulla trasparenza in generale sono disponibili nelle Linee guida del Gruppo di lavoro sulla trasparenza ai sensi del regolamento²⁵.

²³ Autorità norvegese di protezione dei dati. "The Great Data Race - How commercial utilisation of personal data challenges privacy". Relazione, novembre 2015. <https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/> Accesso effettuato il 24 aprile 2017.

²⁴ Articolo 13, paragrafo 1, lettera c), e articolo 14, paragrafo 1, lettera c), del regolamento generale sulla protezione dei dati. L'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g), impongono al titolare del trattamento di informare l'interessato dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4. Questo aspetto è spiegato ulteriormente nel capitolo IV.

²⁵ Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679 (WP 260), 28 novembre 2017 (in inglese) http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accesso effettuato il 18 dicembre 2017.

2. Articolo 15 – diritto di accesso

L'articolo 15 conferisce all'interessato il diritto di ottenere informazioni dettagliate sui dati personali utilizzati per la profilazione, ivi comprese le categorie di dati impiegati per creare un profilo.

Oltre alle informazioni generali sul trattamento, ai sensi dell'articolo 15, paragrafo 3, il titolare del trattamento deve rendere disponibili i dati utilizzati come input per creare il profilo, e consentire l'accesso alle informazioni sul profilo e ai dettagli dei segmenti nei quali l'interessato è stato inserito.

Ciò differisce dal diritto alla portabilità dei dati di cui all'articolo 20, nel contesto del quale il titolare del trattamento è tenuto soltanto a comunicare i dati forniti dall'interessato o osservati dal titolare del trattamento e non il profilo stesso²⁶.

Il considerando 63 offre una certa protezione al titolare del trattamento nei confronti della divulgazione di segreti aziendali o proprietà intellettuale, che può essere particolarmente pertinente in relazione alla profilazione. Tale considerando afferma che il diritto di accesso “non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software”. Tuttavia, il titolare del trattamento non può fare affidamento sulla protezione dei segreti aziendali come scusa per negare l'accesso o rifiutarsi di fornire informazioni all'interessato.

Il considerando 63 specifica inoltre che “ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali”.

3. Articolo 16 – diritto di rettifica; articolo 17 – diritto alla cancellazione; articolo 18 – diritto di limitazione di trattamento

La profilazione può comportare un elemento di previsione, il che aumenta il rischio di inesattezza. I dati di input possono essere inesatti o irrilevanti oppure avulsi dal contesto. L'algoritmo utilizzato per individuare le correlazioni potrebbe presentare lacune.

Il diritto di rettifica di cui all'articolo 16 potrebbe applicarsi, ad esempio, nel caso in cui una persona venga inserita in una categoria che esprime un giudizio sulla propria capacità di eseguire un compito, e tale profilo sia basato su informazioni errate. Le persone potrebbero voler contestare l'esattezza dei dati utilizzati e qualsiasi raggruppamento o categoria che è stata loro applicata.

I diritti di rettifica e di cancellazione²⁷ si applicano tanto ai “dati personali di input” (i dati personali utilizzati per creare il profilo) quanto ai “dati di output” (il profilo stesso o il “punteggio” assegnato alla persona fisica).

L'articolo 16 prevede altresì il diritto dell'interessato di integrare i dati personali con informazioni aggiuntive.

²⁶ Pagina 9 del documento del Gruppo di lavoro, Linee guida sul diritto alla portabilità dei dati, WP 242 <https://www.garanteprivacy.it/documents/10160/5184810/Linee-guida+sul+diritto+alla+portabilit%C3%A0+dei+dati+-+WP+242.pdf>. Accesso effettuato il 8 gennaio 2018.

²⁷ Articolo 17 del regolamento generale sulla protezione dei dati.

Esempio

Il sistema informatico di un centro medico locale colloca una persona in un gruppo che presenta maggiori probabilità di sviluppare malattie cardiache. Questo “profilo” non è necessariamente impreciso nonostante tale persona non abbia mai sofferto di malattie cardiache.

Il profilo afferma semplicemente che la persona in questione ha *maggiori probabilità* di sviluppare malattie cardiache. Ciò può essere di fatto corretto, in termini statistici.

Ciò nonostante l’interessato ha il diritto, tenendo conto della finalità del trattamento, di fornire una dichiarazione integrativa. Nella fattispecie, la dichiarazione potrebbe essere basata, ad esempio, su un sistema informatico medico (e su un modello statistico) più avanzato che include nel calcolo dati aggiuntivi e svolge esami più dettagliati rispetto a quello del centro medico locale con capacità più limitate.

Il diritto di limitazione di trattamento (articolo 18) si applica a qualsiasi fase del processo di profilazione.

4. Articolo 21 – diritto di opposizione

Il titolare del trattamento deve portare *espressamente* all’attenzione dell’interessato informazioni dettagliate in merito al diritto di opposizione di cui all’articolo 21, paragrafi 1 e 2, e presentare tale diritto chiaramente e separatamente da qualsiasi altra informazione (articolo 21, paragrafo 4).

Ai sensi dell’articolo 21, paragrafo 1, l’interessato può opporsi al trattamento (compresa la profilazione), per motivi connessi alla sua situazione particolare. Il titolare del trattamento è specificamente tenuto a riconoscere tale diritto in tutti i casi nei quali il trattamento si basi sull’articolo 6, paragrafo 1, lettere e) o f).

Dopo che l’interessato ha esercitato questo diritto, il titolare del trattamento deve interrompere²⁸ (o evitare di iniziare) il processo di profilazione, a meno che non possa dimostrare l’esistenza di motivi legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell’interessato. Il titolare del trattamento potrebbe altresì dover cancellare i dati personali pertinenti²⁹.

Il regolamento non fornisce alcuna spiegazione di motivi che sarebbero considerati motivi legittimi cogenti³⁰. Può accadere, ad esempio, che la profilazione sia utile per la società in senso lato (o per la comunità più ampia) e non soltanto per gli interessi aziendali del titolare del trattamento, come nel caso della profilazione volta a individuare in anticipo la diffusione di malattie contagiose.

²⁸ Articolo 18, paragrafo 1, lettera d), del regolamento.

²⁹ Articolo 17, paragrafo 1, lettera c), del regolamento.

³⁰ Cfr. la spiegazione di legittimità nel documento del Gruppo di lavoro “Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell’articolo 7 della direttiva 95/46/CE”. 9 aprile 2014. Pagine 28-31. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Accesso effettuato il 24 aprile 2017;

Il titolare del trattamento dovrebbe:

- considerare l'importanza della profilazione per il proprio particolare obiettivo;
- considerare l'impatto della profilazione sugli interessi, sui diritti e sulle libertà dell'interessato, che dovrebbe essere limitato al minimo necessario per conseguire l'obiettivo;
- procedere a una ponderazione.

È sempre necessario procedere a una ponderazione tra gli interessi concorrenti del titolare del trattamento e la base per l'opposizione dell'interessato (che può fondarsi su motivi personali, sociali o professionali). A differenza della direttiva 95/46/CE, l'onere della prova di dimostrare l'esistenza di motivi legittimi cogenti spetta al titolare del trattamento e non all'interessato.

Dalla formulazione dell'articolo 21 risulta evidente che la ponderazione differisce da quella di cui all'articolo 6, paragrafo 1, lettera f). In altre parole, non è sufficiente che il titolare del trattamento dimostri soltanto che la sua precedente analisi dell'interesse legittimo era corretta, occorre inoltre che detto interesse legittimo sia *cogente*, il che implica una soglia maggiore per prevalere rispetto alle opposizioni.

L'articolo 21, paragrafo 2, riconosce all'interessato un diritto *incondizionato* ad opporsi al trattamento dei suoi dati personali per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto³¹. Ciò significa che non è necessario effettuare alcun bilanciamento degli interessi; il titolare del trattamento deve rispettare le volontà dell'interessato senza mettere in discussione i motivi dell'opposizione. Il considerando 70 fornisce ulteriore contesto a questo diritto e afferma che può essere esercitato in qualsiasi momento e gratuitamente.

IV. Disposizioni specifiche relative a decisioni basate unicamente sul trattamento automatizzato di cui all'articolo 22

L'articolo 22, paragrafo 1, afferma che:

l'interessato ha il diritto di non essere sottoposto a una decisione *basata unicamente* sul trattamento automatizzato, compresa la profilazione, che produca *effetti giuridici* che lo riguardano o che *incida in modo analogo significativamente sulla sua persona*.

Il termine "diritto" contenuto nella disposizione non significa che l'articolo 22, paragrafo 1, si applica soltanto se invocato attivamente dall'interessato. L'articolo 22, paragrafo 1, stabilisce un divieto generale nei confronti del processo decisionale basato unicamente sul trattamento automatizzato. Tale divieto si applica indipendentemente dal fatto che l'interessato intraprenda un'azione in merito al trattamento dei propri dati personali.

³¹ In linea con l'articolo 12, paragrafo 2, il titolare del trattamento che raccoglie dati personali da persone fisiche allo scopo di utilizzarli per finalità di marketing diretto dovrebbe, al momento della raccolta, considerare la possibilità di offrire agli interessati un modo semplice per indicare che non desiderano che i loro dati personali siano utilizzati per finalità di marketing diretto, anziché richiedere loro di esercitare il diritto di opposizione in un secondo momento.

In sintesi, l'articolo 22 stabilisce che:

- i) di norma, esiste un divieto generale all'adozione di decisioni completamente automatizzate relative alle persone fisiche, compresa la profilazione, che hanno un effetto giuridico o che incidono in modo analogo significativamente;
- ii) esistono eccezioni alla regola;
- iii) laddove si applichi una di tali eccezioni, devono essere adottate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato³².

Questa interpretazione sostiene l'idea secondo la quale l'interessato deve avere il controllo sui propri dati personali, in linea con i principi fondamentali del regolamento. Interpretare l'articolo 22 come un divieto piuttosto che come un diritto da invocare significa che le persone sono automaticamente protette dagli effetti potenziali che questo tipo di trattamento può avere. La formulazione dell'articolo suggerisce che questa è l'intenzione, sostenuta anche dal considerando 71, che afferma:

tuttavia, **è opportuno che sia consentito** adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri (...), o se è necessario per la conclusione o l'esecuzione di un contratto (...), o se l'interessato ha espresso il proprio consenso esplicito.

Ciò implica che il trattamento ai sensi dell'articolo 22, paragrafo 1, non è consentito in generale³³.

Tuttavia il divieto di cui all'articolo 22, paragrafo 1 si applica *esclusivamente* in circostanze specifiche quando una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, ha un effetto giuridico o incide in modo analogo significativamente su una persona, come spiegato ulteriormente nelle linee guida. Anche in questi casi esistono precise eccezioni che consentono l'esecuzione di tale trattamento.

Le garanzie richieste, discusse in maggior dettaglio in appresso, comprendono il diritto di essere informati (di cui agli articoli 13 e 14 – informazioni specificamente significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste per l'interessato) e garanzie, quali il diritto di ottenere l'intervento umano e il diritto di contestare la decisione (di cui all'articolo 22, paragrafo 3).

Qualsiasi trattamento che possa presentare un rischio elevato per gli interessati impone al titolare del trattamento di svolgere una [valutazione d'impatto sulla protezione dei dati](#)³⁴. Oltre ad affrontare qualsiasi altro rischio connesso al trattamento, una valutazione d'impatto sulla protezione dei dati può essere particolarmente utile per i titolari del trattamento che non sono certi che le attività da loro proposte rientrino nella definizione di cui all'articolo 22, paragrafo 1, e, laddove tali attività siano consentite da un'eccezione individuata, non sappiano quali garanzie debbano essere applicate.

³² Il considerando 71 afferma che tale trattamento dovrebbe essere "subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione".

³³ Ulteriori commenti sull'interpretazione dell'articolo 22 come divieto sono riportati nell'allegato 2.

³⁴ Gruppo di lavoro articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679. 4 aprile 2017. Commissione europea. <https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati> Accesso effettuato il 24 aprile 2017.

A. **“Decisione basata unicamente sul trattamento automatizzato”**

L’articolo 22, paragrafo 1, si riferisce a decisioni “basate unicamente” sul trattamento automatizzato. Ciò significa che non vi è alcun coinvolgimento umano nel processo decisionale.

Esempio

Un processo automatizzato produce ciò che di fatto è una raccomandazione riguardante un interessato. Se un essere umano riesamina il risultato del processo automatizzato e tiene conto di altri fattori nel prendere la decisione finale, tale decisione non sarà “basata unicamente” sul trattamento automatizzato.

Il titolare del trattamento non può eludere le disposizioni dell’articolo 22 creando coinvolgimenti umani fittizi. Ad esempio, se qualcuno applica abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata unicamente sul trattamento automatico.

Per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico. Il controllo dovrebbe essere effettuato da una persona che dispone dell’autorità e della competenza per modificare la decisione. Nel contesto dell’analisi, tale persona dovrebbe prendere in considerazione tutti i dati pertinenti.

Nell’ambito della valutazione d’impatto sulla protezione dei dati, il titolare del trattamento dovrebbe individuare e registrare il grado di coinvolgimento umano nel processo decisionale e la fase nella quale quest’ultimo ha luogo.

B. **Effetti “giuridici” o “in modo analogo significativi”**

Il regolamento riconosce che il processo decisionale automatizzato, compresa la profilazione, può avere gravi conseguenze per le persone fisiche. Il regolamento non definisce i concetti di “giuridico” o “in modo analogo significativi”, tuttavia la formulazione dell’articolo 22 chiarisce che rientreranno nell’applicazione dell’articolo soltanto gli effetti che hanno un impatto grave.

“Decisione che produce effetti giuridici”

Un effetto giuridico richiede che la decisione, basata unicamente su un trattamento automatico, incida sui diritti giuridici di una persona, quali la libertà di associarsi ad altre persone, di votare nel contesto di un’elezione o di intraprendere azioni legali. Un effetto giuridico può altresì essere qualcosa che influisce sullo status giuridico di una persona o sui suoi diritti ai sensi di un contratto. Tra gli esempi di questo tipo di effetto figurano le decisioni automatizzate su una persona fisica che portano:

- alla cancellazione di un contratto;
- alla concessione o alla negazione del diritto a una particolare prestazione sociale concessa dalla legge, come l’indennità di alloggio o le prestazioni per figli a carico;
- al rifiuto dell’ammissione in un paese o la negazione della cittadinanza.

“Incida in modo analogo significativamente sulla sua persona”

Anche se un processo decisionale non ha effetto sui diritti giuridici delle persone, potrebbe comunque rientrare nell’ambito di applicazione dell’articolo 22 se produce un effetto equivalente o in modo analogo significativo in termini di impatto.

In altre parole, anche qualora non vi sia alcun cambiamento nei suoi diritti od obblighi giuridici, l’interessato potrebbe comunque subire ripercussioni sufficienti da richiedere le protezioni previste da questa disposizione. Il regolamento introduce l’espressione “in modo analogo” (non presente nell’articolo 15 della direttiva 95/46/CE) associandola a “incida significativamente”. Di conseguenza la soglia per l’*importanza* deve essere analoga a quella di una decisione che produce un effetto giuridico.

Il considerando 71 fornisce i seguenti esempi tipici: “rifiuto automatico di una domanda di credito online” o “pratiche di assunzione elettronica senza interventi umani”.

Affinché il trattamento dei dati sia considerato incidere in maniera significativa su una persona, i suoi effetti devono essere sufficientemente rilevanti o importanti da meritare attenzione. In altre parole, la decisione deve poter essere in grado di:

- incidere in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell’interessato;
- avere un impatto prolungato o permanente sull’interessato; o
- nel caso più estremo, portare all’esclusione o alla discriminazione di persone.

È difficile essere precisi su ciò che può essere considerato sufficientemente *significativo* per il raggiungimento della soglia, sebbene le seguenti decisioni possano rientrare in tale categoria:

- decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito;
- decisioni che influenzano l’accesso di una persona ai servizi sanitari;
- decisioni che negano a una persona un’opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio;
- decisioni che influenzano l’accesso di una persona all’istruzione, ad esempio le ammissioni universitarie.

Ciò conduce anche al problema della pubblicità online, che si basa sempre più su strumenti automatizzati e implica decisioni basate unicamente sul trattamento automatizzato. Oltre al soddisfacimento delle disposizioni generali del regolamento, trattate nel capitolo III, possono essere pertinenti anche le disposizioni della proposta di regolamento sulla vita privata e le comunicazioni elettroniche. Inoltre, i minori richiedono una protezione maggiore, come sarà esaminato in appresso nel capitolo V.

In numerosi casi tipici, la decisione di proporre pubblicità mirata basata sulla profilazione non inciderà in modo analogo significativamente sulle persone, ad esempio nel caso di una pubblicità per un outlet di moda online basato su un semplice profilo demografico: “donne nella regione di Bruxelles di età compresa tra 25 e 35 che potrebbero essere interessate alla moda e ad alcuni capi di abbigliamento”.

Tuttavia è possibile che ciò possa accadere, a seconda delle particolari caratteristiche del caso, tra le quali:

- l’invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi;
- le aspettative e le volontà delle persone interessate;

- il modo in cui viene reso disponibile l'annuncio pubblicitario; o
- lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti.

Un trattamento che potrebbe avere un impatto minimo sulle persone in generale potrebbe in effetti incidere in maniera significativa su taluni gruppi della società, quali gruppi minoritari o adulti vulnerabili. Ad esempio, una persona di cui sono note le difficoltà finanziarie, effettive o potenziali, e che riceve regolarmente annunci pubblicitari di prestiti ad alto interesse potrebbe sottoscrivere tali offerte e incorrere così in ulteriori debiti.

Anche un processo decisionale automatizzato che si traduce in una fissazione dei prezzi differenziata basata su dati personali o caratteristiche personali potrebbe incidere in maniera significativa se, ad esempio, prezzi proibitivi elevati impediscono effettivamente a una persona di ottenere determinati beni o servizi.

Analogamente, effetti significativi possono risultare anche da azioni di persone diverse dalla persona alla quale fa riferimento la decisione automatizzata. Un'illustrazione di questo caso è riportata in appresso.

Esempio

Ipoteticamente, una società che fornisce carte di credito potrebbe ridurre il limite della carta di un cliente non sulla base dello storico dei rimborsi di quel cliente, bensì su criteri di credito non tradizionali, quali un'analisi di altri clienti che vivono nella medesima area e acquistano presso i medesimi negozi.

Ciò potrebbe comportare la limitazione delle opportunità di una persona sulla base di azioni di terzi.

In un contesto diverso, il ricorso a questi tipi di caratteristiche potrebbe avere il vantaggio di estendere il credito a coloro che non hanno una storia creditizia convenzionale, alle quali sarebbe altrimenti negato l'accesso.

C. Eccezioni al divieto

L'articolo 22, paragrafo 1, stabilisce un divieto generale all'adozione di un processo decisionale unicamente automatizzato relativo alle persone fisiche con effetti giuridici o che incidono in modo analogo significativamente, come descritto sopra.

Di conseguenza il titolare del trattamento non dovrebbe intraprendere il trattamento descritto nell'articolo 22, paragrafo 1, a meno che non si applichi una delle seguenti eccezioni di cui all'articolo 22, paragrafo 2, nel contesto delle quali la decisione:

- a) è necessaria per la conclusione o l'esecuzione di un contratto;
- b) è autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; o
- c) si basa sul consenso esplicito dell'interessato.

Laddove il processo decisionale coinvolga categorie particolari di dati definite all'articolo 9, paragrafo 1, il titolare del trattamento deve altresì garantire di poter soddisfare i requisiti di cui all'articolo 22, paragrafo 4.

1. Esecuzione di un contratto

Il titolare del trattamento potrebbe voler ricorrere a processi decisionali basati unicamente sul trattamento automatizzato per finalità contrattuali ritenendo che sia il modo più appropriato per conseguire l'obiettivo. Talvolta il coinvolgimento umano di routine può essere impraticabile o impossibile in ragione della notevole quantità di dati che vengono trattati.

Il titolare del trattamento deve essere in grado di dimostrare che questo tipo di trattamento è necessario, tenendo conto della possibilità di adottare un metodo più rispettoso della vita privata³⁵. Se esistono altri mezzi efficaci e meno invasivi per il conseguimento del medesimo obiettivo, allora il trattamento non sarà "necessario".

Il processo decisionale automatizzato di cui all'articolo 22, paragrafo 1, può essere necessario anche per un trattamento precontrattuale.

Esempio

Un'azienda pubblicizza un posto di lavoro vacante. Essendo il posto molto ambito, l'azienda riceve decine di migliaia di candidature. In ragione del volume eccezionalmente elevato di candidature l'azienda potrebbe ritenere che non è possibile individuare i candidati idonei senza prima utilizzare mezzi unicamente automatizzati per scartare le candidature non pertinenti. In questo caso potrebbe essere necessario ricorrere a un processo decisionale automatizzato per stilare un elenco ristretto di possibili candidati allo scopo di stipulare un contratto con un interessato.

Il capitolo III (sezione B) fornisce maggiori informazioni sui contratti come base legittima per il trattamento.

2. Autorizzato dal diritto dell'Unione o dello Stato membro

Il processo decisionale automatizzato, compresa la profilazione, potrebbe potenzialmente aver luogo ai sensi dell'articolo 22, paragrafo 2, lettera b), se il diritto dell'Unione o dello Stato membro ne autorizza l'uso. La legislazione pertinente deve altresì prevedere misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Il considerando 71 afferma che tale trattamento potrebbe includere il ricorso al processo decisionale automatizzato di cui all'articolo 22, paragrafo 1, per fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale o a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento.

³⁵ Buttarelli, Giovanni. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit* [Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali. Uno strumentario]. Garante europeo della protezione dei dati, 11 aprile 2017, (in inglese) https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf. Accesso effettuato il 24 aprile 2017.

3. Consenso esplicito

L'articolo 22 richiede il consenso *esplicito*. Il trattamento che rientra nella definizione di cui all'articolo 22, paragrafo 1, pone rischi significativi in termini di protezione dei dati e pertanto si ritiene opportuno un livello elevato di controllo individuale sui dati personali.

Il "consenso esplicito" non è definito nel regolamento; tuttavia le linee guida del Gruppo di lavoro sul consenso³⁶ forniscono orientamenti in merito alla sua interpretazione.

Il capitolo III (sezione B) fornisce maggiori informazioni sul consenso in generale.

D. **Categorie particolari di dati personali – articolo 22, paragrafo 4**

Il processo decisionale automatizzato (di cui all'articolo 22, paragrafo 1) che comporta l'uso di categorie particolari di dati personali è consentito soltanto se sono soddisfatte le seguenti condizioni cumulative (articolo 22, paragrafo 4):

- esiste un'esenzione applicabile in virtù dell'articolo 22, paragrafo 2;
- si applicano la lettera a) o g) dell'articolo 9, paragrafo 2.

Articolo 9, paragrafo 2, lettera a) - consenso esplicito dell'interessato; o
--

Articolo 9, paragrafo 2, lettera g) - trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
--

In entrambi i casi di cui sopra, il titolare del trattamento deve altresì adottare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

E. **Diritti dell'interessato³⁷**

1. **Articolo 13, paragrafo 2, lettera f), e articolo 14, paragrafo 2, lettera g) - diritto di essere informato**

In considerazione dei potenziali rischi e delle interferenze che la profilazione di cui all'articolo 22 pone in relazione ai diritti degli interessati, il titolare del trattamento dovrebbe prestare particolare attenzione agli obblighi in materia di trasparenza.

L'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g), impongono al titolare del trattamento di fornire informazioni specifiche e facilmente accessibili sul processo decisionale

³⁶ Gruppo di lavoro articolo 29, Linee guida sul consenso ai sensi del regolamento 2016/679, WP 259. 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso effettuato il 18 dicembre 2017.

³⁷ L'articolo 12 del regolamento stabilisce le modalità applicabili all'esercizio dei diritti dell'interessato.

automatizzato, basato unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici o in modo analogo significativi³⁸.

Se prende decisioni automatizzate come descritto nell'articolo 22, paragrafo 1, il titolare del trattamento deve:

- comunicare all'interessato che sta svolgendo tale tipo di attività;
- fornire informazioni significative sulla logica utilizzata;
- spiegare l'importanza e le conseguenze previste di tale trattamento.

Fornire queste informazioni aiuterà altresì il titolare del trattamento a garantire il rispetto di talune garanzie obbligatorie di cui all'articolo 22, paragrafo 3, e al considerando 71.

Se il processo decisionale automatizzato e la profilazione non soddisfano la definizione di cui all'articolo 22, paragrafo 1, è comunque buona prassi fornire le informazioni di cui sopra. In ogni caso il titolare del trattamento deve fornire informazioni sufficienti all'interessato in maniera da rendere il trattamento corretto³⁹ e soddisfare tutti gli altri requisiti in materia di informazione di cui agli articoli 13 e 14.

Informazioni significative sulla “logica utilizzata”

La crescita e la complessità dell'apprendimento automatico possono rendere difficile comprendere come funzionano un processo decisionale automatizzato o la creazione di profili.

Il titolare del trattamento dovrebbe trovare modi semplici per comunicare all'interessato la logica o i criteri sui quali si basa l'adozione della decisione. Il regolamento impone al titolare del trattamento di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo⁴⁰. Le informazioni fornite dovrebbero tuttavia essere sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione.

Esempio

Un titolare del trattamento utilizza il punteggio di affidabilità creditizia (*credit scoring*) per valutare e respingere una domanda di prestito di una persona. Tale punteggio può essere stato fornito da un'agenzia di referenze per il credito oppure calcolato direttamente sulla base delle informazioni detenute dal titolare del trattamento.

Indipendentemente dalla fonte (le informazioni sulla fonte devono essere fornite all'interessato ai sensi dell'articolo 14, paragrafo 2, lettera f), qualora i dati personali non siano stati ottenuti dall'interessato), se il titolare del trattamento si basa su tale punteggio, deve essere in grado di spiegarlo e di illustrarne

³⁸ Di cui all'articolo 22, paragrafi 1 e 4. Le linee guida del Gruppo di lavoro sulla trasparenza trattano dei requisiti generali in materia di informazione di cui agli articoli 13 e 14.

³⁹ Considerando 60 del regolamento: “il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa”.

⁴⁰ La complessità non è una scusa per non fornire informazioni all'interessato. Il considerando 58 afferma che il principio di trasparenza è “particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online”.

la logica all'interessato.

Il titolare del trattamento spiega che tale processo lo aiuta a prendere decisioni corrette e responsabili in merito ai prestiti concessi. Fornisce dettagli sulle principali caratteristiche considerate per giungere alla decisione, sulla fonte di tali informazioni e sulla loro importanza. Ciò può includere, ad esempio:

- informazioni fornite dall'interessato nel modulo di domanda;
- informazioni sulla situazione anteriore del conto, compresi eventuali pagamenti arretrati;
- informazioni derivanti da registri pubblici ufficiali, quali i registri di frodi e i registri d'insolvenza.

Il titolare del trattamento include altresì informazioni per spiegare all'interessato che i metodi di valutazione del grado di affidabilità creditizia utilizzati sono sottoposti a verifiche regolari per garantire che rimangano corretti, efficaci ed esenti da distorsioni.

Il titolare del trattamento fornisce i dati di contatto affinché l'interessato possa chiedere il riesame di qualsiasi decisione respinta, in linea con le disposizioni di cui all'articolo 22, paragrafo 3.

“Importanza” e “conseguenze previste”

Questi termini suggeriscono che devono essere fornite informazioni sul trattamento previsto o futuro, nonché sulle possibili conseguenze del processo decisionale automatizzato sull'interessato⁴¹. Per rendere queste informazioni significative e comprensibili, dovrebbero essere forniti esempi reali e concreti del tipo di possibili effetti.

In un contesto digitale, il titolare del trattamento potrebbe essere in grado di utilizzare strumenti aggiuntivi per illustrare tali effetti.

Esempio

Una compagnia assicurativa utilizza un processo decisionale automatizzato per definire i premi assicurativi per gli autoveicoli in funzione del comportamento di guida dei clienti. Per illustrare il significato e le conseguenze previste del trattamento, la compagnia spiega che una guida pericolosa può comportare premi assicurativi più elevati e fornisce un'applicazione che confronta conducenti fittizi, tra i quali uno con abitudini di guida pericolose come rapide accelerazioni e frenate all'ultimo minuto.

Usa elementi grafici per dare consigli su come migliorare tali abitudini e, di conseguenza, su come ridurre i premi assicurativi.

⁴¹ Consiglio d'Europa. *Draft Explanatory Report on the modernised version of CoE Convention 108* [Progetto di relazione esplicativa sulla versione modernizzata della convenzione 108 del CdE], punto 75: “gli interessati dovrebbero avere il diritto di conoscere il ragionamento alla base del trattamento dei loro dati, nonché le conseguenze di tale ragionamento, che ha portato a conclusioni conclusive, in particolare nei casi che prevedono l'uso di algoritmi per il processo decisionale automatizzato, compresa la profilazione. Ad esempio nel caso del grado di affidabilità creditizia, gli interessati dovrebbero avere il diritto di conoscere la logica alla base del trattamento dei loro dati risultante in una decisione “sì” o “no” e non semplicemente informazioni sulla decisione stessa. In assenza di comprensione di questi aspetti non potrebbe esserci alcun effettivo esercizio di altre garanzie essenziali quali il diritto di opposizione e il diritto di proporre reclami presso un'autorità competente”. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2>. Accesso effettuato il 24 aprile 2017;

Il titolare del trattamento può utilizzare tecniche visive simili per spiegare come è stata presa una decisione nel passato.

2. **Articolo 15, paragrafo 1, lettera h) - diritto di accesso**

L'articolo 15, paragrafo 1, lettera h), riconosce agli interessati il diritto di disporre delle medesime informazioni in merito a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, rispetto a quelle previste dall'articolo 13, paragrafo 2, lettera f), e dall'articolo 14, paragrafo 2, lettera g), ossia:

- l'esistenza di processi decisionali automatizzati, compresa la profilazione;
- informazioni significative sulla logica utilizzata;
- l'importanza e le conseguenze previste del trattamento per l'interessato.

Il titolare del trattamento dovrebbe aver già fornito tali dati all'interessato in linea con gli obblighi di cui all'articolo 13⁴².

L'articolo 15, paragrafo 1, lettera h), afferma che il titolare del trattamento deve fornire all'interessato informazioni sulle *conseguenze previste* del trattamento, piuttosto che una spiegazione di una *particolare* decisione. Il considerando 63 chiarisce questo aspetto affermando che ogni interessato dovrebbe avere il diritto di accesso al fine di ottenere "comunicazioni" sul trattamento automatizzato dei dati, compresa la logica in questione e, *almeno* quando è basato sulla profilazione, sulle conseguenze del trattamento.

Esercitando i diritti di cui all'articolo 15, l'interessato può prendere atto di una decisione presa nei suoi confronti, ivi compresa una decisione basata sulla profilazione.

Il titolare del trattamento dovrebbe fornire all'interessato informazioni di carattere generale (in particolare, sui fattori presi in considerazione per il processo decisionale e sul rispettivo "peso" a livello aggregato) che sono utili all'interessato anche per contestare la decisione.

F. Stabilire garanzie adeguate

Se la base per il trattamento è l'articolo 22, paragrafo 2, lettera a), oppure l'articolo 22, paragrafo 2, lettera c), l'articolo 22, paragrafo 3 impone al titolare del trattamento di attuare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati. Ai sensi dell'articolo 22, paragrafo 2, lettera b), il diritto degli Stati membri o dell'Unione che autorizza il trattamento deve altresì prevedere misure di adeguate di tutela.

Tali misure dovrebbero includere quanto meno la possibilità per l'interessato di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione.

L'intervento umano è un aspetto fondamentale. Qualsiasi riesame dovrebbe essere effettuato da una persona che dispone dell'autorità e della competenza adeguate per modificare la decisione. Il responsabile di tale riesame dovrebbe effettuare una valutazione approfondita di tutti i dati pertinenti, comprese eventuali informazioni aggiuntive fornite dall'interessato.

⁴² L'articolo 12, paragrafo 3, del regolamento chiarisce le tempistiche per fornire queste informazioni.

Il considerando 71 sottolinea che *in ogni caso* le garanzie adeguate dovrebbero comprendere anche:

la specifica informazione all'interessato e il diritto (...) di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.

Il titolare del trattamento deve mettere a disposizione dell'interessato un modo semplice per esercitare tali diritti.

Ciò sottolinea la necessità di trasparenza del trattamento. L'interessato sarà in grado di contestare una decisione o esprimere il proprio parere soltanto se comprende pienamente come è stata presa la decisione e su quali basi. I requisiti in materia di trasparenza sono discussi nel capitolo IV (sezione E).

Errori o distorsioni nei dati raccolti o condivisi oppure un errore o una distorsione nel processo decisionale automatizzato possono comportare:

- classificazioni errate e
- valutazioni basate su proiezioni imprecise, che
- incidono negativamente sulle persone fisiche.

Il titolare del trattamento dovrebbe effettuare valutazioni frequenti degli insiemi di dati che tratta, in maniera da rilevare eventuali distorsioni, e sviluppare metodi per affrontare eventuali elementi pregiudizievoli, compreso un eccessivo affidamento sulle correlazioni.

I sistemi che verificano gli algoritmi e i riesami periodici dell'esattezza e della pertinenza del processo decisionale automatizzato, compresa la profilazione, sono ulteriori misure utili.

Il titolare del trattamento dovrebbe introdurre procedure e misure adeguate per prevenire errori, inesattezze⁴³ o discriminazioni sulla base di categorie particolari di dati. Queste misure dovrebbero essere attuate ciclicamente; non soltanto in fase di progettazione, ma anche in continuativamente, durante l'applicazione della profilazione alle persone fisiche. L'esito di tali verifiche dovrebbe andare ad alimentare nuovamente la progettazione del sistema.

Ulteriori esempi di garanzie adeguate sono riportati nella sezione dedicata alle [raccomandazioni](#).

V. Minori e profilazione

Il regolamento introduce ulteriori obblighi per il titolare del trattamento qualora tratti dati personali di minori.

L'articolo 22 di per sé non opera alcuna distinzione in merito al fatto che il trattamento riguardi adulti o minori. Tuttavia, il considerando 71 afferma che le decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che producono effetti giuridici o in modo analogo significativi non dovrebbero riguardare minori⁴⁴. Dato che tale formulazione non si riflette nell'articolo stesso, il Gruppo di lavoro non ritiene che ciò rappresenti un divieto assoluto di questo tipo di trattamento in relazione ai minori. Tuttavia, alla luce di tale considerando, il Gruppo di lavoro

⁴³ Il considerando 71 del regolamento afferma che:

“al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, (...)”.

⁴⁴ Considerando 71: “tale misura non dovrebbe riguardare un minore”.

raccomanda al titolare del trattamento di non fare affidamento, di norma, sulle eccezioni di cui all'articolo 22, paragrafo 2, per giustificare tale trattamento.

Potrebbero tuttavia esservi talune circostanze nelle quali è necessario che il titolare del trattamento prenda decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, aventi effetti giuridici o in modo analogo significativi in relazione ai minori, ad esempio per tutelarne il benessere. In tal caso, il trattamento può essere effettuato sulla base delle eccezioni di cui all'articolo 22, paragrafo 2, lettere a), b) o c), a seconda dei casi.

In questi casi devono essere messe in atto garanzie adeguate, come previsto dall'articolo 22, paragrafo 2, lettera b), e dall'articolo 22, paragrafo 3, e devono pertanto essere appropriate per i minori. Il titolare del trattamento deve garantire che tali garanzie siano efficaci nel tutelare i diritti, le libertà e i legittimi interessi dei minori i cui dati vengono trattati.

L'esigenza di una tutela particolare nei confronti dei minori si riflette nel considerando 38 il quale afferma che:

i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di *marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore.*

L'articolo 22 non impedisce al titolare del trattamento di prendere decisioni basate unicamente sul trattamento automatizzato in relazione ai minori, se tali decisioni non avranno un effetto giuridico o in modo analogo significativo sul minore. Tuttavia, una decisione basata unicamente sul trattamento automatizzato che influenza le scelte e il comportamento di un minore potrebbe potenzialmente avere un effetto giuridico o in modo analogo significativo sullo stesso, a seconda della natura delle scelte e dei comportamenti in questione.

Dato che i minori rappresentano un gruppo più vulnerabile della società, le organizzazioni dovrebbero, in generale, astenersi dal profilarli per finalità di marketing⁴⁵. I minori possono essere particolarmente vulnerabili nell'ambiente online e più facilmente influenzabili dalla pubblicità comportamentale. Ad esempio, nei giochi online, la profilazione può servire per individuare i giocatori che l'algoritmo ritiene più propensi a spendere soldi, oltre a fornire annunci più personalizzati. L'età e la maturità del minore possono influenzarne la capacità di comprendere la motivazione che sta alla base di tale tipo di marketing o le sue conseguenze⁴⁶.

⁴⁵ Il parere 02/2013 del Gruppo di lavoro sulle applicazioni per dispositivi intelligenti (WP 202), adottato il 27 febbraio 2013, nella specifica sezione 3.10 dedicata ai minori, a pagina 26, specifica che “i titolari del trattamento del trattamento non dovrebbero trattare dati di minori, direttamente o indirettamente, a fini di pubblicità comportamentale, poiché è al di fuori della portata della comprensione di un minore e pertanto supera i limiti del trattamento lecito”.

⁴⁶ Uno studio dell'UE sull'[impatto del marketing attraverso i media sociali, i giochi online e le applicazioni mobili sul comportamento dei minori](#) (in inglese) ha rilevato che le prassi di marketing hanno un impatto evidente sul comportamento dei minori. Tale studio era basato su minori di età compresa tra 6 e 12 anni.

L'articolo 40, paragrafo 2, lettera g), fa esplicitamente riferimento alla preparazione di codici di condotta che includano misure per la protezione dei minori; potrebbe altresì essere possibile integrare i codici esistenti⁴⁷.

VI. Valutazioni d'impatto sulla protezione dei dati e responsabile della protezione dei dati

La responsabilizzazione è un aspetto importante e un requisito esplicito ai sensi del regolamento⁴⁸.

In quanto strumento essenziale per la responsabilizzazione, la valutazione d'impatto sulla protezione dei dati consente al titolare del trattamento di valutare i rischi connessi al processo decisionale automatizzato, compresa la profilazione. Essa permette di dimostrare che sono state messe in atto misure adeguate per affrontare tali rischi e dimostrare il rispetto del regolamento.

L'articolo 35, paragrafo 3, lettera a), sottolinea la necessità che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati in caso di:

una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche.

L'articolo 35, paragrafo 3, lettera a), fa riferimento a valutazioni comprendenti la profilazione e decisioni che sono “basate” su un trattamento automatizzato, piuttosto che basate “unicamente” su un trattamento automatizzato. Ciò significa che l'articolo 35, paragrafo 3, lettera a), si applicherà sia a un processo decisionale che comprenda la profilazione e abbia effetti giuridici o in modo analogo significativi che *non* è un processo decisionale interamente automatizzato, sia a una decisione basata unicamente sul trattamento automatizzato di cui all'articolo 22, paragrafo 1.

Se il titolare del trattamento prevede un “modello” in cui adotta decisioni basate *unicamente* su un trattamento automatizzato aventi un *impatto elevato* sulle persone fisiche, fondate su *profili* relativi a queste ultime, e *non può* fare affidamento sul consenso di dette persone, su un contratto stipulato con le stesse o su una legge che autorizza tale trattamento, il titolare del trattamento non dovrebbe procedere.

Il titolare del trattamento può comunque prevedere un “modello” di processo decisionale basato sulla profilazione, aumentando significativamente il livello di intervento umano affinché detto modello *non sia più un processo decisionale interamente automatizzato*, sebbene il trattamento possa comunque presentare rischi per i diritti e le libertà fondamentali delle persone. In tal caso, il titolare del trattamento deve assicurarsi di riuscire a far fronte a tali rischi e soddisfare i requisiti esposti al capitolo III delle presenti linee guida.

⁴⁷ Un esempio di un codice di condotta che tratta di marketing nei confronti dei minori è quello prodotto da FEDMA, Codice di condotta - relazione, disponibile (in inglese) all'indirizzo: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Accesso effettuato il 15 maggio 2017. Cfr. in particolare: “6.2 Gli operatori nel settore del marketing che si rivolgono ai minori e per i quali è probabile che i minori costituiscano una parte del loro pubblico, non dovrebbero sfruttare la credulità, la lealtà, vulnerabilità o la mancanza di esperienza dei minori.; 6.8.5 Gli operatori nel settore del marketing non dovrebbero condizionare l'accesso di un minore a un sito web alla raccolta di informazioni personali dettagliate. In particolare, incentivi speciali quali offerte di premi e giochi non dovrebbero essere usati per invogliare i minori a divulgare informazioni personali dettagliate”.

⁴⁸ Come richiesto dall'articolo 5, paragrafo 2, del regolamento.

Una valutazione d'impatto sulla protezione dei dati può altresì costituire uno strumento utile a disposizione del titolare del trattamento per individuare le misure che introdurrà per far fronte ai rischi per la protezione dei dati connessi al trattamento. Tali misure⁴⁹ potrebbero comprendere:

- informare l'interessato dell'esistenza e della logica utilizzata nel processo decisionale automatizzato;
- spiegare l'importanza e le conseguenze previste del trattamento per l'interessato;
- fornire all'interessato i mezzi per opporsi alla decisione;
- consentire all'interessato di esprimere il proprio punto di vista.

Ulteriori attività di profilazione possono giustificare una valutazione d'impatto sulla protezione dei dati, a seconda delle circostanze del caso. Il titolare del trattamento può consultare le linee guida del Gruppo di lavoro sulle valutazioni d'impatto sulla protezione dei dati⁵⁰ per ulteriori informazioni e per contribuire a determinare la necessità di effettuare una valutazione d'impatto sulla protezione dei dati.

Un requisito aggiuntivo in termini di responsabilizzazione consiste nella designazione di un responsabile della protezione dei dati, nei casi in cui la profilazione e/o il processo decisionale automatizzato costituiscono un'attività centrale del titolare del trattamento e richiedono un monitoraggio regolare e sistematico degli interessati su larga scala (articolo 37, paragrafo 1, lettera b)⁵¹.

⁴⁹ Rispecchiando le prescrizioni di cui all'articolo 13, paragrafo 2, lettera f), all'articolo 14, paragrafo 2, lettera g), e all'articolo 22, paragrafo 3.

⁵⁰ Gruppo di lavoro articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679. 4 aprile 2017. <https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati> Accesso effettuato il 24 aprile 2017.

⁵¹ Gruppo di lavoro articolo 29, Linee guida sui responsabili della protezione dei dati. 5 aprile 2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 Accesso effettuato il 22 gennaio 2018.

ALLEGATO 1 - Raccomandazioni sulle buone prassi

Le seguenti raccomandazioni sulle buone prassi aiuteranno il titolare del trattamento a soddisfare i requisiti stabiliti dalle disposizioni del regolamento generale sulla protezione dei dati in materia di profilazione e processo decisionale automatizzato⁵².

Articolo	Questione	Raccomandazione
5, paragrafo 1, lettera a); 12, 13, 14	Diritto di ottenere informazioni	<p>Il titolare del trattamento dovrebbe consultare le linee guida del Gruppo di lavoro sulla trasparenza (WP 260) per i requisiti generali in materia di trasparenza.</p> <p>Oltre ai requisiti generali, quando tratta dati in linea con l'articolo 22, il titolare del trattamento deve fornire informazioni significative sulla logica utilizzata.</p> <p>Anziché fornire una complessa spiegazione matematica su come funzionano gli algoritmi o l'apprendimento automatico, il titolare del trattamento dovrebbe prendere in considerazione l'utilizzo di metodi chiari ed esaustivi per fornire informazioni all'interessato, ad esempio:</p> <ul style="list-style-type: none"> • categorie di dati che sono state o saranno utilizzate nella profilazione o nel processo decisionale; • motivi per i quali tali categorie sono considerate pertinenti; • modalità di creazione del profilo utilizzato nel processo decisionale automatizzato, ivi comprese le statistiche utilizzate nell'analisi; • motivi per i quali tale profilo è pertinente per il processo decisionale automatizzato; • modalità di utilizzo del profilo ai fini di una decisione riguardante l'interessato. <p>Tali informazioni saranno di norma più pertinenti per l'interessato e contribuiranno alla trasparenza del trattamento.</p> <p>Il titolare del trattamento potrebbe prendere in considerazione tecniche di visualizzazione e interattive in maniera da favorire la trasparenza degli algoritmi⁵³.</p>
6, paragrafo 1, lettera a)	Consenso come base per il trattamento	Se si fonda sul consenso come base per il trattamento, il titolare del trattamento dovrebbe consultare le Linee guida del Gruppo di lavoro sul consenso (WP 259).
15	Diritto di	Il titolare del trattamento potrebbe prendere in considerazione l'attuazione di un meccanismo che consenta agli interessati di

⁵² Il titolare del trattamento deve altresì assicurarsi di disporre di solide procedure destinate a garantire che può adempiere i suoi obblighi ai sensi degli articoli da 15 a 22 entro i termini previsti dal regolamento.

⁵³ Information Commissioner's Office – *Big data, artificial intelligence, machine learning and data protection version 2.0* [Megadati, intelligenza artificiale, apprendimento automatico e protezione dei dati versione 2.0], 03/2017. Pagina 87, punto 194, marzo 2017. <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Accesso effettuato il 24 aprile 2017.

	accesso	verificare il loro profilo, compresi i dettagli delle informazioni e le fonti utilizzate per svilupparlo.
16	Diritto di rettifica	<p>Il titolare del trattamento che fornisce agli interessati accesso al loro profilo nel rispetto dei loro diritti di cui all'articolo 15 dovrebbe consentire agli stessi di aggiornare o modificare eventuali inesattezze presenti nei dati o nel profilo. Ciò può altresì aiutare il titolare del trattamento a rispettare gli obblighi di cui all'articolo 5, paragrafo 1, lettera d).</p> <p>Il titolare del trattamento potrebbe prendere in considerazione la possibilità di introdurre strumenti di gestione delle preferenze online, ad esempio un dashboard per la protezione dei dati, permettendo così agli interessati di gestire l'uso delle loro informazioni in una serie di servizi diversi, consentendo loro di modificare le impostazioni, aggiornare i loro dettagli personali e rivedere o modificare il loro profilo per correggere eventuali inesattezze.</p>
Articolo 21, paragrafi 1 e 2	Diritto di opposizione	<p>Il diritto di opposizione di cui all'articolo 21, paragrafi 1 e 2, deve essere esplicitamente portato a conoscenza dell'interessato e presentato chiaramente e separatamente da altre informazioni (articolo 21, paragrafo 4).</p> <p>Il titolare del trattamento deve garantire che tale diritto venga visualizzato in maniera visibile sul suo sito web o in qualsiasi documentazione pertinente e non sia nascosto all'interno di altre condizioni generali di contratto/servizio.</p>
22 e considerando 71	Garanzie adeguate	<p>L'elenco che segue, sebbene non esaustivo, fornisce alcuni suggerimenti di buone prassi che il titolare del trattamento dovrebbe tenere in considerazione quando prende decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione (definite all'articolo 22, paragrafo 1):</p> <ul style="list-style-type: none"> • controlli regolari di garanzia della qualità dei sistemi per assicurare che le persone siano trattate in maniera equa e non siano discriminate sulla base di categorie particolari di dati personali o in altro modo; • verifica degli algoritmi – testare gli algoritmi utilizzati e sviluppati dai sistemi di apprendimento automatico per dimostrare che stanno effettivamente funzionando come previsto e non producono risultati discriminatori, errati o ingiustificati; • per l'audit indipendente di “terzi” (laddove il processo decisionale basato sulla profilazione abbia un impatto elevato sulle persone fisiche), fornitura all'ispettore di tutte le informazioni necessarie su come funziona l'algoritmo o il sistema di apprendimento automatico; • per gli algoritmi di terzi, ottenimento di garanzie contrattuali che sono stati effettuati audit e test e che l'algoritmo è conforme alle norme concordate; • misure specifiche per la minimizzazione dei dati al fine di prevedere periodi di conservazione chiari per i profili e per tutti i dati personali utilizzati durante la creazione o l'applicazione dei profili;

		<ul style="list-style-type: none"> • utilizzo di tecniche di anonimizzazione o pseudonimizzazione nel contesto della profilazione; • modi per consentire all'interessato di esprimere il proprio punto di vista e contestare la decisione; • un meccanismo per l'intervento umano in determinati casi, ad esempio fornendo un collegamento a una procedura di ricorso nel momento in cui la decisione automatizzata viene trasmessa all'interessato, con termini concordati per il riesame e la designazione di un punto di contatto per qualsiasi domanda. <p>Il titolare del trattamento può altresì valutare opzioni quali:</p> <ul style="list-style-type: none"> • meccanismi di certificazione per i trattamenti; • codici di condotta per la verifica dei processi che comportano apprendimento automatico; • comitati di revisione etica per valutare i potenziali danni e benefici per la società di particolari applicazioni per la profilazione.
--	--	---

ALLEGATO 2 – Principali disposizioni del regolamento

Principali disposizioni del regolamento che fanno riferimento alla profilazione e al processo decisionale automatizzato in generale

Articolo	Considerando	Osservazioni
3, paragrafo 2, lettera b)	24	<p>Il monitoraggio del comportamento [degli interessati] nella misura in cui tale comportamento ha luogo all'interno dell'Unione.</p> <p>Considerando 24: “ (...) tracciate su internet (...) ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, <i>in particolare per adottare decisioni</i> che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali”.</p>

4, paragrafo 4	30	Articolo 4, paragrafo 4 definizione di profilazione Considerando 30: “identificativi online (...), quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza (...) possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, <i>possono essere utilizzate per creare profili delle persone fisiche e identificarle</i> ”.
5 e 6	72	Considerando 72: “la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento (articolo 6) o i principi di protezione dei dati (articolo 5)”.
8	38	Utilizzo dei dati personali dei minori per la profilazione. Considerando 38: “I minori meritano una specifica protezione (...) in particolare [in merito al]l’uso dei dati personali dei minori a fini di (...) creazione di profili di personalità o di utente”.
13 e 14	60	Diritto di essere informato. Considerando 60: “inoltre l’interessato [<i>deve</i>] <i>essere informato dell’esistenza di una profilazione e delle conseguenze della stessa</i> ”.
15	63	Diritto di accesso. Considerando 63: “diritto di conoscere e ottenere comunicazioni (...) in relazione alla finalità per cui i dati personali sono trattati (...) e, <i>almeno</i> quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento”.
21, paragrafi 1, 2 e 3	70	Diritto di opposizione alla profilazione. Considerando 70: “(…) il diritto (...) di opporsi a tale trattamento (...), compresa la profilazione nella misura in cui sia connessa a tale marketing diretto”.
23	73	Considerando 73: “il diritto dell’Unione o degli Stati membri può imporre limitazioni a specifici principi e (...) al diritto di opporsi, alle decisioni basate sulla profilazione (...), ove ciò sia necessario e proporzionato in una società democratica (...)” per la tutela di obiettivi specifici di interesse pubblico generale.
35, paragrafo 3, lettera a)	91	Una valutazione d’impatto sulla protezione dei dati è necessaria nel caso di una “valutazione sistematica e globale di aspetti personali relativi a persone fisiche, <i>basata</i> su un trattamento automatizzato, che include la profilazione, e in base al quale si adottano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche”. Riguarda il processo decisionale, compresa la profilazione, che è non si basa unicamente su un trattamento automatizzato.

Principali disposizioni del regolamento che fanno riferimento al processo decisionale automatizzato di cui all'articolo 22

Articolo	Considerando	Osservazioni
13, paragrafo 2, lettera f) e 14, paragrafo 2, lettera g)	61	<p>Diritto di essere informato in merito a:</p> <ul style="list-style-type: none"> • esistenza di processi decisionali automatizzati ai sensi dell'articolo 22, paragrafi 1 e 4; • informazioni significative sulla logica utilizzata; • importanza e conseguenze previste del trattamento.
15, lettera h)		<p>Diritti di accesso specifici alle informazioni sull'esistenza di un processo decisionale unicamente automatizzato, compresa la profilazione.</p>
22, paragrafo 1	71	<p>Divieto di processo decisionale basato unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici/in modo analogo significativi.</p> <p>Oltre alla spiegazione fornita nel corpo principale delle linee guida, i seguenti punti ampliano la logica per la lettura dell'articolo 22 come un divieto:</p> <ul style="list-style-type: none"> • sebbene il capo III riguardi i diritti dell'interessato, le disposizioni di cui agli articoli 12-22 non riguardano esclusivamente l'esercizio <i>attivo</i> di diritti. Taluni dei diritti sono <i>passivi</i>; non si riferiscono tutti a situazioni nelle quali l'interessato intraprende un'azione, ovvero effettua una richiesta o un reclamo o una domanda di qualche tipo. Gli articoli 15-18 e 20-21 riguardano l'interessato che esercita attivamente i suoi diritti, mentre gli articoli 13 e 14 riguardano i doveri che il titolare del trattamento deve adempiere senza alcun coinvolgimento attivo dell'interessato. Di conseguenza l'inclusione dell'articolo 22 in tale capo non significa di per sé che si tratti di un diritto di opposizione; • l'articolo 12, paragrafo 2, riguarda l'esercizio dei "diritti dell'interessato" ai sensi degli articoli da 15 a 22; ma ciò non significa che l'articolo 22, paragrafo 1 stesso debba essere interpretato come un diritto. All'articolo 22 vi è un diritto attivo, tuttavia esso rientra nelle garanzie che devono essere applicate nei casi in cui è consentito il processo decisionale automatizzato [articolo 22, paragrafo 2, lettere da a) a c)] - il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione. Si applica soltanto in tali casi, poiché è vietato lo svolgimento del trattamento descritto nell'articolo 22, paragrafo 1, su altre basi; • l'articolo 22 si trova in una sezione del regolamento denominata "Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche", il che implica che l'articolo 22 <i>non</i> contiene un diritto di opposizione come l'articolo 21. Ciò è ulteriormente sottolineato dalla mancanza nell'articolo 22 di un obbligo di informazione

		<p>esplicitamente equivalente a quello di cui all'articolo 21, paragrafo 4;</p> <ul style="list-style-type: none"> • se l'articolo 22 dovesse essere interpretato come un diritto di opposizione, l'eccezione di cui all'articolo 22, paragrafo 2, lettera c), non avrebbe molto senso. L'eccezione afferma che il processo decisionale automatizzato può comunque avere luogo se l'interessato ha fornito il proprio consenso esplicito (cfr. in appresso). Ciò sarebbe contraddittorio in quanto l'interessato non può opporsi e acconsentire al medesimo trattamento; • un'opposizione comporterebbe l'obbligo di eseguire l'intervento umano. Le eccezioni di cui all'articolo 22, paragrafo 2, lettere a) e c), prevalgono sulla norma principale di cui all'articolo 22, paragrafo 1, tuttavia soltanto fino a quando l'intervento umano è disponibile per l'interessato, come specificato all'articolo 22, paragrafo 3. Poiché l'interessato (opponendosi) ha già richiesto l'intervento umano, l'articolo 22, paragrafo 2, lettere a) e c), sarebbe automaticamente eluso in ogni caso, rendendo così tali lettere prive di significato. <p>Considerando 71: “(…) Tale trattamento comprende la ‘profilazione’, che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato” (...) <i>“Tale misura non dovrebbe riguardare un minore”</i>.</p>
22, paragrafo 2, lettere da a) a c)	71	<p>L'articolo 22, paragrafo 2 deroga al divieto di trattamento basato: a) sull'esecuzione o la stipula di un contratto; b) sul diritto dell'Unione o degli Stati membri; o c) sul consenso esplicito.</p> <p>Il considerando 71 fornisce ulteriore contesto in merito al articolo 22, paragrafo 2, lettera b), e afferma che il trattamento descritto all'articolo 22, paragrafo 1: “se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento (...)”.</p>
22, paragrafo 3	71	<p>L'articolo 22, paragrafo 3 e il considerando 71 specificano inoltre che anche nei casi di cui all'articolo 22, paragrafo 2, lettere a) e c), il trattamento dovrebbe essere soggetto a garanzie adeguate.</p> <p>Considerando 71: “che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore”.</p>

23	73	Considerando 73: “il diritto dell’Unione o degli Stati membri può imporre limitazioni a specifici principi e (...) al diritto di opporsi, alle decisioni basate sulla profilazione (...), ove ciò sia necessario e proporzionato in una società democratica (...)” per la tutela di obiettivi specifici di interesse pubblico generale.
35, paragrafo 3, lettera a)	91	Come va svolta una valutazione d’impatto sulla protezione dei dati?
47, paragrafo 2, lettera e)		Norme vincolanti d’impresa di cui all’ articolo 47, paragrafo 1 , dovrebbero specificare almeno “(...) il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell’ articolo 22 (...)”.

ALLEGATO 3 - Approfondimenti

Le presenti linee guida tengono conto di quanto segue:

- [Gruppo di lavoro, Documento di consulenza sugli elementi essenziali di una definizione e una disposizione sulla profilazione nel contesto del regolamento generale sulla protezione dei dati dell’UE, adottato il 13 maggio 2013 \(in inglese\);](#)
- [Gruppo di lavoro, Parere 2/2010 sulla pubblicità comportamentale online, WP 171;](#)
- [Gruppo di lavoro, Parere 03/2013 sulla limitazione della finalità, WP 203 \(in inglese\);](#)
- [Gruppo di lavoro, Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell’articolo 7 della direttiva 95/46/CE, WP 217;](#)
- [Gruppo di lavoro, Dichiarazione sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, WP 218, \(in inglese\);](#)
- [Gruppo di lavoro, Parere 8/2014 sui recenti sviluppi nel campo dell’Internet degli oggetti, WP 223;](#)
- [Gruppo di lavoro, Linee guida sui responsabili della protezione dei dati, WP 243;](#)
- [Gruppo di lavoro, Linee guida per l’individuazione dell’autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, WP 244;](#)
- [Gruppo di lavoro, Linee guida sul consenso, WP 259 \(in inglese\);](#)
- [Gruppo di lavoro, Linee guida sulla trasparenza, WP 260 \(in inglese\);](#)
- [Consiglio d’Europa. Raccomandazione CM/Rec \(2010\)13 sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione;](#)
- [Consiglio d’Europa. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 01/2017 \(in inglese\);](#)
- [Information Commissioner’s Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017 \(in inglese\);](#)
- [Office of the Australian Commissioner - Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016 \(in inglese\);](#)

- [Garante europeo della protezione dei dati \(GEPD\) Parere 7/2015 – *Meeting the challenges of big data*, 19 novembre 2015 \(in inglese\);](#)
- [Datatilsynet – *Big Data – privacy principles under pressure* 09/2013 \(in inglese\);](#)
- Consiglio d'Europa. Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale - [Progetto di relazione esplicativa sulla versione modernizzata della convenzione 108 del CdE](#), agosto 2016 (in inglese);
- [Datatilsynet – *The Great Data Race – How commercial utilisation of personal data challenges privacy. Report*, novembre 2015 \(in inglese\);](#)
- [Garante europeo della protezione dei dati – *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* \(in inglese\);](#)
- Comitato congiunto delle autorità europee di vigilanza. *Joint Committee Discussion Paper on the use of Big Data by financial institutions* 2016-86 (in inglese).
https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf;
- Commission de la protection de la vie privée. *Big Data Rapport*
<https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20voor%20MindMap%2022-02-17%20fr.pdf>;
- Senato degli Stati Uniti, Comitato per il commercio, la scienza e i trasporti. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, rapporto informativo per il presidente Rockefeller, 18 dicembre 2013 (in inglese).
<https://www.commerce.senate.gov/public/cache/files/Od2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf>;
- Lilian Edwards e Michael Veale. *Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for* (in inglese). Documento di ricerca, pubblicato il 24 maggio 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855;
- NYTimes.com. *Showing the Algorithms behind New York City Services*.
<https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx&=1>. Accesso effettuato il 24 agosto 2017;
- Consiglio d'Europa. Raccomandazione CM/REC (2018)x del Comitato dei Ministri agli Stati membri sugli orientamenti per promuovere, proteggere e adempiere i diritti dei minori nell'ambiente digitale (progetto riveduto, 25 luglio 2017) (in inglese).
<https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren>. Accesso effettuato il 31 agosto 2017;
- Unicef. *Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World* (in inglese).
https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Accesso effettuato il 31 agosto 2017;
- Camera dei Lord. *Growing up with the internet*. Select Committee on Communications, Seconda relazione delle sessioni 2016–17 (in inglese).
<https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm>. Accesso effettuato il 31 agosto 2017;
- Sandra Wachter, Brent Mittelstadt e Luciano Floridi. *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, 28 dicembre 2016 (in inglese). https://www.turing.ac.uk/research_projects/data-ethics-group-deg/. Accesso effettuato il 13 dicembre 2017.
- Sandra Wachter, Brent Mittelstadt e Chris Russell. *Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 6 ottobre 2017 (in inglese).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Accesso effettuato il 13 dicembre 2017;

- Governo australiano. *Better Practice Guide, Automated Assistance in Administrative Decision-Making. Six steps methodology, plus summary of checklist points Part 7*, febbraio 2007 (in inglese).
<https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf>.
Accesso effettuato il 9 gennaio 2018.