



17/EN

WP251rev.01

**Linee guida sul processo decisionale e profilazione individuale automatizzata
ai fini del Regolamento 2016/679**

Adozione da parte del 3 ottobre 2017

Come rivisto e adottato il 6 febbraio 2018

Questo gruppo di lavoro istituito dall'articolo 29 della direttiva 95/46 / CE. È un organo consultivo europeo indipendente sulla protezione dei dati e sulla privacy. I suoi compiti sono descritti all'articolo 30 della direttiva 95/46 / CE e all'articolo 15 della direttiva 2002/58 / CE.

Il segretariato è fornito dalla direzione C (diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B-1049 Bruxelles, Belgio, ufficio n. MO-59 02/013.

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

IL GRUPPO DI LAVORO SULLA PROTEZIONE DEI SINGOLI PER QUANTO RIGUARDA IL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46 / CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti gli articoli 29 e 30,

visto il suo regolamento,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Courtesy translation
PRIVACYLAB

SOMMARIO

I.	INTRODUZIONE	5
II.	DEFINIZIONI	6
A.	PROFILING.....	6
B.	PROCESSO DECISIONALE AUTOMATIZZATO.....	8
C.	COME IL GDPR AFFRONTA I CONCETTI.....	8
III.	DISPOSIZIONI GENERALI SULLA PROFILAZIONE E IL PROCESSO DECISIONALE AUTOMATIZZATO	9
A.	PRINCIPI DI PROTEZIONE DEI DATI.....	9
1.	<i>Articolo 5, paragrafo 1, lettera a) - lecito, equo e trasparente</i>	9
2.	<i>Articolo 5, paragrafo 1, lettera b) Ulteriore elaborazione e limitazione delle finalità</i>	11
3.	<i>Articolo 5, paragrafo 1, lettera c), riduzione dei dati</i>	11
4.	<i>Articolo 5, paragrafo 1, lettera d) Precisione</i>	11
5.	<i>Articolo 5, paragrafo 1, lettera e) Limitazione dello spazio di archiviazione</i>	12
B.	BASI LEGALI PER L'ELABORAZIONE.....	12
1.	<i>Articolo 6 (1) (a) consenso</i>	12
2.	<i>Articolo 6, paragrafo 1, lettera b): necessario per l'esecuzione di un contratto</i>	13
3.	<i>Articolo 6, paragrafo 1, lettera c): necessario per adempiere a un obbligo giuridico</i>	13
4.	<i>Articolo 6 (1) (d) - necessario per proteggere gli interessi vitali</i>	14
5.	<i>Articolo 6, paragrafo 1, lettera e) - necessario per l'esecuzione di un compito di interesse pubblico o di esercizio di pubblici poteri</i>	14
6.	<i>Articolo 6 (1) (f) - necessario per gli interessi legittimi¹⁸ perseguito dal Titolare del Trattamento o da un terzo</i>	14
C.	ARTICOLO 9 - CATEGORIE SPECIALI DI DATI.....	15
D.	DIRITTI DELL'INTERESSATO ²²	15
1.	<i>Articoli 13 e 14 - Diritto di essere informato</i>	16
2.	<i>Articolo 15 - Diritto di accesso</i>	17
3.	<i>Articolo 16 - Diritto alla rettifica, Articolo 17 Diritto alla cancellazione e Articolo 18 Diritto alla restrizione del trattamento</i>	17
4.	<i>Articolo 21 - Diritto di opporsi</i>	18
IV.	DISPOSIZIONI SPECIFICHE RELATIVE AL PROCESSO DECISIONALE ESCLUSIVAMENTE AUTOMATIZZATO COME DEFINITO ALL'ARTICOLO 22	19
A.	"DECISIONE BASATA UNICAMENTE SULL'ELABORAZIONE AUTOMATIZZATA".....	20
B.	EFFETTI "LEGALI" O "SIMILMENTE SIGNIFICATIVI".....	21
C.	ECCEZIONI DAL DIVIETO.....	23
1.	<i>Esecuzione di un contratto</i>	23

2	<i>Autorizzato dal diritto dell'Unione o dello Stato membro</i>	23
3	<i>Consenso esplicito</i>	25
D.	CATEGORIE SPECIALI DI DATI PERSONALI - ARTICOLO 22, PARAGRAFO 4	25
E.	DIRITTI DELL'INTERESSATO 37	25
4	<i>Articolo 13 (2) (f) e 14 (2) (g) - Diritto di essere informato</i>	25
5	<i>Articolo 15, paragrafo 1, lettera h) - Diritto di accesso</i>	27
F.	STABILIRE GARANZIE APPROPRIATE	28
V.	BAMBINI E PROFILAZIONE	29
VI.	VALUTAZIONE DELL'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) E RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)	30
	ALLEGATO 1 - RACCOMANDAZIONI SULLE BUONE PRATICHE	32
	ALLEGATO 2 - PRINCIPALI DISPOSIZIONI DEL GDPR	34
	PRINCIPALI DISPOSIZIONI GDPR CHE FANNO RIFERIMENTO ALLA PROFILAZIONE GENERALE E AL PROCESSO DECISIONALE AUTOMATIZZATO	34
	PRINCIPALI DISPOSIZIONI DEL GDPR CHE FANNO RIFERIMENTO AL PROCESSO DECISIONALE AUTOMATIZZATO COME DEFINITO ALL'ARTICOLO 22	35
	ALLEGATO 3 - APPROFONDIMENTI	37

Courtesy translation
 PRIVACYLAB

I. introduzione

Il regolamento generale sulla protezione dei dati (GDPR), in particolare, riguarda la profilazione e il processo decisionale individuale automatizzato, compresa la profilazione. ¹

Il profiling e il processo decisionale automatizzato sono utilizzati in un numero crescente di settori, sia privati che pubblici. Banche e finanza, sanità, fiscalità, assicurazioni, marketing e pubblicità sono solo alcuni esempi dei settori in cui la profilazione viene effettuata con maggiore regolarità per aiutare il processo decisionale.

I progressi tecnologici e le capacità di analisi dei big data, intelligenza artificiale e apprendimento automatico hanno reso più facile la creazione di profili e decisioni automatiche con il potenziale di incidere in modo significativo sui diritti e sulle libertà delle persone.

La diffusa disponibilità di dati personali su Internet e dai dispositivi Internet of Things (IoT) e la capacità di trovare correlazioni e creare collegamenti, può consentire di determinare, analizzare e prevedere aspetti della personalità o del comportamento di un individuo, interessi e abitudini.

La profilazione e il processo decisionale automatizzato possono essere utili per individui e organizzazioni, offrendo vantaggi quali:

- maggiore efficienza; e
- risparmio di risorse.

Hanno molte applicazioni commerciali, ad esempio, possono essere utilizzate per segmentare meglio i mercati e adattare servizi e prodotti per allinearsi alle esigenze individuali. Anche la medicina, l'istruzione, l'assistenza sanitaria e i trasporti possono beneficiare di questi processi.

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

Questi processi possono essere opachi. Gli individui potrebbero non sapere di essere profilati o capire cosa è coinvolto.

La profilazione può perpetuare stereotipi esistenti e segregazione sociale. Può anche bloccare una persona in una categoria specifica e limitarle alle loro preferenze suggerite.

¹ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati, e di abrogazione della direttiva 95/46 / CE. La definizione di profili e il processo decisionale individuale automatizzato sono anche disciplinati dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, dell'indagine, dell'individuazione o del perseguimento di reati o dell'esecuzione di sanzioni penali e della libera circolazione di tali dati. Mentre queste linee guida si concentrano sulla profilazione e sull'autocomposizione individuale delle decisioni nell'ambito del GDPR, la guida è anche pertinente per quanto riguarda i due argomenti di cui alla direttiva 2016/680, in relazione alle loro analoghe disposizioni. L'analisi delle caratteristiche specifiche della profilazione e del processo decisionale individuale automatizzato ai sensi della direttiva 2016/680 non è inclusa in queste linee guida, poiché gli orientamenti al riguardo sono forniti dal parere W P258 "Parere su alcune questioni chiave della direttiva sull'applicazione della legge (UE 2016/680) ", adottato dal WP29 il 29 novembre 2017. Il presente parere riguarda il processo decisionale e profiling individuale automatizzato nel contesto dell'elaborazione dei dati da parte delle forze dell'ordine alle pagine 11-14 ed è disponibile all'indirizzo: http://ec.europa.eu/newsroom/article29/item-detail.cfm?ite_m_id=610178

Ciò può minare la loro libertà di scegliere, ad esempio, determinati prodotti o servizi come libri, musica o newsfeed. In alcuni casi, la profilazione può portare a previsioni imprecise. In altri casi può portare a negare servizi e beni e discriminazioni ingiustificate.

Il GDPR introduce nuove disposizioni per affrontare i rischi derivanti dalla profilazione e dal processo decisionale automatizzato, in particolare, ma non limitato, alla privacy. Lo scopo di queste linee guida è quello di chiarire tali disposizioni.

Questo documento copre:

- Definizioni di profilazione e processo decisionale automatizzato e l'approccio GDPR a questi in generale - [Capitolo II](#)
- Disposizioni generali in materia di profilazione e processo decisionale automatizzato - [Capitolo III](#)
- Disposizioni specifiche relative al processo decisionale esclusivamente automatizzato definito all'articolo 22 - [Capo IV](#)
- Bambini e profilazione - [Capitolo V](#)
- Valutazioni d'impatto sulla protezione dei dati e responsabili della protezione dei dati - [Capitolo VI](#)

Gli allegati forniscono raccomandazioni sulle migliori pratiche, sulla base dell'esperienza acquisita negli Stati membri dell'UE.

Il Gruppo di lavoro sulla protezione dei dati ai sensi dell'articolo 29 (WP29) controllerà l'attuazione di questi orientamenti e potrà completarli con ulteriori dettagli, a seconda dei casi.

II. definizioni

Il GDPR introduce disposizioni per garantire che la profilazione e il processo decisionale individuale automatizzato (che includa o meno la profilazione) non siano utilizzati in modi che hanno un impatto ingiustificato sui diritti delle persone; per esempio:

- specifici requisiti di trasparenza ed equità;
- maggiori obblighi di responsabilità;
- basi legali specificate per l'elaborazione;
- i diritti delle persone di opporsi alla profilazione e alla specifica profilazione per il marketing; e
- se sono soddisfatte determinate condizioni, è necessario effettuare una valutazione dell'impatto sulla protezione dei dati.

Il GDPR non si concentra solo sulle decisioni prese come risultato dell'elaborazione o della profilazione automatizzata. Si applica alla raccolta di dati per la creazione di profili, nonché all'applicazione di tali profili alle persone.

A. profiling

Il GDPR definisce la profilazione di cui all'articolo 4, paragrafo 4 come:

qualsiasi forma di trattamento automatizzato di dati personali consistente nell'uso di dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti le prestazioni di tale persona fisica sul lavoro, situazione economica, salute, preferenze personali, interessi , affidabilità, comportamento, posizione o movimenti;

Il profilo è composto da tre elementi:

- deve essere una forma automatizzata di elaborazione;
- deve essere effettuato su dati personali; e
- l'obiettivo della profilazione deve essere quello di valutare gli aspetti personali di una persona fisica.

L'articolo 4, paragrafo 4, fa riferimento a "qualsiasi forma di trattamento automatizzato" anziché il trattamento "esclusivamente" automatizzato (di cui all'articolo 22). La profilazione deve implicare una qualche forma di elaborazione automatizzata - sebbene il coinvolgimento umano non porti necessariamente l'attività fuori dalla definizione.

La profilazione è una procedura che può comportare una serie di detrazioni statistiche. Viene spesso usato per fare previsioni sulle persone, usando dati provenienti da varie fonti per dedurre qualcosa su un individuo, in base alle qualità di altri che appaiono statisticamente simili.

Il GDPR afferma che la profilazione è l'elaborazione automatizzata di dati personali per valutare aspetti personali, in particolare per analizzare o fare previsioni su individui. L'uso della parola "valutando" suggerisce che la profilazione implica una qualche forma di valutazione o giudizio su una persona.

Una semplice classificazione di individui basata su caratteristiche note come età, sesso e altezza non porta necessariamente alla profilazione. Ciò dipenderà dallo scopo della classificazione.

Ad esempio, un'azienda potrebbe voler classificare i propri clienti in base all'età o al sesso a fini statistici e acquisire una panoramica aggregata dei propri clienti senza fare previsioni o trarre conclusioni su un individuo. In questo caso, lo scopo non è la valutazione delle caratteristiche individuali e quindi non è la profilazione.

Il GDPR è ispirato ma non identico alla definizione di profiling nella Raccomandazione CM / Rec (2010) 13² del Consiglio d'Europa (la Raccomandazione), in quanto la Raccomandazione esclude l'elaborazione che non include l'inferenza. Tuttavia, la Raccomandazione spiega utilmente che la profilazione può coinvolgere tre fasi distinte:

- raccolta dati;
- analisi automatizzata per identificare correlazioni;
- applicare la correlazione a un individuo per identificare le caratteristiche del comportamento presente o futuro.

I Titolari del Trattamento che effettuano la profilatura dovranno assicurarsi di soddisfare i requisiti del PIL R in relazione a tutte le fasi sopra descritte.

In generale, la profilazione implica la raccolta di informazioni su un individuo (o gruppo di individui) e la valutazione delle loro caratteristiche o modelli di comportamento al fine di inserirli in una determinata categoria o gruppo, in particolare per analizzare e / o fare previsioni su, ad esempio, il loro :

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

² Consiglio d'Europa. La protezione delle persone rispetto al trattamento automatico dei dati personali nel contesto della profilazione. Raccomandazione CM / Rec (2010) 13 e memorandum esplicativo. 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 24 aprile 2017

Esempio

Un broker di dati raccoglie dati da diverse fonti pubbliche e private, per conto dei suoi clienti o per i propri scopi. Il broker di dati compila i dati per sviluppare profili sugli individui e li inserisce in segmenti. Vende queste informazioni alle aziende che desiderano migliorare il targeting dei loro beni e servizi. Il broker di dati esegue la profilazione inserendo una persona in una determinata categoria in base ai propri interessi.

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

B. Processo decisionale automatizzato

Il processo decisionale automatizzato ha una portata diversa e può parzialmente sovrapporsi o risultare dalla profilazione. Il processo decisionale esclusivamente automatico è la capacità di prendere decisioni con mezzi tecnologici senza coinvolgimento umano. Le decisioni automatizzate possono essere basate su qualsiasi tipo di dati, ad esempio:

- dati forniti direttamente dalle persone interessate (come le risposte a un questionario);
- dati osservati sulle persone (come i dati sulla posizione raccolti tramite un'applicazione);
- dati derivati o dedotti come un profilo dell'individuo che è già stato creato (ad esempio un punteggio di credito).

Le decisioni automatizzate possono essere prese con o senza profilazione; la profilazione può avvenire senza prendere decisioni automatizzate. Tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Qualcosa che inizia come un semplice processo decisionale automatico potrebbe diventare basato sulla profilazione, a seconda di come vengono utilizzati i dati.

Esempio

Imporre multe per eccesso di velocità esclusivamente sulla base delle prove fornite dagli autovelox è un processo decisionale automatico che non implica necessariamente la profilazione.

Sarebbe tuttavia una decisione basata sulla profilazione se le abitudini di guida dell'individuo fossero monitorate nel tempo e, ad esempio, l'ammontare della multa imposta sia il risultato di una valutazione che coinvolge altri fattori, ad esempio se l'eccesso di velocità è un ripetere l'infrazione o se il conducente ha avuto altre violazioni del traffico recenti.

Le decisioni che non sono solo automatizzate potrebbero anche includere la profilazione. Ad esempio, prima di concedere un mutuo, una banca può prendere in considerazione il punteggio di credito del mutuatario, con ulteriori interventi significativi effettuati dagli esseri umani prima che qualsiasi decisione venga applicata a un individuo.

C. Come il GDPR affronta i concetti

Esistono potenzialmente tre modi in cui è possibile utilizzare il profilo:

- (i) profilazione generale;
- (ii) processo decisionale basato sulla profilazione; e
- (iii) il processo decisionale esclusivamente automatizzato, compresa la profilazione, che produce effetti giuridici o interessa in modo significativo la persona interessata (articolo 22 [1]).

La differenza tra (ii) e (iii) è meglio dimostrata dai seguenti due esempi in cui un individuo richiede un prestito online:

- un umano decide se concordare il prestito sulla base di un profilo prodotto con mezzi puramente automatizzati (ii);
- un algoritmo decide se il prestito è concordato e la decisione viene consegnata automaticamente all'individuo, senza alcuna valutazione preventiva e significativa da parte di un essere umano (iii).

I Titolari del Trattamento possono effettuare il profiling e il processo decisionale automatico purché possano soddisfare tutti i principi e avere una base legale per l'elaborazione. Ulteriori salvaguardie e restrizioni si applicano nel caso di decisioni esclusivamente automatizzate, compresa la profilazione, definite all'articolo 22, paragrafo 1.

Il Capitolo III di queste linee guida spiega le disposizioni del GDPR per tutti i processi decisionali individuali e di profilazione. Ciò include i processi decisionali non solo automatizzati.

Il capitolo IV di queste linee guida spiega le disposizioni specifiche che si applicano solo al processo decisionale individuale esclusivamente automatizzato, inclusa la profilazione.³ Un divieto generale su questo tipo di trattamento esiste per riflettere i potenziali rischi per i diritti e le libertà delle persone.

III. Disposizioni generali sulla profilazione e il processo decisionale automatizzato

Questa panoramica delle disposizioni si applica a tutti i processi decisionali di profilazione e automatizzazione. Si applicano ulteriori disposizioni specifiche di cui al capo IV se il trattamento soddisfa la definizione di cui all'articolo 22, paragrafo 1.

A. Principi di protezione dei dati

I principi sono rilevanti per tutti i profili e il processo decisionale automatizzato che coinvolge i dati personali.⁴ Per facilitare la conformità, i Titolari del Trattamento dovrebbero considerare le seguenti aree chiave:

1. Articolo 5, paragrafo 1, lettera a) - lecito, equo e trasparente

La trasparenza dell'elaborazione⁵ è un requisito fondamentale del GDPR.

Il processo di profilazione è spesso invisibile all'interessato. Funziona creando dati derivati o dedotti su individui - "nuovi" dati personali che non sono stati forniti direttamente dagli stessi soggetti di dati. Gli individui hanno livelli diversi di comprensione e potrebbero trovare difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati.

Ai sensi dell'articolo 12.1, il Titolare del Trattamento deve fornire agli interessati informazioni concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei loro dati personali.⁶

³ Come definito nell'articolo 22, paragrafo 1, del GDPR.

⁴ GDPR - Considerando 72 "La profilazione è soggetta alle regole del presente regolamento che disciplinano il trattamento dei dati personali, quali i motivi giuridici per il trattamento o i principi di protezione dei dati."

⁵ Le linee guida sulla trasparenza del WP29 riguardano in generale la trasparenza e in particolare il gruppo di lavoro sull'articolo 29 sulla protezione dei dati. Linee guida sulla trasparenza ai sensi del Regolamento 2016/679 WP260, 28 novembre 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accesso 18 dicembre 2017.

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

Esempio

Alcuni assicuratori offrono tariffe e servizi assicurativi in base al comportamento di guida di una persona. Gli elementi presi in considerazione in questi casi potrebbero includere la distanza percorsa, il tempo trascorso a guidare e il viaggio intrapreso, nonché le previsioni basate su altri dati raccolti dai sensori in un'auto (intelligente). I dati raccolti vengono utilizzati per il profiling per identificare comportamenti di guida errati (come accelerazione veloce, frenata improvvisa e eccesso di velocità). Queste informazioni possono essere incrociate con altre fonti (ad esempio il tempo, il traffico, il tipo di strada) per capire meglio il comportamento del guidatore.

Il Titolare del Trattamento deve assicurarsi di avere una base legale per questo tipo di elaborazione. 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 implicita e sul significato e le conseguenze previste di tale elaborazione.

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

Anche l'elaborazione deve essere equa e trasparente.

La profilazione può essere ingiusta e creare discriminazioni, ad esempio negando alle persone l'accesso a opportunità di lavoro, credito o assicurazioni o indirizzandole a prodotti finanziari eccessivamente rischiosi o costosi. L'esempio seguente, che non rispetterebbe i requisiti dell'articolo 5, paragrafo 1, lettera a), illustra come una profilazione ingiusta possa portare ad alcuni consumatori ad offrire offerte meno interessanti di altri.

Esempio

Un broker di dati vende i profili dei consumatori alle società finanziarie senza il permesso del consumatore o la conoscenza dei dati sottostanti. I profili definiscono i consumatori in categorie (con titoli come "Rurale e a malapena", "Stragieri etnici della Seconda Città", "Inizio difficile: Young Single Parents, ") o "punteggio", concentrandosi sulla vulnerabilità finanziaria dei consumatori. Le società finanziarie offrono a questi consumatori i prestiti di giorno di paga e altri servizi finanziari "non tradizionali" (prestiti ad alto costo e altri prodotti finanziariamente rischiosi).⁷

⁶ Ufficio del Commissario australiano per l'informazione. Bozza di consultazione: Guida ai big data e ai Principi sulla privacy australiani, 05/2016 dice: "Le informative privacy devono comunicare le pratiche di gestione delle informazioni in modo chiaro e semplice, ma anche in modo completo e con una specificità sufficiente per essere significativi. *La stessa tecnologia che porta a una maggiore raccolta di informazioni personali offre anche l'opportunità di comunicazioni sulla privacy 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 24 aprile 2017

⁷ Questo esempio è tratto da: Senato degli Stati Uniti, comitato per il commercio, la scienza e i trasporti. Una revisione del settore dei broker di dati: Raccolta, utilizzo e vendita di dati sui consumatori per scopi di marketing, rapporto del personale per il presidente Rockefeller, 18 dicembre 2013. <https://www.commerce.senate.gov/public/cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-comme-rcce-co-mmitee-report-on-data-broker-industry.pdf>. Vedi pagina ii del Sommario esecutivo e in particolare 12 del corpo principale del documento. Accesso 21 luglio 2017

2. Articolo 5, paragrafo 1, lettera b) Ulteriore elaborazione e limitazione delle finalità

La profilazione può comportare l'utilizzo di dati personali originariamente raccolti per qualcos'altro.

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 anche utilizzati per costruire un profilo sull'interessato per scopi di marketing - per identificare le proprie preferenze alimentari o lo stile di vita in generale. L'interessato si aspetta che i suoi dati vengano utilizzati per trovare ristoranti, ma non per ricevere pubblicità per la consegna della pizza solo perché l'app ha identificato che arrivano a casa tardi. Questo ulteriore utilizzo dei dati relativi all'ubicazione potrebbe non essere compatibile con gli scopi per i quali è stato raccolto in primo luogo e potrebbe quindi richiedere il consenso dell'interessato. ⁸

Se questa elaborazione aggiuntiva è compatibile con gli scopi originali per cui sono stati raccolti i dati dipenderà da una serie di fattori ⁹, comprese le informazioni che il Titolare del Trattamento ha inizialmente fornito al soggetto dei dati. Questi fattori si riflettono nel GDPR ¹⁰ e riassunti di seguito:

- il rapporto tra le finalità per le quali i dati sono stati raccolti e gli scopi dell'ulteriore trattamento;
- il contesto in cui sono stati raccolti i dati e le ragionevoli aspettative degli interessati riguardo al loro ulteriore utilizzo;
- la natura dei dati;
- l'impatto dell'ulteriore trattamento sugli interessati; e
- le salvaguardie applicate dal Titolare del Trattamento per garantire un trattamento equo e per prevenire qualsiasi impatto indebito sugli interessati.

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

Le opportunità di business create dalla profilazione, dai costi di storage più economici e dalla capacità di elaborare grandi quantità di informazioni possono incoraggiare le organizzazioni a raccogliere più dati personali di quelli di cui hanno realmente bisogno, nel caso in cui si rivelino utili in futuro. I Titolari del Trattamento devono assicurarsi che rispettino il principio di minimizzazione dei dati, nonché i requisiti dei limiti delle finalità e dei limiti di archiviazione.

I Titolari del Trattamento dovrebbero essere in grado di spiegare chiaramente e giustificare la necessità di raccogliere e conservare i dati personali, o considerare l'utilizzo di dati pseudonimizzati per la profilazione mediante l'uso di dati aggregati, resi anonimi o (quando questo fornisce una protezione sufficiente).

4. Articolo 5, paragrafo 1, lettera d) Precisione

⁸ Si noti che possono essere applicate anche le disposizioni del futuro Regolamento ePrivacy.

⁹ Evidenziato nel gruppo di lavoro sulla protezione dei dati ai sensi dell'articolo 29. Parere 03/2013 sulla limitazione delle finalità, 2 aprile 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Accesso 24 aprile 2017

¹⁰ GDPR articolo 6, paragrafo 4

I Titolari del Trattamento dovrebbero considerare l'accuratezza in tutte le fasi del processo di profilazione, in particolare quando:

- raccolta dati;
- analizzare i dati;
- costruire un profilo per un individuo; o
- applicare un profilo per prendere una decisione che riguarda l'individuo.

Se i dati utilizzati in un processo decisionale o di profilazione automatizzato non sono accurati, qualsiasi decisione o profilo risultante sarà viziata. Le decisioni possono essere prese sulla base di dati obsoleti o interpretazione errata di dati esterni. Le inesattezze possono portare a previsioni o affermazioni inappropriate relative, ad esempio, alla salute, al credito o al rischio assicurativo di qualcuno.

Anche se i dati grezzi sono registrati in modo accurato, il set di dati potrebbe non essere completamente rappresentativo o l'analisi potrebbe contenere bias nascosti.

I Titolari del Trattamento devono introdurre misure efficaci per verificare e assicurare su base continuativa che i dati riutilizzati o ottenuti indirettamente siano accurati e aggiornati. Ciò rafforza l'importanza di fornire informazioni chiare sui dati personali trattati, in modo che l'interessato possa correggere eventuali inesattezze e migliorare la qualità dei dati.

5. Articolo 5, paragrafo 1, lettera e) Limitazione dello spazio di archiviazione

Gli algoritmi di apprendimento automatico sono progettati per elaborare grandi volumi di informazioni e creare correlazioni che consentano alle organizzazioni di creare profili personali molto completi e intimi. Sebbene possano esservi vantaggi nel conservare i dati in caso di profilazione, dal momento che ci saranno più dati per l'algoritmo da cui apprendere, i Titolari del Trattamento devono rispettare il principio di minimizzazione dei dati quando raccolgono i dati personali e assicurano che conservino tali dati personali per più lungo del necessario e proporzionato alle finalità per le quali i dati personali sono trattati.

La politica di conservazione del Titolare del Trattamento dovrebbe tenere conto dei diritti e delle libertà delle persone in linea con i requisiti 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 per ridurre il rischio di inesattezze. ¹¹

B. Basi legali per l'elaborazione

Il processo decisionale automatizzato definito all'articolo 22, paragrafo 1, è consentito solo se si applica una delle eccezioni descritte nel capo IV (sezioni C e D). Le seguenti basi legali per l'elaborazione sono rilevanti per tutti gli altri processi decisionali e di profilazione individuali automatizzati.

1. Articolo 6 (1) (a) consenso

Il consenso come base per il trattamento in generale è trattato nelle Linee guida del WP29 sul consenso. ¹² Il consenso esplicito costituisce una delle eccezioni al divieto di automatizzare il processo decisionale e la definizione dei profili di cui all'articolo 22, paragrafo 1.

¹¹ Autorità norvegese per la protezione dei dati. The Great Data Race - Come l'utilizzo commerciale dei dati personali mette in discussione la privacy, Report, novembre 2015. Datatilsynet <https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/> Consultato il 24 aprile 2017 ¹² Articolo 29 Gruppo di lavoro per la protezione dei dati. Linee guida sul consenso ai sensi del regolamento 2016/679 WP259, 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso 18 dicembre 2017

La profilazione può essere opaca. Spesso si basa su dati derivati o dedotti da altri dati, piuttosto che dati forniti direttamente dall'interessato.

I Titolari del Trattamento che cercano di basarsi sul consenso come base per la profilazione dovranno dimostrare che i soggetti interessati capiscono esattamente a cosa stanno acconsentendo e ricordarsi che il consenso non è sempre una base appropriata per l'elaborazione.¹³ In tutti i casi, gli interessati dovrebbero disporre di sufficienti informazioni pertinenti sull'uso previsto e sulle conseguenze del trattamento al fine di garantire che qualsiasi consenso da loro fornito rappresenti una scelta informata.

2. Articolo 6, paragrafo 1, lettera b): necessario per l'esecuzione di un contratto

I Titolari del Trattamento potrebbero voler utilizzare il profiling e processi decisionali automatizzati per:

- consentire potenzialmente una maggiore coerenza o equità nel processo decisionale (ad esempio riducendo il potenziale di errore umano, discriminazione e abuso di potere);
- ridurre il rischio che i clienti non riescano a soddisfare i pagamenti per beni o servizi (ad esempio utilizzando la referenziazione del credito); o
- consentirgli di prendere decisioni in tempi più brevi e migliorare l'efficienza.

Indipendentemente da quanto sopra, queste considerazioni 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 WP29 sull'interesse legittimo¹⁴, la necessità dovrebbe essere interpretata in modo restrittivo.

Quello che segue è un esempio di profilazione che non soddisfa la base dell'articolo 6, paragrafo 1, lettera b) per l'elaborazione.

Esempio

Un utente acquista alcuni articoli da un rivenditore on-line. Al fine di soddisfare il contratto, il rivenditore deve elaborare le informazioni della carta di credito dell'utente a fini di pagamento e l'indirizzo dell'utente per consegnare la merce. Il completamento del contratto non dipende dalla costruzione di un profilo dei gusti e delle scelte di vita dell'utente in base alle sue visite al sito web. Anche se la profilazione è specificatamente menzionata nella versione ridotta del contratto, questo fatto da solo non lo rende "necessario" per l'esecuzione del contratto.

3. Articolo 6, paragrafo 1, lettera c): necessario per adempiere a un obbligo giuridico

Ci possono essere casi in cui vi sarà un obbligo legale¹⁵ di eseguire la profilazione, ad esempio in relazione alla prevenzione di frodi o riciclaggio di denaro. Il parere del WP29 sugli interessi legittimi¹⁶ fornisce informazioni utili su questa base per l'elaborazione, comprese le garanzie da applicare.

¹² Gruppo di lavoro sulla protezione dei dati dell'articolo 29. Linee guida sul consenso ai sensi del regolamento 2016/679 WP259, 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso 18 dicembre 2017

¹³ Ibid

¹⁴ Parere 06/2014 sulla nozione di interessi legittimi del Titolare del Trattamento dei dati ai sensi dell'articolo 7 della direttiva 95/46 / CE. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp_217_en.pdf. Accesso 24 aprile 2017

4. Articolo 6 (1) (d) - necessario per proteggere gli interessi vitali

Questo copre situazioni in cui il trattamento è necessario per proteggere un interesse che è essenziale per la vita della persona interessata o di un'altra persona fisica.

Alcuni tipi di trattamento possono servire a importanti motivi di interesse pubblico nonché agli interessi vitali dell'interessato. Esempi di questo possono includere la profilazione necessaria per sviluppare modelli che prevedano 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 solo su motivi di interesse vitale se non sono disponibili altre basi giuridiche per il trattamento.¹⁷ Se il trattamento comprende dati personali di categorie speciali, il Titolare del Trattamento dovrebbe anche assicurarsi di soddisfare i requisiti 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 di esercizio di pubblici poteri

L'articolo 6, paragrafo 1, lettera e) potrebbe costituire una base adeguata per la definizione di profili del settore pubblico in determinate circostanze. Il compito o la funzione devono avere una base chiara in diritto.

6. Articolo 6 (1) (f) - necessario per gli interessi legittimi¹⁸ perseguiti dal Titolare del Trattamento o da un terzo

La profilazione è consentita se è necessaria ai fini degli interessi legittimi¹⁹ perseguiti dal Titolare del Trattamento o da una terza parte. Tuttavia, l'articolo 6, paragrafo 1, lettera f), non si applica automaticamente solo perché il Titolare del Trattamento o il terzo hanno un interesse legittimo. Il Titolare del Trattamento deve effettuare un esercizio di bilanciamento per valutare se i propri interessi sono superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato.

I seguenti sono particolarmente rilevanti:

- il livello di dettaglio del profilo (un soggetto dei dati profilato in un gruppo ampiamente descritto come "persone con un interesse per la letteratura inglese" o segmentato e mirato a livello granulare);
- la completezza del profilo (se il profilo descrive solo un piccolo aspetto della persona interessata, o dipinge un quadro più completo);
- l'impatto della profilazione (gli effetti sull'interessato); e
- le misure di sicurezza volte a garantire equità, non discriminazione e accuratezza nel processo di profilazione.

Sebbene il parere del WP29 sugli interessi legittimi²⁰ sia basato sull'articolo 7 della direttiva 95/46 / CE sulla protezione dei dati (la direttiva), contiene esempi che sono ancora utili e pertinenti per i responsabili del controllo che effettuano la profilazione.

¹⁵ Considerando GDPR 41 e 45

¹⁶ Page 19 Articolo 29 Gruppo di lavoro sulla protezione dei dati. Parere 06/2014 sulla nozione di interessi legittimi del Titolare del Trattamento dei dati ai sensi dell'articolo 7 della direttiva 95/46 / CE. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Accesso 24 aprile 2017

¹⁷ Considerando GDPR 46

¹⁸ Gli interessi legittimi elencati nel considerando 47 della GDPR comprendono l'elaborazione a fini di marketing diretto e il trattamento strettamente necessario ai fini della prevenzione delle frodi.

¹⁹ Il "legittimo interesse" del Titolare del Trattamento non può rendere lecito il profiling se il trattamento rientra nella definizione di cui all'articolo 22, paragrafo 1.

²⁰ Gruppo di lavoro sulla protezione dei dati dell'articolo 29. Parere 06/2014 sulla nozione di interessi legittimi del Titolare del Trattamento dei dati ai sensi dell'articolo 7 della direttiva 95/46 / CE. Commissione europea, 9 aprile 2014, pagina 47, esempi su

Suggerisce inoltre che sarebbe difficile per i Titolari del Trattamento giustificare l'utilizzo di interessi legittimi come base legittima per pratiche di profilazione e tracciamento intrusivo a scopo di marketing o pubblicità, ad esempio quelle che coinvolgono il monitoraggio di individui su più siti Web, sedi, dispositivi, servizi o intermediazione di dati.

Il Titolare del Trattamento dovrebbe inoltre considerare l'uso futuro o la combinazione di profili al momento di valutare la validità del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera f).

C. Articolo 9 - Categorie speciali di dati

I Titolari del Trattamento possono elaborare solo dati personali di categoria speciale se possono soddisfare una delle condizioni di cui all'articolo 9, paragrafo 2, nonché una condizione all'articolo 6. Questo include dati di categorie speciali derivati o dedotti dall'attività di profilazione.

La creazione di profili può creare dati di categorie speciali per deduzione da dati che non sono dati di categorie speciali di per sé ma che diventano tali se combinati con altri dati. Ad esempio, può essere possibile dedurre lo stato di salute di qualcuno dai registri dei loro acquisti alimentari combinati con i dati sulla qualità e il contenuto energetico degli alimenti.

Le correlazioni possono essere scoperte che indicano qualcosa sulla salute delle persone, convinzioni politiche, credenze religiose o orientamento sessuale, come dimostrato dal seguente esempio:

Esempio

Uno studio²¹ ha combinato i "Mi Piace" di Facebook con informazioni limitate sull'indagine e ha rilevato che i ricercatori hanno predetto accuratamente l'orientamento sessuale di un utente maschile per l'88% delle volte; origine etnica di un utente il 95% delle volte; e se un utente fosse cristiano o musulmano l'82% delle volte.

Se le preferenze e le caratteristiche sensibili sono dedotte dalla profilazione, il Titolare del Trattamento dovrebbe assicurarsi che:

- il trattamento non è incompatibile con lo scopo originale;
- hanno identificato una base legale per l'elaborazione dei dati della categoria speciale; e
- informano l'interessato sull'elaborazione.

Il processo decisionale automatizzato ai sensi dell'articolo 22, paragrafo 1, basato su categorie speciali di dati, è trattato nel capitolo IV (sezione D).

D. Diritti dell'interessato²²

pagine 59 e 60 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accesso 24 aprile 2017

21

Michael Kosinski, David Stilwell e Thore Graepel. 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 al 29 marzo 2017

22 Questa sezione è rilevante sia per il profiling che 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.

Il GDPR introduce maggiori diritti per gli interessati e crea nuovi obblighi per i Titolari del Trattamento.

Nel contesto della profilazione questi diritti sono perseguibili nei confronti del Titolare del Trattamento che crea il profilo e del Titolare del Trattamento prende una decisione automatizzata su un soggetto dei dati (con o senza intervento umano), se queste entità non sono le stesse.

Esempio

Un broker di dati effettua la profilazione di dati personali. In linea con gli obblighi di cui agli articoli 13 e 14, il mediatore di dati dovrebbe informare l'interessato in merito al trattamento, compreso se intende condividere il profilo con altre organizzazioni. Il mediatore di dati dovrebbe anche presentare separatamente i dettagli del diritto di opposizione ai sensi dell'articolo 21, paragrafo 1.

Il broker di dati condivide il profilo con un'altra società. Questa azienda utilizza il profilo per inviare il marketing diretto individuale.

La società dovrebbe informare la persona (articolo 14, paragrafo 1, lettera c)) in merito agli scopi dell'utilizzo di questo profilo e da quale fonte ha ottenuto l'informazione (14 (2) (f)). La società deve inoltre informare la persona interessata del suo diritto di opporsi al trattamento, inclusa la profilazione, a fini di marketing diretto (articolo 21, paragrafo 2).

Il mediatore di dati e la società dovrebbero consentire all'interessato il diritto di accedere alle informazioni utilizzate (articolo 15) per correggere eventuali informazioni errate (articolo 16) e in determinate circostanze cancellare il profilo o i dati personali utilizzati per crearlo (articolo 17). Alla persona interessata dovrebbero essere fornite anche informazioni sul loro profilo, ad esempio in cui "segmenti" o "categorie" sono collocati.²³

Se la società utilizza il profilo come parte di un processo decisionale esclusivamente automatico con effetti giuridici o di analogia rilevanza sull'interessato, la società è soggetta alle disposizioni dell'articolo 22. (Ciò non esclude il broker di dati dall'articolo 22 se l'elaborazione soddisfa la soglia pertinente).

1. Articoli 13 e 14 - Diritto di essere informato

Dato il principio fondamentale della trasparenza alla base del GDPR, i Titolari del Trattamento devono garantire che spieghino in modo chiaro e semplice agli individui come funziona la profilazione o il processo decisionale automatizzato.

In particolare, quando il trattamento implica un processo decisionale basato sui profili (indipendentemente dal fatto che sia preso dalle disposizioni dell'articolo 22), allora il fatto che il trattamento sia ai fini di entrambi (a) profilazione e (b) prendere una decisione basata su il profilo generato deve essere reso chiaro all'interessato.²⁴

²³ L'autorità norvegese per la protezione dei dati. The Great Data Race - Quanto l'utilizzo commerciale dei dati personali sfida la privacy. Rapporto, novembre 2015. <https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/> Accesso 24 aprile 2017

²⁴ GDPR - Articolo 13, paragrafo 1, lettera c) e articolo 14, paragrafo 1, lettera c). Ai sensi dell'articolo 13, paragrafo 2, lettera f) e dell'articolo 14, paragrafo 2, lettera g), il Titolare del Trattamento informa la persona interessata dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafi 1 e 4. Questo è ulteriormente spiegato nel Capitolo IV.

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 il diritto di essere informato dal Titolare del Trattamento e, in determinate circostanze, il diritto di opporsi alla "profilazione", indipendentemente dal fatto che avvenga esclusivamente un processo decisionale individuale basato sulla profilazione.

Ulteriori orientamenti in materia di trasparenza in generale sono disponibili nelle linee guida del WP29 sulla trasparenza nell'ambito del GDPR ²⁵.

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, comprese le categorie di dati utilizzati per costruire un profilo.

Oltre alle informazioni generali sul trattamento, ai sensi dell'articolo 15, paragrafo 3, il Titolare del Trattamento ha il dovere di rendere disponibili i dati utilizzati come input per creare il profilo e l'accesso alle informazioni sul profilo e i dettagli dei segmenti nei quali il soggetto è stato inserito.

Ciò differisce dal diritto alla portabilità dei dati ai sensi dell'articolo 20 quando il Titolare del Trattamento deve solo comunicare i dati forniti dall'interessato o osservati dal Titolare del Trattamento e non il profilo stesso. ²⁶

Il considerando 63 offre una certa protezione ai Titolari del Trattamento interessati a rivelare segreti commerciali o proprietà intellettuale, che possono essere particolarmente rilevanti in relazione alla profilazione. Dice che il diritto di accesso "non dovrebbe pregiudicare i diritti o le libertà altrui, compresi i segreti commerciali o la proprietà intellettuale e in particolare il diritto d'autore che protegge il software". Tuttavia, i Titolari del Trattamento non possono fare affidamento sulla protezione dei loro segreti commerciali come scusa per negare l'accesso o rifiutarsi di fornire informazioni all'interessato.

Il considerando 63 specifica inoltre che "laddove possibile, il Titolare del Trattamento dovrebbe essere in grado di fornire l'accesso remoto a un sistema sicuro che fornirebbe all'interessato un accesso diretto ai suoi dati personali".

3. Articolo 16 - Diritto alla rettifica, Articolo 17 Diritto alla cancellazione e Articolo 18 Diritto alla restrizione del trattamento

La profilazione può comportare un elemento di previsione, che aumenta il rischio di inesattezza. I dati di input possono essere inaccurati o irrilevanti o estrapolati dal contesto. Potrebbe esserci qualcosa di sbagliato nell'algoritmo utilizzato per identificare le correlazioni.

Il diritto di rettifica dell'articolo 16 potrebbe applicarsi quando, ad esempio, un individuo viene inserito in una categoria che dice qualcosa sulla sua capacità di eseguire un'attività e tale profilo è basato su informazioni errate. Le persone potrebbero voler contestare l'accuratezza dei dati utilizzati e qualsiasi gruppo o categoria che è stata loro applicata.

²⁵ Gruppo di lavoro sulla protezione dei dati dell'articolo 29. Linee guida sulla trasparenza ai sensi del Regolamento 2016/679 WP260, 28 novembre 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accesso 18 dicembre 2017

²⁶ Page 9, WP29 Linee guida sul diritto alla portabilità dei dati, WP242 http://ec.europa.eu/newsroom/document.cfm?doc_id=45685. Accesso 8 gennaio 2018

I diritti di rettifica e cancellazione ²⁷ si applicano sia ai "dati personali inseriti" (i dati personali utilizzati per creare il profilo) sia ai "dati di output" (il profilo stesso o "punteggio" assegnato alla persona).

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

Esempio

Il sistema informatico di una chirurgia locale colloca un individuo in un gruppo che ha più probabilità di contrarre malattie cardiache. Questo "profilo" non è necessariamente impreciso anche se non soffre mai di malattie cardiache. Il profilo si limita a dire che lui o lei è più propenso a ottenerlo. Ciò può essere di fatto corretto come una questione di statistiche.

Tuttavia, l'interessato ha il diritto, tenendo conto dello scopo del trattamento, di fornire una dichiarazione supplementare. Nello scenario sopra riportato, questo potrebbe essere basato, ad esempio, su un sistema informatico medico più avanzato (e sul modello statistico) che prevede il calcolo di dati aggiuntivi e l'esecuzione di esami più dettagliati rispetto a quello della chirurgia locale con capacità più limitate.

Il diritto di limitare il trattamento (articolo 18) si applicherà a qualsiasi fase del processo di profilazione.

4. Articolo 21 - Diritto di opporsi

Il Titolare del Trattamento deve fornire esplicitamente i dettagli del diritto di opposizione ai sensi dell'articolo 21, paragrafi 1 e 2, all'attenzione dell'interessato e presentarlo in modo chiaro e separato rispetto ad altre informazioni (articolo 21, paragrafo 4).

Ai sensi dell'articolo 21, paragrafo 1, l'interessato può opporsi al trattamento (compresa la profilazione), per motivi relativi alla sua situazione particolare. I Titolari del Trattamento sono specificamente tenuti a fornire questo diritto in tutti i casi in cui il trattamento è basato sull'articolo 6 (1) (e) o (f).

Una volta che l'interessato ha esercitato questo diritto, il Titolare del Trattamento deve interrompere ²⁸ (o evitare di iniziare) il processo di profilazione, a meno che non possa dimostrare motivi legittimi convincenti che annullano gli interessi, i diritti e le libertà dell'interessato. Il Titolare del Trattamento potrebbe anche dover cancellare i dati personali rilevanti. ²⁹

Il GDPR non fornisce alcuna spiegazione di quelli che sarebbero considerati motivi legittimi convincenti. ³⁰ Può essere il caso, ad esempio, che la profilazione sia vantaggiosa per la società in senso lato (o per la comunità più ampia) e non solo per gli interessi commerciali del Titolare del Trattamento, come la profilazione per prevedere la diffusione di malattie contagiose.

²⁷ GDPR - Articolo 17/28 GDPR - Articolo 18, paragrafo 1, lettera d)

²⁸ GDPR - Articolo 18, paragrafo 1, lettera d)

²⁹ GDPR - Articolo 17, paragrafo 1, lettera c)

³⁰ Cfr. Motivazione sulla legittimità, articolo 29, paragrafo 29, del gruppo di esperti in materia di protezione dei dati, sulla nozione di interessi legittimi del Titolare del Trattamento dei dati ai sensi dell'articolo 7 della direttiva 95/46 / CE. 9 aprile 2014. Pagina 24 - 26 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accesso 24 aprile 2017

Il Titolare del Trattamento dovrebbe:

- considerare l'importanza della profilazione per il loro particolare obiettivo;
- considerare l'impatto della profilazione sull'interesse, i diritti e le libertà dell'interessato - questo dovrebbe essere limitato al minimo necessario per raggiungere l'obiettivo; e
- eseguire un esercizio di bilanciamento.

Ci deve sempre essere un esercizio di bilanciamento tra gli interessi concorrenti del Titolare del Trattamento e la base per l'obiezione dell'interessato (che può essere per motivi personali, sociali o professionali).

A differenza della direttiva 95/46 / CE, l'onere della prova per dimostrare motivi legittimi convincenti spetta al Titolare del Trattamento piuttosto che all'interessato.

Dal testo dell'articolo 21 risulta chiaramente che la prova di bilanciamento è diversa da quella di cui all'articolo 6, paragrafo 1, lettera f). In altre parole, non è sufficiente che un Titolare del Trattamento dimostri solo che la loro precedente analisi dell'interesse legittimo era corretta. Questo test di bilanciamento richiede che l'interesse legittimo sia convincente, implicando una soglia più elevata per obiezioni irrisolte.

L'articolo 21, paragrafo 2, conferisce al soggetto interessato il diritto incondizionato di opporsi al trattamento dei dati personali a fini di commercializzazione diretta, compresa la profilazione nella misura in cui è collegata a tale commercializzazione diretta.³¹ Ciò significa che non è necessario alcun bilanciamento degli interessi; il Titolare del Trattamento deve rispettare i desideri dell'individuo senza mettere in discussione i motivi dell'obiezione. Il considerando 70 fornisce un contesto supplementare a questo diritto e afferma che può essere esercitato in qualsiasi momento e gratuitamente.

IV. Disposizioni specifiche relative al processo decisionale esclusivamente automatizzato come definito all'articolo 22

L'articolo 22 (1) dice

L'interessato ha il diritto di non essere soggetto a una decisione basata sul trattamento esclusivamente automatizzato, inclusa la profilazione, che produce effetti legali su di lui o su di lei in modo simile.

Il termine "diritto" nella disposizione non significa che l'articolo 22, paragrafo 1 si applica solo quando è attivamente invocato dall'interessato. L'articolo 22, paragrafo 1 stabilisce un divieto generale per il processo decisionale basato sul trattamento esclusivamente automatizzato. Questo divieto si applica indipendentemente dal fatto che l'interessato intraprenda un'azione in merito al trattamento dei propri dati personali.

In sintesi, l'articolo 22 stabilisce che:

- (i) di norma, vi è un divieto generale di prendere decisioni individuali completamente automatizzate, inclusa la profilazione che ha un effetto legale o di analogia rilevanza;
- (ii) ci sono delle eccezioni alla regola;
- (iii) quando si applica una di queste eccezioni, devono essere adottate misure per salvaguardare i diritti e le libertà dell'interessato e gli interessi legittimi³².

³¹ In linea con l'articolo 12, paragrafo 2, i Titolari del Trattamento che raccolgono dati personali da individui al fine di utilizzarli a fini di marketing diretto dovrebbero, al momento della raccolta, considerare di offrire agli interessati un modo facile per indicare che non desiderano il loro personale dati da utilizzare a fini di marketing diretto, piuttosto che richiedere loro di esercitare il loro diritto di opporsi in una occasione successiva.

³² Il considerando 71 afferma che tale trattamento dovrebbe essere "soggetto a garanzie adeguate, che dovrebbero includere informazioni specifiche all'interessato e il diritto di ottenere l'intervento umano, per esprimere il proprio punto di vista, ottenere una spiegazione della decisione presa dopo tale valutazione e per contestare la decisione".

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

Tuttavia, il processo decisionale basato su tale trattamento, compresa la profilazione, dovrebbe essere consentito se espressamente autorizzato dalla legge dell'Unione o dello Stato membro, o necessario per l'iscrizione o l'esecuzione di un contratto, o quando l'interessato ha fornito il suo o il suo esplicito consenso

Ciò implica che il trattamento ai sensi dell'articolo 22, paragrafo 1, non è generalmente consentito. ³³

Tuttavia, il divieto di cui all'articolo 22, paragrafo 1, si applica solo in circostanze specifiche quando una decisione basata sul trattamento esclusivamente automatizzato, compresa la definizione di profili, ha un effetto giuridico su o influenza in modo analogo in modo significativo su qualcuno, come spiegato ulteriormente negli orientamenti. Anche in questi casi esistono eccezioni definite che consentono l'esecuzione di tale elaborazione.

Le misure di salvaguardia richieste, discusse in maggior dettaglio di seguito, comprendono il diritto di essere informati (di cui agli articoli 13 e 14 - informazioni specificamente significative sulla logica in questione, nonché l'importanza e le conseguenze previste per l'interessato) e le garanzie, come il diritto di ottenere l'intervento umano e il diritto di impugnare la decisione (di cui all'articolo 22, paragrafo 3).

Qualsiasi trattamento che possa comportare un alto rischio per gli interessati richiede che il Titolare del Trattamento effettui una [valutazione dell'impatto sulla protezione dei dati \(DPIA\)](#). ³⁴ Oltre ad affrontare qualsiasi altro rischio connesso al trattamento, una DPIA può essere particolarmente utile per i Titolari del Trattamento che non sono sicuri se le loro attività proposte rientreranno nella definizione di cui all'articolo 22, paragrafo 1 e, se consentita da un'eccezione identificata, quali misure di salvaguardia devono essere applicate

A. "Decisione basata unicamente sull'elaborazione automatizzata"

L'articolo 22, paragrafo 1 si riferisce alle decisioni basate sul trattamento "esclusivamente automatizzato". Ciò significa che non vi è alcun coinvolgimento umano nel processo decisionale.

Esempio

Un processo automatizzato produce ciò che è in effetti una raccomandazione riguardante un soggetto dei dati. Se un essere umano rivede e prende in considerazione altri fattori nel prendere la decisione finale, tale decisione non sarebbe basata sul trattamento "esclusivamente automatizzato".

³³ Ulteriori osservazioni sull'interpretazione dell'articolo 22 come un divieto possono essere trovate nell'allegato 2.

³⁴ Gruppo di lavoro sulla protezione dei dati dell'articolo 29. Linee guida sulla valutazione dell'impatto sulla protezione dei dati (DPIA) e determinare se il trattamento è "suscettibile di comportare un rischio elevato" ai fini del regolamento 2016/679. 4 aprile 2017. Commissione europea. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accesso 24 aprile 2017.

Il Titolare del Trattamento non può evitare le disposizioni dell'articolo 22 fabbricando il coinvolgimento umano. Ad esempio, se qualcuno applica abitualmente profili automaticamente generati a persone senza alcuna influenza effettiva sul risultato, si tratterà comunque di una decisione basata esclusivamente sull'elaborazione automatica.

Per qualificarsi come coinvolgimento umano, il Titolare del Trattamento deve garantire che qualsiasi controllo della decisione sia significativo, piuttosto che un semplice gesto simbolico. Dovrebbe essere eseguito da qualcuno che ha l'autorità e la competenza per cambiare la decisione. Come parte dell'analisi, dovrebbero prendere in considerazione tutti i dati rilevanti.

Come parte della loro DPIA, il Titolare del Trattamento dovrebbe identificare e registrare il grado di coinvolgimento umano nel processo decisionale e in quale fase del processo.

B. Effetti "legali" o "similmente significativi"

Il GDPR riconosce che il processo decisionale automatizzato, inclusa la profilazione, può avere gravi conseguenze per le persone. Il GDPR non definisce "legale" o "similmente significativo", tuttavia la formulazione chiarisce che solo gli effetti di grave impatto saranno coperti dall'articolo 22.

"Decisione che produce effetti giuridici"

Un effetto legale richiede che la decisione, basata su un trattamento esclusivamente automatico, incida sui diritti legali di qualcuno, come la libertà di associarsi ad altri, votare in un'elezione o intraprendere azioni legali. Un effetto legale può anche essere qualcosa che influisce sullo status legale di una persona o sui suoi diritti in base a un contratto. Esempi di questo tipo di effetto includono decisioni automatiche su un individuo che si traducono in:

- cancellazione di un contratto;
- diritto o negazione di una particolare prestazione sociale concessa dalla legge, come ad esempio l'assegno per figli o l'alloggio;
- ha rifiutato l'ammissione in un paese o la negazione della cittadinanza.

"Similmente colpisce significativamente lui o lei"

Anche se un processo decisionale non ha effetto sui diritti legali delle persone, potrebbe comunque rientrare nell'ambito di applicazione dell'articolo 22 se produce un effetto equivalente o similmente significativo nel suo impatto.

In altre parole, anche laddove non vi sia alcun cambiamento nei loro diritti o obblighi legali, l'interessato potrebbe comunque subire un impatto sufficiente a richiedere le protezioni previste da questa disposizione. Il GDPR introduce la parola "similmente" (non presente nell'articolo 15 della direttiva 95/46 / CE) con la frase "influenza significativamente". Pertanto la soglia di rilevanza deve essere simile 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 reclutamento elettronico senza intervento umano".

Affinché l'elaborazione dei dati possa influire in modo significativo su qualcuno, gli effetti dell'elaborazione devono essere sufficientemente grandi o importanti da meritare attenzione. In altre parole, la decisione deve avere il potenziale per:

- influenzare significativamente le circostanze, il comportamento o le scelte delle persone interessate;
- avere un impatto prolungato o permanente sull'interessato; o
- al suo estremo, portano all'esclusione o alla discriminazione delle persone.

È difficile essere precisi su ciò che sarebbe considerato sufficientemente significativo per raggiungere la soglia, anche se le seguenti decisioni potrebbero rientrare in questa categoria:

- decisioni che influenzano le circostanze finanziarie di qualcuno, come la loro idoneità al credito;
- decisioni che influenzano l'accesso di qualcuno ai servizi sanitari;
- decisioni che negano a qualcuno un'opportunità di impiego o le mettono in grave svantaggio;
- decisioni che influenzano l'accesso di qualcuno all'educazione, ad esempio i ricoveri universitari.

Questo ci porta anche al problema della pubblicità online, che si basa sempre più su strumenti automatizzati e implica esclusivamente decisioni individuali automatizzate. Oltre a soddisfare le disposizioni generali del GDPR, di cui al capo III, possono anche essere pertinenti le disposizioni del regolamento e-privacy proposto. Inoltre, i bambini richiedono una protezione migliorata, come sarà discusso di seguito nel capitolo V.

In molti casi tipici, la decisione di presentare pubblicità mirata basata sulla profilazione non avrà un effetto altrettanto significativo sugli individui, ad esempio 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 articoli di abbigliamento".

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

- l'invadenza del processo di profilazione, compreso il tracciamento di individui su diversi siti Web, dispositivi e servizi;
- le aspettative e i desideri delle persone interessate;
- il modo in cui viene pubblicato l'annuncio; o
- usando la conoscenza delle vulnerabilità dei soggetti interessati.

L'elaborazione che potrebbe avere un impatto minimo sugli individui in generale potrebbe in effetti avere un effetto significativo per alcuni gruppi della società, come gruppi di minoranza o adulti vulnerabili. Ad esempio, qualcuno conosciuto o probabile che si trovi in difficoltà finanziarie che è regolarmente preso di mira con annunci di prestiti ad alto interesse può iscriversi a queste offerte e potenzialmente incorrere in ulteriori debiti.

Il processo decisionale automatizzato che si traduce in una tariffazione differenziata basata su dati personali o caratteristiche personali potrebbe anche avere un effetto significativo se, ad esempio, prezzi proibitivi elevati impediscono effettivamente a qualcuno di determinati beni o servizi.

Analogamente, effetti significativi potrebbero anche essere innescati da azioni di individui diversi da quello a cui si riferisce la decisione automatizzata. Un'illustrazione di questo è riportata di seguito.

Esempio

Ipoteticamente, una società di carte di credito potrebbe ridurre il limite di carte di un cliente, basato non sulla storia di rimborso di quel cliente, ma su criteri di credito non tradizionali, come l'analisi di altri clienti che vivono nella stessa area e acquistano presso gli stessi negozi.

Ciò potrebbe significare che qualcuno è privato di opportunità basate sulle azioni degli altri.

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

C. Eccezioni dal divieto

L'articolo 22, paragrafo 1, stabilisce un divieto generale di prendere decisioni individuali unicamente automatizzate con effetti giuridici o di analogia rilevanza, come descritto sopra.

Ciò significa che 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, se la decisione è:

- (a) necessario per l'esecuzione o la stipula di un contratto;
- (b) autorizzato dal diritto dell'Unione o dello Stato membro a cui è soggetto il Titolare del Trattamento e che stabilisce altresì misure idonee a salvaguardare i diritti e le libertà dell'interessato e i legittimi interessi; o
- (c) in base al consenso esplicito dell'interessato.

Laddove il processo decisionale coinvolga categorie speciali di dati definite all'articolo 9, paragrafo 1, il Titolare del Trattamento deve anche garantire che possano soddisfare i requisiti di cui all'articolo 22, paragrafo 4.

1. Esecuzione di un contratto

I Titolari del Trattamento potrebbero voler utilizzare esclusivamente processi decisionali automatizzati a fini contrattuali perché ritengono che sia il modo più appropriato per raggiungere l'obiettivo. Il coinvolgimento umano di routine a volte può essere impraticabile o impossibile a causa della quantità di dati che vengono elaborati.

Il Titolare del Trattamento deve essere in grado di dimostrare che questo tipo di elaborazione è necessario, tenendo conto della possibilità di adottare un metodo meno invasivo per la privacy.³⁵ Se esistono altri mezzi efficaci e meno intrusivi per raggiungere lo stesso obiettivo, allora non sarebbe "necessario".

Anche il processo decisionale automatizzato descritto nell'articolo 22, paragrafo 1 può essere necessario per l'elaborazione precontrattuale.

Esempio

Un'azienda pubblicizza una posizione aperta. Poiché il business per il business in questione è molto diffuso, l'azienda riceve decine di migliaia di candidature. A causa del volume eccezionalmente elevato di candidature, l'azienda potrebbe scoprire che non è praticamente possibile identificare candidati idonei senza prima utilizzare mezzi completamente automatizzati per selezionare candidature irrilevanti. In questo caso, potrebbe essere necessario un processo decisionale automatizzato per stilare un breve elenco di possibili candidati, con l'intenzione di stipulare un contratto con una persona interessata.

Il Capitolo III (Sezione B) fornisce maggiori informazioni sui contratti come base legale per l'elaborazione.

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

³⁵ Buttarelli, Giovanni. Valutare la necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali. Supervisore europeo per la protezione dei dati di AToolkit, 11 aprile 2017,

**Courtesy translation
by
PRIVACYLAB**

Il processo decisionale automatizzato, inclusa la profilazione, potrebbe potenzialmente aver luogo al punto (2) (b) se la legislazione dell'Unione o dello Stato membro ne autorizzasse l'uso. La legge pertinente deve inoltre prevedere misure adeguate per salvaguardare i diritti e le libertà dell'interessato e gli interessi legittimi.

Il considerando 71 afferma che ciò potrebbe includere l'uso del processo decisionale automatico definito all'articolo 22, paragrafo 1, per monitorare e prevenire le frodi e l'evasione fiscale, o per garantire la sicurezza e l'affidabilità di un servizio fornito dal Titolare del Trattamento.

3. Consenso esplicito

L'articolo 22 richiede il consenso esplicito. Il trattamento che rientra nella definizione dell'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 GDPR. Le linee guida WP29 sul consenso³⁶ forniscono indicazioni su come questo dovrebbe essere interpretato.

Il Capitolo III (Sezione B) fornisce più informazioni sul consenso in generale.

D. Categorie speciali di dati personali - Articolo 22, paragrafo 4

Il processo decisionale automatizzato (descritto nell'articolo 22, paragrafo 1) che prevede categorie speciali di dati personali è consentito solo alle seguenti condizioni cumulative (articolo 22, paragrafo 4):

- esiste un'esenzione applicabile all'articolo 22, paragrafo 2; e
- si applica la lettera a) o g) dell'articolo 9, paragrafo 2.

9 (2) (a) - il consenso esplicito dell'interessato; o

9 (2) (g) - il trattamento necessario per motivi di interesse pubblico sostanziale, sulla base del diritto dell'Unione o dello Stato membro, che sia proporzionato all'obiettivo perseguito, rispetta l'essenza del diritto alla protezione dei dati e preveda adeguate e specifiche misure volte a salvaguardare i diritti e gli interessi fondamentali dell'interessato.
--

In entrambi i casi di cui sopra, il Titolare del Trattamento deve adottare misure adeguate per salvaguardare i diritti e le libertà dell'interessato e gli interessi legittimi.

E. Diritti dell'interessato³⁷

4. Articolo 13 (2) (f) e 14 (2) (g) - Diritto di essere informato

Considerati i potenziali rischi e le interferenze che la profilazione individuata dall'articolo 22 pone ai diritti degli interessati, i Titolari del Trattamento dei dati dovrebbero prestare particolare attenzione ai loro obblighi di trasparenza.

³⁶ Gruppo di lavoro sulla protezione dei dati dell'articolo 29. Linee guida sul consenso ai sensi del regolamento 2016/679 WP259. 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Accesso 18 dicembre 2017

³⁷ L'articolo 12 del GDPR prevede le modalità applicabili all'esercizio dei diritti dell'interessato

Gli articoli 13 (2) (f) e 14 (2) (g) richiedono ai Titolari del Trattamento di fornire informazioni specifiche e facilmente accessibili sul processo decisionale automatizzato, basate unicamente sul trattamento automatizzato, inclusa la profilazione, che produca effetti legali o similmente significativi.³⁸

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

- comunicare all'interessato che si sta impegnando in questo tipo di attività;
- fornire informazioni significative sulla logica coinvolta; e
- spiegare il significato e le conseguenze previste del trattamento.

Fornire queste informazioni aiuterà inoltre i Titolari del Trattamento a garantire che soddisfino alcune delle misure di salvaguardia richieste di cui all'articolo 22, paragrafo 3 e al considerando 71.

Se il processo decisionale e la profilazione automatizzate 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 per rendere equo il trattamento,³⁹ e soddisfare tutti gli altri requisiti di informazione di cui agli articoli 13 e 14.

Informazioni significative sulla 'logica coinvolta'

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

Il Titolare del Trattamento dovrebbe trovare metodi semplici per comunicare all'interessato le motivazioni alla base o i criteri invocati per raggiungere la decisione. Il GDPR richiede al Titolare del Trattamento di fornire informazioni significative sulla logica coinvolta, non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo.⁴⁰ Tuttavia, le informazioni fornite dovrebbero essere sufficientemente complete affinché l'interessato possa comprendere le ragioni della decisione.

Esempio

Un Titolare del Trattamento utilizza il punteggio di credito per valutare e respingere la domanda di prestito di una persona. Il punteggio può essere stato fornito da un'agenzia di riferimento di credito o calcolato direttamente sulla base delle informazioni detenute dal Titolare del Trattamento.

Indipendentemente dalla fonte (e 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 dipende da tale punteggio, deve essere in grado di spiegarlo e la motivazione, all'interessato.

Il Titolare del Trattamento spiega che questo processo li aiuta a prendere decisioni di prestito corrette e responsabili.

³⁸ Di cui all'articolo 22, paragrafi 1 e 4. Le Linee guida sulla trasparenza del WP riguardano gli obblighi di informazione generale di cui agli articoli 13 e 14.

³⁹ GDPR Recital 60 "Il Titolare del Trattamento dovrebbe fornire all'interessato qualsiasi ulteriore informazione necessaria a garantire un trattamento equo e trasparente, tenendo conto delle circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre, l'interessato dovrebbe essere informato dell'esistenza della profilazione e delle conseguenze di tale profilazione."

⁴⁰ La complessità non è una scusa per non aver fornito informazioni all'interessato. Il considerando 58 afferma che il principio di trasparenza è "di particolare rilevanza in situazioni in cui la proliferazione di attori e la complessità tecnologica della pratica rendono difficile per l'interessato conoscere e capire se, da chi e per quale scopo i dati personali che lo riguardano vengono raccolti, come nel caso della pubblicità online".

Fornisce dettagli sulle principali caratteristiche considerate nel raggiungere la decisione, la fonte di questa informazione e rilevanza. Questo può includere, ad esempio:

- le informazioni fornite dall'interessato sul modulo di domanda;
- informazioni sulla condotta dell'account precedente, compresi eventuali pagamenti arretrati; e
- informazioni ufficiali sui registri pubblici, come le informazioni su frodi e i registri di insolvenza.

Il Titolare del Trattamento include anche informazioni per informare l'interessato che i metodi di valutazione del merito di credito utilizzati sono regolarmente testati per garantire che rimangano equi, efficaci e imparziali.

Il Titolare del Trattamento fornisce i dettagli di contatto affinché l'interessato possa chiedere che ogni decisione declinata venga riesaminata, in linea con le disposizioni dell'articolo 22, paragrafo 3.

"Significativo" e "conseguenze previste"

Questo termine suggerisce che devono essere fornite informazioni sull'elaborazione prevista o futura e su come il processo decisionale automatizzato potrebbe influire sull'interessato. ⁴¹ Al fine di rendere queste informazioni significative e comprensibili, dovrebbero essere forniti esempi reali e concreti del tipo di effetti possibili.

In un contesto digitale, i Titolari del Trattamento potrebbero essere in grado di utilizzare strumenti aggiuntivi per illustrare tali effetti.

Esempio

Una compagnia assicurativa utilizza un processo decisionale automatizzato per impostare i premi dell'assicurazione auto in base al monitoraggio del comportamento di guida dei clienti. Per illustrare il significato e le conseguenze previste del trattamento, si spiega che una guida pericolosa può comportare pagamenti assicurativi più elevati e fornisce un'app che confronta i guidatori fittizi, incluso uno con abitudini di guida pericolose come accelerazione veloce e frenata dell'ultimo minuto.

Usa la grafica per dare consigli su come migliorare queste abitudini e di conseguenza come ridurre i premi assicurativi.

I Titolari del Trattamento possono utilizzare tecniche visive simili per spiegare come è stata presa una decisione passata.

5. Articolo 15, paragrafo 1, lettera h) - Diritto di accesso

L'articolo 15, paragrafo 1, lettera h) autorizza le persone interessate a disporre delle stesse informazioni in merito al solo processo decisionale automatizzato, compresa la profilazione, come richiesto ai sensi dell'articolo 13, paragrafo 2, lettera f) e dell'articolo 14, paragrafo 2, lettera g), ossia:

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

⁴¹ Consiglio d'Europa. Progetto di relazione esplicativa sulla versione modernizzata della convenzione 108 del CdE, paragrafo 75: "Gli interessati dovrebbero avere il diritto di conoscere il ragionamento alla base del trattamento dei loro dati, comprese 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 inclusa la profilazione. Ad esempio, nel caso del credit scoring, dovrebbero avere il diritto di conoscere la logica alla base del trattamento dei loro dati e determinare una decisione "sì" o "no", e non semplicemente informazioni sulla decisione stessa. Senza una comprensione di questi elementi non potrebbe esserci alcun effettivo esercizio di altre garanzie essenziali come il diritto di obiettare e il diritto di sporgere denuncia presso un'autorità competente. "

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900016806b6e_c2

Accesso 24 aprile 2017

Il Titolare del Trattamento avrebbe dovuto già fornire tali dati in linea con gli obblighi di cui all'articolo 13.⁴²

L'articolo 15, paragrafo 1, lettera h) afferma che il Titolare del Trattamento dovrebbe fornire all'interessato informazioni sulle conseguenze previste del trattamento, piuttosto che una spiegazione di una decisione particolare. Il considerando 63 chiarisce questo, affermando che ogni interessato dovrebbe avere il diritto di accesso per ottenere una "comunicazione" sull'elaborazione automatica dei dati, compresa la logica in questione, e almeno in base alla profilazione, le conseguenze di tale trattamento,

Esercitando i diritti di cui all'articolo 15, l'interessato può prendere atto di una decisione presa nei suoi confronti, inclusa una 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 è anche utile per metterlo in discussione.

F. Stabilire garanzie appropriate

Se la base per il trattamento è 22 (2) (a) o 22 (2) (c), l'articolo 22, paragrafo 3 richiede ai Titolari del Trattamento di attuare misure adeguate per salvaguardare le libertà dei diritti degli interessati e gli interessi legittimi. Ai sensi dell'articolo 22, paragrafo 2, lettera b), il diritto degli Stati membri o dello Stato dell'Unione che autorizza il trattamento deve anche prevedere misure di salvaguardia adeguate.

Tali misure dovrebbero includere come minimo un modo per l'interessato di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione.

L'intervento umano è un elemento chiave. Qualsiasi revisione deve essere eseguita da qualcuno che abbia l'autorità appropriata e la capacità di modificare la decisione. Il revisore deve effettuare una valutazione approfondita di tutti i dati pertinenti, comprese eventuali informazioni aggiuntive fornite dall'interessato.

Il considerando 71 sottolinea che, in ogni caso, le salvaguardie adeguate dovrebbero includere anche:

.. informazioni specifiche all'interessato e il diritto di ottenere una spiegazione della decisione presa dopo tale valutazione e di impugnare la decisione.
--

Il Titolare del Trattamento deve fornire un modo semplice per l'interessato di esercitare tali diritti.

Ciò sottolinea la necessità di trasparenza sull'elaborazione. L'interessato sarà in grado di contestare una decisione o esprimere la propria opinione solo se comprenderà pienamente come è stata fatta e su quali basi. I requisiti di trasparenza sono discussi nel capitolo IV (sezione E).

Errori o pregiudizi nei dati raccolti o condivisi o un errore o pregiudizio nel processo decisionale automatico possono comportare:

- classificazioni errate;
- valutazioni basate su proiezioni imprecise e
- impatto negativo sugli individui.

⁴² L'articolo 12, paragrafo 3, del GDPR chiarisce i tempi per fornire tali informazioni

I Titolari del Trattamento dovrebbero effettuare frequenti valutazioni sui set di dati che elaborano per verificare eventuali pregiudizi e sviluppare metodi per affrontare eventuali elementi pregiudizievoli, inclusa l'eccessiva dipendenza dalle correlazioni. I sistemi che controllano gli algoritmi e le revisioni periodiche dell'accuratezza e della rilevanza del processo decisionale automatizzato, inclusa la creazione di profili, sono altre misure utili.

I Titolari del Trattamento dovrebbero introdurre procedure e misure appropriate per prevenire errori, inesattezze⁴³ o discriminazioni sulla base di dati di categorie speciali. Queste misure dovrebbero essere utilizzate su base ciclica; non solo in fase di progettazione, ma anche in modo continuo, poiché la profilazione viene applicata agli individui. L'esito di tali test dovrebbe tornare alla progettazione del sistema.

Ulteriori esempi di garanzie appropriate sono disponibili nella sezione [Raccomandazioni](#)

V. Bambini e profilazione

Il GDPR crea ulteriori obblighi per i Titolari del Trattamento dei dati quando elaborano dati personali dei minori.

Lo stesso articolo 22 non fa alcuna distinzione se il trattamento riguardi adulti o minori. Tuttavia, il considerando 71 afferma che il solo processo decisionale automatizzato, compresa la profilazione, con effetti giuridici o simili significativi non dovrebbe applicarsi ai bambini. ⁴⁴ Dato che questa formulazione non è riflessa nell'articolo stesso, il WP29 non ritiene che ciò rappresenti un divieto assoluto per questo tipo di trattamento in relazione ai bambini. Tuttavia, alla luce di questo considerando, il WP29 raccomanda che, di norma, i Titolari del Trattamento non facciano affidamento sulle eccezioni di cui all'articolo 22, paragrafo 2, per giustificarlo.

Potrebbero tuttavia esserci alcune circostanze in cui è necessario che i Titolari del Trattamento eseguano esclusivamente processi decisionali automatizzati, tra cui la creazione di profili, con effetti giuridici o simili significativi in relazione ai minori, ad esempio per proteggere il loro benessere. In tal caso, il trattamento può essere effettuato sulla base delle eccezioni di cui all'articolo 22, paragrafo 2, lettere a), b) oc), a seconda dei casi.

In questi casi devono essere predisposte idonee misure di salvaguardia, come previsto dall'articolo 22, paragrafo 2, lettera b) e articolo 22, paragrafo 3, e devono pertanto essere appropriate ai bambini. Il Titolare del Trattamento deve garantire che tali misure di salvaguardia siano efficaci nel proteggere i diritti, le libertà e gli interessi legittimi dei minori di cui trattano i dati.

L'esigenza di una protezione particolare per i bambini si riflette nel considerando 38, che afferma:

<p>I minori meritano una protezione specifica per quanto riguarda i loro dati personali, in quanto potrebbero essere meno consapevoli dei rischi, delle conseguenze e delle garanzie in questione e dei loro diritti in relazione al trattamento dei dati personali. Tale protezione specifica dovrebbe, in particolare, applicarsi all'utilizzo dei dati personali dei minori ai fini della commercializzazione o della creazione di profili di personalità o di utenti e della raccolta di dati personali relativi ai minori quando si utilizzano servizi offerti direttamente a un minore.</p>

⁴³ Il considerando 71 della GDPR afferma che:

"Al fine di garantire un trattamento equo e trasparente nei confronti dell'interessato, tenendo conto delle circostanze specifiche e del contesto in cui i dati personali sono trattati, il Titolare del Trattamento dovrebbe utilizzare procedure matematiche o statistiche appropriate per la profilazione, attuare misure tecniche e organizzative è opportuno per garantire, in particolare, che i fattori che determinano inesattezze nei dati personali siano corretti e che il rischio di errori sia ridotto al minimo, ..."

⁴⁴ Considerando 71 - "tale misura non dovrebbe riguardare un bambino".

L'articolo 22 non impedisce ai Titolari del Trattamento di prendere decisioni esclusivamente automatiche sui minori, se la decisione non avrà un effetto legale o di effetto analogo sul minore. Tuttavia, il solo processo decisionale automatico che influenza le scelte e il comportamento di un bambino potrebbe potenzialmente avere un effetto legale o simile su di essi, a seconda della natura delle scelte e dei comportamenti in questione.

Poiché i bambini rappresentano un gruppo più vulnerabile della società, le organizzazioni dovrebbero, in generale, astenersi dal profilare per scopi di marketing.⁴⁵ I bambini possono essere particolarmente suscettibili nell'ambiente online e più facilmente influenzati dalla pubblicità comportamentale. Ad esempio, nel gioco online, la profilazione può essere utilizzata per indirizzare i giocatori che l'algoritmo considera più propensi a spendere soldi per il gioco, oltre a fornire annunci più personalizzati. L'età e la maturità del bambino possono influenzare la loro capacità di comprendere la motivazione dietro questo tipo di marketing o le conseguenze.⁴⁶

L'articolo 40, paragrafo 2, lettera g) si riferisce esplicitamente alla preparazione di codici di condotta che includano salvaguardie per i minori; potrebbe anche essere possibile sviluppare codici esistenti.⁴⁷

VI. Valutazione dell'impatto sulla protezione dei dati (DPIA) e Responsabile della protezione dei dati (DPO)

La responsabilità è un'area importante e un requisito esplicito ai sensi del GDPR.⁴⁸

Come strumento chiave di responsabilità, una DPIA consente al Titolare del Trattamento di valutare i rischi implicati nel processo decisionale automatico, inclusa la profilazione. È un modo per dimostrare che sono state messe in atto misure adeguate per fronteggiare tali rischi e dimostrare la conformità con il GDPR.

L'articolo 35, paragrafo 3, lettera a) sottolinea la necessità che il Titolare del Trattamento effettui una DPIA nel caso di:

una valutazione sistematica e approfondita degli aspetti personali relativi alle persone fisiche che si basa su un trattamento automatizzato, compresa la profilazione, e su cui si basano le decisioni che producono effetti giuridici riguardanti la persona fisica o che influenzano in modo significativo la persona fisica;

L'articolo 35, paragrafo 3, lettera a) fa riferimento a valutazioni comprendenti la profilazione e le decisioni che sono "basate" sull'elaborazione automatizzata, piuttosto che sulla "sola" elaborazione automatizzata. Consideriamo ciò che l'articolo 35, paragrafo 3, lettera a) si applicherà in caso di adozione di decisioni, compresa la profilazione di effetti giuridici o di analogia rilevanza non completamente automatizzati, nonché un processo decisionale esclusivamente automatico definito all'articolo 22 (1).

⁴⁵ L'Opinione WP29 02/2013 sulle app su dispositivi intelligenti (WP202), adottata il 27 febbraio 2013, nella sezione specifica 3.10 su Bambini, specifica a pagina 26 che "i Titolari del Trattamento dei dati non devono trattare i dati dei bambini a scopo di pubblicità comportamentale, né direttamente né indirettamente, dal momento che questo sarà fuori dal campo di applicazione della comprensione del bambino e quindi superare i limiti del trattamento legale".

⁴⁶ Uno studio dell'UE [sull'impatto del marketing attraverso i social media, i giochi online e le applicazioni mobili sul comportamento dei bambini](#) ha scoperto che le pratiche di marketing hanno un chiaro impatto sul comportamento dei bambini. Questo studio era basato su bambini di età compresa tra 6 e 12 anni.

⁴⁷ Un esempio di un codice di condotta relativo al marketing per i bambini è quello prodotto dal Codice di condotta di FEDMA, memorandum esplicativo, disponibile all'indirizzo: <http://www.oecd.org/sti/ieconomy/2091875.pdf> Accesso 15 maggio 2017. Vedi, in particolare: "6.2 I marketer che si rivolgono ai bambini, o per i quali è probabile che i bambini rappresentino una parte del loro pubblico, non devono sfruttare la credulità, la lealtà, la vulnerabilità o la mancanza di esperienza dei bambini; I professionisti del marketing non dovrebbero rendere l'accesso di un minore a un sito web in base alla raccolta di informazioni personali dettagliate.

In particolare, gli incentivi speciali come le offerte e i giochi non dovrebbero essere usati per invogliare i bambini a divulgare informazioni personali dettagliate. "

⁴⁸ Come richiesto dal GDPR articolo 5, paragrafo 2

Se il Titolare del Trattamento prevede un "modello" in cui prende solo decisioni automatiche che hanno un forte impatto sugli individui sulla base dei profili realizzati su di loro e non può fare affidamento sul consenso dell'individuo, su un contratto con l'individuo o su una legge che lo autorizza, il Titolare del Trattamento non dovrebbe procedere.

Il Titolare del Trattamento può anche immaginare un "modello" di decisione basato sulla profilazione, aumentando significativamente il livello dell'intervento umano in modo tale che il modello non sia più un processo decisionale completamente automatico, sebbene il trattamento possa ancora presentare rischi per le fondamentali diritti e libertà. In tal caso, il Titolare del Trattamento deve assicurarsi di poter affrontare tali rischi e soddisfare i requisiti descritti nel capitolo III delle presenti linee guida.

Una DPIA può anche essere un modo utile per il Titolare del Trattamento di identificare quali misure introdurrà per affrontare i rischi di protezione dei dati coinvolti nell'elaborazione. Tali misure ⁴⁹ potrebbero includere:

- informare la persona interessata dell'esistenza e della logica implicata 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; e
- consentendo all'interessato di esprimere il proprio punto di vista.

Altre attività di profilazione possono garantire una DPIA, a seconda delle specifiche del caso. I Titolari del Trattamento potrebbero voler consultare le linee guida WP29 sui DPIA ⁵⁰ per ulteriori informazioni e per aiutare a determinare la necessità di eseguire una DPIA.

Un requisito aggiuntivo di responsabilità è la designazione di un responsabile della protezione dei dati, laddove la definizione dei profili e / o il processo decisionale automatizzato è un'attività centrale del Titolare del Trattamento e richiede un monitoraggio regolare e sistematico degli interessati su vasta scala (articolo 37, paragrafo 1, lettera b).) ⁵¹

⁴⁹ Rispecchiare i requisiti 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 sulla protezione dei dati dell'articolo 29. Linee guida sulla valutazione dell'impatto sulla protezione dei dati (DPIA) e determinare se il trattamento è "suscettibile di comportare un rischio elevato" ai fini del regolamento 2016/679. 4 aprile 2017. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accesso 24 aprile 2017.

⁵¹ Gruppo di lavoro sull'articolo 29 sulla protezione dei dati. Linee guida sul responsabile della protezione dei dati (DPO). 5 aprile 2017;

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 Consultato il 22 gennaio 2018

ALLEGATO 1 - Raccomandazioni sulle buone pratiche

Le seguenti raccomandazioni sulle buone pratiche aiuteranno i Titolari del Trattamento dei dati a soddisfare i requisiti delle disposizioni GDPR sulla profilazione e il processo decisionale automatizzato.⁵²

Articolo	Problema	Raccomandazione
5(1)(a), 12, 13, 14	Diritto di avere informazioni	<p>I Titolari del Trattamento dovrebbero consultare le linee guida WP29 sulla trasparenza WP260 per i requisiti generali di trasparenza.</p> <p>Oltre ai requisiti generali, quando il Titolare del Trattamento elabora dati come definiti nell'articolo 22, devono fornire informazioni significative sulla logica in questione.</p> <p>Invece di fornire una spiegazione matematica complessa su come funzionano gli algoritmi o l'apprendimento automatico, il Titolare del Trattamento dovrebbe considerare l'utilizzo di metodi chiari e completi per fornire le informazioni all'interessato, ad esempio:</p> <ul style="list-style-type: none"> • le categorie di dati che sono state o saranno utilizzate nella profilazione o nel processo decisionale; • perché queste categorie sono considerate pertinenti • come viene costruito qualsiasi profilo utilizzato nel processo decisionale automatico, incluse le statistiche utilizzate nell'analisi; • perché questo profilo è rilevante per il processo decisionale automatico; e • come viene utilizzato per una decisione riguardante l'interessato. <p>Tali informazioni saranno generalmente più pertinenti per l'interessato e contribuiranno alla trasparenza del trattamento.</p> <p>I Titolari del Trattamento potrebbero voler considerare la visualizzazione e le tecniche interattive per favorire la trasparenza algoritmica⁵³.</p>
6(1)(a)	Consenso come base per l'elaborazione	Se i Titolari del Trattamento fanno affidamento sul consenso come base per l'elaborazione, dovrebbero consultare le Linee guida WP29 sul consenso WP259.
15	Diritto di accesso	I Titolari del Trattamento potrebbero voler prendere in considerazione l'implementazione di un meccanismo che consenta agli interessati di verificare il loro profilo, compresi i dettagli delle informazioni e le fonti utilizzate per svilupparlo.
16	Diritto di rettifica	<p>I Titolari del Trattamento che forniscono agli interessati l'accesso al loro profilo in relazione ai loro diritti di cui all'articolo 15 dovrebbero consentire loro di aggiornare o modificare eventuali inesattezze nei dati o nel profilo.</p> <p>Ciò può anche aiutarli a rispettare gli obblighi di cui all'articolo 5, paragrafo 1, lettera d).</p> <p>I Titolari del Trattamento potrebbero prendere in considerazione l'introduzione di strumenti di gestione delle preferenze online come una dashboard sulla privacy.</p>

⁵² I Titolari del Trattamento devono anche assicurarsi di disporre di solide procedure per garantire che possano adempiere ai loro obblighi ai sensi degli articoli 15-22 nei tempi previsti dal GDPR.

⁵³ Ufficio dei Commissari informativi - Big data, intelligenza artificiale, apprendimento automatico e protezione dei dati versione 2.0, 03/2017. Pagina 87, paragrafo 194, marzo 2017. <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> Accesso 24 aprile 2017

		<p>Ciò conferisce ai soggetti interessati la possibilità di gestire ciò che sta accadendo alle loro informazioni attraverso una serie di servizi diversi, consentendo loro di modificare le impostazioni, aggiornare i loro dati personali e rivedere o modificare il loro profilo per correggere eventuali inesattezze.</p>
21 (1) e (2)	Diritto di obiettare	<p>Il diritto di opporsi all'articolo 21, paragrafi 1 e 2, deve essere esplicitamente portato a conoscenza dell'interessato e presentato chiaramente e separatamente dalle altre informazioni (articolo 21, paragrafo 4).</p> <p>I Titolari del Trattamento devono garantire che questo diritto venga visualizzato in modo visibile sul loro sito web o in qualsiasi documentazione pertinente e non nascosto in altri termini e condizioni.</p>
22 e considerando 71	Adeguate misure di sicurezza	<p>Il seguente elenco, sebbene non esaustivo, fornisce alcuni suggerimenti di buone pratiche da tenere in considerazione ai Titolari del Trattamento quando prendono decisioni esclusivamente automatiche, inclusa la profilazione (definita nell'articolo 22, paragrafo 1):</p> <ul style="list-style-type: none"> • controlli regolari della garanzia della qualità dei loro sistemi per garantire che le persone siano trattate in modo equo e non discriminate, sulla base di categorie speciali di dati personali o in altro modo; • auditing algoritmico - testare gli algoritmi utilizzati e sviluppati dai sistemi di machine learning per dimostrare che stanno effettivamente funzionando come previsto, e non producendo risultati discriminatori, errati o ingiustificati; • per l'audit indipendente di "terze parti" (in cui il processo decisionale basato sulla profilazione ha un forte impatto sugli individui), fornire all'auditor tutte le informazioni necessarie su come funziona l'algoritmo o il sistema di apprendimento automatico; • ottenendo garanzie contrattuali per gli algoritmi di terze parti che sono stati effettuati audit e test e che l'algoritmo è conforme agli standard concordati; • misure specifiche per la minimizzazione dei dati da incorporare in modo chiaro • periodi di conservazione dei profili e dei dati personali utilizzati durante la creazione o l'applicazione dei profili; • utilizzando 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; e, • un meccanismo per l'intervento umano in determinati casi, ad esempio fornendo un collegamento a un processo di ricorso nel momento in cui la decisione automatizzata viene consegnata all'interessato, con tempi concordati per la revisione e un punto di contatto designato • per qualsiasi domanda. <p>I Titolari del Trattamento possono anche esplorare opzioni come:</p> <ul style="list-style-type: none"> • meccanismi di certificazione per le operazioni di trattamento; • codici di condotta per i processi di controllo che coinvolgono l'apprendimento automatico; • commissioni di revisione etica per valutare i potenziali danni e benefici per la società di particolari applicazioni per la profilazione.

ALLEGATO 2 - Principali disposizioni del GDPR

Principali disposizioni GDPR che fanno riferimento alla profilazione generale e al processo decisionale automatizzato

Articolo	recital	Commenti
3(2)(b)	24	Il monitoraggio del comportamento dei soggetti di dati per quanto riguarda il loro comportamento si svolge all'interno dell'Unione. Considerando 24 "... tracked su internet uso di tecniche di trattamento dei dati personali che consistono nel profilare una persona fisica, in particolare al fine di prendere decisioni riguardanti lei o lui o per analizzare o predire lei o la sua preferenze personali, comportamenti o atteggiamenti ".
4(4)	30	Articolo 4, paragrafo 4, definizione della profilazione Considerando 30 "Identificatori online, Come indirizzi di Protocollo Internet, identificatori di cookie o altri identificatori come etichette di identificazione a radiofrequenza ... possono lasciare tracce che, in particolare se combinate con identificatori univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone naturali e identificarle. "
5 e 6	72	Considerando 72: "La profilazione è soggetta alle regole del presente regolamento che disciplinano il trattamento dei dati personali, quali i motivi giuridici per il 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 bambini meritano una protezione specifica ... in particolare, ... per l'uso dei dati personali dei bambini allo scopo di ... creare personalità o profili utente".
13 e 14	60	Diritto di essere informato Considerando 60: "Inoltre, l'interessato deve essere informato dell'esistenza della profilazione e delle conseguenze di tale profilazione."
15	63	Diritto di accesso. Considerando 63: "Diritto di conoscere e ottenere comunicazioni ... conformemente alle finalità per le quali i dati personali sono trattati, ... e, almeno in sede di profilazione, le conseguenze di tale profilazione".
21 (1) (2) e (3)	70	Diritto di opporsi alla profilazione. Considerando 70 "... il diritto di opporsi a tale elaborazione, inclusa la profilazione nella misura in cui è correlata a tale marketing diretto."
23	73	Considerando 73: "Restrizioni relative a principi specifici e concernenti Il diritto di opposizione e le decisioni basate sulla profilazione possono essere imposte dall'Unione o

		Diritto degli Stati membri nella misura necessaria e proporzionata in una società democratica ... "per salvaguardare obiettivi specifici di interesse pubblico generale.
35(3)(a)	91	Una DPIA è richiesta nel caso di "una valutazione sistematica e approfondita degli aspetti personali relativi alle persone fisiche che si basa su un trattamento automatizzato, compresa la profilazione, e su cui si basano le decisioni che producono effetti giuridici riguardanti la persona fisica o che influenzano significativamente in modo significativo la persona fisica; "Comprende il processo decisionale compresa la profilazione che non è solo automatica d.

Principali disposizioni del GDPR che fanno riferimento al processo decisionale automatizzato come definito all'articolo 22

Articolo	recital	Commenti
13 (2) (f) e 14 (2) (g)	61	Diritto di essere informato su: <ul style="list-style-type: none"> • l'esistenza di processi decisionali automatizzati ai sensi della A22 (1) e (4); • informazioni significative sulla logica coinvolta; • significato e le conseguenze previste di tale trattamento.
15(h)		Diritti di accesso specifici alle informazioni sull'esistenza di processi decisionali esclusivamente automatizzati, inclusa la profilazione.
22(1)	71	<p>Divieto del processo decisionale basato esclusivamente sul trattamento automatizzato, inclusa la profilazione, che produce effetti legali / similmente significativi.</p> <p>Oltre alla spiegazione fornita nel corpo principale degli orientamenti, i seguenti punti ampliano la motivazione alla base della lettura dell'articolo 22 come divieto:</p> <ul style="list-style-type: none"> • Sebbene il capo III riguardi i diritti dell'interessato, le disposizioni degli articoli 12-22 non riguardano esclusivamente l'esercizio attivo dei diritti. Alcuni dei diritti sono passivi; non si riferiscono tutte a situazioni in cui l'interessato intraprende un'azione, cioè fa una richiesta o una lamentela o una richiesta di qualche tipo. Gli articoli 15-18 e 20-21 riguardano l'interessato che esercita attivamente i propri diritti, ma gli articoli 13 e 14 riguardano i doveri che il Titolare del Trattamento deve soddisfare, senza alcun coinvolgimento attivo dell'interessato. Quindi l'inclusione dell'articolo 22 in quel capitolo non significa di per sé che sia un diritto di obiettare; • L'articolo 12, paragrafo 2, parla dell'esercizio dei "diritti degli interessati" ai sensi degli articoli da 15 a 22; ma questo non significa che l'articolo 22 (1) stesso debba essere interpretato come un diritto. C'è un diritto attivo in A22, ma fa parte delle garanzie che devono essere applicate nei casi in cui è consentito il processo decisionale automatizzato (articolo 22 (2) (ac)) - il diritto di ottenere l'intervento umano, esprimere la sua o il suo punto di vista e di contestare la decisione. Si applica solo in quei casi, poiché è vietata la realizzazione del trattamento descritto nell'articolo 22, paragrafo 1, su altre basi; • L'articolo 22 si trova in una sezione del GDPR intitolata "Diritto di opporsi e processo decisionale individuale automatizzato", il che implica che l'articolo 22 non è un diritto di contestare l'articolo 21. Ciò è ulteriormente sottolineato dalla mancanza nell'articolo 22 di un obbligo di informazione esplicitamente equivalente a quello di cui all'articolo 21, paragrafo 4; • Se l'articolo 22 dovesse essere interpretato come un diritto di opposizione, l'eccezione in questione

		<p>L'articolo 22, paragrafo 2, lettera c) non avrebbe molto senso. L'eccezione afferma che il processo decisionale automatizzato può ancora avere luogo se l'interessato ha dato il consenso esplicito (vedi sotto). Ciò sarebbe contraddittorio in quanto l'interessato non può opporsi e acconsentire allo stesso trattamento;</p> <ul style="list-style-type: none"> • Un'obiezione significherebbe che l'intervento umano deve aver luogo. L'articolo 22, paragrafo 2, lettere a) ec), fa eccezione rispetto alla norma principale di cui all'articolo 22, paragrafo 1, ma solo fino a quando l'interessato non è a disposizione dell'interessato, come specificato all'articolo 22, paragrafo 3. Poiché la persona interessata (obiettando) ha già richiesto l'intervento umano, l'articolo 22, paragrafo 2, lettere a) ec), sarebbe automaticamente eluso in ogni caso, rendendo in tal modo privi di significato. <p>Considerando 71: "... Tale trattamento comprende la" profilazione "che consiste in qualsiasi forma di trattamento automatizzato di dati personali che valuti gli aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti le prestazioni del soggetto interessato sul lavoro, situazione economica, salute, personale, preferenze o interessi, affidabilità o comportamento, posizione o movimenti "..... "Tale misura non dovrebbe riguardare un bambino"</p>
22(2)(a-c)	71	<p>L'articolo 22, paragrafo 2, abolisce il divieto di trattamento basato sulla (a) esecuzione o di stipulare un contratto, (b) legge dell'Unione o dello Stato membro, o (c) consenso esplicito.</p> <p>Il considerando 71 fornisce ulteriori informazioni sul 22 (2) (b) e afferma che il trattamento descritto in A22 (1): "Dovrebbe essere consentito se espressamente autorizzato dal diritto dell'Unione o dello Stato membro a cui è soggetto il Titolare del Trattamento, anche a scopo di controllo e prevenzione delle frodi e evasione fiscale, conformemente ai regolamenti, alle norme e alle raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di controllo e garantire la sicurezza e l'affidabilità di un servizio fornito dal Titolare del Trattamento ... "</p>
22(3)	71	<p>L'articolo 22, paragrafo 3 e il considerando 71 specificano anche che, anche nei casi di cui all'articolo 22, paragrafo 2, lettere a) ec), il trattamento dovrebbe essere soggetto a garanzie adeguate.</p> <p>Considerando 71: "Che dovrebbe includere informazioni specifiche all'interessato e il diritto di ottenere l'intervento umano, di esprimere il proprio punto di vista, ottenere una spiegazione della decisione presa dopo tale valutazione e contestare la decisione. Tale misura non dovrebbe riguardare un bambino ".</p>
23	73	<p>Considerando 73: "Restrizioni relative a principi specifici e concernenti Il diritto di opposizione e le decisioni basate sulla profilazione possono essere imposte dal diritto dell'Unione o degli Stati membri nella misura necessaria e proporzionata in una società democratica ..." per salvaguardare obiettivi specifici della collettività interesse.</p>
35(3)(a)	91	<p>Requisito per effettuare una DPIA.</p>
47(2)(e)		<p>Le regole aziendali vincolanti di cui all'articolo 47, paragrafo 1 devono specificare almeno "... Il diritto a non essere assoggettato a decisioni basate esclusivamente sul trattamento automatizzato, compresa la profilazione conformemente all'articolo 22 ... "</p>

ALLEGATO 3 - Approfondimenti

Queste linee guida tengono conto di quanto segue:

- [WP29 Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted 13 May 2013;](#)
- [WP29 Opinion 2/2010 on online behavioural advertising, WP171;](#)
- [WP29 Opinion 03/2013 on Purpose limitation, WP 203;](#)
- [WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217](#)
- [WP29 Statement on the role of a risk-based approach to data protection legal frameworks, WP218;](#)
- [WP29 Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223;](#)
- [WP29 Guidelines on Data Protection Officers \(DPOs\), WP243;](#)
- [WP29 Guidelines on identifying a controller or processor's lead supervisory authority WP244;](#)
- [WP29 Guidelines on consent, WP259](#)
- [WP29 Guidelines on transparency, WP260](#)
- [Council of Europe. Recommendation CM/Rec\(2010\)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling;](#)
- [Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 01/2017](#)
- [Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0, 03/2017](#)
- [Office of the Australian Commissioner - Consultation draft: Guide to big data and the Australian Privacy Principles, 05/2016](#)
- [European Data Protection Supervisor \(EDPS\) Opinion 7/2015 – Meeting the challenges of big data, 19 November 2015](#)
- [Datatilsynet – Big Data – privacy principles under pressure 09/2013](#)
- [Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data - Draft explanatory report on the modernised version of CoE Convention 108, August 2016](#)
- [Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy. Report, November 2015](#)
- [European Data Protection Supervisor – Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit](#)
- [Joint Committee of the European Supervisory Authorities. Joint Committee Discussion Paper on the use of Big Data by financial institutions 2016-86. \[https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf\]\(https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf\)](#)
- [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>](#)
- [United States Senate, Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller, December 18, 2013. \[https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf\]\(https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf\)](#)
- [Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for. Research paper, posted 24 May 2017. \[https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855\]\(https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855\)](#)

- 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?amp=1>. Accesso 24 agosto 2017
- Council of Europe. Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfil children’s rights in the digital environment (revised draft, 25 July 2017). <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 al 31 agosto 2017
- Unicef. Privacy, protection of personal information and reputation rights. Discussion paper series: Children’s Rights and Business in a Digital World. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Accesso al 31 agosto 2017
- House of Lords. Growing up with the internet. Select Committee on Communications, 2nd Report of Sessions 2016 – 17. <https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm>. Accesso al 31 agosto 2017
- Sandra Wachter, Brent Mittelstadt and Luciano Floridi. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, 28 December 2016. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/ . Accesso 13 dicembre 2017
- Sandra Wachter, Brent Mittelstadt and Chris Russell. Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR, 6 October 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Accesso 13 dicembre 2017
- Australian Government. Better Practice Guide, Automated Assistance in Administrative Decision-Making. Six steps methodology, plus summary of checklist points Part 7 February 2007. <https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf>. Accesso 9 gennaio 2018

Courtesy of the Privacy Law Centre