

ALMA MATER STUDIORUM · UNIVERSITÀ DI
BOLOGNA

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il management

Gli strumenti di profilazione nella società dell'informazione

Relatore:
Chiar.ma Prof.ssa
Matilde Ratti

Presentata da:
Gianluca Gueli
Matricola: 915130

Sessione III

Anno Accademico 2021/2022

"Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire."

Edward Snowden

Indice

Introduzione	4
1 Il diritto dell'infosfera della società dell'informazione	5
1.1 Excursus storico in materia di protezione dei dati personali . . .	5
1.2 GDPR: dato personale	9
1.3 I soggetti del trattamento	11
1.4 I principi applicabili al trattamento di dati personali	12
1.5 Informativa privacy e consenso dell'utente	15
2 Profilazione	18
2.1 Un caso specifico di trattamento dei dati personali	18
2.2 Questioni giuridiche ed economiche	22
2.3 Cookie: accetta tutto o rifiuta tutto?	28
2.4 Pubblicità personalizzata	33
3 Conformità al GDPR: Analisi di alcune informative privacy	39
3.1 Informativa privacy	39
3.2 Dati raccolti da Meta	42
3.3 Dati raccolti da Google	47
3.4 Come diminuire le proprie impronte digitali	51
Conclusioni	56
Bibliografia	57

Introduzione

La quantità di dati generati, copiati e consumati globalmente è in rapida crescita e ha raggiunto i 64,2 zettabyte nel 2020¹. Un zettabyte corrisponde a un bilione di terabyte (10^{21} byte) e si è stimato che un terabyte stampato in libri richiederebbe una pila da qui al sole per ben 5 volte. Una società che è, quindi, sempre più produttrice e consumatrice di dati di qualsiasi natura, arrivando a generare una media di circa 117 gigabyte di dati per ogni utente di internet². Molto più spesso di quanto si pensi, lasciamo impronte digitali quando compiano azioni comuni: effettuiamo un prelievo allo sportello Bancomat, leggiamo una notizia sul sito web della testata giornalistica preferita, richiediamo visite ed esami al servizio sanitario, paghiamo con il bancomat o con carte pregate. Tutte queste tracce, oltre a fornire informazioni sul soggetto che le compie, possono essere raccolte, ad esempio, per ricostruire la capacità di spesa di un soggetto o conoscere le sue preferenze³. Sempre più aspetti della società sono gestiti da sistemi informativi, come dimostrato dal fatto che uno dei tre assi strategici di Italia Domani, piano nazionale di ripresa e resilienza, è proprio la digitalizzazione e innovazione di processi digitali⁴. Anche il considerando 6 del GDPR evidenzia la rapida evoluzione tecnologica che da

¹ Total Data Volume Worldwide 2010-2025 in *Statistics*, su www.statista.com, consultato in data 24/10/2022

² Floria Grone, Pierre Péladeau and Rawia Abdel Samad, *Tomorrow's Data Heroes*, su <https://www.strategy-business.com/article/Tomorrows-Data-Heroes>, consultato in data 24/10/2022

³ Finocchiaro, *Diritto di internet*, Bologna, 2020, p. 54.

⁴ PNRR-Piano nazionale di ripresa e resilienza, p. 15.

un lato ha trasformato l'economia e le relazioni sociali e dall'altro ha portato all'utilizzo dei dati personali nello svolgimento delle loro attività. Questi dati spesso e volentieri sono raccolti e analizzati per “prevedere – e influenzare- modelli di comportamento, abitudini, interessi, propensioni”⁵. La nostra società è sempre più interconnessa al punto che difficilmente riusciamo a distinguere tra la vita online e quella offline: “onlife” è il termine coniato dal filosofo Luciano Floridi e inserito nel 2019 tra le voci della Treccani proprio per indicare questa nuova forma di comportamento. Il virtuale diventa reale grazie alle nuove tecnologie e le modalità di comunicazione, vivendo in un ambiente che è contemporaneamente analogico e digitale⁶. Il soggetto a cui i dati si riferiscono perde il controllo su di essi, mentre questi vengono raccolti e processati a costi nulli e, spesso, senza l'adeguato consenso⁷. È all'interno di questo contesto che nasce la regolamentazione per tutelare la vita privata delle persone ed evitare trattamenti dei dati non autorizzati, i quali possano avere anche un'influenza sulla capacità di scelta e determinazione dell'utente. In questo elaborato di tesi saranno trattati i problemi e rischi della profilazione, quale caso specifico di trattamento automatizzato dei dati personali, delineando un quadro normativo di riferimento. Verranno analizzate anche le informative privacy di alcune società dell'informazione per prendere coscienza di quali (e quanti) dati vengono condivisi durante l'utilizzo dei loro servizi gratuiti. Infine, verrà fornita una descrizione di quali possano essere gli strumenti software, le azioni da compiere per lasciare meno impronte digitali possibili.

⁵ Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation* in nuovi leggi civ., 2018, 1209 ss.

⁶ Giuliano, *Regolare l'infosfera*, Roma, 2021, p. 1.

⁷ Giuliano, *Regolare l'infosfera*, cit., p. 2.

Capitolo 1

Il diritto dell'infosfera della società dell'informazione

1.1 Excursus storico in materia di protezione dei dati personali

Il primo strumento giuridico che ha riconosciuto e imposto la protezione dei dati personali è la “Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale” firmata a Strasburgo il 28 gennaio 1981⁸. In questi anni iniziano a diffondersi i primi computer che con la loro nuova potenza di calcolo danno inizio alla gestione e collezione di grandi banche dati. Diventa possibile, non solo archiviare più dati, ma intrecciarli tra loro per ricavare maggiori informazioni. È questo il contesto nella quale nasce la Convenzione, che vuole garantire e assicurare il corretto trattamento dei dati personali a fronte delle aumentate possibilità di raccolta e incrocio dei dati⁹. Successivamente il 24 ottobre 1995 il Parlamento Europeo e del Consiglio ema-

⁸ Definita anche convenzione 108 del Consiglio d'Europa; nel 2018 il Consiglio ha modificato il testo per modernizzarla ed essere in linea con l'evoluzione tecnologica.

⁹ D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, Napoli, 2021, p. 46.

na la Direttiva 95/46/CE relativa alla Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati con oggetto “la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali”¹⁰. All’art. 15 *Decisioni individuali automatizzate* si riconosce a qualsiasi persona il diritto a non essere sottoposti “ad una decisione che produca effetti giuridici [...] fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della personalità, quali il rendimento professionale, il credito, l’affidabilità, il comportamento, ecc..”¹¹. Risale al 31 dicembre 1996, invece, la prima legge sulla tutela del trattamento dei dati personali. Si chiama legge sulla privacy e la sua finalità è quella di disciplinare la raccolta sui dati personali. L’esigenza di tutelare la privacy del consumatore nasce con l’inizio della raccolta di dati per realizzare profili di potenziali acquirenti a cui inviare offerte specifiche di prodotti o servizi. Di per sé la raccolta dei dati non viene vietata dalla legislatura, a patto che il soggetto interessato ne sia informato e si riconosca ad esso il diritto ad esercitare un controllo sui dati raccolti¹². Al fine di assicurare il diritto alla vita privata e alla riservatezza, “con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all’interno della Comunità”¹³ viene emanata la Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio il 12 luglio 2002. Il 1° gennaio 2004, invece, entra in vigore il Codice in materia di protezione dei dati personali, d. lgs 30 giugno 2003, n. 196 all’interno della legislatura italiana riguardo il tema privacy. Bisogna precisare che privacy e protezione dei dati personali non sono la stessa cosa, anche se i due aspetti sono connessi tra loro. Con il termine

¹⁰ Direttiva 95/46/CE.

¹¹ Art. 15 direttiva 95/46/CE.

¹² Finocchiaro, *Diritto di Internet*, cit, 113.

¹³ Direttiva 2002/58/CE.

“privacy” ci si riferisce solamente alla riservatezza, quale diritto ad essere lasciati soli¹⁴. I due concetti, inoltre, risultano essere molto importanti e infatti l’Unione Europea li ha riconosciuti come diritti fondamentali rispettivamente nell’art. 7 e nell’art. 8 della Carta dei diritti fondamentali dell’Unione europea¹⁵. Per quel che riguarda il diritto a non essere sottoposto a una valutazione unicamente automatizzata risiede dapprima nell’art. 17 della legge n. 675 del 31 dicembre 1996¹⁶ e poi nell’art. 14 del decreto legislativo n. 196 del 30 giugno 2003¹⁷. Arriva il 27 aprile 2016 una riforma fondamentale riguardo alla protezione dei dati personali da parte dell’Unione Europea attraverso il Regolamento n. 679/2016 (di seguito General Data Protection Regulation o “GDPR”) che abroga la direttiva 95/46/CE. L’obiettivo della disciplina è volta a garantire sia la libera circolazione dei dati personali sia la tutela dei dati dei soggetti interessati presenti sul territorio comunitario durante lo svolgimento di un’attività commerciale o professionale¹⁸. Il nuovo regolamento adotta un nuovo approccio, non più volto a individuare regole precise da seguire con la conseguente sanzione, ma piuttosto sul concetto di responsabilizzazione della modalità adottata per il trattamento, che sarà esaminata dall’autorità di con-

¹⁴ Fabiano, *GDPR & Privacy: Consapevolezza e Opportunità. Analisi Ragionata Della Protezione Dei Dati Personali Tra Etica e Cybersecurity: Prefazione Di Giovanni Buttarelli*, Firenze, 2019, p. 15.

¹⁵ L’art. 7 è sul rispetto della vita private e della vita familiare affermando che “ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. L’art.8, comma 1 è sulla protezione dei dati di carattere personale ed afferma che “ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano”

¹⁶ “Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su una trattamento automatizzato di dati personali volta a definire il profilo o la personalità dell’interessato”

¹⁷ Ibidem.

¹⁸ Cfr. Considerando n. 18 GDPR: “Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell’ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un’attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l’uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell’ambito di tali attività a carattere personale o domestico.”

trollo o dal giudice¹⁹. In questo modo l'onere di effettuare le valutazioni sulla gestione del rischio e avere una procedura per verificare l'efficacia delle misure di sicurezza spettano al titolare come previsto dall'art. 32 del GDPR²⁰. Secondo il principio di accountability, infatti, il titolare deve essere in grado sia di fornire le modalità d'esercizio di quanto dichiarato, sia di effettuare una verifica delle misure messe in pratica²¹. Spetta al titolare, dunque, fornire le prove che le misure adottate siano idonee a garantire la reale protezione dei dati personali e che siano in linea con lo scopo dichiarato, come indicato anche nell'art 24 del Regolamento²². L'Italia si adegua alle disposizioni del regolamento GDPR attraverso il decreto legislativo n. 101 del 10 agosto 2018. Vediamo, quindi, che il tema della protezione dei dati personali è disciplinato dal regolamento europeo 2016/679 e dal d. lgs 196/2003, quest'ultimo modificato dal d. lgs 101/2018. In particolare, l'art 22 del regolamento europeo 2016/679 riguardante il divieto di trattamenti automatizzati, estende il suo ambito di applicazione a tutti i casi in cui vi sia una decisione basata unicamente sul trattamento automatizzato a differenza dell'art. 14, comma 1 del decreto legislativo 30 giugno 2003²³ che applicava il divieto solamente ai settori amministrativi e giudiziari. Al fine di adeguarsi agli sviluppi tecnologici, in particolare ai servizi di comunicazione over-the-top ("OTT") , quali il voice-over-IP, la messaggistica istantanea e i servizi di posta elettronica basati sulla rete che non sono di norma soggetti alla direttiva 2002/58/CE, il Parlamento Europeo e del Consiglio ha proposto

¹⁹ Finocchiaro, *Gdpr tra novità e discontinuità- Il principio di accountability*, Giur. it., 2019, p. 12.

²⁰ Art. 32, comma 1, GDPR: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio [...]"

²¹ Finocchiaro , *Gdpr tra novità e discontinuità- Il principio di accountability*, cit., 4.

²² "[...] il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento"

²³ "Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato."

un regolamento (“ePrivacy”) relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE²⁴.

1.2 GDPR: dato personale

La definizione di dato personale è contenuta nell’art. 4, comma 1 del GDPR:

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dalla definizione emerge che è dato personale qualsiasi informazione riferibile direttamente o indirettamente ad un soggetto. Tutto ciò che in qualche modo permette di identificare una persona va considerato dato personale, indipendente dalla forma in cui è trattato o dal supporto su cui è archiviato. I dati personali, comunque, si riferiscono a informazioni di una persona fisica che ha la volontà di poterne disporre ed essendo elementi distintivi della personalità meritano di tutela²⁵. Al dato personale, però, è stato attribuito anche un valore economico. Infatti, sono sempre più i servizi digitali a “prezzo zero” per i quali il valore di scambio per l’impresa deriva dall’aggregazione dei dati personali degli utenti, che tramite algoritmi, permette di profilarli, raggruppandoli in categorie alle quali inviare offerte mirate e basate sui propri interessi

²⁴ COM(2017) 10 final, 2.

²⁵ Fabiano, *GDPR & Privacy: Consapevolezza e Opportunità. Analisi Ragionata Della Protezione Dei Dati Personali Tra Etica e Cybersecurity: Prefazione Di Giovanni Buttarelli*, cit, p. 26.

personali²⁶. La proposta di direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale²⁷ all'art.3, comma 1, viene stabilito come in cambio del servizio offerto il consumatore può offrire “attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato”²⁸. A tal proposito il Garante Europeo ha dichiarato il suo dissenso a monetizzare e assoggettare un diritto fondamentale ad una transazione economica²⁹. All'interno dei dati personali vi sono anche una categoria di dati relativi alla personalità etica-sociale dell'individuo, i cosiddetti “dati sensibili”. Il Codice in materia di protezione dei dati personali ha vietato il loro trattamento salvo i casi in cui, ad esempio, l'interessato ne abbia espresso il consenso esplicito per una finalità, sia necessario per tutelare un interesse vitale dell'interessato o il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato³⁰. Vi è, quindi, una attenzione particolare per i dati personali “che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona”³¹, in quanto il loro trattamento illecito provoca un danno maggiore alla persona. Sono esclusi dall'ambito di applicazione del regolamento i dati anonimi, ovvero tutti quei dati che non permettano di identificare in alcun modo una persona.

²⁶ Batteli, *I modelli negoziali di business degli operatori digitali a “prezzo zero” non sono “gratuiti”* in Contratti, 2022, p. 355 ss.

²⁷ COM(2015) 634.

²⁸ COM(2015) 634.

²⁹ Opinion 4/2017 Sulla proposta di Direttiva relativa a determinati aspetti dei contratti di Fornitura di contenuti digitali, p. 7.

³⁰ Finocchiaro, *Diritto Di Internet*, cit, p. 115.

³¹ Art. 9, comma 1, GDPR: “E’ vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.”

1.3 I soggetti del trattamento

Le figure principali che rivestono un ruolo importante all'interno del GDPR sono l'interessato, il titolare e il responsabile. L'interessato è la persona fisica, la persona giuridica, l'ente o l'associazione i cui dati sono oggetto di trattamento. Può esercitare una serie di diritti nei confronti del titolare del trattamento per tutelare i propri dati personali. In caso di lesione del diritto all'identità personale, l'interessato ha il diritto ad un risarcimento, come affermato dalla sentenza n. 12929 del 2007 della Corte di Cassazione. Il titolare è la persona giuridica, l'ente o l'associazione cui compete prendere la decisione della finalità, della modalità del trattamento e di quali strumenti adottare per garantire la sicurezza dei dati personali. Nella definizione di "titolare del trattamento" riportata nell'art. 4 comma 7 del GDPR, si precisa che più soggetti possano essere titolari di quel determinato trattamento. In questo caso si parla di contitolarità e il Real-Time Bidding ne è un esempio. In tale sistema di pubblicità online sono tre i protagonisti che intervengono nel processo: l'editore, colui che ospita l'inserzione in spazi appositi all'interno della propria pagina web o APP; l'inserzionista, colui che offre gli annunci pubblicitari e le agenzie pubblicitarie ("Advertasing network"). Queste ultime sono ad esempio Google Ads o Amazon che hanno come compito principale e non affatto secondario, quello di decidere quali annunci far visualizzare all'utente in base a suoi interessi e quindi alla profilazione effettuata tramite diversi meccanismi, quali ad esempio i marcatori ("cookie")³². Il titolare ha la libertà di scegliere sul come e quale tipo di trattamento realizzare concretamente, ma allo stesso tempo è responsabile delle scelte effettuate, che saranno poste al vaglio ex post del giudice o del Garante³³. Quando si effettua una qualsiasi operazione per conto del titolare

³² D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., pp. 141 e ss.

³³ Finocchiaro, *Gdpr tra novità e discontinuità - il principio di accountability*, cit, p. 8.

del trattamento si è “responsabili del trattamento”³⁴. Affinché ciò possa avvenire nel rispetto della legge, deve avere luogo un atto di designazione di uno o più soggetti competenti in grado di garantire il rispetto delle disposizioni in materia di trattamento di dati personali e deve esserci un’esigenza organizzativa da soddisfare. La delegazione è redatta in forma scritta e deve contenere le istruzioni del titolare circa il trattamento dei dati. Qualora il soggetto sia esterno alla struttura il flusso di dati che intercorre tra esso ed il titolare viene definito diffusione³⁵.

1.4 I principi applicabili al trattamento di dati personali

Quando si effettuano operazioni sui dati personali bisogna farlo rispettando precise modalità di raccolta ed elaborazioni nonché garantire specifici requisiti dei dati. L’art. 5 del Regolamento 679/2016 (rubricato proprio “Principi applicabili al trattamento dei dati personali”) elenca i seguenti principi: la “liceità, correttezza e trasparenza”, la “limitazione della finalità”, la “minimizzazione dei dati”, l’“esattezza”, la “limitazione della conservazione”, l’“integrità e riservatezza”, la “responsabilizzazione”. Per liceità si intende quando è conforme alla legge e in particolare quando è conforme al Codice stesso. Il trattamento, inoltre, deve essere conforme al principio di buona fede (principio di correttezza) ed essere impostato fin dalla fase iniziale di raccolta dei dati in modo trasparente rispetto agli scopi inseguiti.³⁶ Le finalità del trattamento devono essere determinate, legittime e rese note attraverso l’informativa per permettere all’interessato di esercitare i diritti previsti (cancellazione, rettifica o integrazione) e manifestare

³⁴ Art. 4, comma 8, GDPR.

³⁵ Finocchiaro, *Diritto di Internet*, cit, p. 117.

³⁶ Finocchiaro, *Diritto di Internet*, cit, p. 123.

un consenso libero ed informato, ove previsto³⁷. Per valutare, quindi, che il trattamento sia lecito occorre determinare in modo chiaro e preciso le finalità del trattamento. Il trattamento dovrà essere adeguato alle finalità attuate tenendo in considerazione il contesto, i soggetti coinvolti e se vi è la possibilità di applicare misure meno invasive per il raggiungimento dello stesso scopo, considerando gli interessi di entrambe le parti³⁸. Per minimizzazione dei dati si intende che i dati personali raccolti debbano essere solamente quelli strettamente necessari alla finalità stabilita e ed essere cancellati o anonimizzati una volta raggiunto lo scopo (limitazione della conservazione). Tale principio però entra in contrasto con le tecniche di big data analytics e machine learning che richiedono un'ingente massa di dati da processare per essere il più precise possibili³⁹. Per il principio di esattezza, l'interessato deve essere messo nelle condizioni di poter richiedere l'aggiornamento e la rettifica dei propri dati al fine di ottenere una rappresentazione fedele circa l'identità della persona. Un aspetto alquanto rilevante per il trattamento riguarda le modalità di conservazione dei dati personali: bisogna garantire la protezione tramite misure tecniche, evitarne la perdita (anche dovuta da danni accidentali) e la distruzione. La violazione dei dati personali (data breach) che comporta, accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati, deve essere comunicata dal titolare del trattamento senza ingiustificato ritardo entro 72 ore dal momento in cui è avvenuto a conoscenza del fatto⁴⁰. Un altro principio di rilievo e di ampia discussione, anche se non espressamente dichiarato nel GDPR, è quello di explicability, soprattutto a fronte di decisioni automatiche. Secondo tale principio l'interessato ha il diritto di comprendere com'è avvenuto il processo di decisione che ha portato a quella

³⁷ Finocchiaro, *Diritto di Internet*, cit, p. 124.

³⁸ Finocchiaro, *Diritto Di Internet*, cit, p. 125.

³⁹ Proietti, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, *Contratto e Impr.*, 2022, p. 5.

⁴⁰ Garante privacy, *Data Breach - Violazioni di dati personali* su <https://www.garanteprivacy.it/data-breach>, consultato in data 22/10/2022.

determinata scelta, stabilendone i criteri utilizzati e le ragioni⁴¹. Infatti, si ha il diritto di contestare la decisione basata unicamente su un trattamento automatizzato, compresa la profilazione e di esprimere la propria opinione, come stabilito dall'art. 22, par. 3 del Regolamento⁴². Per cui il titolare dovrà mettere l'interessato nelle condizioni di comprendere la logica del funzionamento dell'algoritmo di profilazione e su quali criteri di scelta si basa⁴³. Tali diritti sono fondamentali qualora si verificano degli errori decisionali che portano a previsioni errate che arrecano danni all'interessato: bisogna tenere a mente che tale tecniche di previsioni si basano su procedure statistiche e per loro natura hanno un fattore intrinseco di aleatorietà⁴⁴. A tal proposito il considerando 71 del GDPR mette in luce come sia opportuno utilizzare delle tecniche matematiche o statistiche appropriate per la profilazione che minimizzino l'errore impedendo allo stesso tempo effetti discriminatori degli interessati "sulla base della razza o dell'origini etiche, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale"⁴⁵. Per il Gruppo di lavoro ex art. 29 il principio di trasparenza comporta che «(...) l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano. (...)». Inoltre, il Gruppo afferma anche che bisogna dichiarare in modo chiaro e preciso, con un linguaggio non ambiguo, quali saranno gli effetti sull'interessato tramite l'informativa privacy.

⁴¹ Proietti, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, Contratto e Impr., 2022, p. 880 ss.

⁴² "Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione."

⁴³ D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 80.

⁴⁴ Ibidem.

⁴⁵ Considerando n. 71 GDPR.

1.5 Informativa privacy e consenso dell'utente

L'informativa privacy è lo strumento attraverso il quale l'interessato vede garantito il suo diritto alla protezione dei dati personali. Qualunque soggetto che tratti dati personali deve fornire l'informativa prima di procedere al trattamento o alla prima comunicazione dei dati⁴⁶. L'art. 13 del Regolamento definisce quali informazioni fornire all'interessato nel caso in cui conferisca i propri i dati personali: gli estremi identificativi del titolare, le finalità del trattamento “nonché la base giuridica”⁴⁷, i legittimi interessi perseguiti, eventuali destinatari dei dati personali, l'intenzione di trasferimento dati a un paese terzo, il periodo di conservazione dei dati, i diritti dell'interessato, quali la rettifica, cancellazione dei dati trattarsi, l'opposizione al trattamento e la portabilità dei dati, la obbligatorietà o meno del conferimento dei dati e le conseguenze di un eventuale rifiuto e l'esistenza di un processo decisionale automatizzato. Le pubbliche amministrazioni non devono richiedere l'informativa qualora una norma vigente ne richiedesse il trattamento di dati sensibili poiché il presupposto di legittimità è dato dalla norma di legge. Il consenso non va richiesto all'interessato se vi sia un obbligo di legge, si debba eseguire un contratto tra le parti interessate, si trattino dati anonimi per finalità di ricerca scientifica o statistica, si svolga un'attività professionale giornalistica, quando vi è la necessità di salvaguardare la vita della persona poiché impossibilitato nel prestare il consenso per incapacità di intendere e di volere o quando si effettua un'indagine investigativa per ottenere delle prove⁴⁸. Il consenso, quando necessario, comunque, deve essere libero, specifico, informato⁴⁹ conferito in modo inequivocabile. Qualora il soggetto si senta obbligato ad acconsentire o avrà effetti

⁴⁶ Finocchiaro, *Diritto Di Internet*, cit, p. 45.

⁴⁷ Art. 13, comma 1,c.

⁴⁸ Art. 6, comma 1.

⁴⁹ Art. 4, comma 11, GDPR: "Qualsiasi manifestazione di volontà dell'interessato, data liberamente, specifica, informata e inequivocabile con la quale l'interessato, con una dichiarazione o con un chiaro atto affermativo, esprime consenso al trattamento di dati personali che lo riguardano".

negativi in caso di non accettazione, il consenso non sarà ritenuto libero e quindi valido⁵⁰. In linea generale qualsiasi elemento di pressione o influenza che possa impedire “all’interessato di esercitare il proprio libero arbitrio, rende nullo il consenso”⁵¹. Quando un titolare del trattamento richiede di trattare dati personali non strettamente necessari durante l’esecuzione di un contratto, il contratto non è la base giuridica appropriata, quindi “le due basi legittime per il trattamento legittimo di dati personali, ovvero il consenso e il contratto, non possono essere fuse e sfumate”⁵². All’interessato che decide di opporsi al trattamento dei dati personali, deve essere garantita la stessa qualità di servizio offerto di colui che invece ha accettato il trattamento. Prima di esprimere il proprio consenso l’interessato deve essere informativo, cioè deve venire a conoscenza dell’informativa privacy per decidere liberamente se acconsentire o meno al trattamento. Per tale motivo la richiesta di consenso deve essere espressa in forma comprensibile e facilmente accessibile con un linguaggio semplice e diretto⁵³. Tuttavia, l’onere di dimostrare che l’utente ha prestato il proprio consenso spetta al titolare del trattamento, per cui viene consigliato a quest’ultimo di progettare meccanismi per la richiesta di consenso in modo che siano comprensibili, non ambigui e accertarsi che l’interessato abbia manifestato il proprio consenso attraverso un’azione precisa⁵⁴. Lo scopo alla base del Regolamento è quello di permettere all’interessato di avere il controllo sulla circolazione delle proprie informazioni personali. L’interessato detiene il diritto di revoca del proprio consenso con la stessa facilità con la quale ha fornito il consenso. Tale revoca non può pregiudicare un abbassamento del livello di servizio né può comportare la richiesta di un corrispettivo da parte del titolare. Oggigiorno, navigando nel web, siamo invasi dalle richieste di consenso

⁵⁰ WP258 rev.01, 5

⁵¹ WP258 rev.01, 6.

⁵² WP258 rev.01, 8.

⁵³ WP258 rev.01, 14.

⁵⁴ WP258 rev.01, 17.

che richiedono un clic e/o swipe e ciò comporta un “affaticamento del clic”⁵⁵ da parte dell’utente con la conseguenza che sempre meno vengono lette per intero le informative sulla privacy ma accettate ugualmente pur di accedere alla pagina web. Una possibile soluzione a questo problema potrebbe essere quella di ottenere il consenso tramite le impostazioni del browser⁵⁶. In questo modo, qualora l’utente desideri non essere profilato, potrà bloccare *di default* tutte le richieste e cancellare automaticamente i dati di sessione alla chiusura del browser. Ad esempio, Firefox tramite la protezione antitracciamento avanzata “blocca molti elementi traccianti che seguono l’utente online per raccogliere informazioni sulle sue abitudini e sui suoi interessi di navigazione senza compromettere la funzionalità del sito”⁵⁷.

⁵⁵ WP258 rev.01, 17.

⁵⁶ WP258 rev.01, 17.

⁵⁷ Firefox, *La protezione antitracciamento avanzata in Firefox per desktop* su <https://support.mozilla.org/it/kb/protezione-antitracciamento-avanzata-firefox-desktop>, consultato in data 22/10/2022.

Capitolo 2

Profilazione

2.1 Un caso specifico di trattamento dei dati personali

Il Codice in materia di protezione dei dati personali definisce con il termine trattamento qualsiasi operazione effettuata sui dati, indipendente dal supporto sul quale sono salvati⁵⁸. Se il trattamento ha luogo in modo che i dati personali raccolti non permettano più di identificare l'interessato, senza avere delle informazioni aggiuntive, allora si parla di "psedonimizzazione"⁵⁹. Una forma particolare di trattamento è la cosiddetta profilazione, intesa come un trattamento automatizzato di dati personali che ha lo scopo di prevedere aspetti circa "il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spo-

⁵⁸ Art.4,comma 2, GDPR: "Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

⁵⁹ Art. 4, comma 5, GDPR: "Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate sepa ratamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"

stamenti di detta persona fisica”⁶⁰. Tramite la profilazione si é, quindi, in grado di creare categorie di individui per prevederne i comportamenti, le loro abitudini, le preferenze, le tendenze. L’utilizzo di tale forma di trattamento viene impiegata principalmente per due motivazioni: in primo luogo per migliorare e personalizzare il servizio offerto agli utenti aumentando il loro gradimento e interesse verso il servizio stesso. In secondo luogo, invece, per svolgere un’attività di marketing attraverso la pubblicità mirata. Questo modello di business è alla base delle piattaforme che offrono i loro servizi a “prezzo zero”, in quanto non si esegue una controprestazione di natura pecuniaria, ma si richiede il consenso al trattamento dei dati personali al fine di individuare il cliente giusto al momento giusto e al prezzo che il consumatore è disposto a pagare⁶¹. Dal momento che si tratta di un’attività commerciale, dove a fronte dell’utilizzo del servizio si trattano dati personali, si dovrà fare riferimento anche al diritto contrattuale, a quello del consumatore e a quello della concorrenza. L’applicabilità dei diritti che entrano in gioco non sono in competizione tra loro ma piuttosto, garantiscono una maggiore tutela al consumatore sotto diversi profili giuridici⁶². I dati personali sono diventati una risorsa più preziosa dell’olio⁶³ e non si limitano più ad essere una rappresentazione della persona ma sono il carburante di un’economia digitale "che fonda in internet la sua genesi"⁶⁴. Attraverso l’analisi delle abitudini di navigazione e acquisto sul web si possono conoscere i bisogni e le preferenze dei consumatori, offrendo loro offerte mirate e personalizzate. La quantità di dati prodotti e la loro aggregazione hanno acquistato valore per

⁶⁰ Art.4, comma 4, GDPR: "«profilazione»: 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 parti colare 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;"

⁶¹ IAB Europe, *Programmatic Trading white paper*, 2014, p. 3.

⁶² Batteli, *I modelli negoziali di business degli operatori digitali a “prezzo zero” non sono “gratuiti”*, cit., pp. 355 ss.

⁶³ *The world’s most valuable resource is no longer oil, but data*, The Economist, 2017.

⁶⁴ Leone, *Servizi digitali “zero price” e diritti dei consumatori*, in Dir. Industriale, 2022, pp. 233 ss.

via della loro successiva circolazione a fini commerciali nell'ecosistema digitale⁶⁵. Le imprese digitali che detengono la capacità di connettere "molti utenti commerciali con molti utenti finali"⁶⁶, che hanno un impatto significativo sul mercato interno e detengono una posizione consolidata e duratura nell'ambito delle proprie attività, sono definite "gatekeeper", come indicato nell'art.3 del regolamento EU 2022/1925⁶⁷. È presente una forte dipendenza sia da parte degli utenti finali che da quelli commerciali nell'utilizzo di tali servizi. Inoltre gli effetti di lock-in, l'integrazione verticale, la multilateralità dei servizi offerti possono compromettere la contendibilità e ridurre la scelta per gli utenti. Le caratteristiche precedentemente descritte conferiscono, quindi, una posizione di controllore dell'accesso a chi fornisce il servizio gratuito⁶⁸. Un altro modello di business, invece, è quello in cui avviene lo scambio diretto dei dati, dove si riconosce agli utenti il valore che le piattaforme attribuiscono ai dati personali "attraverso processi di patrimonializzazione consistenti in attività di profilazione ai fini di sfruttamento economico"⁶⁹. Vi è, quindi, l'idea di monetizzare il dato personale attraverso mezzi finanziari per averne un controllo e risarcire i proprietari dei dati personali per la loro perdita di privacy⁷⁰, dove a seguito della fornitura del dato personale, quindi, corrisponderebbe una somma di denaro. La monetizzazione del dato personale non è condivisa da tutti, infatti, trasformando il bene giuridico (dato personale) in mera merce di scambio, si alienerebbe un diritto di libertà. Se, infatti, si legittimasse la remunerazione del consenso al trattamento, "si rischierebbe la rifeudalizzazione dei rapporti sociali, ammettendo che per necessità si possa essere disposti a cedere, con i

⁶⁵ Leone, *Servizi digitali "zero price" e diritti dei consumatori*, cit., p. 233.

⁶⁶ Considerando 2, regolamento (EU) 2022/1925.

⁶⁷ Al fine di garantire che questi mercati siano equi e contendibili in tutta l'Europa, a vantaggio degli utenti commerciali e degli utenti finali è stato emanato il regolamento (EU) 2022/1925 (Digital markets act).

⁶⁸ Considerando n. 2, regolamento (EU) 2022/1925.

⁶⁹ Battelli, *I modelli negoziali di business degli operatori digitale a "prezzo zero" non sono gratuiti*, cit., p. 355 s.

⁷⁰ Li, Miklau, Suciu, *A Theory of Pricing Private Data*, Digital Library, 27 Novembre 2017.

dati, la propria libertà”⁷¹. Anche l’European Data Protection Board (Edpd) non considera i dati personali come un bene commerciale, infatti ha affermato che “il denaro può essere contato, il che significa che è possibile confrontare i prezzi in un mercato concorrenziale e di norma i pagamenti in denaro possono essere effettuati soltanto con la partecipazione dell’interessato. Inoltre i dati personali possono essere sfruttati da più servizi contemporaneamente. Una volta perduto il controllo sui propri dati personali, non è detto che tale controllo possa essere ripristinato”⁷². Comunque la profilazione non è solamente legata all’attività di marketing anche se il loro rapporto è sempre più stretto e connesso⁷³. Ad esempio, è utilizzata anche all’interno della pubblica amministrazione per valutare quanto un intervento politico sia stato efficace, per allocare le risorse in maniera efficiente in base alle esigenze dei cittadini⁷⁴. Quando suddividiamo solamente il bacino di utenza dei clienti in cluster si sta svolgendo un’attività di pura classificazione: pensiamo alle tariffe agevolate dei mezzi pubblici per determinate categorie di utenti, oppure ad un negozio di abbigliamento che suddivide i capi in categorie (casual, elegante ec. . .). Per evidenziare la differenza tra una mera classificazione e una forma di profilazione prendiamo come esempio un sistema di videosorveglianza che controlla gli accessi in una zona a traffico limitato: se tale sistema si pone solamente l’obiettivo di individuare le automobili non autorizzate e provvedere, in caso, ad una sanzione amministrativa, saremo di fronte al primo caso, se invece, il sistema è

⁷¹ Pasquale Stanzone, presidente dell’Autorità Garante Italiana, in un’intervista a CorCom

⁷² Linea guida 2/2019 sul trattamento di dati personali ai sensi dell’art. 6, par. 1, lett. b del Gdpr nel contesto della fornitura di servizi online agli interessati, adottate l’8 ottobre 2019, ha precisato che “considerando che la protezione dei dati è un diritto fondamentale garantito dall’articolo 8 della Carta dei diritti fondamentali, e che una delle finalità principali del Gdpr è quella di fornire agli interessati il controllo sulle informazioni che li riguardano, i dati personali non possono essere considerati un bene commerciabile. Anche se l’interessato può acconsentire al trattamento di dati personali, non può cedere i propri diritti fondamentali attraverso tale accordo»

⁷³ D’ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 20.

⁷⁴ D’ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 21.

arricchito con altri dati, come ad esempio lo stile di guida, la propensione del soggetto a parcheggiare in divieto di sosta, l'ostentamento a pagare le sanzioni, e tramite un algoritmo cerchiamo di prevedere la probabilità che il soggetto compia un'altra infrazione, saremo di fronte ad un caso di profilazione. Lo scopo della profilazione è quindi quello di prevedere determinati accadimenti, basandosi sulle abitudini e comportamenti passati che magari sono stati ripetuti nel tempo.

2.2 Questioni giuridiche ed economiche

La raccolta dei dati online riveste un ruolo importante perchè si ha la facoltà di desumere informazioni utili o utilizzabili per scopi commerciali, sociali, politici⁷⁵. Ad esempio, si possono predire *trend* di consumo e di comportamento e addirittura anticiparne i bisogni, conoscendo in modo preciso i singoli interessi dei consumatori. L'utilizzo di algoritmi predittivi comporta un vantaggio sia per l'utente finale, a cui viene offerto un bene o servizio di suo interesse, sia per l'impresa che conoscendo meglio il proprio bacino di utenza otterrà maggiori margini di profitto⁷⁶. Dall'osservazioni delle scelte del consumatore si possono risalire alle preferenze che le hanno prodotte, quindi da un numero sufficiente di osservazioni si può stimare la funzione di utilità relativa alle scelte osservate⁷⁷. Quando si propongono ai consumatori prezzi diversi o leggermente diversi per l'acquisto dello stesso bene, basando la scelta del prezzo sulle caratteristiche conosciute o desunte del consumatore, si tratta di una discriminazione del prezzo⁷⁸. Esistono tre gradi di discriminazione del prezzo: quella di terzo grado si verifica quando il prezzo del servizio offerto varia in base alla categoria

⁷⁵ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 23

⁷⁶ D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 26.

⁷⁷ Hal R. Varian, *Microeconomia*, Settima edizione italiana, Cafoscarina, p. 80.

⁷⁸ D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 27.

del consumatore; quella di secondo grado, invece, si ha quando il prezzo è in relazione alla qualità o alla quantità: ad esempio, il posto in prima classe ha un costo più elevato rispetto ad uno in classe *economy*; quella di terzo grado, infine, è quella in cui viene fissato il prezzo per il bene o servizio uguale alla disponibilità a pagare del consumatore. La conoscenza del prezzo al quale il consumatore è disposto a spendere per quel bene o servizio viene definito *prezzo di riserva* e in una discriminazione di primo grado si preclude al consumatore la possibilità di risparmio⁷⁹. Ad esempio, Booking, un sistema online per la prenotazione di alloggi, tramite l'utilizzo di cookie, fingerprint o il login all'applicazione stessa, utilizza un algoritmo che permette all'utente di trovare un alloggio in maniera rapida ad un prezzo, però, leggermente più elevato e all'albergatore di avere, con un'alta probabilità, tutte le stanze occupate, in cambio dei costi di commissione⁸⁰. Booking, così come anche Amazon, sono delle piattaforme che operano in mercati a due versanti, ossia detengono un ruolo da intermediario fra agenti economici che operano in mercati tra loro distinti ma che entrano in comunicazione tramite la piattaforma⁸¹. È quest'ultima, quindi, che intervenendo in tutte le fasi della transizione, ottiene i profitti e i vantaggi migliori perchè detiene tutte le informazioni necessarie per far incontrare domanda e offerta. Invece, chi non utilizza la piattaforma rischia d'essere tagliato fuori dal settore, mentre chi la utilizza non ha il potere di decidere il prezzo di scambio⁸². Inoltre, la piattaforma che "ha più utenti dispone di più dati per migliorare il proprio servizio, attirando a sua volta ancora più utenti e determinando così effetti di rete diretti, che si traducono in barriere all'uscita per gli utenti e in un più difficile ingresso per nuovi operatori"⁸³. Un'altra carat-

⁷⁹ D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., pp. 28 ss.

⁸⁰ D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 30.

⁸¹ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 72

⁸² D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 30.

⁸³ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 72

teristica dei mercati nel settore digitale è la presenza di significative economie di scala e di scopo, dove a fronte un elevato costo iniziale irrecuperabile (c.d. "sunk cost") vi sono dei costi variabili irrisori. Tutto ciò rappresenta anche una forte barriera all'entrata con la conseguenza che vi saranno una ristretta cerchia di fornitori di tali servizi. Il fenomeno di lock-in, che si manifesta, conferisce un significativo vantaggio competitivo a coloro i quali, per primi, sono entrati nel mercato (*first mover*) ed esclude tutti gli altri ⁸⁴. Un altro rischio legato all'attività di profilazione si ha quando i dati usati in fase di addestramento esprimono o riflettono un pregiudizio, sono inesatti, scorretti o contengono delle distorsioni ("*bias*"), con la conseguenza di ottenere delle forme di discriminazione⁸⁵. "Garbage in garbage out" è un'espressione che indica come una qualità scadente dei dati in ingresso abbia conseguenze dirette sulla previsione dell'algoritmo, il cui errore diventa sistematico. Infatti, i sistemi di intelligenza artificiale sono come delle scatole nere (c.d. "*black box*") in quanto "mappano le caratteristiche di un utente in una classe o in un punteggio senza rivelarne le ragioni"⁸⁶. Ad esempio, nel 2015 Google Photos, app di Google per la raccolta delle foto, aveva classificato una persona di colore come un gorilla e per questo motivo, Google ha deciso di rimuovere il termine dalla ricerca dei tag delle immagini⁸⁷. Un altro esempio è quello di ProPublica, "una redazione indipendente e senza scopo di lucro che produce giornalismo investigativo con forza morale"⁸⁸, che ha trovato un pregiudizio razziale negli algoritmi utilizzati dai tribunali e dalle commissioni di libertà vigilata per prevederne il futuro comportamento criminale. In particolare, l'inchiesta ha rilevato che l'algoritmo

⁸⁴ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 73

⁸⁵ Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, cit., p. 3.

⁸⁶ Pedreschi, *Meaningful Explanations of Black Box AI Decision Systems*, Proceedings of the AAAI Conference on Artificial Intelligence, 2019.

⁸⁷ The guardian, *Google's solution to accidental algorithmic racism: ban gorillas* su <https://www.theguardian.com/technology/>, consultato in data 28/10/2022.

⁸⁸ ProPublica, *About Us* su <https://www.propublica.org/about/>, consultato in data 28/10/2022.

aveva l'effetto di identificare le persone nere come futuri criminali più spesso rispetto alle controparti bianche⁸⁹. L'attività di profilazione si basa su una tecnica nota come *Knowledge Discovery in Databases* (KDD) che "fornisce risposte a domande che non sono state formulate"⁹⁰. Il processo della "catena del valore" dei dati inizia con l'acquisizione dei dati, di seguito, tramite tecniche di machine learning unsupervised, i dati raccolti vengono processati da algoritmi in grado di individuare correlazioni (regolarità) ed infine vengono creati dei modelli comportamentali, senza sapere a priori quale tipo di risultato aspettarsi⁹¹. Con un certo alto grado di probabilità, tali modelli riescono a predire il comportamento futuro analizzando schemi, tendenze, abitudini come l'acquisto di un prodotto, la non restituzione di un prestito, l'essere o meno in una determinata condizione medica. Infatti, "Facebook definisce chi siamo, Amazon cosa vogliamo, Google cosa pensiamo"⁹²: la nostra reputazione, che viene ricostruita interpretando le tracce che lasciamo in rete e sulla base di dati disponibili, "definisce il nostro orizzonte di opportunità"⁹³. Lo scopo principale delle grandi piattaforme (c.d. GAFA(M) - Google, Apple, Facebook, Amazon e Microsoft⁹⁴) è quello di catturare il più possibile l'attenzione del consumatore. Una volta conquistata, cercano di far compiere all'utente il maggior numero di azioni (*scroll, like, search ecc...*) e conservare quanti più dati possibili. In questo modo conoscono quali contenuti sono di forte impatto emotivo e quali

⁸⁹ Angwin e Larson, *Bias in Criminal Risk Scores Is Mathematically Inevitable*, *Researchers Say*, su <https://www.propublica.org/article/>, consultato in data 28/10/2022.

⁹⁰ Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, cit., p. 4.

⁹¹ Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, cit., p. 4.

⁹² Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, cit., p. 2.

⁹³ Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, cit., p. 2.

⁹⁴ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 29.

possono maggiormente attirare l'attenzione dell'utente. Inoltre, i nuovi contenuti mostrati sono fortemente collegati all'attività online, generando fenomeni come *filter bubble*⁹⁵ e *self-confirmation bias*⁹⁶, nei quali "l'utente con le proprie scelte, rivela le informazioni che lo interessano e, a sua volta, la selezione delle informazioni operata dall'algoritmo influenza le scelte dell'utente, confermandone la visione pregressa del mondo"⁹⁷. Si vengono a creare, in questo modo, dei fattori di polarizzazione, quali il pensiero di gruppo (*groupthink*) e le "camere d'eco", che isolano gli ambienti di discussione e favoriscono la realizzazione di "strategie di microtargeting per campagne di disinformazione e malinformazione, aventi ad oggetto tematiche ad alto impatto politico, culturale o commerciale"⁹⁸. Tali conseguenze patologiche sono visibili all'interno dei *social network*, dove vengono a crearsi dei "cluster omogenei di 'amici' che condividono la stessa visione relativa ad argomenti sociali, politici e di attualità"⁹⁹. Le tecniche di profilazione, quindi, possono anche rimodellare le abitudini degli utenti verso scelte che non avrebbero intrapreso oltre che a predirne il comportamento. Un esempio noto è il caso di *cambridge analytica* che tramite i dati raccolti aveva tentato di influenzare le elezioni politiche americane del 2016¹⁰⁰. Oltre a ciò, gli algoritmi predittivi permettono di attribuire un punteggio agli utenti sottoposti a valutazione: il titolare del trattamento potrebbe escludere dall'offrire il servizio a qualcuno solamente perché non ha raggiunto la soglia minima. Il *social credit systems* è, infatti, un sistema di social scoring che attribuisce un punteggio ai singoli utenti in base alla loro condotta, caratteristiche

⁹⁵ Consiste nel personalizzare le ricerche effettuate in modo che siano in linea con i propri interessi, creando in questo modo una bolla culturale o ideologica. Il termine è stato coniato dall'attivista Eli Pariser nel suo libro *The Filter Bubble: What the Internet Is Hiding from You*.

⁹⁶ È la tendenza a ricercare, interpretare le informazioni in modo da confermarne la convinzione o credenza.

⁹⁷ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 33

⁹⁸ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 35

⁹⁹ AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 34

¹⁰⁰ Garante privacy, *Cambridge Analytica: il Garante privacy multa Facebook per 1 milione di euro* su <https://www.garanteprivacy.it/web/guest/home/docweb>, consultato in data 28/10/2022

e preferenze, creando uno schema sociale di vincitori e perdenti¹⁰¹. Dal 2020, in Cina, tale sistema é diventato obbligatorio ai fini di valutare l'affidabilità del cittadino, migliorarne la fiducia, promuovere una cultura di sincerità e di credibilità giudiziaria, come dichiarato dal Governo stesso¹⁰². L'ottenimento di un punteggio elevato comporta dei benefici ai vari servizi pubblici e privati, quali ad esempio, assicurazione o sistemi previdenziali, mentre preclude l'accesso agli stessi con un punteggio basso. Una rappresentazione distopica di tale sistema è rappresentata nell'episodio *Nosedive* della serie britannica *Black Mirror*, dove attraverso un applicazione dello smartphone ogni cittadino riceve ed esprime un giudizio per ogni aspetto della quotidianità¹⁰³. Se è vero che la conoscenza perfetta del cittadino permetta una migliore allocazione delle risorse o una più efficiente erogazione del servizio, come app di contract tracing per contrastare la diffusione del virus, è vero anche che tali sistemi possano risultare strumenti di sorveglianza se non implementati rispettando i principi alla base della protezione dei dati personali¹⁰⁴. I titolari del trattamento, però, non sono interessati a conoscere l'esatta l'identità dell'utente, quanto, piuttosto, a definire dei "tipi-ideali", ovvero un modello di utente che rappresenta migliaia di utenti e al quale si possono desumere le scelte con certa grado di affidabilità¹⁰⁵.

¹⁰¹Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale Dir. Amm.*, 2021, p. 317.

¹⁰²Soro, *La protezione dei dati personali nell'era digitale*, in *Nuova Giur.*, 2019, p. 245.

¹⁰³Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale Dir. Amm.*, 2021, p. 317.

¹⁰⁴D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 28.

¹⁰⁵AGCOM, *Indagine conoscitiva sui BIG DATA*, p. 24

2.3 Cookie: accetta tutto o rifiuta tutto?

I cookie sono dei file di testo memorizzati nel computer quando viene visitato un sito web¹⁰⁶. A livello giuridico vengono definiti "marcatori temporali"¹⁰⁷ e per il loro accesso si deve ottenere il consenso dell'utente dopo che ne è stato informato, come indicato nell'art. 5, par. 3, direttiva 2002/58/CE¹⁰⁸. Tecnicamente sono degli "identificatori persistenti"¹⁰⁹ e vengono utilizzati per l'autenticazione dell'utente, per memorizzare informazioni sulla sessione di navigazione (esempio lingua utilizzata, dimensioni schermo del dispositivo per la visualizzazione del sito), per tracciare la navigazione degli utenti a fini statistici¹¹⁰. Un sito di *e-commerce*, ad esempio, utilizza i cookie per permettere il funzionamento del carrello virtuale (funzionalità tecnica necessaria affinché vi sia una corrispondenza univoca con i dati memorizzati nel server) ma anche per tenere traccia degli interessi a fini pubblicitari. Era il 1994 quando Lou Montulli inventò i cookie perchè stava cercando di "portare la memoria sul web"¹¹¹. Oggi Google, proprio grazie ai cookie, è in grado di tracciare gli utenti durante la loro navigazione e registrare tale percorso al fine di profilarli¹¹². "Tutti abbiamo avuto la sensazione di essere inseguiti sul web da pubblicità

¹⁰⁶Gestione dei cookie su <https://support.mozilla.org/it/kb/Gestione%20dei%20cookie> consultato in data 28/10/2022.

¹⁰⁷Considerando n. 30, GDPR

¹⁰⁸Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

¹⁰⁹Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

¹¹⁰Lo scopo in questo caso consiste nell'individuare quali parti del sito sono maggiormente visualizzate, cliccate e in generale avere un feedback sulla fruibilità del sito.

¹¹¹Vox, *How ads follow you around the internet* su <https://www.youtube.com/watch>, consultato in data 28/10/22.

¹¹²Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

basate su cose che abbiamo cercato o letto. Ad esempio cerchiamo un paio di stivali e per giorni, questi stivali vi seguiranno dovunque andiate"¹¹³. Questa forma di persuasione esiste anche nel mondo fisico: nei supermercati, ad esempio, le caramelle sono poste all'altezza del bambino vicino alle casse per invogliarlo all'acquisto mentre è in coda con i propri genitori. Nel mondo digitale, tali architetture persuasive, invece, possono incidere maggiormente sui singoli consumatori perchè possono essere inviate "direttamente sugli schermi privati dei nostri telefoni"¹¹⁴. Il GDPR considera i cookie come dati pseudonimi che comunque sono ritenuti dati personali in quanto si riesce a risalire al dispositivo utilizzato dall'utente tramite un'incrocio dei dati. La normativa in materia di tutela dei dati personali riconosce il dispositivo sul quale vengono salvati i cookie parte della sfera private e perciò "va protetto contro qualsiasi intrusione non autorizzata"¹¹⁵. La Cookie Law, invece, riguarda esclusivamente l'invio e la registrazione di informazioni (cookie) sul dispositivo. Le analisi che vengono effettuate successivamente alla fase di raccolta e archiviazione, invece, sono tutelate dal codice in materia di protezione dei dati personali. Il gestore del sito web diventa responsabile per i cookie impostati da una terza parte e deve obbligatoriamente esporre l'informativa all'utente. L'unica categoria di cookie che invece, non richiede il consenso, sono quelli tecnici¹¹⁶. Il Garante italiano ha pubblicato delle linee guida sui cookie e altri strumenti di tracciamento dove indica, ad esempio, che i cookie wall sono illeciti e che lo scrolling della pagina non equivale al consenso ¹¹⁷. Come visto anche nel primo capitolo, l'ottenimento del consenso deve avvenire prima del trattamento e in maniera libera, inequivocabile, volontaria, specifica ed informata. L'utente

¹¹³Zeynep, *We're bulding a dystopia jus to make people click on ads* su https://www.ted.com/talks/zeynep_tufekcin, consultato in data 28/10/2022.

¹¹⁴Ibidem.

¹¹⁵Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

¹¹⁶Ibidem.

¹¹⁷Garante privacy, 10/06/2021, doc. web n. 9677876 su <https://www.garanteprivacy.it>.

deve quindi avere una scelta reale (consenso libero) e non essere costretto ad accettare tutti i cookie per accedere al sito. La preclusione del servizio può essere lecita, "a meno che il sito non offra dei servizi non sostituibili (es. siti di enti pubblici, vedi Cass. Sez. I Civ, 11/05/2018 - 2/07/2018, n.17278)"¹¹⁸ in quanto la normativa non prevede il fatto che il sito debba funzionare anche senza cookie. Al soggetto, però, non può essere negata la possibilità di utilizzare un servizio offerto dal sito che non necessita dei cookie, invece "qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste"¹¹⁹. La Cookie Law non prevede una modalità di acquisizione specifica ma deve comunque trattarsi di un comportamento attivo: lo scrolling della pagina non rappresenta un consenso valido, la casella preselezionata non è ammessa, non bisogna essere costretti ad accettare i cookie di profilazione per accedere al contenuto del sito, deve essere possibile dimostrare che si sia ottenuto il consenso dall'interessato. Deve esserci, quindi, "un momento nel corso dell'esperienza di navigazione dell'utente e ovviamente preliminare rispetto alla fruizione delle funzionalità, nel quale gli sia appunto consentito scegliere tra più, diverse alternative"¹²⁰ relativamente ai cookie e al livello di profilazione voluto. All'utente deve essere anche spiegato come poter revocare il consenso per rispettare il fatto che questo sia volontario. Solitamente l'informativa breve, è posta in un banner che catturi l'attenzione dell'utente durante la sua navigazione: un banner che si "nasconde" scorrendo semplicemente la pagina web non è considerato valido. Deve essere presente un link che rimanda all'informativa estesa¹²¹ e deve espressamente indicare se utilizza cookie di

¹¹⁸Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

¹¹⁹Considerando n. 32, GDPR.

¹²⁰GPDP, *Provvedimento prescritto nei confronti di Google Inc. sulla conformità al Codice dei trattamenti di dati personali effettuati ai sensi della nuova privacy policy*, 10 Luglio 2014, doc. web n. 3283078.

¹²¹L'informativa sui cookie è una sezione dell'informatica privacy e non un documento separato anche se può essere resa disponibile in una pagina separata purchè sia presente un collegamento all'informativa privacy.

terze parti e di profilazione. Il rifiuto all'utilizzo dei cookie può essere espresso anche tramite la chiusura del banner premendo sulla X. Non è conforme il caso in cui il rifiuto preveda "una defatigante deselegione di decine di caselle"¹²². La tecnica dei cookie wall consiste nel consentire l'accesso a un contenuto solamente se si presta il proprio consenso al trattamento dei dati personali¹²³. Risale a fine Ottobre 2022 il caso di alcune testate giornalistiche che consentono l'accesso al loro sito web o accettando l'installazione dei cookie di profilazione oppure sottoscrivendo un abbonamento¹²⁴. A tal proposito il Garante privacy ha aperto un istruttoria sull'uso dei cookie wall "per accertare la conformità di tali iniziative con la normativa europea"¹²⁵. Tale meccanismo vincolante che segue l'approccio c.d. "*take it or leave it*" non è da ritenersi valido, a meno che "l'editore o fornitore non offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il consenso all'installazione e all'uso dei cookie o altri strumenti di tracciamento"¹²⁶. Nel caso precedentemente descritto l'interessato è immediatamente informato sulla modalità di fruibilità ed è posto nella condizione di scegliere tra le alternative proposte, pertanto tale approccio è da ritenersi valido. I cookie possono essere suddivisi in queste categorie: quelli tecnici, di analytics e personalizzazione, di terze parti e di profilazione e pubblicitari. I cookie dell'ultima categoria sono quelli che permettono la profilazione dell'utente a fini pubblicitari tramite una raccolta dei dati di navigazione. Avendo un grado di invasività elevato richiedono il

¹²²Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

¹²³Agenda digitale, *Cookie wall dei giornali, non è questione di "prendere o lasciare": ecco perchè* su <https://www.agendadigitale.eu/sicurezza/privacy/>, consultato in data 28/10/2022.

¹²⁴Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

¹²⁵Garante Privacy, *Il Garante privacy apre istruttorie su uso dei cookie wall*, doc. web n. 9816536, 21/10/2022.

¹²⁶D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., pp. 133 ss.

preventivo consenso e devono scadere al massimo entro 12 mesi¹²⁷. Anche qualora l'attività del sito dipenda strettamente dai guadagni pubblicitari bisogna richiederne il consenso ed offrire la possibilità di rifiutarsi. La base giuridica del trattamento quindi è solamente il consenso e non possono essere i legittimi interessi del titolare. I cookie di terze parti, invece, sono impostati da un sito web diverso da quello che si sta visitando e sono quelli più invasivi per la privacy degli utenti. Vengono utilizzati oltre che per la profilazione anche per il tracciamento dell'utente al fine di conoscere quali sono le pagine visitate, i link cliccati e quindi essere a conoscenza delle preferenze, realizzando un profilo a cui inviare pubblicità personalizzata¹²⁸. Con il termine terza parte ci si riferisce al fatto che questi cookie non sono impostati dal titolare del trattamento, ma da soggetti terzi, i quali saranno quest'ultimi a trattare i dati in questione. È proprio per questo motivo che i titolari del trattamento non possono garantire un controllo su questi cookie ma limitarsi solamente a indicare l'informativa privacy delle terzi parti che tratteranno effettivamente i dati. Il titolare risponde, però, ugualmente anche se non è il diretto responsabile: è un caso di contitolarità dove le effettive finalità del trattamento sono decise dalla terza parte¹²⁹. Un esempio sono i social plugin che utilizzano principalmente i cookie di terze parti per funzionare. Possono essere inseriti all'interno del sito web tramite iFrame¹³⁰ e consentono all'utente di condividere il contenuto direttamente sul proprio profilo social con un semplice click. Per fare ciò il plugin invia un identificatore univoco e l'url della pagina web che si vuole condividere al server del Social tramite un cookie¹³¹. Per utilizzare i cookie in questione si deve richiedere il consenso all'utente e in caso venissero negati, non

¹²⁷Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

¹²⁸Ibidem.

¹²⁹Ibidem.

¹³⁰È un elemento HTML che viene "ancorato" all'interno della pagina.

¹³¹Seatta, *Cookie law* su <https://protezionedatipersonali.it/cookie-law>, consultato in data 28/10/2022.

rendere visibile il plugin. Ad esempio, i Facebook Social Plugins "Mi piace" e "Commenta" in Europa saranno visibili solamente se gli utenti hanno effettuato l'accesso al proprio account e hanno fornito il consenso al controllo "Cookie dell'app e del sito web"¹³², come indicato nella pagina di Meta dedicata agli sviluppatori¹³³. I social non si limitano solamente a permettere la condivisione dei contenuti ma tracciano e raccolgono tutti i dati di navigazione dell'utente. Spesso, infatti, profilano anche utenti non iscritti al Social, generando un fenomeno che prende il nome di *shadow profiles*. Tali profili vengono realizzati tramite le informazioni condivise dall'utente che iscrivendosi al servizio presta, ad esempio, il proprio consenso all'accesso della propria rubrica¹³⁴.

2.4 Pubblicità personalizzata

È una pratica basata sull'attività di navigazione in Internet nel tempo e su diversi siti e/o app, e consente alle aziende di fornire agli utenti online annunci che riflettono i loro interessi¹³⁵. Abbiamo già visto che l'obiettivo principale dei GAFAM è "tenere l'utente per più tempo possibile sulla loro piattaforma potendo così mostrargli inserzioni pubblicitarie da cui ottengono la remunerazione per la loro attività d'impresa"¹³⁶. Nel caso della "*programmatic advertising*", la pubblicità mostrata viene stabilita da una piattaforma tecnologica (*ad exchange*) che stabilisce i prezzi dello spazio pubblicitario in base ad aste in tempo reale (*Real Time Biddings* o RTB). Più nel dettaglio, quando un utente visita un sito web ne richiede il contenuto all'editore (*publisher content server*), il quale a sua volta invia il contenuto insieme ad alcuni spazi

¹³²Facebook, *Social Plugins* su <https://developers.facebook.com/docs/plugins/> consultato in data 28/10/2022.

¹³³Meta for Developers: <https://developers.facebook.com/docs/plugins/>.

¹³⁴Capitolo 3 per maggiori dettagli sui dati raccolti dalle principali piattaforme.

¹³⁵YouOnlineChoices, *A proposito della pubblicità comportamentale* su <https://www.youonlinechoices.com/it/a-proposito>, consultato in data 29/10/22.

¹³⁶D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 139.

da riempire con inserzioni pubblicitarie. Tali spazi pubblicitari verranno colmati dall'*ad exchange* con le interazioni pubblicitarie più attinenti in base al profilo dell'utente. A differenza di altri sistemi di pubblicità online, nel RTB l'interazione tra inserzionisti e l'agenzia pubblicitaria viene gestita in maniera completamente automatizzata tramite aste istantanee¹³⁷. Per cui, ad esempio, un annuncio di vendita di auto sarà mostrato ad un utente che nelle ultime tre settimane avrà visitato un sito sulle recensioni delle auto, un sito sulla richiesta di un prestito ed avrà effettuato qualche ricerca su Google circa il modello di auto preferito. Il processo termina una volta che viene "individuata l'inserzione più appropriata all'interno della rete di agenzie pubblicitarie collegate (*supply-side platform server*), l'*ad exchange* aggiudica l'asta, riscuote il pagamento da parte dell'inserzionista, e fa apparire l'annuncio negli spazi dedicati sul sito Internet dell'editore al quale l'utente sta accedendo"¹³⁸. Un grosso problema che gli inserzionisti devono affrontare è individuare quale parte della pubblicità è sprecata e quale invece è in grado di raggiungere il consumatore finale. "*Half the money I spend on advertising is wasted; the trouble is I don't know which half*" è la citazione del mercante e politico statunitense John Wanamaker ed esprime un grosso problema noto nel mondo pubblicitario. Ma, oggi, grazie al Web, gli inserzionisti possono conoscere meglio l'impatto che sta avendo una determinata pubblicità. Tramite l'analisi dell'interazioni e quindi il monitoraggio dell'utente, infatti, si stima l'impatto e l'efficacia di un annuncio pubblicitario, conferendo alla pubblicità online una modalità "dinamica", a differenza di quella tradizionale come la stampa, la radio o la televisione che per loro natura non permettono questa interconnessione con l'utente. Questa nuova forma di pubblicità basata su un'accurata profilazione dell'utente a cui inviare un'annuncio pubblicitario "mirato" viene definita pubblicità persona-

¹³⁷D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 147.

¹³⁸D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 148.

lizzata o "targetizzata". Questa si suddivide in tre macrocategorie: pubblicità contestuale, pubblicità segmentata e pubblicità comportamentale¹³⁹. In quella contestuale l'annuncio mostrato varia in base alle informazioni che in quel preciso istante l'utente ha cercato o sta visualizzando. A tal proposito, la *Nederlandse Publieke Omroep*, ovvero l'emittente pubblica olandese "ha deciso di non utilizzare più tecnologie di tracciamento e quindi annunci personalizzati in base alla navigazione dell'utente"¹⁴⁰ ma utilizzando la pubblicità contestuale ha registrato un aumento delle entrate del 62% (gennaio 2020) e del 79% (febbraio 2020) rispetto all'anno precedente¹⁴¹. Anche il *New York Times* ha deciso di interrompere il *targeting* comportamentale con risultati significativi per quanto riguarda le entrate pubblicitarie¹⁴². In quella segmentata, invece, vengono create delle categoria di utenti in base alle caratteristiche (età, sesso, ubicazione, interessi, ecc...) che vengono fornite dall'interessato, ad esempio, in fase di registrazione al sito. Infine in quella comportamentale, a differenza delle altre due categoria, si basa sul "monitoraggio (*rectius* "tracciamento") del comportamento delle persone nel tempo e attraverso più siti"¹⁴³. Attraverso l'analisi delle azioni degli utenti, quali ad esempio visualizzare certi contenuti, interagire con determinati elementi all'interno della pagina, la condivisione di contenuti, si cerca di comprendere gli schemi alla base del comportamento ed elaborare quindi un "profilo specifico sulla base del quale, successivamente, inviare messaggi pubblicitari che corrispondano agli interessi dedotti"¹⁴⁴. Spesso pubblicità comportamentale e RTB sono due sistemi che vengono sovrapposti e integrati: si pensi a quando si ricerca su Google una meta per le vacanze e di seguito, negli altri siti visitati o sui social network appaiono pubblicità di

¹³⁹D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 149.

¹⁴⁰Ibidem.

¹⁴¹Ibidem.

¹⁴²Ibidem.

¹⁴³Ibidem.

¹⁴⁴D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 153.

biglietti aerei o hotel per la destinazione cercata. La pubblicità comportamentale, però, va ben oltre questa profilazione "grossolana", infatti i software che mostrano gli annunci pubblicitari sui *newsfeed* di Facebook o Instagram registrano ogni minima interazione che viene eseguita: "si accorge se l'utente ha fatto scorrere il pollice sullo schermo dello smartphone più o meno velocemente [...], se stando fermi su un annuncio abbiamo spostato il pollice per scoprire una parte dello schermo piuttosto che un'altra, dando modo ad un algoritmo di capire se e cosa stessimo cercando di leggere in quell'annuncio"¹⁴⁵. Tutti questi comportamenti, apparentemente impercettibili e banali, che vengono ricavati dall'utilizzo dell'app o sito, nascondono, in verità, importanti informazioni commerciali perchè in grado di rilevare se quel determinato annuncio è stato efficace¹⁴⁶. Mentre il RTB si basa principalmente sui cookie di terzi parti, la pubblicità comportamentale, invece, fa uso anche di altri marcatori quali ad esempio i *web beacon*¹⁴⁷ e gli identificatori dei device (*device fingerprinting*). Riguardo ai *device fingerprinting* la *Noib - European Center for Digital Rights*, assicurazione non-profit a tutela dei diritti degli interessati, il 13 maggio 2020, ha presentato un reclamo circa il monitoraggio degli utenti per finalità commerciali in base all'art 77 del Regolamento¹⁴⁸. Secondo *Noyb* il tracciamento dell'utente "avverrebbe senza un sistema di "opt-in" che sia idoneo a configurare una sorta di consenso dell'utente al tracciamento ma anche senza nessuna effettiva possibilità di controllo dell'identificativo"¹⁴⁹. Erroneamente si pensa che riuscire ad anticipare i bisogni e utilizzare quindi una forma di pubblicità comportamentale sia una fonte di ampio guadagno. Ma come "in una corsa all'oro, gli unici ad arricchirsi sono quelli che vendono pale e picconi. Infatti, i

¹⁴⁵D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 155.

¹⁴⁶Ibidem

¹⁴⁷È una tecnica usata nella pagine web per controllare se un utente abbia accesso a quel contenuto e viene implementato utilizzando JavaScript.

¹⁴⁸D'ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 160.

¹⁴⁹Ibidem.

soldi veri e certi, vanno a chi gestisce le aste online, non a chi produce i contenuti [...]”¹⁵⁰. I casi di *Nederlandse Publieke Omroep* e di *New York Times*, precedentemente analizzati, sono la prova che esistono altre fonti di guadagno pubblicitario che non impattano in modo significativo sulla privacy dell’utente. È interessante, infine, analizzare quanto valgano i dati generati dagli utenti attraverso *search*, social network e intrattenimento gratuito. Secondo una stima di AGCOM tale valore oscilla tra i 10 e 40 euro per utente (come mostrato in figura 2.1), dove quelli di ricerca, che esprimono maggiormente gli interessi dell’utente, sono quelli che hanno un valore maggiore¹⁵¹. Il rapporto tra i ricavi pubblicitari conseguiti nell’anno e il numero medio di utenti raggiunti (ARPU) mondiale di Google è di circa 37 euro per utente.

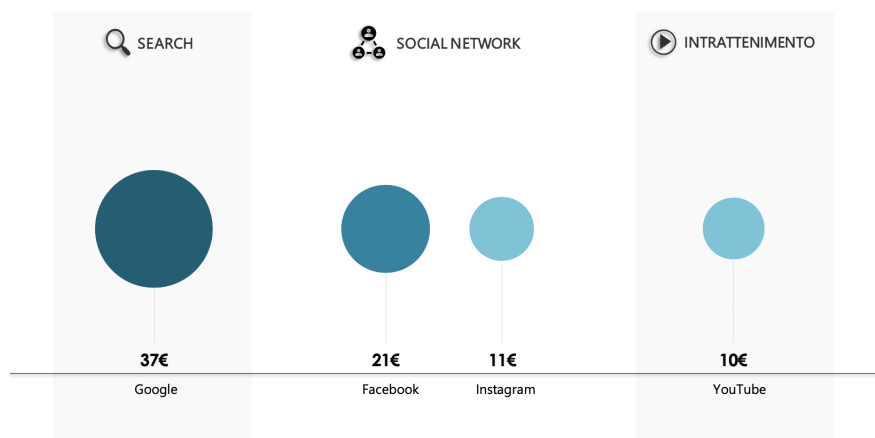


Figura 2.1: ARPU Mondiale dei servizi gratuiti (2018)

¹⁵⁰Vannini, *DataKnightmare: L’algoritmico è politico* su <https://podcasts.apple.com/it/podcast/dataknightmare-lalgoritmico-è-politico/id1163697417>, ascoltato in data 28/10/2022

¹⁵¹AGCOM, *Osservatorio sulle piattaforme digitali online*, p. 23.

Per gli USA, che registra un PIL pro capite più alto e quindi una maggiore disponibilità a pagare, l'URPU è più elevato rispetto alle altre aree geografiche, arrivando a circa 150 euro nel *search* e 90 euro nei social (figura 2.2).

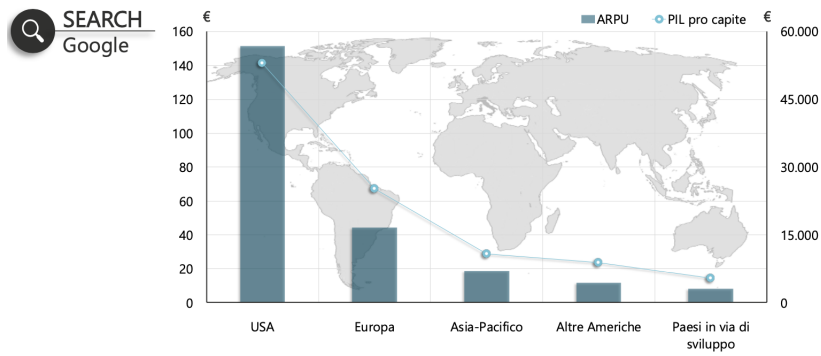


Figura 2.2: ARPU dei servizi gratuiti per area geografica(2018)

Capitolo 3

Conformità al GDPR: Analisi di alcune informative privacy

3.1 Informativa privacy

L'informativa privacy è una comunicazione rivolta all'interessato con lo scopo di informarlo sulle finalità e sulle modalità del trattamento operate dal titolare. Quest'ultimo, infatti, secondo il principio di accountability, deve assicurare la trasparenza e la correttezza dei trattamenti fin dalla fase di progettazione ed essere in grado di provarlo in qualsiasi momento. Inoltre, qualora il trattamento richieda il consenso come base giuridica, l'informativa diventa una condizione di legittimità del trattamento. Tramite essa, infatti, l'interessato ha il potere di controllare la circolazione delle informazioni che lo riguardano¹⁵². Il contenuto dell'informativa è stabilito dagli art. 13 e 14 del GDPR e contiene le seguenti informazioni:

Identità del titolare: deve riportare i dati di contatto del titolare del trattamento.

Finalità e base giuridica del trattamento: devono essere indicate le mo-

¹⁵²Finocchiaro, *Diritto di internet*, cit., p. 147.

tivazioni del trattamento e secondo quale base giuridica si trattano i dati¹⁵³.

Legittimo interesse: se il trattamento si basa sul legittimo interesse deve essere indicato qual è.

Soggetti destinatari: deve essere indicato se si ha intenzione di comunicare i dati ad altri soggetti esterni al titolare.

Trasferimento dati personali a un paese terzo: bisogna dichiarare se si ha intenzione di trasferire i dati in paese extra UE.

Periodo di conservazione dei dati: deve essere stabilito il periodo di conservazione dei dati e se non è possibile determinarlo allora dovranno essere indicati i criteri utilizzati per determinare tale periodo.

Diritti dell'interessato: l'interessato può chiedere al titolare "l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati"¹⁵⁴.

Diritto di revoca del consenso: l'interessato può revocare il proprio consenso "in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca"¹⁵⁵.

Diritto al reclamo: l'interessato ha il diritto di proporre un reclamo a un'autorità di controllo.

Natura obbligatoria o facoltativa del conferimento dei dati: deve essere indicato se "l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati"¹⁵⁶.

¹⁵³ Sono le basi giuridiche previste dal regolamento e sono espresse all'art.6 del GDPR.

¹⁵⁴ Art. 13, paragrafo 2, comma b).

¹⁵⁵ Art. 13, paragrafo 2, lettera c).

¹⁵⁶ Art. 13, paragrafo 2, lettera e).

Esistenza di un processo decisionale automatizzato: ad esempio in caso di profilazione devono essere indicate anche le logiche di tali processi decisionali, "nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"¹⁵⁷.

Inoltre, se il titolare del trattamento utilizza cookie nel suo sito web dovrà redigere anche l'informativa sui cookie, che è una sezione dell'informativa privacy. All'interno dell'informativa sui cookie deve essere indicata anche la modalità di disabilitazione dei cookie e nel caso di utilizzo di cookie di terze parti devono essere indicati i link alle pagine delle informative privacy dei contitolari. Affinché venga rispettato il principio di trasparenza, l'informativa privacy deve utilizzare un linguaggio semplice e chiaro, deve essere in forma concisa, chiara, facilmente accessibile ed intellegibile. In caso di trattamenti valutativi (ad esempio scoring bancario o finanziario), trattamenti basati su decisioni automatizzate, come il tracciamento del comportamento online, trattamento di dati che riguardano soggetti vulnerabili (minori, migranti ecc.), nei sistemi di videosorveglianza e in generale per trattamenti effettuati con nuove tecnologie come machine learning, il titolare deve effettuare anche un'analisi preventiva circa le eventuali conseguenze del trattamento dei dati personali sulle libertà e i diritti degli interessati. Tale valutazione del rischio viene definita *Data Protection Impact Assessment* ed è, quindi, un processo "volto a descrivere il trattamento, valutarne la necessità e la proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento"¹⁵⁸. La nuova visione del GDPR, infatti, è focalizzata sul controllo del dato personale, nel senso che l'interessato "deve poter sapere se i suoi dati sono usati e come vengono usati per tutelare lui e l'intera collettività dai rischi insiti nel

¹⁵⁷ Art. 13, paragrafo 2, lettera f) GDPR

¹⁵⁸ Saetta, *Regolamento generale per la protezione dei dati* su <https://protezionedatipersonali.it/valutazione-impatto-e-rischio-trattamento>, consultato in data 06/11/2022

trattamento dei dati"¹⁵⁹. In questo capitolo verranno analizzate le informative privacy di Meta e Google. In particolare, ci si focalizzerà su quali informazioni vengono raccolte, come queste vengono usate, con chi vengono condivise, per quanto tempo e qual base giuridica ammette il trattamento.

3.2 Dati raccolti da Meta

Il 4 Febbraio 2004 Mark Zuckerberg assieme ai cofondatori Dustin Moskovitz, Chris Hughes e Eduardo Saverin lanciano il *social network* Facebook, offrendo alle persone la possibilità di avere un luogo dove scambiarsi messaggi con i propri amici. Undici mesi dopo, 1 milione di persone sono attive sul social, ma solamente nel 2007 decidono di lanciare un proprio servizio di Ads¹⁶⁰. Nel 2010 gli utenti attivi su Facebook diventano 500 milioni e nel 2012 Facebook annuncia di volere acquistare Instagram e a fine di quell'anno gli utenti attivi salgono a più di un miliardo. Nel 2014 Facebook acquista anche WhatsApp e Oculus con la conseguenza che l'anno seguente gli utenti attivi diventano un miliardo al giorno. Nel 2016 viene introdotto Facebook Marketplace per la vendita di oggetti e nel 2017, invece, viene lanciato Instagram Shopping con lo stesso scopo. È interessante notare come solamente nel 2018 vengono introdotti degli strumenti per misurare il tempo speso su Facebook e Instagram. Nel 2019 viene lanciato Facebook Pay, mentre i pagamenti su WhatsApp vengono resi disponibili nel 2020. Nel 2021 la società cambia nome da Facebook a Meta. L'informativa di Meta Platforms Ireland Limited copre i prodotti di Facebook, Messenger, Instagram, Shops, Marketplace, Spark AR, Strumenti business di Meta, Audience Network, Facebook View. Le informazioni che

¹⁵⁹Saetta, *Regolamento generale per la protezione dei dati* su <https://protezionedatipersonali.it/regolamento-generale-protezione-dati>, consultato in data 06/11/2022

¹⁶⁰Our History in *Facebook*, su <https://about.meta.com/company-info/>, consultato in data 06/11/2022.

raccolgono possono essere suddivise in quattro categorie: la prima riguarda l'attività ("tutto quello che puoi fare con i nostri Prodotti"¹⁶¹) compiute utilizzando il servizio e le informazioni fornite, la seconda su amici e i follower, la terza sulle informazioni dell'app, browsers e dispositivi e infine la quarta sulle informazioni provenienti da partner, fornitori o terzi. Le informazioni fornite riguardano ad esempio i posti, i commenti, i contenuti audio creati, e tutto ciò che si vede attraverso la fotocamera del dispositivo¹⁶². Oltre ai metadati dei contenuti e dei messaggi, come il luogo in cui è stata scattata la foto, la data di creazione del file, il tipo messaggio, la data, l'ora in cui è stato inviato il messaggio, viene registrata anche la tipologia dei contenuti visualizzati e le modalità di interazioni come l'ora, la frequenza e la durata delle attività sui prodotti. Infatti, gli insights di una pagina Facebook sono delle statistiche aggregate create proprio a partire dall'interazione degli utenti con la pagina, riuscendo ad avere quindi una panoramica circa la data e l'ora di interazione, la città, la lingua, il gruppo di età, il tipo di dispositivo utilizzato e ID dell'utente di Facebook¹⁶³. Per la categoria di amici e follower le informazioni raccolte riguardano gli indirizzi email e i numeri di telefono dei contatti quando, ad esempio, si fornisce l'accesso alla rubrica del proprio dispositivo¹⁶⁴. Di fatto, possono essere raccolti i contatti di chi non risulta essere iscritto e al fine di garantire ai non-utenti di esercitare il diritto d'opposizione al trattamento è stata creata una pagina web per richiedere l'eliminazione delle proprio informazioni dal database delle rubriche di Meta¹⁶⁵. Vengono collezionate anche le informazioni sul tipo di dispositivo utilizzato, sul suo sistema operativo, sui dettagli hardware e software, il livello di batteria, la potenza del segnale, lo spazio di archiviazione disponibile, tipo di browser, nomi e tipologia di app e i plug-in

¹⁶¹Ibidem

¹⁶²Ibidem

¹⁶³Ibidem

¹⁶⁴Informazioni per le persone che non usano i Prodotti di Meta in *Facebook*, su <https://www.facebook.com/help> , consultato in data 06/11/2022.

¹⁶⁵Disponibile al seguente <https://www.facebook.com/contacts/removal>.

utilizzati. Così come anche i segnali GPS, Bluetooth, punti di accesso Wi-Fi, beacon e celle telefoniche vengono raccolti. Meta, inoltre, raccoglie il nome dell'operatore di telefonia mobile o fornitore del servizio internet (ISP), la lingua, il fuso orario, numero di cellulare, l'indirizzo IP, la velocità di connessione, le informazioni su altri dispositivi nelle vicinanze o connessi alla tua rete. "Un motivo per cui raccogliamo queste informazioni è migliorare la tua esperienza. Ad esempio, se sappiamo che il tuo cellulare e la tua TV sono connessi alla stessa rete, possiamo aiutarti a usare il cellulare per controllare uno streaming video sulla TV"¹⁶⁶. Invece, i contenuti come nome utente Facebook o Instagram, immagine del profilo sono pubbliche e infatti possono essere visualizzati, accessi da servizi terzi come ad esempio i motori di ricerca, le API Graph¹⁶⁷ di Meta, i media e la TV. Le attività online di utilizzo della piattaforma vengono monitorate e suddivise in categorie dai fornitori di servizi pubblicitari, i quali aiutano l'azienda a misurare la risposta alle iniziative di marketing e l'efficacia della pubblicità¹⁶⁸. Inoltre, anche l'identificato del dispositivo viene condiviso con i fornitori di servizi pubblicitari per mostrare all'utente inserzioni di suo interesse. Gli Strumenti business di Meta, infatti, sono delle tecnologie che "aiutano proprietari di siti web, editori, sviluppatori di app e partner commerciali, inclusi inserzionisti e altri utenti [...] a comprendere e misurare i loro prodotti e servizi e raggiungere in maniera più efficace le persone che usano o potrebbero essere interessate ai loro prodotti e servizi"¹⁶⁹. Un esempio sono i plug-in social di Facebook dei pulsanti "mi piace" e "condividi", attraverso i quali vengono condivise informazioni sugli utilizzatori. Le finalità di raccolta delle informazioni precedentemente analizzate servono, in primo luogo, per

¹⁶⁶Informazioni sulla rete a cui è connesso il dispositivo in *Facebook*, su <https://www.facebook.com/privacy/policy>, consultato in data 06/11/2022.

¹⁶⁷Application Program Interface è il modo principale per inserire ed estrarre dati dalle piattaforme.

¹⁶⁸In che modo i fornitori supportano le nostre iniziative pubblicitarie e di marketing in *Facebook*, su <https://www.facebook.com/privacy/policy>, consultato in data 06/11/2022.

¹⁶⁹Gli strumenti business di Meta in *Facebook*, su <https://www.facebook.com/help>, consultato in data 06/11/2022.

personalizzare i prodotti offerti, come, ad esempio, il feed di Facebook o di Instagram, le storie e le inserzioni. Iscrivendosi presso un panificio locale su Facebook "potrebbero essere mostrate inserzioni relative ad altri panifici locali su Instagram"¹⁷⁰. Infatti gli ads su Meta funzionano nel seguente modo: gli inserzionisti scelgono il bacino di utenza che vogliono raggiungere. Di seguito, quando l'utente utilizza il social, viene effettuata una verifica dell'attinenza all'inserzione in base alle pagine ai cui ha messo "mi piace", alle informazioni del suo profilo, ai post pubblicati o con cui interagisce e i luoghi visitati. In più, gli inserzionisti possono creare una lista con gli indirizzi e-mail di chi ha interagito con loro al di fuori di Facebook, ad esempio quando si effettua un'acquisto oppure si crea un account per un programma a premi. Quindi si possono "trovare corrispondenze per gli utenti tramite tale lista per aiutare l'inserzionista a raggiungere le persone che potrebbero essere interessate alla sua azienda, senza che Facebook acquisisca nuove informazioni personali sugli utenti"¹⁷¹. Un'altra motivazione per cui vengono raccolte tali informazioni è di natura tecnologica ovvero verificare il corretto funzionamento delle applicazioni e raccogliere feedback sul loro utilizzo. Meta effettua anche ricerche sui luoghi in cui si recano le persone durante la crisi affinché "le organizzazioni di soccorso possano inviare aiuti nei luoghi giusti"¹⁷². Ad esempio, attraverso il servizio *Data for Good* hanno realizzato rappresentazioni grafiche "sull'atteggiamento nei confronti dei vaccini a livello locale, sulla vicinanza delle popolazioni all'acqua potabile e sull'accessibilità a Internet a livello mondiale"¹⁷³. Inoltre, le app o siti web presso cui si effettua l'accesso tramite Facebook Login o nei

¹⁷⁰Le tue attività sui nostri Prodotti in *Facebook*, su <https://www.facebook.com/privacy/policy>, consultato in data 06/11/2022.

¹⁷¹Perché vedo le inserzioni di un inserzionista su Facebook? in *Facebook*, su <https://www.facebook.com/help/>, consultato in data 06/11/2022.

¹⁷²Ricerca e innovazione per il bene comune della società in *Facebook*, su <https://www.facebook.com/privacy/policy/ResearchingAndInnovatingFor>, consultato in data 06/11/2022.

¹⁷³Data for good in *Facebook*, su <https://dataforgood.facebook.com>, consultato in data 06/11/2022.

quali si connette il proprio account Instagram, accedono alle informazioni private, "a meno che non ci risulti che tu non abbia usato l'app o il sito web per 90 giorni"¹⁷⁴. Gli inserzionisti che utilizzano i prodotti di Meta sanno quante persone hanno interagito con le inserzioni, il momento in cui hanno interagito ma non possono accedere alle informazioni identificabili, quali ad esempio nome o indirizzo e-mail, a meno che non vi sia data l'autorizzazione. All'interno dell'azienda Meta vengono condivise informazioni, ad esempio si può usare l'account Facebook Pay per effettuare pagamenti su WhatsApp o chattare con amici su altri prodotti delle aziende di Meta connettendo il proprio account WhatsApp. Oltre a questi esempi funzionali, nell'informativa privacy è indicato che i video caricati "possono aiutare ad addestrare i nostri prodotti a riconoscere oggetti, come gli alberi, o attività, come un cane che insegue una palla"¹⁷⁵. Per cui, di fatto, vengono utilizzati i dati degli utenti come training set degli algoritmi di machine learning di Meta. La base giuridica per il trattamento dei dati personali è quella del consenso, per cui l'utente gode di tutti i diritti visti precedentemente. Riguardo all'utilizzo dei prodotti, bisogna far riferimento anche alle condizioni d'uso che trattano i dati personali per l'esecuzione del contratto. Gli interessi legittimi che perseguono, invece, sono quelli di fornire report precisi e affidabili ai loro inserzionisti, sviluppatori e altri partner, per garantire prezzi e statistiche accurati sulle prestazioni e per dimostrare il valore che i loro partner ottengono usando i prodotti delle aziende di Meta. Ma anche per gli interessi di inserzionisti e sviluppatori "per aiutarli a comprendere i loro clienti e migliorare le proprie aziende, convalidare i nostri modelli di prezzo e valutare l'efficacia dei loro contenuti e della loro pubblicità

¹⁷⁴Quando usi un prodotto o servizio di un Partner integrato in *Facebook*, su <https://www.facebook.com/privacy/policy/WhenYouUseAn>, consultato in data 06/11/2022.

¹⁷⁵Perché condividiamo informazioni all'interno delle aziende di Meta in *Facebook*, su <https://www.facebook.com/privacy/policy>, consultato in data 06/11/2022.

online all'interno e all'esterno dei Prodotti delle aziende di Meta"¹⁷⁶. Un altro loro interesse legittimo è quello di promuovere i prodotti delle aziende di Meta ed effettuare il marketing diretto.

3.3 Dati raccolti da Google

Google venne fondata nel 1998 da Larry Page e Sergey Brin, studenti alla Stanford, con la commercializzazione del loro motore di ricerca basato sul algoritmo di PageRank¹⁷⁷. Il motore di ricerca rimane il core business dell'azienda ma la principale fonte di guadagno è dovuta a servizi pubblicitari¹⁷⁸.

I servizi coperti dall'informativa privacy sono le app, siti e dispositivi Google come Ricerca, YouTube, Google Home, il browser Chrome, il sistema operativo Android e i prodotti integrati in app e siti di terze parti come annunci e analisi. Le informazioni raccolte quando si utilizzano tali servizi possono essere suddivisi in due macro categorie: le informazioni direttamente fornite dagli utenti e le informazioni raccolte durante l'utilizzo del servizio. Durante la creazione di un account oltre al nome, l'utente potrebbe fornire informazioni anche sul proprio numero di telefono e i dati di pagamento. Vengono collezionati anche tutti i contenuti creati o ricevuti utilizzando i servizi, come ad esempio le email scritte e ricevute, le foto e i video salvati, i documenti e i fogli di lavoro creati e i commenti sui video di YouTube. Anche se non è stato eseguito l'accesso a un account Google, vengono raccolte informazioni tramite identificatori univoci del browser utilizzati per "mantenere le stesse preferenze tra una sessione di navigazione e l'altra, ad esempio la tua lingua preferita o se visualizzare o

¹⁷⁶Privacy Policy in *Facebook*, su <https://www.facebook.com/privacy/policy>, consultato in data 06/11/2022.

¹⁷⁷Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University, Roma, 2019, p. 114.

¹⁷⁸Google: global annual revenue 2002-2021 in *Statistics*, su <https://www.statista.com/statistics/>, consultato in data 06/11/2022.

meno annunci o risultati di ricerca più pertinenti in base alle tue attività"¹⁷⁹. Riguardo al dispositivo utilizzato per accedere al servizio vengono memorizzati quindi gli identificativi univoci, il sistema operativo, il numero di telefono, il numero di versione dell'applicazione, l'indirizzo IP, le attività di sistema, la data, l'ora e l'URL referrer della richiesta. Inoltre si può scegliere se far salvare o meno una registrazione audio quando si interagisce con la ricerca Google o con l'assistente vocale registrando la voce e l'audio, "oltre ad alcuni secondi precedenti all'attivazione"¹⁸⁰. Per chi utilizza i servizi Google per effettuare o ricevere chiamate e messaggi vengono raccolte le informazioni sul numero del chiamante, numero del ricevente, indirizzi email del mittente e del destinatario, ora e data, durata e la tipologia e volumi di chiamate e messaggi. La posizione dell'utente viene determinata in base al GPS combinando l'uso dell'accelerometro per determinare la velocità e quella del giroscopio per stabilire la direzione, ma anche attraverso l'indirizzo IP e i ripetitori di segnale e i punti di accesso Wi-Fi che si trovano nelle vicinanze. Google riceve informazioni da parte di servizi pubblicitari poiché quest'ultimi hanno caricato dati provenienti dalla loro carta fedeltà "al fine di comprendere meglio il rendimento delle loro campagne pubblicitarie"¹⁸¹. Per raccogliere le informazioni precedentemente descritte vengono usate varie tecnologie tra cui cookie, tag di pixel¹⁸², archiviazione locale, ad esempio spazio di archiviazione web del browser oppure cache di dati delle applicazioni, database e log del server. I server di Google registrano automaticamente la richiesta web, l'indirizzo IP, il tipo di browser utilizzato, la data e l'ora e uno o più cookie per identificare il browser in ma-

¹⁷⁹Desideriamo che tu comprenda i tipi di informazioni che raccogliamo quando utilizzi i nostri servizi in *Google*, su <https://policies.google.com/privacy>, consultato in data 06/11/2022.

¹⁸⁰Informazioni vocali e audio in *Google*, su <https://policies.google.com/privacy>, consultato in data 06/11/2022.

¹⁸¹Servizi pubblicitari e di ricerca per loro conto in *Google*, su <https://policies.google.com/privacy>, consultato in data 06/11/2022.

¹⁸²Sono delle tecnologie impiegate nei siti web o nel corpo di un'email per determinare ad esempio se è stata aperta l'email oppure se è già stato visualizzato quel sito web.

niera univoca. Ad esempio la ricerca del termine "auto" sul motore di ricerca Google tra un browser Firefox su un sistema operativo Windows, genera il seguente log:

123.45.67.89 - 13/Dic/2022 09:42:00 -
<http://www.google.com/search?q=auto>
Firefox 1.0.7; Windows NT 5.1 -740674ce2123e969.

Le motivazioni per le quali utilizzano i dati raccolti sono per la fornitura dei servizi, come restituire risultati pertinenti o ottenere un suggerimento del destinatario a cui condividere quel contenuto. Ad esempio dalla ricezione di un email di conferma di un volo viene creato un pulsante "check-in" direttamente su Gmail. Oltre che per migliorare il servizi, come ad esempio migliorare la funzionalità di controllo ortografico partendo dagli errori ortografici più frequenti, utilizzano le informazioni raccolte per " per creare servizi su misura per te, ad esempio offrendoti consigli, contenuti personalizzati e risultati di ricerca personalizzati"¹⁸³. Infatti, quando cerchiamo "Mountain bike" su Google e successivamente visitiamo un sito che mostra annuncio pubblicati da Google, vedremo annunci di attrezzatura sportiva. Gli annunci comunque non si basano sui contenuti in Drive, Gmail o Foto e non vengono condivise con gli inserzionisti le informazioni quali nome o indirizzo email a meno che ad esempio si clicchi sul pulsante "Tocca per chiamare" quando vogliamo contattare un negozio in zona. Google collabora con oltre 2 milioni di siti web e app di terze parti per la pubblicazione di annunci¹⁸⁴ e al fine di comprendere il rendimento delle campagne pubblicitarie degli inserzionisti viene utilizzato, ad esempio, Google Analytics. Questo strumento permette a Google di collegare le informazioni "sulle tue attività nel sito che stai visitando o nell'app che stai

¹⁸³Offrire servizi personalizzati, inclusi contenuti e annunci in *Google*, su <https://policies.google.com/privacy> , consultato in data 06/11/2022.

¹⁸⁴Collaborare con Google in *Google*, su <https://policies.google.com>, consultato in data 06/11/2022.

usando con le attività in altri siti o app che utilizzano i nostri servizi pubblicitari"¹⁸⁵. Un'altra finalità riguarda la protezione, la sicurezza, l'affidabilità dei servizi Google: il rilevamento di attività fraudolente, abusi, rischi per la sicurezza. Google condivide le informazioni con terze parti quando è stato chiesto l'esplicito consenso all'utente, oppure quando si tratta di una società consociata, ovvero "una persona giuridica appartenente al gruppo della società Google, tra cui le seguenti società che forniscono servizi per i consumatori nell'UE: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp e Google Dialer Inc"¹⁸⁶. Google si avvale di affiliati per "esaminare i contenuti dei video di YouTube per garantire la sicurezza pubblica, nonché per analizzare e ascoltare campioni di audio salvato degli utenti per contribuire a migliorare le tecnologie di riconoscimento audio di Google"¹⁸⁷. Al fine di moderare i contenuti online all'interno dei servizi, Google condivide le richieste di rimozione di contenuti con un progetto di terze parti chiamato Lumen. Quest'ultimo è una "ricerca indipendente gestita dal Berkman Klein Center for Internet & Society dell'Università di Harvard"¹⁸⁸. Il periodo di conservazione dei dati varia in base alla tipologia dei dati, ad esempio le informazioni caricati dagli utenti come foto, documenti e contenuti creati o caricati possono essere eliminati in qualsiasi momento. Per le informazioni sull'attività si può scegliere di eliminarli automaticamente dopo un determinato periodo di tempo oppure verranno conservati " finché non li rimuoverai o non deciderai di farli rimuovere"¹⁸⁹. I dati pubblicitari nei log dei server, invece, vengono eliminati o resi anonimi automaticamente dopo 9 mesi per gli indirizzi IP e dopo 18 mesi per i cookie.

¹⁸⁵Misurare il rendimento in *Google*, su <https://policies.google.com/privacy>, consultato in data 06/11/2022.

¹⁸⁶Affiliata in *Google*, su <https://policies.google.com>, consultato in data 06/11/2022.

¹⁸⁷Per trattamenti esterni in *Google*, su <https://policies.google.com>, consultato in data 06/11/2022.

¹⁸⁸Informazioni su Lumen in *Google*, su <https://support.google.com/legal/answer/>, consultato in data 06/11/2022.

¹⁸⁹Conservazione delle tue informazioni in *Google*, su <https://policies.google.com>, consultato in data 06/11/2022.

Le informazioni relative alla frequenza di utilizzo dei servizi Google vengono conservate fino all'eliminazione dell'account. Dal momento che Google protegge i dati da perdite accidentali o danni fisici e conserva copie di backup e copie dei dati, la rimozione completa dei dati richiede circa due mesi. Le basi giuridiche di Google sono il consenso per gli annunci personalizzati. Attraverso le condizioni d'uso, invece, vengono trattati i dati personali per l'esecuzione del contratto. I legittimi interessi, invece, sono quelli di offrire, mantenere migliorare i servizi, sviluppare nuovi prodotti e funzionalità, capire come le persone utilizzano i servizi al fine di garantire e migliorarne il rendimento, fare uso di marketing, personalizzare i servizi per offrire un'esperienza migliore e adempiere agli obblighi di legge.

3.4 Come diminuire le proprie impronte digitali

Le aziende pubblicitarie tengono traccia di quello che le persone fanno online e offline aggregando e condividendo dati personali. Prendiamo l'esempio di un padre e una figlia che decidono di trascorrere una giornata al parco. Alla mattina il padre controlla il meteo e legge le ultime notizie utilizzando il computer, mentre usa un'app di navigazione per controllare il traffico nel tracciato da casa al parco. Molte app dello smartphone, incluso il navigatore, che accedono ai dati di localizzazione in background vendono tali informazioni alle agenzie pubblicitarie per mostrare annunci basati sulla posizione dell'utente. Infatti, durante il tragitto la figlia utilizza il tablet per giocare ad un app e vede una pubblicità di un monopattino: tale inserzione è stata stabilita in pochi millisecondi attraverso un'asta in tempo reale basata sui dati personali raccolti. Al parco decidono di postare una loro foto sul Social Network, in questo modo, rilasciano metadati come il luogo, la data, l'ora di scatto e il dispositivo utilizzato. Al ritorno decidono di fermarsi a prendere un gelato e acquistare un giocattolo in un negozio vicino alla loro abitazione: adesso le agenzie pubblicitarie hanno raccolto informazioni sugli acquisti appena effettuati senza un

reale consenso espresso liberamente. A fine giornata, il padre ha "inconsapevolmente" interagito con svariate aziende di tutto il mondo, utilizzando le app e i servizi gratuiti e permettendole loro di conoscere i posti che frequenta, i prodotti che cerca, i negozi che ha visitato e le sue abitudini di acquisto¹⁹⁰.

In realtà, l'utente può utilizzare svariati strumenti digitali gratuiti e non che gli permettano di non essere profilati durante il loro utilizzo. Ad esempio, DuckDuckGo è un motore di ricerca in grado di soddisfare il bisogno informativo dell'utente senza l'utilizzo di *online tracking*¹⁹¹. Nato nel 2008 da Gabriel Weinberg con l'idea di non tenere traccia della storia delle ricerche effettuate. In questo caso quando l'utente effettua una ricerca, quest'ultima non viene condivisa con il sito a cui si clicca e nemmeno gli annunci mostrati sono basati sul profilo degli utenti. Infatti, i termini di ricerca possono essere inviati al sito attraverso l'utilizzo di *Referer HTTP request*¹⁹², il quale viene utilizzato per contenere la stringa di richiesta quando si clicca sul link¹⁹³. Per prevenire questo comportamento tramite le impostazioni di DuckDuckGo, si può utilizzare una richiesta POST anziché GET, come normalmente accade. L'utilizzo di POST, però, compromette il corretto funzionamento del tasto indietro e rende impossibile condividere la barra degli indirizzi del browser in modo semplice attraverso un copia e incolla¹⁹⁴.

Esistono anche delle alternative ai social network più diffusi, Mastodon ne è un esempio. È un social network decentralizzato che fa parte di fediverso, una comunità internazionale composta da "oltre 6 milioni di iscritti distribuiti su circa 14000 server indipendenti"¹⁹⁵. "A differenza dei social tradizionali è open

¹⁹⁰ Apple, *Un giorno nella vita dei tuoi dati*, Aprile 2021.

¹⁹¹ Your personal data is nobody's business in *DuckDuckGo* su <https://duckduckgo.com/about>, consultato in data 07/11/2022.

¹⁹² È un tipo particolare di HTTP headers, ovvero un metodo che permette lo scambio di informazioni tra cliente e server.

¹⁹³ Refer HTTP in *Mozilla Developer*, su <https://developer.mozilla.org>, consultato in data 07/11/2022.

¹⁹⁴ We don't collect or share personal information in *DuckDuckGo*, su <https://duckduckgo.com/privacy1>, consultato in data 07/11/2022.

¹⁹⁵ Benvenuti su Mastodon Italia in *Mastodon* su <https://mastodon.it>, consultato in data

source, non raccoglie i dati degli iscritti, non ha pubblicità o algoritmi segreti che decidono cosa devi vedere"¹⁹⁶. Il fediverso è in pratica un'insieme di server gestiti da diverse persone che comunicano tra loro utilizzando il protocollo ActivityPub¹⁹⁷. In questo modo le identità che vengono create dagli utenti sui diversi server (istanze), possono comunicare tra loro anche se ospitate su istanze diverse. L'utilizzo del social network Mastodon è aumentato soprattutto dopo che il 28 Ottobre Elon Musk ha acquistato Twitter¹⁹⁸. Dal momento che non implementano nessuna strategia di monetizzazione nel software, utilizzano strategie di crowdfunding tramite Patreon o servizi simili per il mantenimento del sistema informatico.¹⁹⁹.

Per quanto riguarda i servizi cloud di archiviazione di foto, video, documenti e fogli di lavoro, Nextcloud rappresenta una valida alternativa a Google Drive. Fondato da Frank Karlitschek e altri esperti imprenditori ed esperti ingegneri open source "per consentire agli utenti di riprendere il controllo dei loro dati e delle loro comunicazioni"²⁰⁰. È una piattaforma basata su software open source, per cui chiunque può decidere di installare e gestire su un proprio server privato il software. A differenza delle soluzioni SaaS²⁰¹, Nextcloud permette al cliente di avere il totale e diretto controllo dei dati o attraverso un provider oppure in locale.

Anche la scelta del browser incide sul rilascio di impronte digitali: Firefox "blocca automaticamente più di 2000 elementi traccianti, impedendo alle azien-

07/11/2022.

¹⁹⁶ Benvenuti su Mastodon Italia in *Mastodon*, su <https://mastodon.it>, consultato in data 07/11/2022.

¹⁹⁷ Cos'è e come funziona la federazione dei social network: il Fediverso in *Mastodon*, su <https://mastodon.it/it/fediverso>, consultato in data 07/11/2022.

¹⁹⁸ Anche scienziati tra utenti che potrebbero lasciare Twitter in *Ansa*, su <https://www.ansa.it/>, consultato in data 07/11/2022.

¹⁹⁹ Finanziamento e monetizzazione in *Mastodon*, su <https://mastodon.it/it/fediverso>, consultato in data 07/11/2022.

²⁰⁰ About Us in *Nextcloud*, su <https://nextcloud.com/about/>, consultato in data 07/11/2022.

²⁰¹ Software as a Service, ovvero il software viene messo a disposizione e il cliente paga per il suo utilizzo.

de di raccogliere informazioni sulle tue attività online"²⁰². Chrome, il browser di Google, invece, tiene traccia di qualunque cosa venga digitato o cliccato in piccoli frammettenti, definiti "testo ombra" dalla sociologa Shoshana Zuboff nel libro "Il capitalismo della sorveglianza". Tali informazioni, appartenente banali, se raccolti su larga scala tramite algoritmi permettono di essere "una materia prima da accumulare e analizzare per fini commerciali [...] e dice di noi più di quanto noi stessi possiamo sapere"²⁰³.

²⁰²Usa i browser che mettono la tua privacy al primo posto, da sempre in *Mozilla*, su <https://www.mozilla.org/it/firefox/browsers/>, consultato in data 07/11/2022.

²⁰³Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, cit., p. 199.

Conclusioni

In questo elaborato è stata presentata dapprima una panoramica sul diritto che protegge i dati personali, soffermandosi su cosa sia un dato personale, quali sono i diritti e le responsabilità dei soggetti coinvolti nel trattamento, quali principi si applicano e cosa sia l'informativa privacy, quale strumento che racchiude tutto ciò. In particolare si è analizzata la profilazione come un caso specifico di trattamento dei dati personali. Da questa specifica tipologia di trattamento derivano questioni giuridiche ed economiche, quali, ad esempio, la discriminazione del prezzo, la presenza di pregiudizi negli algoritmi utilizzati poiché a sua volta basati su dati distorti e l'effetto di polarizzazione degli utenti all'interno dei social network perché proprio tramite i dati raccolti si è grado di prevedere tratti e attributi privati della persona²⁰⁴. Dopo una valutazione delle informative privacy di Meta e Google sono stati illustrati alcuni dei possibili strumenti tecnologici utilizzabili al fine di prevenire o diminuire le proprie impronte digitali. Infatti "siamo noi a dare loro ogni giorno questi dati; ogni volta che clicchiamo "accetta" alle infinite notifiche che arrivano sul nostro smartphone forniamo una quantità di informazioni su noi stessi, sulla nostra vita, di cui nemmeno ci accorgiamo"²⁰⁵. Un aspetto sul quale si dovrebbe puntare è appunto la consapevolezza da parte degli utenti circa le opportunità e i poteri che gli algoritmi offrono, altrimenti vi è il rischio che questi diventino un

²⁰⁴Kosinski, Stillwell, Graepel, *Private traits and attributes are predictable from digital records of human behavior*, Proceedings of the national academy of sciences, 2013.

²⁰⁵Vespignani, *L'algoritmo e l'oracolo*, Il saggiatore, 2019.

qualcosa di oscuro e incomprensibile. A tal proposito il Parlamento Europeo si sta muovendo nella direzione di una maggiore trasparenza degli algoritmi utilizzati nei sistemi di profilazione attraverso il Digital Service Act²⁰⁶. Infatti un processo di profilazione applicato a un gruppo di persone può influenzare il comportamento, a differenza dei fenomeni naturali e degli animali che non hanno tale sensibilità e pertanto non ne possono subire le conseguenze. La pubblicità targetizzata, ad esempio, "ha un particolare potere di persuasione, e se scorrettamente effettuata può trascendere in una vera e propria manipolazione della volontà umana, se non mercificazione dell'attenzione dell'utente a vantaggio di pochi e a detrimento del singolo"²⁰⁷. Tanto è vero che gli algoritmi sono diventati sempre più come oracoli a cui rivolgersi: solo una corretta interpretazione degli esiti valutativi e un controllo diretto sul loro funzionamento permettono all'uomo di essere libero di scegliere se seguire o meno l'algoritmo.

²⁰⁶The Digital Services Act: ensuring a safe and accountable online environment in *European Commission*, su <https://ec.europa.eu/>, consultato in data 08/11/2022

²⁰⁷D'ippolito, *Profilazione e Pubblicità Targetizzata On-Line: Real-Time Bidding e Behavioural Advertising*, cit., p. 248.

Bibliografia

- [1] Batteli, *I modelli negoziali di business degli operatori digitali a “prezzo zero” non sono “gratuiti”*. in *Contratti*, 2022.
- [2] D’ippolito, *Profilazione e Pubblicità Targettizzata On-Line: Real-Time Bidding e Behavioural Advertising*. Edizioni Scientifiche Italiane, 2021.
- [3] Fabiano, *GDPR & Privacy: Consapevolezza e Opportunità. Analisi Ragionata Della Protezione Dei Dati Personali Tra Etica e Cybersecurity: Prefazione Di Giovanni Buttarelli*. goWare, 2019.
- [4] Finocchiaro, *Diritto di internet*. Zanichelli, 2020.
- [5] Finocchiaro, *Gdpr tra novità e discontinuità- Il principio di accountability*. in *Giurisprudenza italiana*, 2019.
- [6] Giuliano, *Regolare l’infosfera*. in *Contratti e Impresa*, 2021.
- [7] Kosinski et al., *Private traits and attributes are predictable from digital records of human behavior*. in *Proceedings of the national academy of sciences*, 2013.
- [8] Leone, *Servizi digitali “zero price” e diritti dei consumatori*. in *Diritto industriale*, 2022.
- [9] Pedreschi, *Meaningful Explanations of Black Box AI Decision Systems*. in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2019.
- [10] Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell’algoritmo nella cornice della responsible research and innovation*. in *Nuovi Leggi Civile Commerciale*, 2018.

- [11] Proietti, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*. in *Contratti e impresa*, 2018.
- [12] Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*. in *Giornale Diritto Amministrativo*, 2021.
- [13] Soro, *La protezione dei dati personali nell'era digitale*. in *Nuova Giurisprudenza*, 2019.
- [14] Varian, *Microeconomia*. Cafoscarina, 2007.
- [15] Vespignani, *L'algoritmo e l'oracolo*. Il Saggiatore, 2019.
- [16] Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. LUISS University, 2019.

Strumenti Esegetici

- [17] Gruppo di lavoro *ex art. 29*, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, (WP258).
- [18] European Data Protection Supervisor, *Opinion 4/2017* Sulla proposta di Direttiva relativa a determinati aspetti dei contratti di Fornitura di contenuti digitali.
- [19] IAB Europe, *Programmatic Trading white paper*, 2014.
- [20] AGCOM, *Indagine conoscitiva sui BIG DATA*.
- [21] AGCOM, *Osservatorio sulle piattaforme digitali online*.
- [22] Garante per la protezione dei dati personali, 10/06/2021, doc. web. n. 9677876.

Sentenze e provvedimenti

[23] Provv. Garante Privacy, 10/07/2014, doc. web n. 3283078.

Sitografia

- [24] Angwin e Larson (2016), *Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say*
<https://www.propublica.org/article/> (Da ultimo visitato il 28/10/2022).
- [25] DuckdDuckGo (2022), *About* <https://duckduckgo.com/about> (Da ultimo visitato il 07/11/2022).
- [26] Gambazza & Riccio (2022), *Cookie wall dei giornali, non è questione di “prendere o lasciare”: ecco perché*
<https://www.agendadigitale.eu/sicurezza/privacy/> (Da ultimo visitato il 28/10/2022).
- [27] Google (2022), *Norme sulla privacy* <https://policies.google.com/> (Da ultimo visitato il 06/11/2022).
- [28] Hern A. (2018), *Google’s solution to accidental algorithmic racism: ban gorillas* <https://www.theguardian.com/> (Da ultimo visitato il 28/10/2022).
- [29] Mastodon Social (2022), *Benvenuti su Mastodon Italia* <https://mastodon.it>
(Da ultimo visitato il 07/11/2022).
- [30] Meta (2022), *Informativa sulla privacy* <https://www.facebook.com/> (Da ultimo visitato il 06/11/2022).
- [31] Meta (2022), *Our History* <https://about.meta.com/> (Da ultimo visitato il 06/11/2022).
- [32] Meta (2022), *Social Plugins* <https://developers.facebook.com/> (Da ultimo visitato il 28/10/2022).

- [33] NextCloud (2022), *About Us* <https://nextcloud.com/about/> (Da ultimo visitato il 07/11/2022).
- [34] Saetta (2017), *Cookie law* <https://protezionedatipersonali.it/cookie-law> (Da ultimo visitato il 28/10/2022).
- [35] Saetta (2020), *Ombre e criticità del sistema pubblicitario digitale: un futuro senza annunci personalizzati è possibile?*
<https://www.valigiablu.it/futuro-pubblicita/>
(Da ultimo visitato il 28/10/2022).
- [36] Saetta (2018), *Valutazione di impatto (DPIA) e rischio del trattamento*
<https://protezionedatipersonali.it/valutazione-impatto> (Da ultimo visitato il 06/11/2022).
- [37] Statista (2022), *Annual revenue of Google from 2002 to 2021*
<https://www.statista.com/statistics/> (Da ultimo visitato il 06/11/2022).
- [38] Vannini (2022), *DataKnighmare: L'algorithmico é politico*
<https://podcasts.apple.com/it> (Da ultimo visitato il 28/10/2022).
- [39] Redazione Ansa (2022), *Anche scienziati tra utenti che potrebbero lasciare Twitter* https://www.ansa.it/canale_scienza/ (Da ultimo visitato il 07/11/2022).
- [40] Vox (2020), *How ads follow you around the internet*
<https://www.youtube.com/> (Da ultimo visitato il 28/10/2022).
- [41] Zeynep (2017), *We're building a dystopia just to make people click on ads*
<https://www.ted.com/talks> (Da ultimo visitato il 28/10/2022).