



Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2025/2026

Titolo

Il bilanciamento costituzionale tra protezione dei dati e libertà di iniziativa economica: Analisi della tecnica di profiling nel quadro del GDPR.

Relatore: Ch.mo prof. Bergonzini Giuseppe

Laureando: Marchiani Yuri
Matricola: 2078114

Indice

Introduzione	3
Capitolo I - L'inquadramento costituzionale della profilazione: tra dignità umana e logiche di mercato	6
1.1 Il diritto alla riservatezza come diritto fondamentale ...	6
1.2 La libertà di iniziativa economica e i suoi limiti.....	11
1.3 Principio di proporzionalità e la necessità di bilanciamento	13
1.4 Il profiling: definizione legale e tecnologica.....	15
Capitolo II - Il GDPR come strumento di bilanciamento: principi, liceità e tutele contro il profiling	19
2.1 Il GDPR in breve.....	19
2.2 Articolo 6 GDPR: Liceità del trattamento	22
2.3 I diritti dell'interessato: la contromisura al profiling aggressivo	25
Capitolo III – Il bilanciamento in concreto: decisioni dell'autorità garante	29
3.1 Natura e funzione dell'Autorità Garante.....	30
3.2 La profilazione nel settore <i>retail</i> : il caso “Rinascente”	33
3.3 La profilazione <i>social</i> : il caso “TikTok”	35
Conclusioni.....	39
Bibliografia.....	42

Introduzione

Nel secolo in cui viviamo, il dato costituisce una risorsa fondamentale, che alimenta un'economia digitale basata sulla capacità di profilare in maniera predittiva e accurata il comportamento dell'uomo. L'economia di cui parliamo è anche detta *data-driven economy*¹, ossia un'economia basata sui dati personali. Nomi, e-mail, preferenze online sono alcune delle molte informazioni che caratterizzano la monetizzazione dei dati personali e che permettono ad aziende ed enti di migliorare i servizi, di ottimizzare campagne pubblicitarie e offrire contenuti a costi vantaggiosi.

In questo scenario, la tecnica della profilazione svolge un ruolo fondamentale nella trasformazione del dato grezzo in un vero e proprio *asset* economico. Questa tecnica, qualificata dalla normativa europea come trattamento automatizzato finalizzato a valutare aspetti della sfera personale², si discosta dalla semplice analisi statica dell'utente ma punta, piuttosto, a prevedere preferenze, interessi e comportamenti futuri. Se da un lato questa capacità predittiva consente alle imprese di giocare d'anticipo sulla domanda, essa apre inevitabilmente complessi interrogativi giuridici. La difficile convivenza tra le dinamiche della *data economy* e la salvaguardia dell'individuo impone un'opera di ponderazione costituzionale. Si trovano quindi contrapposti la libertà di iniziativa economica, che rappresenta il motore dell'ecosistema digitale,

¹ Privacy Studio, *Dati personali: la nuova valuta nell'economia digitale*, in *Privacy Studio*, disponibile all'indirizzo: <https://www.privacystudio.it/dati-personali-la-nuova-valuta-nelleconomia-digitale/>.

² Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), art. 4, punto 4.

e i diritti inviolabili della persona, *in primis* riservatezza e protezione dei dati. Ne consegue che la vera sfida per l'interprete non si esaurisce nell'applicazione della legge, ma si estende alla necessità di evitare che il progresso tecnologico eroda le garanzie fissate dalla Costituzione e dalla Carta di Nizza³. Alla luce di tali premesse, il presente elaborato si articola in tre capitoli, volti ad analizzare l'evoluzione del rapporto tra tutela della persona e libertà d'impresa. Nel primo capitolo vengono analizzati i fondamenti costituzionali della materia, esaminando l'evoluzione del diritto alla riservatezza, da intendersi oggi come "autodeterminazione informativa", e il suo rapporto con la libertà di iniziativa economica sancita dall'articolo 41 della Costituzione. Viene inoltre definita la profilazione non solo sotto il profilo tecnologico, ma come fattispecie giuridica che richiede precisi limiti per non ledere la dignità umana. Proseguendo con la ricerca, nel secondo capitolo del Regolamento Europeo (GDPR) si individua la soluzione per bilanciare la tensione tra gli interessi in gioco. L'approfondimento si concentra sui requisiti di liceità del trattamento e, in particolare, gli strumenti di tutela posti a garanzia dell'interessato di fronte a forme di *profiling* invasivo: il diritto di opposizione (art. 21) e la tutela avverso le decisioni automatizzate (art. 22). In questo contesto, tali norme fungono da tutela legale per proteggere la dignità umana dai pericoli della discriminazione algoritmica. Infine, il terzo capitolo è incentrato sull'analisi della dimensione applicativa, anche attraverso l'esame della

³ Cfr. Costituzione della Repubblica Italiana, artt. 2 e 41, co. 2, il quale sancisce che l'iniziativa economica privata «non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana». Si vedano inoltre gli artt. 7 (Rispetto della vita privata e della vita familiare) e 8 (Protezione dei dati di carattere personale) della Carta dei diritti fondamentali dell'Unione europea (2012/C 326/02).

recente prassi decisoria dell'Autorità Garante. Con l'osservazione di casi emblematici in ambito marketing e profilazione, come ad esempio, i provvedimenti *Rinascenza* e *TikTok*, è interessante notare come le categorie teoriche trovino una concreta realizzazione nell'attività sanzionatoria, contribuendo in modo significativo a guidare l'evolversi del mercato digitale.

Capitolo I - L'inquadramento costituzionale della profilazione: tra dignità umana e logiche di mercato

1.1 Il diritto alla riservatezza come diritto fondamentale

Da tempo il dibattito giuridico nazionale si interroga sul rapporto tra attività giurisdizionale e innovazione tecnologica, con particolare attenzione all'automazione delle decisioni⁴. I costituzionalisti avvertono che per comprendere la portata di queste innovazioni è necessario guardare oltre il dato tecnico: le nuove tecnologie stanno infatti ridisegnando profondamente i processi decisionali, con conseguenze inevitabili sull'equilibrio democratico del sistema⁵. L'adozione di questi strumenti tecnologici all'interno delle dinamiche decisionali è tutt'altro che priva di conseguenze: è fondamentale sottolineare, infatti, come questi sistemi tendano ad imporre la loro architettura logica⁶, costringendo l'utente ad operare entro dei paletti prestabiliti dalla macchina o dall'ingegnere che l'ha programmata, anziché dalla volontà del decisore legittimo. Queste nuove dinamiche rischiano di causare uno spostamento di potere capace di minare le fondamenta istituzionali su cui si regge lo Stato contemporaneo. Per indagare più nel dettaglio la relazione che intercorre tra il soggetto e l'ecosistema digitale, è

⁴ C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo, Rivista trimestrale Speciale*/2019, 101-130.

⁵ E. LONGO, *Predizione, profilazione e giustizia* in A. ADINOLFI, A. SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022, 581-608.

⁶ E. LONGO, *La giustizia nell'era digitale*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica. Atti del Convegno Annuale dell'Associazione "Gruppo di Pisa" (Genova, 18-19 giugno 2021)*, Napoli, 2022, 5.

essenziale ripercorrere l'evoluzione storica del concetto di *privacy*. Ben lontano dal configurarsi come una struttura statica, questo diritto ha vissuto un profondo mutamento, adattandosi con elasticità sulle trasformazioni sociali e, ancor di più, sulle rivoluzioni tecnologiche che hanno caratterizzato la modernità. L'interpretazione storica del diritto alla riservatezza individua il suo *incipit* obbligato nel panorama giuridico statunitense, dove la nozione di *privacy* fu inizialmente teorizzata come risposta giuridica alle nuove sfide poste dal progresso tecnico. Vi è un ampio consenso dottrinale nel ricondurre l'origine di tale diritto al celebre saggio *The Right to Privacy*, pubblicato nel 1890 sulla *Harvard Law Review* a cura di Samuel Warren e Louis Brandeis⁷. L'urgenza di tale tutela sorgerà come reazione al dilagare del c.d. *yellow journalism* (la stampa scandalistica) e alla commercializzazione della fotografia istantanea (un esempio fu la "snap camera" di Kodak), innovazioni che per la prima volta permettevano di cogliere e diffondere scatti intimi dell'esistenza privata, mettendo a repentaglio la serenità domestica. Mancando un esplicito fondamento costituzionale, gli autori hanno definito il *right to be let alone* come un diritto derivante dal principio della tutela della personalità inviolata dell'individuo.

Distinto dal diritto di proprietà, il diritto appena citato mirava quindi a tutelare la sfera emotiva e le sensazioni personali da intrusioni esterne, riconoscendo al contempo delle eccezioni, come nel caso di pubblicazioni su fatti di pubblico interesse o coperte da privilegio giuridico. Il successivo *iter* evolutivo dell'ordinamento nordamericano si è articolato lungo due direttrici: quella della *Tort Law* (responsabilità civile) e quella di rango costituzionale. Per quanto riguarda la

⁷ S. D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, Project Gutenberg, 1890, 192-220.

responsabilità civile, la giurisprudenza ha formalizzato, complice l'elaborazione di William Prosser nel 1960⁸, quattro distinte figure di lesione (*privacy torts*): l'intrusione nella solitudine altrui (*intrusion upon seclusion*), la rivelazione pubblica di fatti privati (*public disclosure of private facts*), la falsa rappresentazione agli occhi del pubblico (*false light*) e, infine, l'appropriazione indebita del nome o dell'immagine (*appropriation*). Sul fronte costituzionale, la Corte Suprema degli Stati Uniti ha riconosciuto la privacy come diritto fondamentale, sfruttando la dottrina delle “penombre” (*penumbras*), tale garanzia venne dedotta da un'interpretazione approfondita degli Emendamenti I, IV, V e IX. Uno snodo cruciale è segnato dalla pronuncia *Katz v. United States* del 1967⁹, attraverso la quale la Corte ha definitivamente oltrepassato la visione spaziale della privacy (ancora legata alla proprietà materiale), sancendo il principio per cui il IV Emendamento "protegge le persone, non i luoghi".

In tale occasione è stato pensato il test della *reasonable expectation of privacy*, secondo il quale, la tutela scatta quando una persona si aspetta ragionevolmente la riservatezza, e la società riconosce tale aspettativa come oggettivamente ragionevole. Va tuttavia notato che, con l'avvento dell'era digitale, l'ordinamento statunitense ha mantenuto un approccio "settoriale" (*sectoral approach*), caratterizzato da una frammentazione normativa (leggi specifiche per sanità, video, credito) e basato principalmente sul meccanismo del *notice and choice*¹⁰,

⁸ W. PROSSER , *Privacy*, in *California Law Review*, Vol. 48, No. 3, 1960, 383-423.

⁹ *Supreme Court of the United States*, 18 dicembre 1967, *Katz v. United States*, 389 U.S. 347.

¹⁰ Meccanismo di autoregolamentazione tipico dell'ordinamento USA, basato sull'informativa all'utente (*notice*) e sulla sua facoltà di accettare o rifiutare il

differenziandosi così in modo evidente dal modello europeo che si andrà ad analizzare. Nel contesto giuridico italiano, il riconoscimento del diritto alla riservatezza ha affrontato un percorso decisamente più complesso, a causa della iniziale chiusura ermeneutica della giurisprudenza di legittimità. Sino alla metà degli anni Settanta, infatti, la Suprema Corte non riconosceva l'esistenza di un autonomo diritto alla *privacy* non esplicitamente sancito dalla legge, orientamento cristallizzato nel noto caso Caruso del 1956¹¹. In quell'occasione, i giudici di Piazza Cavour rigettarono le pretese degli eredi del tenore Enrico Caruso, i quali si opponevano alla rappresentazione cinematografica delle sue vicende private, stabilendo che il solo "desiderio di riserbo" non si asserisse a interesse giuridicamente tutelato e che la curiosità del pubblico, per quanto "non elevata", non integrasse di per sé gli estremi dell'illecito. Il vero e proprio cambiamento giurisprudenziale si materializzò soltanto con la storica sentenza Soraya del 1975 (Cass. n. 2129)¹², nata dalla pubblicazione di scatti ritraenti l'ex imperatrice di Persia in momenti di intimità domestica. Attraverso un'audace operazione pretoria, la Cassazione sancì per la prima volta l'esistenza del diritto alla riservatezza, definendolo come tutela di "quelle situazioni e vicende strettamente personali e familiari che, anche se verificatesi *extra moenia*, non presentano per i terzi un interesse socialmente apprezzabile". L'ancoraggio costituzionale di tale tutela è stato individuato nell'articolo 2 della Carta fondamentale, presidio dei diritti inviolabili dell'uomo. La riservatezza si impose così

trattamento (*choice*); è spesso criticato per ridursi a un sistema 'prendere o lasciare' (*take-it-or-leave-it*) che presume il consenso con l'utilizzo del servizio.

¹¹ Corte di Cassazione, Sez. I civ., sentenza 22 dicembre 1956, n. 4487 (*Caso Caruso*).

¹² Corte di Cassazione, Sez. I civ., sentenza 27 maggio 1975, n. 2129 (*Caso Soraya*).

al rango di diritto della personalità costituzionalmente garantito, condizione fondamentale per il libero sviluppo dell'individuo, al sicuro da ingerenze indebite. Tuttavia, una tale consacrazione comportò inevitabilmente un bilanciamento con altre prerogative di rango costituzionale, *in primis* il diritto di cronaca (Art. 21 Cost.). La giurisprudenza, per giustificare la divulgazione di notizie sulla vita privata, ha stabilito dei criteri specifici, conosciuti come il “Decalogo del giornalista¹³”. Questi criteri prevedono che la riservatezza possa essere sacrificata solo in presenza di tre requisiti: l'utilità sociale della notizia, la veridicità (anche solo presunta) dei fatti narrati e la “continenza” formale nell'esposizione. Ne consegue che la sola fama di un individuo non è sufficiente a legittimare un'ingerenza nella sua vita privata, in mancanza di un effettivo interesse pubblico alla divulgazione delle informazioni.

L'avvento della società digitale e il rapido progresso tecnologico hanno evidenziato i limiti di una visione puramente “statica” della privacy, tradizionalmente intesa come il diritto di escludere gli altri. In ambito europeo, si è fatta strada una seconda dimensione di tutela: il diritto alla protezione dei dati personali. Se la riservatezza protegge l'intimità, la *data protection* assicura all'individuo il controllo sulla circolazione delle proprie informazioni. La Carta dei Diritti Fondamentali dell'Unione Europea sancisce solennemente questa contrapposizione. (Carta di Nizza) in due norme separate: l'Articolo 7, posto a tutela della vita privata e familiare, e l'Articolo 8, che riconosce specificamente il diritto alla protezione dei dati di carattere personale¹⁴. È su questo principio che si basa la moderna legislazione comunitaria, il cui apice è

¹³ Corte di Cassazione, Sez. I civ., sentenza 18 ottobre 1984, n. 5259.

¹⁴ Carta dei diritti fondamentali dell'Unione europea (2012/C 326/02), artt. 7 e 8.

rappresentato dal Regolamento UE 2016/679 (GDPR), testo che sancisce il passaggio dal paradigma della segretezza a quello dell'autodeterminazione informativa, restituendo all'interessato la sovranità sui processi decisionali che impattano sulla sua identità digitale.

1.2 La libertà di iniziativa economica e i suoi limiti

L'articolo 2 della Costituzione, che tutela la persona e i suoi dati, costituisce il fondamento della protezione dei dati. L'articolo 41, invece, rappresenta il pilastro su cui si basa l'architettura del mercato dei dati. Tale norma sancisce al primo comma che «l'iniziativa economica privata è libera». Questa disposizione rappresenta il “punto cruciale” della c.d. *Costituzione economica*, riconoscendo all'imprenditore il diritto di organizzare i mezzi di produzione e di definire le strategie di mercato per il perseguimento del profitto. Oggi, nel mondo digitale, questa libertà significa che le aziende, specialmente i grandi colossi tecnologici e chi si occupa di marketing, possono creare nuovi modi di guadagnare sfruttando i dati. Il loro *business* si basa proprio sull'analizzare come si comportano le persone e sul creare profili degli utenti per scopi commerciali¹⁵. L'Assemblea costituente, però, ci aveva visto lungo. Rifiutando sia l'idea di un mercato senza regole sia quella di uno Stato che controlla tutto, ha quindi deciso che la libertà di impresa non può essere assoluta. Non è il diritto di fare tutto

¹⁵ Sul rapporto tra iniziativa economica e nuove tecnologie si veda G. FINOCCHIARO, *Diritto di internet 4. Ed.*, Zanichelli, 2023, 22-27; si veda anche F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 8-9.

ciò che si vuole, ma una libertà che deve sempre rispettare dei limiti e servire anche all'interesse di tutti. Il secondo comma dell'articolo 41 pone infatti dei limiti invalicabili: l'iniziativa economica “*non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana*”.

È proprio in queste clausole limitative che si nasconde il cuore del problema giuridico legato alla profilazione. L'utilità sociale è spesso usata come parametro per valutare la legittimità delle attività d'impresa. Tuttavia, ci si chiede se un modello di business che prospera sulla manipolazione occulta delle scelte individuali o sulla discriminazione algoritmica possa davvero essere considerato socialmente vantaggioso. La tutela della dignità umana e della libertà assume indubbiamente un'importanza cruciale. La dottrina costituzionale ha infatti sottolineato come, nell'ecosistema digitale, la dignità possa essere minacciata dalla ‘datificazione’ dell'individuo. Questo processo prevede infatti che la persona venga ridotta a un ‘profilo’, tutti i dati statistici ad esso collegati diventano così un asset facilmente scambiabile sul mercato, facendo sì che la propria unicità e complessità vada perduta¹⁶. Parallelamente, la libertà tutelata dall'art. 41 va letta in chiave evolutiva, non limitandosi alla sola libertà fisica ma comprendendo la piena autodeterminazione delle scelte individuali.

La grande diffusione delle tecniche di profilazione le ha rese così intrinseche da essere in grado di bypassare i processi decisionali dell'utente (sfruttando *dark patterns* o strategie di *micro-targeting* comportamentale), ciò ha portato al crearsi di un conflitto diretto con il

¹⁶ S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 140-141, ove l'autore discute la "mercificazione" della persona.

divieto costituzionale di limitare la libertà umana. Occorre inoltre considerare la riforma introdotta dalla legge costituzionale n. 1/2022, che ha modificato l'art. 41 inserendo espressamente la tutela della salute e dell'ambiente. Tale intervento conferma che l'ordinamento attribuisce prevalenza a valori di rango superiore rispetto alla mera utilità economica. Nel contesto digitale, la tutela della "salute" riguarda il benessere psicofisico dell'utente, potenzialmente compromesso da fenomeni di dipendenza dalle piattaforme, mentre il concetto di "sicurezza" è riferito alla protezione delle infrastrutture essenziali e alla salvaguardia dei dati personali dalle minacce informatiche, nell'ambito della *cybersecurity*.

1.3 Principio di proporzionalità e la necessità di bilanciamento

Dall'analisi combinata dell'articolo 2 (tutela della persona/privacy) e dell'articolo 41 (libertà d'impresa) emerge un conflitto tra diritti di pari rango costituzionale. Nel nostro ordinamento non esiste una gerarchia rigida che faccia prevalere a priori l'uno sull'altro; pertanto, la giurisprudenza, sia costituzionale che europea, fa ricorso alla tecnica del *bilanciamento*¹⁷.

Il principio di *proporzionalità* è lo strumento ermeneutico chiave per raggiungere questo equilibrio. Tale principio, con origine tedesca e comunitaria, impone che ogni limitazione di un diritto fondamentale (nel nostro caso, la limitazione della privacy per fini economici, o

¹⁷ Sulla tecnica del bilanciamento tra diritti fondamentali, cfr. G. VILLANACCI, *La ragionevolezza nella proporzionalità del diritto*, Torino, 2020, 90-92; R. BIN, G. PITRUZZELLA, *Diritto Pubblico*, Torino, 2023, 380-410.

viceversa la limitazione dell'impresa per fini di privacy) debba soddisfare tre requisiti progressivi:

1. *Idoneità*: La misura adottata (es. la profilazione) deve essere effettivamente capace di raggiungere l'obiettivo legittimo perseguito (es. mostrare pubblicità pertinente).
2. *Necessità*: La misura adottata deve essere la meno limitante tra quelle disponibili, si deve valutare se è possibile ottenere lo stesso risultato economico trattando una quantità inferiore di dati. Se la risposta è affermativa, la profilazione massiva è da considerarsi illegittima in quanto non necessaria e dunque in violazione del principio di minimizzazione dei dati.
3. *Proporzionalità in senso stretto*: Il sacrificio arrecato al destinatario del trattamento deve essere adeguatamente proporzionato ai benefici ottenuti. Anche se una tecnica di profilazione fosse idonea e necessaria, essa diventerebbe illecita se il danno alla dignità o alla riservatezza dell'utente fosse intollerabile rispetto al vantaggio economico ottenuto dall'azienda¹⁸.

Come sottolineato dalla dottrina, il bilanciamento non è un processo statico, ma piuttosto dinamico: Il “punto di equilibrio” varia in base alla sensibilità dei dati gestiti e alla potenza della tecnologia utilizzata. Concludendo, l'articolo 41 Cost. legittima l'impresa basata sui dati, ma il principio di proporzionalità ne disegna i limiti: il profitto è tutelato fintanto che non trasforma l'essere umano da soggetto di diritto a mero oggetto di scambio, violando quel nucleo essenziale di dignità che nessun interesse economico può intaccare.

¹⁸ A. MORRONE, *Il bilanciamento nello Stato costituzionale*, Torino, 2014, 69.

1.4 Il profiling: definizione legale e tecnologica

Nel contesto della tensione tra libertà economica e tutela della persona fin qui descritta, la profilazione (*profiling*) rappresenta lo strumento tecnico-operativo attraverso il quale si realizza il modello di business della *data-driven economy*. Se i dati sono la materia prima, la profilazione è il processo di raffinazione che trasforma informazioni grezze in valore economico. Sotto un profilo strettamente tecnologico, la profilazione non è un'attività statica di mera raccolta, bensì un processo dinamico e inferenziale. Essa è basata sull'utilizzo di tecniche di *big data analytics* e *machine learning* che permettono di correlare grandi quantità di dati eterogenei (dati anagrafici, cronologia di navigazione, acquisti, geolocalizzazione, "mi piace" sui social network) per individuare *pattern* (modelli) ricorrenti¹⁹. L'obiettivo non è più limitato a descrivere l'identità dell'utente, ma è arrivare alla costruzione di un vero e proprio "gemello digitale" (*digital twin*), con lo scopo di poterne prevedere le scelte.

Con questo nuovo approccio si passa da una profilazione puramente descrittiva, incentrata su chi l'utente è nel presente, a una profilazione predittiva, orientata a ciò che farà in futuro, nella quale gli algoritmi, diversamente dai modelli tradizionali comunemente basati su categorie rigide, elaborano *cluster comportamentali dinamici* fondati su correlazioni statistiche spesso difficilmente percepibili.

¹⁹ Sul funzionamento tecnico dei Big Data e le implicazioni giuridiche, V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, 130-134 e 233-237.

Questi algoritmi sono in grado di dedurre informazioni che l'utente non ha mai fornito esplicitamente, come l'orientamento politico, lo stato di salute o la propensione al rischio²⁰.

La diffusione di questa tecnica ha reso indispensabile una definizione giuridica precisa, stabilita dal legislatore europeo per definire chiaramente i suoi limiti. Il Regolamento (UE) 2016/679 (GDPR) definisce la profilazione all'articolo 4, punto 4, come:

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

Dalla lettura della norma spiccano tre elementi costitutivi che devono coesistere affinché si possa parlare giuridicamente di profilazione²¹:

1. Modalità di trattamento: Il trattamento deve essere svolto, almeno in parte, attraverso l'ausilio di mezzi informatici (es. algoritmi).
2. L'oggetto del trattamento: Il trattamento deve riguardare dati personali riferibili a una persona identificata o identificabile.
3. La finalità del trattamento: L'attività deve essere finalizzata a "valutare" delle caratteristiche attuali o "prevedere" dei comportamenti futuri.

²⁰ G. NOTO LA DIEGA, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies*, Londra/New York, 2022, 251-258.

²¹ *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da G. FINOCCHIARO, Bologna, 2017, commento all'art. 4 (a cura di Caterina Del Federico e Anna Rita Popoli), 95-100.

Le linee guida del *Gruppo di lavoro articolo 29* (ora EDPB) differenziano la profilazione dal semplice trattamento statistico, sottolineando che la prima ha un impatto diretto sull'individuo. La profilazione, infatti, è finalizzata alla formulazione di un giudizio sulla persona, che può comportare conseguenze giuridiche rilevanti nella sua vita, come l'esclusione da un'offerta o l'applicazione di un prezzo maggiorato²². Il marketing è l'ambito applicativo in cui la profilazione si dimostra più efficace, ma è anche dove si pongono i maggiori rischi per i diritti fondamentali. La libertà di iniziativa economica (art. 41 Cost.) spinge le imprese a massimizzare l'efficienza degli investimenti pubblicitari, abbandonando il vecchio modello "generalista" (es. spot televisivi uguali per tutti) in favore del *marketing comportamentale* (*behavioral advertising*). In questo contesto, la profilazione serve ad erogare la c.d. *targeted advertising* (pubblicità mirata). L'algoritmo, analizzando le tracce digitali dell'utente, è in grado di mostrare il messaggio giusto, alla persona giusta, nel momento di massima vulnerabilità o ricettività. Tuttavia, l'evoluzione tecnologica ha spostato il confine ben oltre la semplice "pertinenza" commerciale. Oggi si assiste a fenomeni di profilazione psicometrica, dove il marketing non fa leva solo sui bisogni del consumatore, ma sfrutta le sue fragilità emotive, i suoi bias cognitivi e anche i suoi stati d'animo transitori. È qui che il "profiling" può minacciare la dignità e l'autodeterminazione. Quando la profilazione diventa così sofisticata da aggirare la barriera critica dell'individuo, riuscendo ad orientare le sue scelte di consumo (o addirittura politiche) senza che questi ne sia consapevole, non si parla

²² Gruppo di Lavoro Articolo 29 (WP29), *Linee guida sul processo decisionale automatizzato e sulla profilazione ai fini del regolamento (UE) 2016/679*, adottate il 3 ottobre 2017 e approvate dall'EDPB.

più di legittima persuasione commerciale ma bensì di manipolazione occulta²³. A questo si aggiunge l'importante asimmetria informativa dovuta alla poca trasparenza degli algoritmi (c.d. *black box society*): l'impresa conosce tutto del consumatore, mentre il consumatore non ha la minima idea dei criteri e dei processi che hanno portato alla sua profilazione e categorizzazione²⁴. Anche questo rende più evidente la necessità di quel bilanciamento discusso in precedenza: la profilazione, pur essendo un'espressione legittima della libertà d'impresa, richiede correttivi e garanzie, come trasparenza, consenso e diritto di opposizione, per evitare che l'utente diventi un semplice input per algoritmi di calcolo.

²³ G. BUSIA, L. LIGUORI, P. ORESTE, *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 101-126.

²⁴ Sulla trasparenza degli algoritmi e il problema della "scatola nera", P. BENANTI, *Le macchine sapienti*, Bologna, 2018, 54 e 56-57.

Capitolo II - Il GDPR come strumento di bilanciamento: principi, liceità e tutele contro il profiling

2.1 Il GDPR in breve

La risposta normativa alle sfide derivanti dall'imporsi della *data-driven economy* e dai rischi della profilazione pervasiva, delineati nel capitolo precedente, è da individuarsi nel Regolamento UE 2016/679, noto come *General Data Protection Regulation* (GDPR). Il GDPR, entrato pienamente in vigore il 25 maggio 2018, non rappresenta una semplice evoluzione della precedente Direttiva 95/46/CE, ma rappresenta un cambiamento radicale nella governance dei dati personali all'interno dell'Unione Europea.

La scelta dello strumento giuridico del Regolamento, atto direttamente applicabile in tutti gli Stati membri senza necessità di recepimento nazionale, risponde a una precisa esigenza di uniformità. Il legislatore europeo si prefiggeva due obiettivi principali: da un lato, eliminare la frammentazione normativa che aveva caratterizzato i vent'anni precedenti, istituendo un vero e proprio mercato unico digitale con regole chiare per le aziende; dall'altro, volle assicurare un elevato e uniforme livello di tutela dei diritti fondamentali delle persone fisiche in tutta l'Unione²⁵. Il GDPR funge da strumento operativo incaricato di raggiungere il delicato equilibrio costituzionale tra la libera circolazione dei dati, essenziale per l'economia, e la tutela dei diritti fondamentali (funzionale alla dignità della persona), come specificato

²⁵ F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 30-31. L'autore evidenzia come il Regolamento sia lo strumento necessario per l'armonizzazione reale del mercato.

fin dal Considerando n. 4, ove si legge che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta», ma va considerato «alla luce della sua funzione sociale» ed equilibrato con altri diritti fondamentali²⁶.

L'architettura del GDPR non può esistere isolatamente, essa infatti affonda le sue radici nel costituzionalismo multilivello europeo. Il Regolamento è, in sostanza, la concretizzazione legislativa di principi sanciti ai più alti livelli dell'ordinamento sovranazionale e nazionale. Il punto di riferimento principale è la *Carta dei Diritti Fondamentali dell'Unione Europea* (c.d. Carta di Nizza), che ha assunto lo stesso valore giuridico dei Trattati con l'entrata in vigore del Trattato di Lisbona. La Carta opera una distinzione fondamentale, spesso trascurata, tra due diritti contigui ma autonomi:

- Articolo 7 (Rispetto della vita privata e familiare): Tutela la classica *privacy* intesa come riservatezza, ossia il diritto a non subire ingerenze nella propria sfera intima (corrispondente all'art. 8 della CEDU).
- Articolo 8 (Protezione dei dati di carattere personale): Istituisce un diritto moderno e proattivo, sancendo che i dati devono essere gestiti in modo responsabile “*secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo*”²⁷.

L'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea rappresenta il cuore del GDPR. Grazie a questo articolo, la protezione

²⁶ *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da G. FINOCCHIARO, Bologna, 2017, approfondimento sull'ambito di applicazione del Regolamento (a cura di Alessandra Spangaro), 23-27.

dei dati personali non è più un diritto passivo, come il semplice diritto alla privacy, ma diventa un diritto attivo, che consente a ciascun individuo di esercitare un reale controllo sulle proprie informazioni. Questo approccio si sposa alla perfezione con i principi costituzionali italiani. Come illustrato nel primo capitolo, l'articolo 2, interpretato alla luce della normativa europea, non si limita più alla tutela della riservatezza dei dati, ma promuove lo sviluppo della personalità umana nell'era digitale.

La Corte di Cassazione e la dottrina italiana hanno recepito questa visione integrata, affermando che il GDPR rappresenta la “costituzione” dell'individuo digitale, è quindi fondamentale tutelare la dignità dell'individuo, garantendo che non venga trattato come un semplice oggetto di analisi algoritmica, in linea con i valori costituzionali. Il quadro normativo descritto introduce un cambiamento radicale, superando definitivamente la concezione di *privacy* dell'Ottocento. Nell'economia dei dati, dove la condivisione delle informazioni è spesso inevitabile per accedere a servizi fondamentali o partecipare alla vita sociale, il diritto alla segretezza assoluta risulta superato e irrealizzabile.

Il GDPR recepisce il principio di *autodeterminazione informativa*, garantendo agli interessati il potere di conoscere e controllare le modalità di trattamento dei propri dati personali.

Questo principio venne teorizzato dalla dottrina tedesca e introdotto in Italia da giuristi accreditati come Stefano Rodotà e sostiene che la protezione dei dati non si ottenga nascondendoli, ma gestendoli. L'autodeterminazione informativa è il diritto di un individuo di monitorare la circolazione dei propri dati, esso è libero di decidere a chi

condividerli, per quali scopi, per quanto tempo e, soprattutto, mantenendo la facoltà di revocarne l'accesso²⁸.

Il Regolamento, quindi, trasforma questo concetto filosofico in istituti giuridici concreti. L'intero GDPR è concepito per restituire all'interessato (*data subject*) il controllo sulle proprie informazioni:

- Il *consenso* (art. 7) non si esprime più con una semplice firma, ma richiede una manifestazione di volontà libera e chiara;
- I *diritti dell'interessato* (accesso, rettifica, cancellazione, portabilità) sono gli strumenti attuativi di questo controllo continuo;
- Il *principio di responsabilizzazione (accountability)* richiede alle imprese non solo di rispettare le normative, ma anche di dimostrare attivamente di aver tutelato i dati come beni preziosi di terzi.

2.2 Articolo 6 GDPR: Liceità del trattamento

L'architettura del GDPR si fonda su un principio di liceità "chiuso": ogni trattamento di dati personali è intrinsecamente vietato, a meno che non intervenga una specifica norma a legittimarlo. L'articolo 6 del Regolamento assolve a questa funzione di "chiusura del sistema", individuando un elenco tassativo di condizioni, le c.d. basi giuridiche,

²⁸ S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014 21-26; L. CALIFANO, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *Federalismi.it*, n. 16, 2019, 2-5.

che rendono lecito ciò che altrimenti costituirebbe un'ingerenza indebita nella sfera giuridica dell'interessato²⁹.

Nel contesto specifico della profilazione a fini di marketing, le opzioni disponibili si riducono notevolmente. Escluse le basi giuridiche di natura pubblicistica o contrattuale (che mal si conciliano con l'attività promozionale pura), il dibattito dottrinale e giurisprudenziale si concentra principalmente attorno a due istituti contrapposti: il consenso dell'interessato (art. 6, par. 1, lett. a) e il legittimo interesse del titolare (art. 6, par. 1, lett. f). Questa dicotomia non è solo tecnica, ma rispecchia le due anime costituzionali in conflitto: il consenso è lo strumento di sovranità individuale (Art. 2 Cost.), mentre il legittimo interesse è il canale che permette l'esercizio della libertà d'impresa (Art. 41 Cost.).

La base giuridica d'elezione per le attività di profilazione, specialmente quando queste sono caratterizzate da un elevato grado di invasività (come il tracciamento comportamentale online), è il consenso. Il GDPR, all'articolo 4, par. 11, ha ridefinito profondamente questo istituto, trasformandolo da mera formalità burocratica ad atto di volontà *libero, specifico, informato e inequivocabile*. Si passa quindi da un modello di opt-out (silenzio-assenso) a un modello di opt-in stringente, in cui solo un'azione esplicita dell'utente può legittimare il trattamento dei dati³⁰. Perché il consenso possa legittimare la profilazione, deve soddisfare criteri di "qualità" estremamente rigorosi. In primo luogo, deve essere *granulare*: l'interessato deve avere la facoltà di acconsentire

²⁹ L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 133.

³⁰ *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da G. Finocchiaro, Bologna, 2017, definizione di consenso dell'interessato e suo inquadramento giuridico (a cura di Fabio Bravo), 142-157.

separatamente alle diverse finalità (es. distinguendo tra l'erogazione del servizio e la profilazione marketing), pena l'invalidità dell'intero trattamento. In secondo luogo, deve essere realmente libero: le linee guida dell'EDPB hanno stabilito che la pratica dei c.d. *cookie walls*, ovvero quei sistemi che bloccano l'accesso a un sito web se non si accetta il tracciamento, invalidano il consenso alla radice. Questa decisione è giustificata dal fatto che l'autorizzazione, che dovrebbe essere data liberamente e spontaneamente, verrebbe ottenuta sfruttando una posizione di squilibrio³¹. Il consenso, in questo contesto, si afferma come lo strumento fondamentale per l'autodeterminazione informativa: l'utente, infatti, accetta di rivelare le proprie preferenze in cambio di un servizio personalizzato, mantenendo però intatto il potere di revoca (art. 7, par. 3), che deve essere garantito con la stessa semplicità con cui è stato concesso inizialmente.

In alternativa al consenso, l'articolo 6, par. 1, lett. f) del GDPR offre una base giuridica più flessibile: il trattamento è lecito se “*necessario per il perseguimento del legittimo interesse del titolare del trattamento*” a patto che non prevalgano i diritti e le libertà fondamentali dell'interessato. Questa disposizione introduce un meccanismo di bilanciamento flessibile, in base al quale spetta al titolare del trattamento dimostrare la legittimità di alcune attività di marketing diretto svolte anche senza il previo consenso dell'interessato, come previsto dal Considerando 47 del Regolamento. Tuttavia, il ricorso a questa base giuridica non è automatico. Per utilizzarla, l'impresa deve effettuare una valutazione rigorosa (c.d. LIA - *Legitimate Interest Assessment*), verificando tre condizioni progressive: l'esistenza di un

³¹ European Data Protection Board (EDPB), *Linee guida 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, paragrafi 39-41.

interesse lecito, la stretta necessità del trattamento per perseguirlo, e l'assenza di un pregiudizio sproporzionato per l'utente³². Il discrimine fondamentale risiede nel concetto di ragionevole aspettativa (*reasonable expectation*): la profilazione basata sul legittimo interesse è consentita solo se l'utente, nel momento in cui avviene la raccolta dei dati, può ragionevolmente aspettarsi che questi vengano utilizzati per scopi commerciali (es. profilazione "leggera" sui propri clienti per offrire prodotti simili). Al contrario, quando la profilazione diventa occulta, pervasiva o trasversale (incrociando dati provenienti da fonti diverse o monitorando la navigazione su siti terzi), l'aspettativa di riservatezza dell'utente prevale sull'interesse economico dell'azienda. In questi casi, come stabilito dalla giurisprudenza della Corte di Giustizia (sentenza Planet49), il legittimo interesse perde rilevanza e il consenso diventa l'unica base giuridica valida per giustificare l'intrusione³³.

2.3 I diritti dell'interessato: la contromisura al profiling aggressivo

Nel disegno sistematico del GDPR, i diritti dell'interessato trascendono la mera dimensione procedurale per assumere la funzione di "scudi costituzionali". Se l'articolo 6 (basi giuridiche) legittima l'ingresso dell'impresa nella sfera giuridica dell'individuo, l'articolo 21 (diritto di opposizione) rappresenta il necessario contrappeso, ossia lo strumento che impedisce alla libertà economica (art. 41 Cost.) di diventare tirannia

³² F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, 22. L'autore sottolinea come il bilanciamento sposti il rischio giuridico sul titolare del trattamento.

³³ Corte di Giustizia dell'Unione Europea (Grande Sezione), sentenza 1° ottobre 2019, causa C-673/17, *Bundesverband der Verbraucherzentralen c. Planet49 GmbH*.

sui dati. L'articolo 21 disciplina il *right to object*, istituto che inverte la dinamica del potere tra titolare e interessato. La norma non è un concetto univoco, ma si divide in due categorie distinte che rispecchiano una chiara gerarchia di valori:

1. L'opposizione nel bilanciamento (par. 1): per i trattamenti basati sul legittimo interesse “generico” (ad esempio, la prevenzione delle frodi e la sicurezza delle reti), la normativa impone una verifica specifica. L'interessato deve dimostrare che la propria “situazione particolare” giustifica l'opposizione, ad esempio in presenza di una specifica condizione di vulnerabilità. In questo caso, il bilanciamento tra interessi resta aperto: il titolare del trattamento può prevalere solo se riesce a provare, con un elevato onere probatorio, l'esistenza di “motivi legittimi cogenti” in grado di prevalere sugli interessi, i diritti e le libertà dell'interessato. Si crea così una presunzione a favore della privacy, che spetta all'impresa dimostrare di aver effettivamente superato.
2. L'*opposizione alla profilazione di marketing* (par. 2): nel contesto del direct marketing, il legislatore europeo ha preso una decisione di valore fondamentale quando si tratta di profilazione, risolvendo il conflitto *ex ante* a favore della persona. In questo ambito, il diritto di opposizione diventa assoluto (*unconditional*). L'asimmetria è assoluta: l'utente non è tenuto a fornire spiegazioni e l'impresa non ha facoltà di replica. Nel caso in cui l'individuo esprima il suo dissenso (*stop profiling*), il trattamento

deve cessare immediatamente e i dati non devono più essere trattati per tale scopo (art. 21, par. 3)³⁴.

Costituzionalmente, questa disposizione tutela l'inviolabilità della sfera privata dalle logiche di profitto. Il diritto a “non essere profilati commercialmente” è un'estensione del diritto all'autodeterminazione sancito dall'articolo 2 della Costituzione. Questo diritto mira a garantire agli individui la possibilità di opporsi alla sorveglianza economica, impedendo che la loro identità venga scomposta e ricostruita in profili pubblicitari. La delega del giudizio alle macchine è una minaccia particolarmente rilevante che la data economy porta con sé. L'articolo 22 del GDPR, che garantisce il diritto a “*non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione*”, funge da norma di chiusura del sistema a tutela della persona. Questa disposizione non è un divieto assoluto alla tecnologia, ma piuttosto una garanzia costituzionale a tutela di tre principi essenziali:

A) La tutela della dignità contro la reificazione (Art. 2 Cost.)

La dignità umana, valore fondamentale del nostro ordinamento, impone che ogni persona sia considerata nella sua unicità e complessità. Per sua natura, la profilazione algoritmica agisce riducendo la realtà (riduzionismo) di conseguenza il “profilo” non è la persona ma una sua rappresentazione matematica parziale. Affidare a un automatismo decisioni fondamentali, come l'accesso al credito, le assunzioni o le cure mediche, significherebbe ridurre l'essere umano a un semplice oggetto, violando il nucleo essenziale dell'articolo 2 della Costituzione.

³⁴ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 31-34. L'autore evidenzia come il potere di opposizione sia l'ultimo scudo della sovranità individuale contro la mercificazione del dato.

L'articolo 22 del GDPR sancisce implicitamente un diritto al giudizio umano ("*right to human intervention*") secondo il quale ciascuno ha il diritto di essere valutato da un altro individuo, capace di comprendere quelle sfumature, contesti ed eccezioni che un algoritmo non può cogliere³⁵.

B) Il principio di uguaglianza sostanziale (Art. 3 Cost.)

Gli algoritmi di profilazione non possono essere considerati strumenti neutrali. Poiché vengono addestrati su dati storici che riflettono assetti sociali già segnati da disuguaglianze, essi finiscono spesso per riprodurre pregiudizi preesistenti, dando luogo al fenomeno del c.d. *bias algoritmico*. È il caso, ad esempio, di software impiegati nei processi di e-recruiting, che potrebbero penalizzare in modo sistematico le donne o le minoranze etniche sulla base di correlazioni tratte dal passato, configurando ipotesi di discriminazione indiretta. In questo contesto, l'articolo 22 assume una funzione di contenimento di tali scenari: introducendo il divieto delle decisioni esclusivamente automatizzate, il legislatore impone la reintroduzione di un controllo umano consapevole nel processo decisionale, indispensabile per individuare e correggere le distorsioni della macchina e per assicurare il rispetto di quell'uguaglianza sostanziale sancita dall'art. 3, comma 2, della Costituzione³⁶.

C) Il diritto alla difesa e alla spiegazione (Art. 24 Cost.)

³⁵ S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 315-327. L'autore evidenzia come la riduzione della persona a "traccia digitale" costituisca una delle più gravi minacce alla dignità umana nel XXI secolo.

³⁶ G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019, n. 7, 1670 ss.

Infine, la norma si salda con il diritto di difesa. Una decisione algoritmica "a scatola nera" (*black box*), in cui l'input porta a un output senza che si conosca il procedimento logico intermedio, è per definizione incontestabile. Se non so *perché* sono stato scartato, non posso difendermi. Per questo, l'articolo 22, letto in combinato disposto con i Considerando e gli artt. 13-15 GDPR, fonda un diritto alla spiegazione (*right to explanation*) secondo il quale, l'impresa deve essere in grado di fornire informazioni significative sulla "logica utilizzata" nella profilazione. La trasparenza dell'algoritmo diventa quindi una condizione fondamentale per l'esercizio del diritto di difesa costituzionalmente garantito³⁷. In sostanza, i diritti dell'interessato non sono semplici linee guida, ma i baluardi dello Stato di diritto nell'ecosistema digitale. Garantiscono che l'efficienza tecnologica non metta mai in ombra l'umanità del diritto.

³⁷ G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del Diritto*, n. 2, 2019, 199-236. L'autore argomenta che senza "explainability" non vi è *due process* (giusto processo).

Capitolo III – Il bilanciamento in concreto: decisioni dell'autorità garante

3.1 Natura e funzione dell'Autorità Garante

Per comprendere come il conflitto tra libertà economica e tutela della persona venga risolto nella pratica, è necessario analizzare il ruolo dell'istituzione a ciò preposta: il Garante per la protezione dei dati personali. Istituito dalla legge n. 675/1996 e oggi disciplinato dal Regolamento UE 2016/679 (artt. 51 e ss.) e dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003), il Garante appartiene alla categoria delle Autorità Amministrative Indipendenti. Questa qualificazione giuridica è fondamentale. A differenza degli organi governativi, il Garante opera in posizione di terzietà e autonomia rispetto al potere esecutivo (Governo) e agli interessi di parte. La sua missione non è politica, ma di garanzia costituzionale: esso agisce come un "corpo intermedio" incaricato di vigilare sull'effettivo rispetto di quei diritti fondamentali (dignità, riservatezza, identità personale) che abbiamo visto essere minacciati dalla *data economy*³⁸. Nel contesto della profilazione, il Garante svolge una funzione para-giurisdizionale, esso infatti rappresenta il "giudice naturale" del bilanciamento. È compito dell'Autorità, infatti, valutare caso per caso se un determinato trattamento di marketing, anche se puramente astratto, si basa sul legittimo interesse dell'impresa (art. 41 Cost.), superi o meno la soglia di tollerabilità imposta dal rispetto della persona (art. 2 Cost.). I poteri dell'Autorità sono stati notevolmente rafforzati dal GDPR, che l'ha

³⁸ Sulla natura e le funzioni delle Autorità Indipendenti, cfr. F. MERLONI, *Istituzioni di diritto amministrativo*, Torino, 2022, 125 ss.

trasformata da organo prevalentemente consultivo a vero e proprio regolatore del mercato, talvolta con poteri incisivi. L'articolo 58 del Regolamento attribuisce al Garante una serie di poteri che possono essere classificati in tre macro-aree, tutte funzionali a ripristinare l'equilibrio violato:

1. *Poteri di indagine*: Il Garante ha facoltà di accedere a qualsiasi locale dell'impresa, richiedere informazioni, effettuare ispezioni e audit sugli algoritmi utilizzati per la profilazione. Questo potere colma l'asimmetria informativa tra l'utente (che non sa come viene profilato) e l'azienda.
2. *Poteri correttivi*: L'Autorità ha il potere di limitare o addirittura vietare un trattamento, oltre a sanzionarlo, rendendola l'attore più importante per il bilanciamento. Infatti, se il Garante ritiene che una campagna di profilazione sia troppo invasiva, ha il potere di imporre un divieto provvisorio o definitivo al trattamento, terminando l'attività economica illegittima, facendo così prevalere la tutela della privacy sulla libertà d'impresa.
3. *Poteri sanzionatori*: Il GDPR cambia radicalmente il modo in cui le aziende valutano i rischi legati al trattamento dei dati. Esso ha introdotto sanzioni che possono arrivare a 20 milioni di euro o il 4% del fatturato globale. L'obiettivo non è solo punire chi non rispetta la normativa, ma rendere economicamente svantaggioso ignorare i diritti degli utenti, spingendo le imprese a rivedere le proprie strategie in chiave di conformità. Grazie a questa strategia sanzionatoria, il costo di violare i diritti degli interessati ricade sull'azienda stessa, rendendo l'inosservanza della legge un'opzione economicamente insensata e spingendo quindi le

aziende a perseguire il profitto rispettando le regole sulla protezione dei dati³⁹.

Per garantire il bilanciamento discusso nei precedenti capitoli, il Garante opera attraverso il principio di proporzionalità. Quando l'Autorità esamina un caso di profilazione (es. una carta fedeltà o un'app di tracciamento), non applica la norma in modo meccanico, ma effettua una ponderazione complessa:

- Valuta la necessità del trattamento rispetto allo scopo commerciale dichiarato.
- Verifica se l'impresa ha adottato misure di minimizzazione (usando meno dati possibile).
- Controlla se sono state applicate garanzie per la tutela dei diritti degli interessati (es. facilità di "opt-out").

Il Garante, con le sue decisioni, traccia il limite che l'iniziativa economica non deve superare, ad esempio, stabilendo che i dati di marketing non possono essere conservati per più di 24 mesi (salvo eccezioni). L'Autorità stabilisce un criterio che concilia l'interesse pubblicitario dell'azienda con la protezione del diritto all'oblio del consumatore. In sostanza, il Garante funge da ingegnere che regola i pesi sulla bilancia costituzionale, garantendo che il profitto non sovrasti mai la dignità umana.

³⁹ *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da G. Finocchiaro, Bologna, 2017, commento all'art. 83 (a cura di Matilde Ratti), 595-609. L'autrice sottolinea la funzione "general-preventiva" delle sanzioni amministrative nel nuovo sistema europeo.

3.2 La profilazione nel settore *retail*: il caso “Rinascente”

Il provvedimento n. 245 dell'8 giugno 2023⁴⁰, con cui il Garante ha sanzionato Rinascente S.p.A. per 300.000 euro, rappresenta un esempio paradigmatico di come la tutela del singolo possa evolvere in una correzione strutturale del mercato. Tutto nasce da un episodio che, almeno all'apparenza, sembrava trascurabile: una cliente ha segnalato che, dopo un battibecco in negozio, il suo profilo fedeltà era stato modificato senza che ne fosse a conoscenza, con la sostituzione del nome con un'espressione offensiva (“donzella svampita”). Questa violazione dell'integrità dei dati personali ha portato a un'indagine approfondita da parte del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT) della Guardia di Finanza.

Dall'indagine è risultato che il sistema di gestione dei dati, con cui avveniva la profilazione dei clienti, era caratterizzato da gravi carenze strutturali. Il fulcro giuridico della decisione è da individuarsi nel principio di limitazione della conservazione. (art. 5, par. 1, lett. e, GDPR). Rinascente conservava i dati degli acquisti dei clienti per un arco temporale ritenuto eccessivo dall'Autorità. Nello specifico, la società applicava una retention di 7 anni per i dati di marketing, giustificandola sulla base di prassi di altre aziende del settore lusso (come Bulgari o Ferragamo). A tal proposito, per comprendere la ratio della sanzione, è necessario richiamare il quadro normativo di riferimento utilizzato dall'Autorità per valutare la congruità dei tempi. Il Garante ha basato la sua valutazione sui principi del Provvedimento

⁴⁰ Garante per la protezione dei dati personali, provvedimento 8 giugno 2023, n. 245, *Ordinanza ingiunzione nei confronti di Rinascente S.p.A.* [doc. web n. 9909907].

generale del 24 febbraio 2005 sulle “Fidelity card”⁴¹. Pur essendo un provvedimento datato, questo rimane il punto di riferimento per valutare il rispetto del principio di proporzionalità nel settore retail. Stabilisce che i dati trattati per la profilazione possono essere conservati per un massimo di 12 mesi, mentre quelli per il marketing diretto possono essere conservati per un massimo di 24 mesi. Il garante ha sottolineato che secondo il GDPR e il principio di accountability è concesso al titolare di conservare i dati per un periodo differente da quello standard, solo con motivazioni concrete e documentate che Rinascente non è stata in grado di fornire. Il Garante ha escluso che si possano applicare gli stessi criteri dei marchi di lusso, chiarendo che il periodo di conservazione dei dati deve adattarsi alla natura dei prodotti. Nel caso di articoli acquistati frequentemente, come vestiti e cosmetici, mantenerne le informazioni per sette anni, ben oltre i normali 12-24 mesi, costituisce una forma di sorveglianza sproporzionata sulle abitudini dei consumatori. Differente il caso dei beni acquistati raramente, come gioielli o automobili di lusso, dove uno storico di lungo periodo può essere giustificato. Di conseguenza, l’Autorità ha ordinato la cancellazione o l’anonimizzazione dei dati più vecchi, riducendo significativamente la “memoria” dell’algoritmo.

Un altro punto critico sollevato dal provvedimento riguarda l’utilizzo di piattaforme terze, in particolare Facebook (Meta), per arricchire i dati. L’istruttoria ha infatti rivelato che Rinascente si serviva delle c.d. funzioni di Custom Audience (Pubblico personalizzato) caricando sulla piattaforma social gli indirizzi e-mail e i numeri di telefono dei propri

⁴¹ Garante per la protezione dei dati personali, provvedimento generale 24 febbraio 2005, “Fidelity card” e garanzie per i consumatori. *Le regole del Garante per i programmi di fidelizzazione* [doc. web n. 1103045].

clienti con il fine di bersagliarli con pubblicità mirata, senza, però, averli adeguatamente informati di questo specifico trattamento e senza una base giuridica idonea. Questa pratica viola il principio di trasparenza (artt. 12-13 GDPR): l'informativa resa ai clienti era generica e non esplicitava che i loro dati sarebbero stati incrociati con i database dei social network per finalità di profilazione incrociata (cross-platform profiling). Infine, il Garante ha sanzionato una carenza procedurale sostanziale: la mancata effettuazione della “valutazione d'impatto sulla protezione dei dati” (DPIA - art. 35 GDPR). Trattandosi di una profilazione sistematica su larga scala, che incrociava dati di acquisto, preferenze e comportamenti online, l'azienda avrebbe dovuto valutare preventivamente i rischi per i diritti e le libertà degli interessati.

Il provvedimento fissa paletti rigidi per il settore *retail*:

1. Stop alla conservazione indefinita: i tempi di conservazione devono essere proporzionati alla frequenza di acquisto media del settore specifico, non a standard generici.
2. Trasparenza sui "partner" tecnologici: se si usano i social per profilare (es. *Custom Audience*), l'utente deve saperlo ed esprimere un consenso specifico.
3. Sicurezza interna: I sistemi di CRM devono essere protetti da accessi o modifiche non autorizzate (come nel caso del cambio nome offensivo), garantendo l'integrità del dato contro ritorsioni o errori dei dipendenti.

3.3 La profilazione *social*: il caso “TikTok”

Un passaggio cruciale nella definizione dei confini giuridici della profilazione è rappresentato dalla vicenda che ha coinvolto TikTok

Technology Limited nel luglio 2022, culminata nel provvedimento di avvertimento n. 224 del Garante per la protezione dei dati personali. Il caso assume un rilievo sistematico poiché non riguarda una mera violazione operativa, bensì il tentativo di una Big Tech di ridefinire unilateralmente le regole del bilanciamento tra profitto e privacy, modificando la base giuridica del trattamento per finalità di marketing. La controversia ha avuto origine dalla comunicazione con cui la piattaforma annunciava una modifica della propria privacy policy, segnalando l'intenzione di abbandonare il consenso dell'interessato (art. 6, par. 1, lett. a, GDPR) come base legale per l'invio di pubblicità personalizzata, avvalendosi invece del legittimo interesse (art. 6, par. 1, lett. f, GDPR). L'azienda voleva eliminare il meccanismo di adesione volontaria (opt-in), pensando che il proprio interesse economico a vendere spazi pubblicitari, insieme all'aspettativa dell'utente di ricevere contenuti "pertinenti", potesse avere la meglio sul diritto alla privacy. Questa interpretazione è comune tra i giganti del web, i quali cercano di ampliare la definizione di legittimo interesse per superare la cosiddetta "fatica del consenso" (*consent fatigue*) e quindi massimizzare la raccolta dati. Questa pratica è stata spesso criticata dalla dottrina in quanto alimenta il rischio di svuotare di significato il principio di autodeterminazione informativa⁴² e proprio per questo l'Autorità Garante è intervenuta tempestivamente, bloccando il trattamento per prevenire un rischio concreto di lesione grave dei diritti degli iscritti. Il ragionamento giuridico sviluppato nel provvedimento

⁴² L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 118. Gli autori evidenziano come la flessibilità di tale istituto non debba tradursi in una elusione delle garanzie dell'interessato.

smonta la tesi dell'automatismo della profilazione basandosi su due argomentazioni dirimenti. In primo luogo, l'Autorità ha richiamato il rapporto di specialità tra la normativa ePrivacy e il GDPR. Indipendentemente dalla base giuridica astrattamente individuata per il trattamento dei dati, l'accesso alle informazioni archiviate sul dispositivo dell'utente (come i cookie o gli advertising ID, indispensabili per il tracciamento comportamentale) rimane soggetto alla disciplina dell'articolo 122 del Codice Privacy, che recepisce la Direttiva 2002/58/CE. Come chiarito anche dalle Linee Guida dell'EDPB, tale norma impone ineludibilmente il consenso preventivo e specifico per qualsiasi forma di archiviazione o accesso a informazioni non strettamente tecniche⁴³. Ne consegue che il legittimo interesse non può mai essere invocato per aggirare una norma speciale che richiede esplicitamente l'autorizzazione dell'utente, rendendo di fatto impraticabile la strategia ipotizzata da TikTok.

In secondo luogo, il Garante ha posto l'accento sulla tutela rafforzata dei soggetti vulnerabili, considerando che la piattaforma è frequentata prevalentemente da minori. L'applicazione del legittimo interesse richiede, ai sensi dell'articolo 6 GDPR, un test di bilanciamento (balancing test) tra gli interessi del titolare e i diritti dell'interessato. Nel caso di specie, tale bilanciamento non può che risolversi a favore dell'utente: non esiste, infatti, una ragionevole aspettativa da parte del minore di essere monitorato nelle sue interazioni intime e comportamentali per fini commerciali. La profilazione di minori basata

⁴³ Cfr. European Data Protection Board (EDPB), *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR*. Il documento chiarisce che il consenso richiesto dalla direttiva ePrivacy prevale sulle basi giuridiche alternative del GDPR per quanto concerne l'accesso al terminale dell'utente.

sul legittimo interesse esporrebbe questi ultimi a rischi di manipolazione occulta, sfruttando la loro minore consapevolezza delle dinamiche digitali e violando i principi costituzionali di protezione dell'infanzia e della gioventù (art. 31 Cost.)⁴⁴. L'intervento dell'Autorità ha così riaffermato l'imprescindibilità del consenso per la pubblicità comportamentale (*behavioral advertising*), costringendo la piattaforma a mantenere il modello basato sulla scelta libera e revocabile dell'utente.

⁴⁴ Garante per la protezione dei dati personali, provvedimento 7 luglio 2022, n. 224, *Avvertimento a TikTok Technology Limited* [doc. web n. 9788429].

Conclusioni

L'indagine condotta nel presente elaborato ha preso le mosse da un interrogativo giuridico fondamentale: in un'economia guidata dai dati (*data-driven economy*), in cui il profitto delle imprese dipende strutturalmente dalla capacità di profilare i consumatori, è ancora possibile garantire una tutela effettiva della dignità umana?

L'analisi dell'evoluzione normativa e giurisprudenziale permette di fornire una risposta affermativa, seppur condizionata. La libertà di iniziativa economica prevista dall'articolo 41 della Costituzione e i diritti inviolabili sanciti dall'articolo 2 non costituiscono mai un equilibrio stabile e si trovano infatti in una tensione continua che richiede un costante riequilibrio per garantire che l'una non prevalga a scapito dell'altra.

Tra i diritti più incisivi introdotti dal GDPR spiccano quello di opporsi al marketing, sancito dall'articolo 21, e il divieto di decisioni basate esclusivamente su processi automatizzati, previsto dall'articolo 22. Questi diritti rappresentano per l'individuo le "armi costituzionali" necessarie per non soccombere di fronte all'asimmetria di potere informativo delle grandi piattaforme. Tuttavia, l'esame del "diritto in azione" analizzato nel terzo capitolo, attraverso i casi Rinascente e TikTok, ha evidenziato le criticità applicative. La realtà mostra che molte aziende trattano ancora i dati personali come risorse senza padrone, accumulandoli senza limiti o aggirando le regole e che le sanzioni del Garante, pur consistenti sul piano economico, arrivano spesso a posteriori, quando la violazione è già diffusa e consolidata.

Alla luce di ciò, la normativa attuale, seppur necessaria, si rivela insufficiente. La sfida futura richiede un salto di qualità, come suggerito dal filosofo Luciano Floridi, che implica di ripensare l'ontologia stessa

della persona nell'era digitale. Viviamo ormai in una condizione di *Onlife*, dove la distinzione tra online e offline è venuta meno. In questo ecosistema, l'essere umano non è più solo un utente che "ha" dei dati, ma è un organismo informativo (*inforgh*) che è costituito dai suoi dati. La profilazione algoritmica non riguarda solamente beni materiali o esterni, ma agisce direttamente sulla struttura stessa dell'identità personale, influenzando percezioni, comportamenti e scelte dell'individuo⁴⁵. È perciò evidente che la tutela della privacy non si limita alla protezione dei dati, ma è una garanzia fondamentale della dignità umana, come sancito dall'articolo 2 della Costituzione. Nel mondo in cui ci troviamo, ogni informazione digitale può modellare decisioni e opportunità, e dunque manipolare i dati significa incidere sulla persona stessa, rendendo la privacy una condizione imprescindibile per preservare l'integrità e l'autonomia dell'individuo. Inoltre, l'avvento dell'intelligenza artificiale pone a rischio il principio di uguaglianza sostanziale (art. 3, co. 2 Cost.). Come osservato dalla dottrina costituzionalista, la "decisione robotica" rischia di cristallizzare le disuguaglianze sociali attraverso bias occulti, creando una "discriminazione algoritmica" che sfugge al controllo democratico⁴⁶. La delega di decisioni vitali alla macchina minaccia di ridurre l'essere umano a oggetto di calcolo, violando quel "diritto a una spiegazione" che è il presupposto del diritto di difesa (art. 24 Cost.)⁴⁷.

⁴⁵ L. FLORIDI, *La quarta rivoluzione*, Milano, 2017, 105. L'autore argomenta che la violazione della privacy nell'infosfera equivale a una violazione dell'integrità personale, non della proprietà privata.

⁴⁶ M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, n. 3, 2018, 882-883.

⁴⁷ A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019, 73.

L'approvazione del nuovo *AI Act* segna la naturale evoluzione del percorso iniziato con il GDPR, estendendo la protezione dei diritti individuali nell'era digitale. La tutela della persona non può più essere lasciata alla sola vigilanza dei singoli: serve un cambio di paradigma. Il principio di *accountability* deve trasformarsi in una vera e propria *Infraetica*, come la definisce Floridi, ovvero un'infrastruttura etica che sostenga le leggi, facendo sì che rispettare la dignità umana non sia un obbligo formale, ma la condizione fondamentale per operare legittimamente nell'infosfera. Solo così l'innovazione tecnologica potrà essere, come auspica la Costituzione, un fattore di progresso umano e non uno strumento di sorveglianza commerciale.

Bibliografia

Dottrina (monografie, saggi e articoli giuridici)

A. MORRONE, *Il bilanciamento nello Stato costituzionale*, Torino, 2014, 69.

A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019, 73.

A. SPANCARO, *Approfondimento sull'ambito di applicazione del Regolamento*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 23-27.

C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo, Rivista trimestrale Speciale/2019*, 101-130.

C. DEL FEDERICO – A. R. POPOLI, *Commento all'articolo 4*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 95-100.

E. LONGO, *La giustizia nell'era digitale*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica. Atti del Convegno Annuale dell'Associazione "Gruppo di Pisa" (Genova, 18-19 giugno 2021)*, Napoli, 2022, 5.

E. LONGO, *Predizione, profilazione e giustizia* in A. ADINOLFI, A. SIMONCINI, *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022, 581-608.

F. BRAVO, *Il “diritto” a trattare dati personali nello svolgimento dell’attività economica*, Padova, 2018, 22.

F. BRAVO, *definizione di consenso dell’interessato e suo inquadramento giuridico*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 142-157.

F. MERLONI, *Istituzioni di diritto amministrativo*, Torino, 2022, 125 ss.

F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 31-34.

F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 8-9 e 30-31.

G. BUSIA, L. LIGUORI, P. ORESTE, *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive*, Roma, 101-126.

G. FINOCCHIARO, *Diritto di internet* 4. ed, Bologna, 2023, 22-27.

G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019, 1670.

G. NOTO LA DIEGA, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies*, Londra/New York, 2022, 251-258.

G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del Diritto*, n. 2, 2019, 199-236.

G. VILLANACCI, *La ragionevolezza nella proporzionalità del diritto*, Torino, 2020, 90-92.

L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 118 e 133.

L. CALIFANO, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *Federalismi.it*, n. 16, 2019, 2-5.

L. FLORIDI, *La quarta rivoluzione*, Milano, 2017, 105.

M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, n. 3, 2018, 882-883.

M. RATTI, *Commento all'articolo 83*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 595-609.

P. BENANTI, *Le macchine sapienti*, Bologna, 2018, 54 e 56-57.

PRIVACY STUDIO, *Dati personali: la nuova valuta nell'economia digitale*, in *Privacy Studio*, 30 ottobre 2024, disponibile all'indirizzo: <https://www.privacystudio.it/dati-personali-la-nuova-valuta-nelleconomia-digitale/>.

R. BIN, G. PITRUZZELLA, *Diritto Pubblico*, Torino, 2023, 380-410.

S. D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, Project Gutenberg. 192-220.

S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 140-141 e 315-327.

S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, 21-26.

V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, 130-134 e 233-237.

W. PROSSER, *Privacy*, in *California Law Review*, Vol. 48, No. 3, 1960, 383-423.

Giurisprudenza Sovranazionale ed Estera

Corte di Giustizia dell'Unione Europea (Grande Sezione), sentenza 1° ottobre 2019, causa C-673/17, *Bundesverband der Verbraucherzentralen c. Planet49 GmbH*.

Supreme Court of the United States, 18 dicembre 1967, *Katz v. United States*, 389 U.S. 347.

Giurisprudenza Nazionale

Corte di Cassazione, Sez. I civ., sentenza 18 ottobre 1984, n. 5259.

Corte di Cassazione, Sez. I civ., sentenza 27 maggio 1975, n. 2129 (*Caso Soraya*).

Corte di Cassazione, Sez. I civ., sentenza 22 dicembre 1956, n. 4487 (*Caso Caruso*).

Provvedimenti dell'Autorità Garante per la protezione dei dati personali

Garante per la protezione dei dati personali, provvedimento 8 giugno 2023, n. 245, *Ordinanza ingiunzione nei confronti di Rinascente S.p.A.* [doc. web n. 9909907].

Garante per la protezione dei dati personali, provvedimento 7 luglio 2022, n. 224, *Avvertimento a TikTok Technology Limited* [doc. web n. 9788429].

Garante per la protezione dei dati personali, provvedimento generale 24 febbraio 2005, *“Fidelity card” e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione* [doc. web n. 1103045].