**ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA**

**Corso di Laurea in**
**Scienze della Comunicazione**

# LA RICCHEZZA DEL NUOVO MILLENNIO: I NOSTRI DATI

Tesi di Laurea in

Diritto dell'Informazione e della Comunicazione

**Relatore:**
**Prof. Daniele Donati**

**Presentata da:**
**Nadia Lenzi**

**Appello II**

**Anno Accademico 2020-2021**

# INDICE

**CAPITOLO 3**

**IL CASO DI FACEBOOK E CAMBRIDGE ANALYTICA**

## *INTRODUZIONE*

L'obiettivo di questa tesi è offrire una riflessione sull'inestimabile valore che i nostri dati personali stanno conquistando per le aziende e i conseguenti rischi per la privacy delle persone. Sempre più abitualmente in rete, e non solo, vengono offerti agli utenti servizi gratuiti in cambio della condivisone di alcune informazioni specifiche, solitamente sono sempre compresi il nome, il cognome e l'indirizzo e-mail.

I nostri dati sono ormai diventati una nuova forma di pagamento e prima di regalarli a qualcuno bisognerebbe fare un'attenta considerazione sul valore che questi posseggono per le aziende che li richiedono e su come vengono utilizzati. Ad oggi, per legge, le persone devono sempre essere messe al corrente delle finalità di utilizzo dei loro dati e hanno la possibilità di consentire o negare il trattamento attraverso l'accettazione o il rifiuto dei termini e delle condizioni d'uso, troppo spesso però si tratta di documenti che vengono firmati o accettati senza essere stati letti.

È quindi ormai frequente barattare i propri dati in cambio di un prodotto o un servizio, ma cosa se ne fanno le aziende di questi dati e quali sono i rischi per la nostra privacy? Dopo un excursus storico sulla nascita e l'evoluzione del diritto alla privacy si è cercato di rispondere a queste domande trattando il tema della profilazione in rete e, più nel dettaglio, sui *social network*. È principalmente sui *social* infatti che i dati delle persone vengono utilizzati e analizzati, ce ne rendiamo conto per esempio quando sulla *home* di Facebook o Instagram si mette "mi piace" ad un post o a una foto che ha determinati contenuti e immediatamente dopo appaiono pubblicità sponsorizzate analoghe agli argomenti cui avevamo manifestato interesse. Infine viene ripercorso lo scandalo che vede coinvolto il famosissimo *social* Facebook, una società di consulenza britannica di nome Cambridge Analytica e i dati di milioni di utenti.

# CAPITOLO 1

# IL DIRITTO ALLA PRIVACY E LA SUA EVOLUZIONE

## 1.1 La nascita del diritto alla privacy

Le origini moderne del diritto alla privacy risalgono alla fine dell'Ottocento, quando la vita delle persone inizia a cambiare profondamente in seguito ai mutamenti sociali ed economici dovuti allo sviluppo di nuove tecnologie come la fotografia, il telefono e la stampa. I progressi tecnico-scientifici hanno da sempre apportato numerosi benefici alla vita delle persone, ma hanno anche accresciuto i rischi di incorrere in situazioni potenzialmente lesive per la privacy delle stesse. È in questo contesto che i due avvocati statunitensi Samuel Warren e Louis Brandeis scrivono il saggio *The right to privacy.*

Nel 1882 Samuel Warren prese in sposa Mabel Bayard, figlia del senatore Thomas F. Bayard. La stampa aveva sempre nutrito un forte interesse per la vita dei propri rappresentanti politici e quella della figlia del senatore non fece eccezione. Sin dal giorno del suo matrimonio, definito dal reporter inviato come "il matrimonio dell'anno per il quale c'erano state speranze e paure, battiti di cuore e silenziosi desideri[1]", Warren percepì la stampa come invadente ed ebbe l'intenzione di contenerla con l'aiuto del già allora collega Brandeis. Negli anni successivi ci furono diverse pubblicazioni sui giornali riguardanti la vita di Warren e della moglie, articoli che riguardavano eventi mondani, ma anche cose molto private. In particolare la moglie di Warren perse, nel giro di due settimane, sia la madre che la sorella e la notizia apparse sulle prime pagine dei giornali dell'epoca con commenti, descrizioni e resoconti dei funerali. L'anno successivo a questi eventi il senatore Thomas F. Bayard si risposò con una donna più giovane e il *gossip* sui giornali non si fece attendere. Warren e Brandeis elaborarono una causa contro le indiscrezioni sulla vita della moglie dello stesso Warren da parte della *Evening Gazette* di Boston ritrovandosi a riflettere su quali informazioni riguardanti la vita privata di una persona potessero essere di pubblico dominio e quali, invece, meritassero una protezione dall'invadenza altrui.

[1] Si veda GDPC, *Privacy: le origini*, [online], gdpc.altervista.org, 09.01.20 <www.gdpc.altervista.org> (ultimo accesso: 08.07.21).

Il 15 dicembre 1890 i due avvocati pubblicano sulla celebre rivista *Harvard Law Review* l'articolo *The Right to Privacy* riconoscendo un generale diritto alla privacy. In questo articolo il diritto alla privacy veniva esplicitato come *the right to be let alone* ovvero "il diritto ad essere lasciati soli", dove la funzione della riservatezza era quella di riparare dagli attacchi di un giornalismo che era finalizzato a scandalizzare più che informare. La tesi dei due giuristi merita attenzione ancora oggi considerando l'enorme divario tecnologico che separa il XXI secolo dall'epoca in cui sono vissuti Warren e Brandeis. Nella società odierna, dove l'informazione assume sempre più rilevanza, i potenti strumenti tecnologici che si hanno a disposizione, come i *mass media* dell'informatica e internet, conferiscono all'uomo una grande libertà di espressione e possibilità di informazione e conoscenza, ma al contempo rischiano di trasformarlo in un "uomo di vetro"[2]. Nato negli Stati Uniti con l'accezione di "diritto ad essere lasciati soli" il diritto alla privacy oggi indica il diritto alla riservatezza delle informazioni personali e della sfera privata dell'individuo.

### 1.2 L'evoluzione normativa in Italia e in Europa

In Italia la Costituzione nasce in un momento storico in cui la disciplina in materia di privacy era del tutto assente, eppure si possono rintracciare alcuni riferimenti che anticipano le norme sul tema negli articoli 14, che tutela il domicilio della persona, 15, che tutela la liberà e la segretezza della corrispondenza e 21, che tutela invece la libertà di manifestazione del pensiero. Un primo accenno alla privacy è oggi riconosciuto nell'articolo 2 che la include tra i diritti inviolabili dell'uomo[3].

Una delle prime sentenze a lambire il tema della privacy fu quella della Corte di Cassazione n. 4487 del 1956: in seguito all'uscita dell'opera cinematografica "Leggenda di una voce" gli eredi del tenore napoletano Enrico Caruso intentarono azione contro la casa produttrice del film che aveva raccontato in forma romanzata la vita del tenore descrivendolo come di bassa estrazione e mostrandolo in stato di ebrezza. Con questa sentenza fu identificato il diritto alla privacy nella tutela delle situazioni e vicende personali e familiari che non hanno per i terzi un interesse socialmente utile, si siano esse

[2] Si veda G. Fioriglio, *Privacy. Evoluzioni e cenni sulla normativa*, Roma, 2019, p. 2.
[3] Con la sentenza n. 38 del 1973 la Corte Costituzionale ha osservato che l'articolo 21 della Costituzione (principio della libertà di manifestazione del pensiero) incontra un primo limite nell'articolo 2 della Costituzione.

verificate all'interno o all'esterno del domicilio domestico. Di seguito vi furono ulteriori sentenze sul tema, come quella del 1963 riguardante il caso di Claretta Petacci[4]. Attraverso la citazione dell'art. 8 della CEDU[5], ratificata in Italia con la Legge 4 agosto 1955, n. 848[6], ai sensi della quale "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza", venne ritenuta fondata la pretesa dei familiari di Claretta Petacci a non raccontare in un libro vicende private in assenza di interesse pubblico.

Nelle sentenze sopracitate non si riconosce formalmente il diritto alla privacy inteso come diritto alla riservatezza, ma si riconosce la necessità di una tutela in tale ambito. In seguito a queste pronunce, il legislatore interviene emanando lo Statuto dei lavoratori che segna un passo in avanti per la tutela della privacy in quanto contenente alcune previsioni a tutela degli stessi[7]. Tale legge è però applicabile solo nell'ambito lavorativo e pertanto si è reso necessario un intervento legislativo che riconoscesse e tutelasse il diritto alla riservatezza in maniera più ampia.

È a metà degli anni Settanta, ed in particolare con la pronuncia della Corte di Cassazione sul c.d. caso Soraya, che si riconosce per la prima volta in Italia in modo esplicito il diritto alla privacy[8]. La questione verte sulla richiesta di risarcimento portata avanti da Soraya Esfandiary, ex imperatrice dell'Iran, per danno all'immagine. La donna era stata fotografata all'interno della propria dimora in atteggiamenti intimi con un uomo, e a causa di ciò in seguito era stata ripudiata dal marito. Nel 1975 la Cassazione sancisce il diritto di Soraya al risarcimento del danno stabilendo che

> il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente

[4] Cass. Civ. 20 aprile 1963 n. 990.
[5] Art. 8 Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, *Diritto al rispetto della vita privata e familiare.*
[6] Legge n. 848, 4 agosto 1955, Ratifica ed esecuzione della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 e del protocollo addizionale alla convenzione stessa, firmata a Parigi il 20 marzo 1952.
[7] Tra le più significative si può segnalare il divieto di utilizzo di impianti audiovisivi per finalità di controllo a distanza (art. 4) e il divieto di svolgere indagini su opinioni politiche, religiose o sindacali (art. 8). Si veda Legge n. 300, 20 maggio 1970, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale edell'attività sindacale nei luoghi di lavoro e norme sul collocamento.
[8] Cass. Civ. Sez. I. 27 maggio 1975, n. 2129.

speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti. (Cass. Civ. 2129/1975)

Negli anni Ottanta il dibattito in materia di privacy si accende in seguito all'esigenza di bilanciare il diritto all'informazione con quello alla tutela della reputazione e dell'onore delle persone. L'elaborazione di criteri di bilanciamento si deve alla Sentenza della Cassazione n. 5259 del 1984 (c.d. sentenza Decalogo[9]) che ha individuato le condizioni "scriminanti[10]" con riguardo a informazioni dal contenuto potenzialmente ingiurioso o diffamatorio, rappresentando al tempo stesso i limiti all'esercizio del diritto di cronaca.

Per quanto riguarda il contesto Europeo, nel 1950 viene adottata la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), volta a tutelare i diritti umani e le libertà fondamentali degli stati aderenti. Con lo sviluppo di nuove tecnologie e nuovi mezzi dell'informazione e di comunicazione si avverte sempre più il bisogno di tutelare in modo adeguato il diritto alla riservatezza delle persone. Per questa ragione il Consiglio d'Europa adotta la Convenzione n. 108 del 1981[11] che rappresenta un importante documento per la protezione dei dati personali delle persone riguardante il trattamento automatizzato di dati. La Convenzione ha infatti come oggetto le "collezioni automatizzate di dati a carattere personale e all'elaborazione automatica di tali dati nei settori pubblico e privato". Viene offerta qui una definizione di dato personale, quale dato relativo ad una persona fisica identificata o identificabile. L'importanza della Convenzione è data anche dal suo essere vincolante a livello internazionale poiché possono aderirvi anche paesi non facenti parte dell'Unione Europea.

Nel 1992 il processo di integrazione del mercato unico europeo arriva al culmine con il Trattato di Maastricht e la creazione della Comunità Europea. È pertanto necessario avere una normativa a livello europeo sulla protezione dei dati personali poiché in seguito

[9] Cass. Civ. Sez. I. 18 ottobre 1984, n. 5259.
[10] Si tratta di condizioni che limitano l'esercizio del diritto di cronaca imponendo di utilizzare espressioni ingiuriose o diffamatorie solo al ricorrere dei seguenti presupposti: l'utilità sociale del contenuto dell'informazione, la verità dei fatti esposti e la continenza delle espressioni, ossia l'utilizzo di una forma espositiva civile.
[11] Convenzione di Strasburgo n. 108/1981. Tra il 2016 e il 2018 il testo della Convenzione viene rivisto in funzione delle nuove sfide tecnologiche e il 18 maggio 2018 viene approvato un nuovo testo noto come Convenzione 108+ che presenta alcune innovazioni volte a garantire flessibilità, trasparenza e solidità, facilitando il passaggio dei dati attraverso le frontiere, assicurando al contempo garanzie contro gli abusi. Tra le innovazioni si possono segnalare una maggiore responsabilità dei titolari del trattamento, l'obbligo di dichiarare *data breach*, una maggiore trasparenza nel trattamento dei dati e nuovi diritti per le persone per quanto riguarda processi decisionali automatizzati.

ad un mercato unico anche i dati devono poter circolare liberamente. Viene quindi emanata in data 24 ottobre 1995 la Direttiva n. 46, anche nota come "Direttiva madre", in materia di tutela delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La scelta di emanare una Direttiva e non un Regolamento è stata elaborata poiché all'epoca la protezione dei dati era agli esordi e non era possibile adottare una norma uniforme e vincolante per tutti gli Stati. Fu quindi permesso a ciascun paese di interpretare la Direttiva e di adottare norme nazionali per recepirla. In particolare, in Italia la Direttiva è stata attuata con Legge n. 675, 31 dicembre 1996, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" (c.d. Legge sulla privacy).

In pochi anni la Legge sulla privacy ha subito numerose modifiche ed è stata abrogata dal d.lgs. 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali". Il Codice è diviso in tre parti: nella prima vi sono le disposizioni generali, nella seconda alcune disposizioni specifiche riguardanti i trattamenti irrinunciabili per perseguire obblighi legali o per eseguire compiti di interesse pubblico e nella terza le norme relative alle forme di tutela, alle sanzioni ed all'ufficio del Garante per la protezione dei dati personali. All'art. 23 del Codice è previsto il diritto a non vedere trattati i propri dati personali in assenza di consenso, ma anche l'adozione di cautele tecniche ed organizzative che tutti devono rispettare per procedere in maniera corretta al trattamento dei dati altrui.

L'Unione Europea nel 2012 ha intrapreso un lungo cammino finalizzato all'individuazione di nuove regole comuni a tutti gli Stati membri in materia di tutela dei dati personali. Alla base di tale decisione vi era, innanzitutto, la convinzione che il sistema di norme vigenti, operanti sotto la "Direttiva madre", non fosse più in più grado di far fronte in maniera adeguata alle complesse sfide provenienti dall'utilizzo sempre più intenso di tecniche di profilazione e tecnologie di comunicazione. La Commissione Europea presenta quindi il "pacchetto protezione dati" che si compone di due diversi strumenti: una proposta di Regolamento relativo alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" e una proposta di Direttiva per regolamentare la prevenzione, il contrasto, la repressione dei crimini e l'esecuzione delle sanzioni penali. Il 4 maggio 2016 il Regolamento e la Direttiva vengono pubblicati sulla Gazzetta Ufficiale dell'Unione Europea. Il

Regolamento, noto come General Data Protection Regulation (GDPR[12]), è entrato in vigore il 24 maggio 2016 ed è diventato operativo a partire dal 25 maggio 2018. Il GDPR ha abrogato la direttiva 95/46/CE, che fino a quel momento aveva rappresentato il principale strumento giuridico in materia di protezione dei dati personali in ambito europeo.

### 1.3 GDPR: General Data Protection Regulation

Il Regolamento generale per la protezione dei dati personali 2016/679 (*General Data Protection Regulation* o GDPR) è la principale normativa europea in materia di protezione dei dati personali e si compone di 173 considerando e 99 articoli, questi ultimi suddivisi in 11 capi. L'adozione di un Regolamento in materia di protezione dati personali avrebbe permesso di assicurare la protezione degli stessi in tutta l'Unione Europea poiché dotato di una maggiore incisività rispetto alla Direttiva 95/46/CE.

Il Regolamento prevede misure da mettere in atto per regolare sia il trattamento che la libera circolazione dei dati delle persone fisiche, garantendo a queste ultime diversi diritti: il diritto di informazione, consistente nel diritto ad ottenere le informazioni su quanti e quali dati vengono trattati dal titolare; il diritto di accesso, consistente nella possibilità di ottenere dal titolare i dati che ha in possesso in maniera chiara; il diritto di vedere aggiornati o rettificati i propri dati; il diritto alla cancellazione dei dati, meglio noto come diritto all'oblio; la possibilità di esercitare l'opposizione totale o parziale al trattamento dei dati; il diritto di revoca del consenso in qualsiasi momento; il diritto di opposizione ai trattamenti automatizzati e a non essere sottoposti a trattamenti di profilazione basati su decisioni totalmente automatizzate; il diritto di trasformazione in forma anonima dei dati; il diritto di chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento; il diritto alla portabilità dei dati, cioè la facoltà per l'interessato di ricevere i dati personali che lo riguardano e di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare originario.

L'introduzione del GDPR ha comportato la necessità di adeguare la normativa nazione alle disposizioni del GDPR, modificando quella contenuta nel Codice Privacy italiano. A tale fine è stato emanato il d.lgs. 101/2018, recante "Disposizioni per

[12] Regolamento UE 2016/679, *Regolamento generale sulla protezione dei dati*.

l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

La prima definizione che si incontra nel GDPR è quella di dato personale, da intendersi come

> 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 (Art. 4, GDPR)

Il dato personale concerne qualsiasi informazione riguardante una persona, come la sua situazione economica, la sua salute o i suoi gusti. Un'altra definizione importante è quella di *trattamento*, inteso come

> 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. (Art. 4, GDPR)

Questa definizione chiarisce come qualsiasi operazione compiuta su un dato personale si caratterizzi come trattamento, anche la semplice raccolta di un dato.

Tra le principali novità apportate dal Regolamento del 2016 vi è l'introduzione di alcuni principi. Il principio cardine del nuovo Regolamento è quello di *accountability*[13]. Si tratta del concetto di responsabilizzazione secondo il quale il titolare del trattamento, ovvero colui che determina le finalità e i mezzi del trattamento di dati personali, è obbligato ad attuare delle misure organizzative opportune per garantire il rispetto del Regolamento ed essere in grado di documentare e dimostrare che il trattamento dei dati sia stato effettuato secondo il rispetto del Regolamento europeo. Ad integrare il principio di *accountability* vi sono i principi di *privacy by design e privacy by default*[14]. Il primo

[13] Art. 24 General Data Protection Regulation.
[14] Art. 25 General Data Protection Regulation.

impone alle aziende l'obbligo di avviare un progetto prevedendo sin dall'inizio i rischi che si possono incontrare nella tutela dei dati personali, ancor prima che il trattamento cominci. Il secondo implica che le imprese trattino i dati personali solamente per le finalità e il periodo strettamente necessario al raggiungimento dei propri fini. In questo modo viene imposto il divieto di ricorrere all'utilizzo dei dati senza motivi specifici. Tra le misure di sicurezza che vengono considerate adeguate può essere presa ad esempio la crittografia *end-to-end* utilizzata dalla famosa applicazione di messaggistica Whatsapp. Questa misura di sicurezza impedisce che il messaggio che viene inviato da un mittente ad un ricevente possa essere letto da una terza persona poiché i messaggi vengono codificati e decodificati al momento dell'invio e della ricezione.

Con l'introduzione di questi principi è stato sostituito l'approccio prescrittivo del Codice Privacy, il quale prevedeva delle misure minime di sicurezza che tutti i titolari dovevano adottare, con un approccio basato sul rischio inteso come la combinazione della probabilità che un evento si verifichi e dell'impatto che esso può avere. Nella valutazione dei rischi si deve tenere conto anche del tipo di dati trattati, per esempio i dati che coinvolgono minori prevederanno obblighi maggiormente rilevanti.

Sulla base dei principi di *accountability, privacy by design, privacy by default* e dell'approccio basato sul rischio, il GDPR ha previsto l'adempimento obbligatorio del *data protection impact assessment (*dpia)[15]. Si tratta di una valutazione d'impatto che permette di assicurare trasparenza e protezione nelle operazioni di trattamento dei dati personali. Il titolare si serve di questo strumento per effettuare l'analisi dei rischi sviluppando, prima di iniziare un qualsiasi trattamento, una valutazione delle possibili conseguenze. Durante lo svolgimento di tale valutazione il titolare deve confrontarsi con una nuova figura introdotta dal Regolamento: il *data protection officer* (DPO)[16] che ha il compito di fornire un parere sulla valutazione d'impatto. Il *data protection officer* è il responsabile della protezione dati e ha la funzione di informare, sorvegliare e cooperare con il titolare, gli addetti e i responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo.

Il nuovo Regolamento europeo nasce quindi dall'esigenza di tutelare le persone fisiche in seguito allo sviluppo di sempre più efficienti e articolati metodi e strumenti tecnologici di raccolta dati. Per questo viene chiarito dal GDPR che l'informativa da

[15] Art. 35 General Data Protection Regulation.
[16] Art. 37 e Art. 39 General Data Protection Regulation.

rendere agli interessati deve essere concisa, trasparente, facilmente accessibile, con un linguaggio semplice e chiaro. Deve essere comprensibile per tutti quindi si può far uso anche di icone o disegni. L'interessato deve essere in grado di esprimere in maniera chiara e dimostrabile il consenso. Inoltre qualsiasi *data breach,* cioè qualsiasi violazione dei dati personali derivante da attacchi informatici o incidenti, deve essere notificata entro 72 ore al Garante[17], l'autorità di controllo designata ai fini dell'attuazione sulla protezione dei dati personali.

[17] Art. 51 General Data Protection Regulation.

# CAPITOLO 2

# PRIVACY E PROFILAZIONE

## 2.1 La profilazione

### *2.1.1 Definizione e soggetti coinvolti*

Non sempre quando i dati delle persone finiscono in possesso di qualcun altro si è verificato un *data breach*. Capita di frequente che i dati vengano raccolti da soggetti pubblici o privati al fine della profilazione, attività di raggruppamento ed elaborazione di dati che ha lo scopo di incrociare le informazioni ottenute al fine di costruire i profili dei singoli utenti. Vi sono almeno due tipi di informazioni che possono essere reperite e che riguardano un soggetto determinato: in primo luogo vi sono le informazioni primarie, ovvero i caratteri personalissimi dell'individuo come nome e cognome; in secondo luogo le informazioni secondarie, inerenti le abitudini sociali ed i gusti commerciali dell'utente interessato. Sono proprio questi due tipi di informazioni che, elaborate tra loro, permettono la profilazione dell'utente.

L'obiettivo principale della profilazione è la creazione della pubblicità comportamentale che, soprattutto all'interno di siti *web* e *social*, prevede il tracciamento delle informazioni rilasciate dagli utenti durante la navigazione in internet al fine di mostrare le inserzioni pubblicitarie più appropriate per ogni persona, sulla base quindi degli interessi del singolo soggetto non solo per l'acquisto di beni, ma anche per i servizi.
Il GDPR definisce e regolamenta la profilazione all'articolo 4, definendola come

> qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica (Art. 4, GDPR)

Secondo la definizione offerta dal GDPR la profilazione prevede un trattamento automatizzato che viene eseguito sui dati personali e che ha lo scopo di valutare gli aspetti più personali di una persona, ma la definizione sembrerebbe prendere in considerazione

solo il trattamento automatizzato dei dati, non comprendendo i trattamenti manuali quali, per esempio, l'intervento di una persona nell'attività di profilazione. In realtà al considerando numero 24 del GDPR la profilazione viene considerata come una tecnica di trattamento che può essere anche solo in parte automatizzato.

### *2.1.2 Strumenti della profilazione: i cookies*

La profilazione non è una pratica recente e non viene effettuata solo *online*. Esiste infatti anche la profilazione *offline,* che viene svolta, ad esempio, mediante questionari cartacei. Vero è che oggi la profilazione si manifesta soprattutto *online*, e specialmente attraverso i cc.dd. *cookies.* Si tratta di piccole stringhe di codice che vengono memorizzate sui dispositivi utilizzati per navigare in internet, contenenti un codice in formato testo e diversi dati come il *server* da cui proviene e un identificatore numerico. Quando un utente si muove all'interno di un *sito web,* solitamente scarica *cookies* presenti sul sito. Questi svolgono funzioni utili per il visitatore, ma ce ne sono alcuni che tengono traccia della navigazione effettuata sui siti internet.

I *cookies* hanno pertanto due funzioni fondamentali: far funzionare un sito o un'applicazione e monitorare le attività di un utente. I primi sono chiamati *cookies* tecnici perché possono rendere più efficace e veloce la navigazione e l'utilizzo del sito *web,* i secondi sono detti *cookies* di profilazione. Questi ultimi hanno lo scopo di memorizzare la navigazione effettuata dall'utente sui siti internet in modo da determinare un profilo dell'utente in base ai suoi gusti e alle sue abitudini per poi proporgli messaggi pubblicitari in linea con le sue preferenze. Vista la particolare invasività di questi *cookies,* esiste una puntuale regolazione a livello europeo in materia.

I soggetti che vengono sottoposti alla profilazione hanno diversi diritti, ai sensi dell'articolo 21 del GDPR i soggetti hanno il diritto di opposizione. Se qualcuno non vuole che i propri dati vengano raccolti per finalità di profilazione egli ha infatti il diritto di esprimere il proprio dissenso. Al considerando numero 58 del GDPR viene riconosciuto il diritto di informazione, che, perseguendo il principio di trasparenza, consente al soggetto di ricevere informazioni concise e di facile comprensione, deve essere infatti utilizzato un linguaggio chiaro e semplice. Anche al considerando numero 61 del GDPR viene tutelato il diritto di informazione dell'individuo, egli infatti deve essere sempre messo al corrente dell'uso che si sta facendo dei suoi dati personali. Ai

sensi del considerando numero 63 del GDPR il soggetto che è stato profilato ha poi il diritto di accesso, ossia la possibilità, se lo desidera, di accedere al profilo che è stato creato in base ai dati che ha fornito e in base ai suoi comportamenti. Un ulteriore diritto in capo al soggetto profilato è il diritto di rettifica o di cancellazione espresso dal considerando numero 39 del GDPR, in base al quale l'utente ha diritto di chiedere che il suo profilo e i suoi dati raccolti vengano rimossi o rettificati.

Al fine di tutelare le persone, il GDPR impone a coloro che vogliono mettere in pratica la profilazione l'obbligo non solo di spiegare in maniera chiara, semplice e concisa le finalità per le quali si intendono raccogliere i dati (considerando 58), ma anche di richiedere in maniera chiara il consenso al trattamento degli stessi da parte dei soggetti. Il considerando numero 32 del GDPR chiarisce infatti che

> il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. (considerando 32, GDPR)

Il consenso può essere manifestato in vari modi: con una dichiarazione scritta, oralmente oppure, come accade più frequentemente, attraverso la selezione di un'apposita casella in un sito *web*. Al considerando 32 viene inoltre sottolineato che il silenzio, l'inattività o la preselezione di eventuali caselle all'interno di siti *web* non configurano il consenso. Pertanto nel momento in cui si accede ad un sito che fa uso di *cookies* deve comparire un *banner* ben visibile in cui vi è un'informativa chiara dove è possibile concedere o negare il consenso all'installazione dei *cookies*, tuttavia l'obbligo del *banner* informativo non sussiste per tutti quei siti che fanno uso solamente di *cookies* tecnici in quanto necessari solamente al corretto funzionamento del sito.

Oltre che per la loro funzione i *cookies* si possono distinguere anche in base alla loro durata e alla loro provenienza. In base alla durata, il primo tipo di *cookie* è detto *cookie* di sessione ed è il più comune: la sua durata è limitata, viene attivato quando l'utente entra su un sito *web* e viene cancellato quando l'utente abbandona il sito. Il suo scopo è quello di riconoscere l'utente che naviga da una pagina ad un'altra del sito in modo che il sistema sappia che si tratta sempre della stessa persona. È utile per esempio per agevolare la navigazione sui siti di *e-commerce* di modo che l'utente possa spostarsi tra le pagine del sito senza perdere gli eventuali oggetti che ha riposto nel "carrello". I *cookies* di sessione differiscono dai *cookies* persistenti che rimangono invece

memorizzati e si cancellano soltanto dopo un certo periodo di tempo, permettendo di riconoscere un utente che torna su un sito già visitato in precedenza.
Sulla base della provenienza si distinguono invece i *cookies* originali e i *cookies* di terze parti: i *cookies* originali sono inviati direttamente dal sito che si sta visitando mentre i *cookies* di terze parti sono gestiti da un altro soggetto.

### 2.2 Processi decisionali automatizzati e profilazione: l'articolo 22 del GDPR

Il processo di profilazione *online* può essere automatizzato in maniera parziale o totale: si considera profilazione in parte automatizzata quando, dopo la creazione del profilo utente, un soggetto ne effettua la valutazione; un processo decisionale interamente automatizzato consiste, invece, in una decisione assunta da un algoritmo senza l'intervento umano. Poiché la profilazione automatizzata, totale o parziale, è sempre più praticata nel *web* in quanto risulta essere efficiente, economica e facilmente applicabile, la legislazione europea si preoccupa di regolamentarla.

Per questa ragione il principio di trasparenza è un requisito fondamentale che viene imposto dal GDPR e riveste un ruolo importante in quanto la conoscenza dei processi tecnologici che sottostanno alla profilazione è diversa per ogni persona. È per questa ragione che, oltre ai diritti già menzionati nel precedente paragrafo, all'articolo 22 del GDPR all'interessato che subisce un trattamento dei suoi dati personali, inclusa la profilazione, viene riconosciuto "il diritto a non essere sottoposto ad una decisione che è basata unicamente su un trattamento automatizzato dei dati che possa produrre effetti giuridici che lo riguardano o che incidano in modo significativo sulla sua persona". La norma richiamata fa pertanto riferimento a quei trattamenti finalizzati a produrre decisioni totalmente automatizzate con effetti giuridici sulle persone oppure con conseguenze rilevanti sulla loro vita[18]. In un contesto che vede uno sviluppo sempre maggiore di intelligenza artificiale e *Machine Learning*, i procedimenti decisionali automatizzati che influiscono sui diritti dei cittadini necessitano di una adeguata regolamentazione. Per questo motivo, la prerogativa dell'articolo 22 è quella di stabilire il diritto del cittadino a pretendere di non essere sottoposto ad un trattamento svolto interamente in forma automatizzata che può condurre ad effetti giuridici sugli interessati.

[18] Ai sensi del considerando 71 GDPR, una decisione che potrebbe influire sui diritti e le libertà degli individui è per esempio il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica che avvengano senza l'intervento umano.

Al secondo paragrafo dell'articolo sono tuttavia previste alcune ipotesi eccezionali al ricorrere delle quali può effettuarsi un trattamento completamente automatizzato di dati. In primo luogo, ciò può accadere quando la decisione risulta essere necessaria al fine di concludere o eseguire un contratto tra l'interessato e un titolare del trattamento; in questo caso il titolare del trattamento deve essere in grado di dimostrare che la profilazione fosse necessaria. In secondo luogo, il trattamento automatizzato può svolgersi quando la decisione è autorizzata dal diritto dell'UE o dello Stato membro cui è soggetto il titolare del trattamento. Ciò in quanto la legislazione degli Stati membri in alcuni casi può autorizzare i processi decisionali interamente automatizzati per il controllo e la prevenzione di frodi, evasioni fiscali e per garantire sicurezza e affidabilità del servizio. Infine, può accadere quando la decisione si basa sul consenso esplicito dell'interessato che deve avvenire tramite una dichiarazione espressa e inequivocabile.

Tali decisioni non possono tuttavia essere prese se riguardanti il trattamento di categorie particolari di dati personali[19] - come i dati che rivelino l'origine etnica, le opinioni politiche, le convinzioni religiose, l'appartenenza o meno ad un sindacato - a meno che l'interessato non abbia manifestato il suo consenso esplicito al trattamento di questa categoria particolare di dati oppure perché il trattamento risulti necessario per motivi di interesse pubblico, rilevante sulla base del diritto dell'Unione o degli Stati membri, essendo comunque proporzionato alla finalità perseguita, rispettando l'essenza del diritto alla protezione dei dati e prevedendo misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato[20].

Quando si fa riferimento al trattamento di dati in maniera interamente automatizzata i rischi sono vari e differenti. Per questo il GDPR chiarisce il diritto dell'interessato non solo a negare il consenso, ma anche a conoscere in cosa consistono i trattamenti che verranno effettuati sui suoi dati. L'interessato ha infatti il diritto di conoscere l'esistenza del processo decisionale automatizzato, di conoscere la logica e i criteri che vengono messi in pratica per raggiungere la decisione e di conoscere le conseguenze che il trattamento dei dati può comportare[21]. Visti i rischi che un trattamento interamente automatizzato può comportare, all'articolo 32 del GDPR viene specificato che il titolare ha il compito di tutelare i dati dell'interessato attuando misure di sicurezza appropriate. Esse comprendono la pseudonimizzazione e la cifratura dei dati personali.

[19] Articolo 9, par. 1 GDPR.
[20] Articolo 9, par 2, lett. *a)* e *g)*
[21] Articolo 13, par. 2, lett. *f)* e Articolo 15, par. 1, lett. *h)* GDPR.

Quest'ultima consiste nel trattamento dei dati in modo tale che essi non possano più essere associati a uno specifico interessato senza l'utilizzo di informazioni aggiuntive. Le misure di sicurezza comprendono anche la capacità di assicurare riservatezza all'utente, la capacità di ripristinare velocemente la disponibilità e l'accesso dei propri dati personali in caso di incidente e una procedura per testare e valutare l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento. Inoltre l'interessato può richiedere, se lo desidera, l'intervento umano[22].

## 2.3 Profilazione nei *social network*

### *2.3.1 Cosa sono i social network*

Oggi il luogo per eccellenza in cui viene praticata la profilazione è quello dei *social network.* Si tratta di servizi informatici *online* che permettono la realizzazione di reti sociali individuali[23]. Una delle caratteristiche principali dei *social network* è la possibilità di elaborare un proprio profilo personale che generalmente comprende il nome e cognome dell'utente, una foto profilo e altre informazioni a seconda del tipo di *social* che si sta utilizzando. Altra caratteristica tipica dei *social network* è la funzione di creare una rete di "amici" che si sviluppa cercando il nominativo del profilo interessato. Solitamente è inoltre prevista la possibilità di esplorare il profilo degli amici o di sconosciuti, di pubblicare e condividere testi, foto o video ed esprimere la propria approvazione, disapprovazione o gradimento attraverso l'uso dei cc.dd. "*like*" o "mi piace". I motivi che possono portare una persona ad entrare a far parte del mondo dei *social network* possono essere vari a seconda della tipologia di *social*: per lavoro, per esempio per cercare offerte d'impiego oppure per pubblicizzare la propria attività; per tenersi in contatto con amici e conoscenti tramite le *chat*, la condivisione di foto o video; per intrattenimento.

Negli ultimi anni i *social* sono diventati il principale mezzo di comunicazione mediatica su internet. Tra le piattaforme più famose vi sono Youtube, popolare per i suoi video e "canali", Whatsapp, famosa applicazione di messaggistica, Instagram e Facebook, due protagonisti nel mondo dei *social network*. Di *social* ne esistono veramente di ogni tipo, per esempio vi sono veri e propri *social network* "professionali". Uno dei più famosi

[22] Articolo 22, par. 3 GDPR.
[23] Definizione Enciclopedia Treccani.

è LinkedIn, nato con lo scopo di far creare all'utente un profilo basato sulle sue esperienze di studio e di lavoro andando così a creare una sorta di curriculum-social visibile a tutti. L'utente ha poi la possibilità di "collegarsi" con altre persone conosciute o meno, talvolta anche suggerite dal *social* stesso. Gli obiettivi sono quelli di trovare un impiego, offrire un lavoro e ottenere referenze dagli altri utenti.

### *2.3.2 Perché i social network sono gratuiti*

Per avere accesso ai *social network* non è necessario sottoscrivere abbonamenti, è infatti sufficiente registrarsi mediante l'utilizzo della propria e-mail e l'accettazione dei termini e delle condizioni d'uso. In questo senso i *social network* sono piattaforme gratuite in quanto non viene richiesto nessun pagamento. Ci si chiede allora come sia possibile che queste piattaforme riescano a garantire questi servizi senza chiedere contributi agli utenti. In realtà gli utenti contribuiscono con i loro dati: attraverso i *social* gli utenti si fanno conoscere, non solo comunicando il proprio nome, cognome, la propria età, ma soprattutto attraverso le manifestazioni di interesse che esprimono comunicando i propri gusti e le proprie idee.

Una volta ottenuti questi dati, i *social* sono in grado di profilare gli utenti in maniera molto dettagliata dividendoli in segmenti. Inoltre, i *social* offrono a chiunque lo desideri l'opportunità di pubblicizzare i propri prodotti e servizi in spazi pubblicitari a pagamento. La possibilità di sponsorizzare ciò che si intende vendere ad un pubblico estremamente segmentato è molto utile perché una delle migliori strategie di marketing è proprio quella di andare a colpire chi potrebbe essere interessato a ciò che si offre. Questo tipo di pubblicità è estremamente efficiente poiché riesce ad intercettare un pubblico specifico che quasi sicuramente è interessato al prodotto o al servizio offerto. Il successo della pubblicità online sta proprio nella sua possibilità di essere visibile solo agli utenti potenzialmente interessati a ciò che si sta mostrando. Il *social* Facebook, per esempio, permette agli utenti di pubblicare degli annunci chiamati Facebook Ads consentendo agli inserzionisti di definire perfettamente il tipo di persone che vogliono raggiungere e questo è possibile grazie ai dati degli utenti che Facebook raccoglie ogni giorno. Per far sì che un annuncio possa apparire solo alle persone che soddisfano determinate caratteristiche, Facebook utilizza i dati dei suoi utenti. È opportuno precisare che i dati delle persone non sono venduti; ciò che viene messo in commercio è la possibilità di utilizzarli in modo anonimo. Così

facendo gli inserzionisti che pagano Facebook non hanno mai accesso alle informazioni personali degli utenti.

### *2.3.3 La Filter Bubble*

Uno dei diversi possibili rischi della profilazione è rappresentato dall'isolamento intellettuale. Chiamato dall'imprenditore e attivista Eli Pariser "*filter bubble*", l'isolamento intellettuale viene paragonato a una bolla di filtraggio, ossia a "quel personale ecosistema di informazioni che viene soddisfatto da alcuni algoritmi", determinando l'effetto della personalizzazione dei dati[24].

Eli Pariser spiega che la responsabilità di questo fenomeno è da attribuire proprio agli algoritmi della profilazione: è infatti unendo tutti gli algoritmi che profilano gli utenti che si ottiene la *filter bubble*. Il problema di avere questo universo personalizzato *online* è rappresentato dal fatto che non si può scegliere cosa far entrare nella propria bolla, ma soprattutto non si può vedere cosa c'è fuori. La bolla che ognuno di noi ha intorno a sé è il frutto di ciò che si fa su internet, ma non sempre rispecchia realmente la persona; spesso le manifestazioni di interesse che si esprimono sui *social network* sono temporanee o fatte con superficialità. Eli Pariser spiega che internet ha grandi potenzialità e che dovrebbe essere utilizzato come uno strumento di connessione con gli altri utenti per conoscere nuove idee, nuove persone e acquisire nuove prospettive, ma se continuerà ad essere utilizzato in questo modo, invece che essere uno strumento di conoscenza potrebbe trasformarsi - se già non è così - in un muro che separa gli utenti.

---

[24] E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, New York, 2011. PARISER, E., *Attenti alle "filter bubble" in rete*, [video file]. L'autore in una conferenza (cfr https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=it#t-511300) spiega come ha capito di trovarsi all'interno di una *filter bubble.* Egli si definisce un progressista, ma non per questo, spiega, non si dimostra disposto ad ascoltare le opinioni dei conservatori, eppure si è accorto che dalla sua pagina Facebook tutti i conservatori sono scomparsi. Questo è accaduto perché il *social network* aveva registrato le sue ricerche e le sue interazioni e, essendo risultato interessato alle idee progressiste, il sistema gli aveva nascosto quelle conservatrici.

# CAPITOLO 3

# IL CASO DI FACEBOOK E CAMBRIDGE ANALYTICA

## 3.1 I soggetti coinvolti

### *3.1.1 Facebook*

Facebook, protagonista nel panorama dei *social network*, nasce nel 2004 all'università di Harvard per opera di Mark Zuckerberg, attuale amministratore delegato della Facebook Inc., e dei suoi compagni di stanza, come servizio gratuito per gli studenti, successivamente aperto anche a ragazzi di altre scuole e università. Lo scopo era quello di far conoscere fra loro i giovani. Riscontrando fin da subito un notevole successo, Facebook venne ampliato anche all'uso commerciale: è infatti attualmente disponibile uno strumento dedicato al *social marketing*, chiamato *Facebook for Business*.

Come per gli altri *social network*, gli utenti possono accedere a Facebook attraverso una registrazione gratuita inserendo alcuni dati personali. Tra le funzionalità di Facebook vi è quella del "*Facebook-Login*": esso permette di iscriversi ad una applicazione utilizzando le stesse credenziali (e-mail e password) con le quali si accede a Facebook. In questo modo l'utente riesce ad accedere rapidamente ai servizi senza ulteriori registrazioni. Tuttavia, diversi problemi sono sorti riguardo all'uso di questa funzione. Quando si effettua un *Facebook-Login* si accetta che il sito al quale ci si sta registrando ottenga alcuni dati personali dell'utente. Le applicazioni e i siti che si servono di questo sistema che offre la possibilità di accedere senza la creazione di nuovi username e password solitamente riguardano attività completamente separate dal *social*, ma che per offrire le proprie prestazioni nel momento in cui l'utente effettua il *Facebook-Login* hanno accesso alle informazioni contenute su Facebook. Fino al 2015 le informazioni a cui avevano accesso queste applicazioni non riguardavano solamente i dati dell'utente che si registrava**,** ma anche quelli di tutti i suoi amici virtuali su Facebook. Le condizioni d'uso del *Facebook-Login* cambiarono in seguito alle conseguenze della creazione dell'applicazione *This is your digital life* per opera del ricercatore Aleksandr Kogan.

### *3.1.2 Aleksandr Kogan*

Aleksandr Kogan, ricercatore presso l'Università di Cambridge, nel 2015 ha realizzato un'applicazione chiamata "*This is your digital life"* con cui le persone potevano ottenere i profili psicologici e di previsione del loro comportamento a partire dalle attività svolte in rete. L'applicazione consentiva alle persone di scoprire il proprio profilo psicologico attraverso un questionario che riguardava gli aspetti della personalità. Per poter utilizzare l'applicazione, agli utenti veniva richiesto di registrarsi tramite il *Facebook-Login.* Con le informazioni ottenute dalle risposte al questionario e dal profilo del *social network,* lo sviluppatore era riuscito a costruire un database di utenti.

### *3.1.3 Cambridge Analytica*

Cambridge Analytica era una società di consulenza britannica fondata nel 2013 dall'informatico Robert Mercer - principale investitore - e Steve Bannon, facente parte del consiglio d'amministrazione ed ex consigliere politico di Donald Trump[25]. La società era specializzata nell'analisi dei dati ricavati dai *social network*: la sua attività consisteva nell'incrociare le informazioni ottenute da quei dati al fine di andare a profilare gli utenti.

Alexander Nix, ex amministratore delegato di Cambridge Analytica, ha spiegato che la società profilava gli utenti servendosi di un modello di analisi psicometrica basata sul metodo "*OCEAN*". Il metodo consisteva nella classificazione degli utenti in una delle cinque tipologie psicologiche che erano state individuate (Openness, apertura mentale; Conscientiousness, scrupolosità; Extroversion, estroversione; Agreeableness, cooperatività; Neuroticism, facilità ad arrabbiarsi), così da riuscire a pubblicizzare il medesimo prodotto tramite messaggi differenti a seconda del profilo psicologico di ognuno[26]. L'algoritmo di cui si serviva Cambridge Analytica era detto di "*microtargeting comportamentale*": grazie all'enorme mole di informazioni ottenute, la società riusciva a far leva non solo sui gusti degli utenti, come attualmente fanno molte altre società di marketing, ma anche sulle loro emozioni riuscendo a diffondere il messaggio più efficace per l'utente nel momento in cui era più predisposto a vederlo.

[25] V. Lanzetta, *Come lo scandalo "Cambridge Analytica" ha cambiato il modo in cui le multinazionali, del web e non, trattano i dati personali*. Tesi di laurea in Giurisprudenza. Università LUISS di Roma, a.a. 2019/20, p. 11.
[26] Concordia Annual Summit, New York, 2016.

Tra le consulenze più importanti che Cambridge Analytica ha svolto si può menzionare il suo lavoro per conto dell'organizzazione Leave.EU, a favore dell'uscita del Regno Unito dall'Unione Europea, e per conto dell'ex presidente americano Donald Trump nella sua campagna elettorale del 2016[27].

Cambridge Analytica è fallita nel 2018 a causa dello scandalo che la vide coinvolta insieme a Facebook[28]. Secondo quanto riportato da due inchieste condotte dai noti giornali *The New York Times*[29] e *The Guardian*[30] era emerso un collegamento fra il *social network* Facebook, l'applicazione di Kogan e Cambridge Analytica dimostrando che quest'ultima era entrata in possesso dei dati di milioni di utenti in modo illecito.

### 3.2 La vicenda

Il lavoro svolto da Cambridge Analytica non era segreto, ma assunse rilievo pubblico con le pubblicazioni del 2018 degli articoli su *The New York Times* e *The Guardian* che riportavano alcune dichiarazioni di Christopher Wylie, l'ex Data Scientist di Cambridge Analytica[31]. Oltre a raccontare ai giornalisti il lavoro di analisi dati che svolgeva presso la società, Christopher Wylie rivelò che Cambridge Analytica era entrata in possesso delle informazioni di milioni di utenti in modo illecito: tali dati erano stati venduti alla società da Alexander Kogan, il quale condivise l'enorme archivio che aveva creato, comprendente informazioni sulla posizione geografica delle persone, gli interessi e le fotografie degli utenti.

La raccolta e lo studio dei dati che fece Kogan nel 2015 non violavano i termini e le condizioni d'uso di Facebook del tempo che prevedevano che gli sviluppatori potessero scaricare i dati delle persone al fine di profilarle. Quello che andava contro ai termini e le

---

[27] V. Lanzetta, *Come lo scandalo "Cambridge Analytica" ha cambiato il modo in cui le multinazionali, del web e non, trattano i dati personali*. Tesi di laurea in Giurisprudenza. Università LUISS di Roma, a.a. 2019/20, p. 38. E. Franceschini, *Cambridge Analytica e il furto dei dati: "Così influenzavano le elezioni"*, [online], Repubblica.it, 18.03.18 <www.repubblica.it> (ultimo accesso: 30.09.21).

[28] B. Simonetta, *Scandalo Cambridge Analytica. Così i nostri dati su Facebook finiscono nel mercato delle app,* [online], ilsole24ore.com, 20.03.18 <www.ilsole24ore.com> (ultimo accesso: 30.09.21).

[29] M. Rosenberg, N. Confessore, C. Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions,* [online], nytimes.com, 17.03.18 <www.nytimes.com> (ultimo accesso: 30.09.21).

[30] C. Cadwalladr e E. Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* [online], Theguardian.com, 17.03.18 <www.theguardian.com> (ultimo accesso: 30.09.21).

[31] The Guardian, *The Cambridge Analytica Files* [video file] https://www.youtube.com/watch?v=FXdYSQ6nu-M, in cui l'ex dipendente di Cambridge Analytica testualmente, ha riferito: "Abbiamo sfruttato Facebook per raccogliere i profili di milioni di persone. E abbiamo costruito modelli per sfruttare quello che sapevamo su di loro e per prendere di mira i loro demoni interiori".

condizioni d'uso del *social network* era la condivisione o l'acquisto dei dati raccolti presso terze parti: Cambridge Analytica non poteva acquistare i dati degli utenti che Kogan era riuscito a raccogliere attraverso il *Facebook-Login*, ma avrebbe dovuto rivolgersi a Facebook perché le condizioni d'uso del *social* imponevano questo. Secondo Mike Schropfer, direttore tecnico di Facebook, furono le informazioni di 87 milioni di utenti, principalmente negli Stati Uniti, ad essere state condivise in modo improprio con Cambridge Analytica[32]. Poiché tra le sanzioni previste da Facebook è compresa la sospensione dell'account, Christopher Wylie affermò che Cambridge Analytica, temendo l'esclusione dal *social*, si autodenunciò nel momento in cui scoprì di avere ottenuto i dati violando i termini e le condizioni d'uso di Facebook.

Dopo le rivelazioni di Wylie, anche Brittany Kaiser, ex direttrice dello sviluppo *business* di Cambridge Analytica, fece alcune rivelazioni raccontando il coinvolgimento politico che poteva aver avuto Cambridge Analytica nella campagna elettorale di Trump del 2016 servendosi dei dati ottenuti illegalmente[33]. I dati ottenuti in maniera illecita sarebbero stati utilizzati da Cambridge Analytica anche a favore della campagna "Vote Leave" in Gran Bretagna a sostegno della Brexit. A dichiararlo fu la giornalista investigativa Carole Cadwalladr, una delle prime a far emergere lo scandalo di Cambridge Analytica attraverso una pubblicazione su *The Guardian*. In particolare, nel 2019, durante una conferenza, affermò che Cambridge Analytica aveva svolto un ruolo importante nell'orientare il consenso del pubblico durante il referendum sulla Brexit e che il referendum si era svolto "nel buio più assoluto perché di fatto si era svolto su Facebook"[34],

---

[32] M. Schrooepfer*, An Update on Our Plans to Restrict Data Access on Facebook*, [online], about.fb.com, 4.04.18 <www.about.fb.com> (ultimo accesso: 30.09.21).

[33] Brittany Kaiser, in un'intervista, ha riferito che: "Cambridge Analytica ha comprato, venduto ed eseguito modellazioni di dati per capire come si sarebbero comportati gli elettori e per convincerli a sostenere Donald Trump, oppure nel caso dei sostenitori di Hillary per spingerli a non credere più in lei e non andare nemmeno alle urne. Questa è la tragedia che la nostra democrazia ha vissuto nel 2016" *(*cfr D. Procaccianti, *Tutti spiati?*, 2020 [video file]. Durante l'intervista (cfr. https://www.youtube.com/watch?v=cckZ6Eom2bU) Brittany raccontò che la campagna di Trump aveva individuato un gruppo target che era stato definito "gli scoraggiabili" composto cioè da persone che dovevano essere scoraggiate all'andare ai seggi perché avrebbero scelto Hillary Clinton e siccome sarebbe stato impossibile convincere a votare per Donald Trump i soldi erano stati spesi per indurli a non votare.

[34] Durante la conferenza (cfr. https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy?language=it#t-230376) la giornalista racconta che nel 2016 si recò a Ebbw Vale (Galles) dove c'era stato il maggior numero di voti favorevoli all'uscita dall'Unione Europea, ma non ne comprese le ragioni. Le persone con le quali parlò affermarono che l'UE non aveva fatto nulla per loro e che erano stanchi degli immigrati. Eppure dalle ricerche condotte dalla giornalista emerse che diversi finanziamenti erano arrivati alla città dall'UE e che quella zona aveva uno dei minori tassi d'immigrazione.

arrivando alla conclusione che per favorire la campagna *Vote Leave* erano state diffuse notizie false.

### 3.3 Conseguenze per Cambridge Analytica e Facebook

Lo scandalo che ha coinvolto Cambridge Analytica e Facebook ha avuto conseguenze decisive per la società di profilazione che a maggio 2018 ha dovuto dichiarare bancarotta[35].

Facebook invece ha dovuto fronteggiare un'importante crisi reputazionale: dopo alcuni giorni dall'uscita delle inchieste sui giornali, Mark Zuckerberg si è scusato pubblicamente in un post riconoscendo le proprie responsabilità e dichiarando che quando era venuto a conoscenza del passaggio di informazioni da Kogan a Cambridge Analytica aveva imposto la cancellazione dei dati, ma solo in seguito alla pubblicazione delle inchieste sui giornali aveva appreso che non erano stati eliminati e per questa ragione sospese i loro servizi solo in un secondo momento[36].

Il 10 e l'11 aprile 2018 Mark Zuckerberg è chiamato davanti al Congresso per rispondere in merito all'utilizzo illecito dei dati di milioni di utenti avvenuto attraverso il suo *social network*. Al Congresso ha ammesso nuovamente le colpe di Facebook, provando comunque a giustificare l'accaduto affermando testualmente: *"*Penso che sia praticamente impossibile avviare un'azienda nella stanza del tuo dormitorio e poi portarla a crescere fino al punto in cui siamo ora senza commettere qualche errore*"*[37]. Il tema della privacy è stato centrale durante la sua audizione. Il senatore Richard Durbin ha provocatoriamente chiesto a Zuckerberg se potesse rivelare a tutti i presenti il nome dell'albergo dove aveva soggiornato e delle persone con cui si era messo in comunicazione. Ottenendo una risposta negativa, il senatore volle sottolineare il valore della privacy che su Facebook si era perso[38].

In vista dell'entrata in vigore del GDPR, lo sviluppatore di Facebook è stato chiamato anche davanti al Parlamento dell'Unione Europea. Il Presidente ha esordito trattando il tema della diffusione di contenuti a scopo terroristico e di notizie false

---

[35] M. Valsania, *Cambridge Analytica travolta dal Datagate: bancarotta e chiusura immediata*, [online], ilsole24ore.com, 02.05.18 <www.ilsole24ore.com> (ultimo accesso: 05.10.21).
[36] M. Piretti, *Scandalo Facebook, Mark Zuckerberg si scusa: "Sono responsabile dell'accaduto"*, [online], dire.it, 22.03.18 <www.dire.it> (ultimo accesso: 05.10.21).
[37] M. Piretti, op.cit.
[38] *Scandalo Facebook - Cambridge Analytica, Zuckerberg alla camera Usa (con traduzione simultanea)*, [video file] https://www.youtube.com/watch?v=msDrnmjMI4s.

attraverso i *social network.* Zuckerberg non ha negato la presenza di questi problemi, ma ha affermato che è anche grazie ai suoi *social* che dopo gli attentati terroristici di Parigi, Londra e Berlino le persone sono riuscite a mettersi in contatto e che Facebook è in grado di rimuovere la maggior parte dei contenuti prima che arrivino agli utenti. Confermando la presenza di notizie false e di interferenze con le elezioni, Zuckerberg si è impegnato a risolvere i problemi al fine di garantire sicurezza, citando il mezzo miliardo di profili falsi che erano già stati rimossi. Sicuramente non aiutato dal tempo a disposizione e dal format[39], lasciò prive di risposta diverse domande che gli erano state poste. Gli venne per esempio chiesto come intendeva garantire la reale cancellazione dei dati che erano stati raccolti e se era possibile non ricevere pubblicità mirata su Facebook. Per quanto riguarda il GDPR, Zuckerberg ha affermato che Facebook si sarebbe messo in regola entro la sua entrata in vigore, ma in realtà seguirono diversi problemi[40].

A fine luglio dello stesso anno, alla crisi reputazionale si è affiancata la crisi finanziaria che ha visto crollare il titolo in borsa. Nello stesso mese, l'autorità britannica garante per la protezione dei dati personali ha inflitto la prima sanzione a Facebook del valore massimo previsto – ossia 500.000 sterline - per stimolare l'interesse pubblico sulla questione della privacy. A fine dicembre 2018 il governo degli Stati Uniti ha fatto causa al *social network* per il caso Cambridge Analytica per il suo fallimento nella protezione della privacy degli utenti[41].

[39] Il tempo a disposizione era di un'ora e il format prevedeva che prima i parlamentari esponessero tutte le domande e che in seguito Zuckerberg prendesse parola per rispondere in un unico momento. (V. Tiani, *Le domande del Parlamento europeo a cui Zuckerberg non ha risposto*, [online], wired.it, 22.05.18 <www.wired.it> (ultimo accesso: 06.10.21) ).

[40] Tra i più recenti si può evidenziare quello che vede coinvolto Max Schrems, a capo dell'associazione per i diritti digitali Noyb, che accusa Facebook di aver aggirato i principi del GDPR secondo i quali l'utente ha il diritto di autorizzare o di rifiutare in maniera esplicita il trattamento dei suoi dati personali. Facebook ha però inserito il trattamento dei dati personali per le pubblicità personalizzate all'interno delle condizioni di servizio (che non possono essere rifiutate). Il *social* aveva inoltre inserito gli annunci personalizzati all'interno dei termini contrattuali in quanto secondo il GDPR un'azienda è autorizzata al trattamento dei dati degli utenti se esso risulta "necessario per l'esecuzione di un contratto". (K. Carboni, *Facebook è sotto accusa per aver "bypassato" il Gdpr*, [online], wired.it, 15.03.21 <www.wired.it> (ultimo accesso: 06.10.21) ).

[41] *Scandalo dati, prima multa a Facebook: 500mila sterline*, [online], rainews.it, 11.07.18 <www.rainews.it> (ultimo accesso: 06.10.21).

## *CONCLUSIONI*

A partire da una analisi storica del concetto di privacy è emerso quanto "il diritto ad essere lasciati soli" di Warren e Brandeis dall'Ottocento ad oggi si sia evoluto e trasformato soprattutto in seguito ai continui mutamenti tecnologici. La "Direttiva madre", nata in seguito alla creazione di un mercato unico europeo e della Comunità Europea, poneva la sua attenzione sul tipo di dati raccolti, ma i continui progressi tecnologici hanno reso difficile per gli utenti riuscire a capire che cosa succede in rete durante la navigazione, quali dati stanno lasciando e in che modo. Per questo in Europa è stato approvato il GDPR che si focalizza sulla responsabilizzazione del titolare del trattamento (principio di *accountability*) e impone alle aziende di mettere in atto delle misure di prevenzione a tutela dell'utente. Ad oggi il GDPR impone alle aziende l'obbligo di trattare i dati delle persone solo dopo un consenso esplicito da parte di queste ultime. Poiché il principio di trasparenza sta alla base del GDPR le aziende sono tenute a chiedere il consenso in modo chiaro, semplice ed esaustivo di modo che esso possa essere accettato o rifiutato in maniera inequivocabile.

In un mondo sempre più interconnesso il GDPR cerca di dare un ordine all'enorme flusso di informazioni delle persone in rete. I dati sono molto preziosi per le aziende che se ne servono per profilare gli utenti e offrigli la pubblicità più indicata per loro, raccogliendo i dati delle persone infatti sono in grado di "targettizzarle". Per esempio una scuola guida avrà più interesse ad apparire nelle ricerche dei neodiciottenni al posto che nelle ricerche dei minorenni oppure un ristorante di Milano avrà poco interesse ad apparire nella *home* di Facebook di persone che vivono a Catania così come una macelleria non otterrà nulla ad apparire nei risultati Google di una persona vegetariana o vegana. Tutte queste informazioni (età, posizione geografica, gusti personali e tante altre) sono estrapolabili dalle nostre attività in rete.

Terreno fertile per la profilazione è quello dei *social network*. Essi sono infatti i principali fornitori di spazi pubblicitari per le aziende, conoscendo bene gli utenti essi sono in grado di indirizzare le pubblicità delle aziende verso le persone che sono più disposte e vederle. Sin dal momento della registrazione ai *social* condividiamo le nostre informazioni: il nostro nome, cognome e indirizzo e-mail, ma facciamo molto di più. Attraverso i "mi piace" (funzione ormai presente su ogni piattaforma *social*), i commenti o le condivisioni mostriamo quali sono i nostri interessi. Inoltre attraverso la creazione di

una rete di amici è possibile risalire a quali sono i tipi di persone che ci piacciono, al punto che spesso è il *social* stesso a consigliarcele. Quando ci registriamo gratuitamente ad un *social network* è necessario essere consapevoli di questi fatti. Si tratta di informazioni che per legge sono contenute nei termini e nelle condizioni d'uso che siamo tenuti ad accettare se vogliamo entrare a far parte del mondo virtuale, ma che non vengono lette quasi mai. A seconda di chi li raccoglie o li usa, i nostri dati possono essere elaborati per gli obiettivi più vari: dalla creazione di pubblicità comportamentale alla personalizzazione dell'esperienza degli utenti in rete (che talvolta potrebbe essere finalizzata ad influenzare le nostre opinioni).

Per quanto riguarda il caso che ha coinvolto Facebook e Cambridge Analytica è interessante riflettere sui termini e le condizioni d'uso che erano previsti da Facebook al momento dei fatti: uno sviluppatore che sceglieva di servirsi del *Facebook-Login* (nel caso specifico si trattò di Kogan) poteva avere accesso non solo ai dati personali dell'utente che utilizzava l'applicazione, ma anche a quelle di tutti i suoi amici virtuali. In questo modo un utente Facebook cedeva i suoi dati agli sviluppatori anche senza ricorrere ad applicazioni particolari, ma semplicemente essendo "amico" di un utente che le utilizzava. Si potrebbe pensare che se i termini e le condizioni fossero stati letti forse ci sarebbero stati meno iscritti a Facebook, eppure ad oggi, dopo lo scandalo di Cambridge Analytica, molti altri casi di lesione della privacy degli utenti e una maggiore trasparenza del *social,* che nei termini e nelle condizioni d'uso spiega molto chiaramente in che modo i nostri dati vengono "affittati" alle aziende per fini di profilazione, continua ad essere scaricato e utilizzato da milioni di utenti.

In questo panorama digitale in continuo sviluppo è importante essere consapevoli del valore dei dati. Le nostre informazioni e le azioni che compiamo ogni giorno in rete, sui *social* e non solo, possono essere convertite in dati ed è importante conoscere la qualità che questi dati hanno assunto negli ultimi anni. La velocità con cui lo sviluppo tecnologico sta progredendo pone delle sfide costanti alla legislazione che dovrà essere sempre più attenta e abile nel far rispettare il GDPR e creare in futuro ulteriori regolamentazioni qualora risultasse necessario.

**BIBLIOGRAFIA**


Bianca, M., *La filter bubble e il problema dell'identità digitale*, [online], in Rivista di diritto n. 2/2019.

Bonavita, S., Pardolesi, R., *GDPR e diritto alla cancellazione (oblio)*, 2018.

Cass. Civ. Sez I. 22 dicembre 1956, n. 4487.

Cass. Civ. 20 aprile 1963, n. 990.

Cass. Civ. Sez. I. 27 maggio 1975, n. 2129.

Cass. Civ. Sez. I. 18 ottobre 1984, n. 5259.

Di Ciollo, G., *L'ambito di applicazione della normativa privacy: analisi comparata tra GDPR e direttiva 95/46/CE*, in Rivista Semestrale di Diritto Ius in Itinere, 14.07.19.

Fioriglio, G., *Privacy. Evoluzioni e cenni sulla normativa*, Roma, 2019.

Gorla, S., Iaselli, M., *Storia della privacy*, Roma, 2015.

Lanzetta, V., *Come lo scandalo "Cambridge Analytica" ha cambiato il modo in cui le multinazionali, del web e non, trattano i dati*, Tesi di laurea in Giurisprudenza. Università LUISS di Roma, a.a. 2019/20.

Mantelero, A., *GDPR tra novità e discontinuità – gli autori del trattamento dati: titolare e responsabile*, 2019.

Messina, D., *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *federalismi.it, rivista di diritto pubblico italiano, comparato, europeo*, n.20, 2018.

Soro, A., *La protezione dei dati personali nell'era digitale*, 2019.

**SITOGRAFIA**


Assiteca S.p.A., *Privacy: cos'è il diritto alla privacy e perché è bene tutelarlo*, [online], assiteca.it, 05.03.21, <www.assiteca.it>.

Baldon, V., *Cambridge Analytica: dopo due anni, cos'è cambiato?,* [online], instantdeveloper.com, 14.04.20, <www.instantdeveloper.com>.

Bassa, F., *GDPR e Marketing: la profilazione*, [online], privacylab.it, 25.06.21 <www.privacylab.it>.

Cadwalladr, C., Graham-Harrison, E., *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* [online], Theguardian.com, 17.03.18 <www.theguardian.com>.

Cadwalladr, C., *Il ruolo di Facebook nella Brexit – e le minacce alla democrazia*, 2019 [video file], https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy?language=it#t-230376)

Capalbo, M., *This is your digital life*, [online], ermeticamente.it, 05.04.18, <www.ermeticamente.it>.

Carboni, K., *Facebook è sotto accusa per aver "bypassato" il Gdpr*, [online], wired.it, 15.03.21 <www.wired.it>.

Castroreale, R., *Processo decisionale automatizzato e profilazione: cosa sono, differenze e sinergie*, [online], agendadigitale.eu, 22.10.20 <www.agendadigitale.eu>.

Cosimi, S., *Cambridge Analytica, il caso dalla A alla Zuckerberg*, [online], repubblica.it, 22.03.18, <www.repubblica.it>.

Crisci, D., *Privacy: profili di diritto comparato*, [online], diritto.it, 08.10.18 <www.diritto.it>.

Donofrio, V. M., *La protezione dei diritti nell'era digitale: tratti essenziali e capisaldi normativi*, [online], altalex.com, 12.08.20, <www.altalex.com>.

Fasoli, G., Fellin, E., Franceschetto, S., Guaita, M., Imbalzano, F., Lussignoli, A., Manzoni, C., *La profilazione online: risorsa o rischio?,* [online], culturedigitali.org, 25.05.20, <www.culturedigitali.org>.

Ferrari, M., *Facebook non è gratis: l'utente "paga" il servizio con i propri dati personali*, [online], altalex.com, 14.04.21, <www.altalex.com>.

Franceschini, E., *Cambridge Analytica e il furto dei dati: "Così influenzavano le elezioni"*, [online], Repubblica.it, <www.repubblica.it>.

GDPC, *Privacy: le origini*, [online], gdpc.altervista.org, 09.01.20 <www.gdpc.altervista.org>.

Iaselli, M., *Big Data, il problema della profilazione e della dispersione dei dati personali*, [online], federprivacy.org, 05.10.19 <www.federprivacy.org>.

Miranda, C., *Dalla direttiva 95/46/CE al nuovo regolamento 2016/679/UE (GDPR)*, [online], altalex.com, 08.01.18, <www.cyberlaws.it>.

Pariser, E., *Attenti alle "filter bubble" in rete*, 2011 [video file], https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=it#t-511300

Piretti, M., *Scandalo Facebook, Mark Zuckerberg si scusa: "Sono responsabile dell'accaduto"*, [online], dire.it, 22.03.18 <www.dire.it>.

Pizzetti, F., *GDPR e trattamento automatizzato di dati personali, ecco le tutele personali per gli utenti,* [online], agendadigitale.eu, 10.11.17 <www.agendadigitale.eu>.

Procaccianti, D., *Tutti spiati?,* 2020 [video file] https://www.youtube.com/watch?v=cckZ6Eom2bU

Prosperi, M., *Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento*, [online], privacy.it, <www.privacy.it>.

Rosenberg, M., Confessore, N., Cadwalladr, C., *How Trump Consultants Exploited the Facebook Data of Millions,* [online], nytimes.com, 17.03.18 <www.nytimes.com>.

Rovesti, A., *Il "decalogo" della Cassazione sui limiti del diritto di cronaca*, [online], iusinitinere.it, 04.04.17, < www.iusinitinere.it>.

Saliola, S., *Il caso Soraya e l'applicazione diretta della CEDU*, [online], iurisprudentes.it, 04.04.17, <www.iurisprudentes.it>.

*Scandalo Facebook - Cambridge Analytica, Zuckerberg alla camera Usa (con traduzione simultanea)*, [video file] https://www.youtube.com/watch?v=msDrnmjMI4s**.**

Schrooepfer, M., *An Update on Our Plans to Restrict Data Access on Facebook*, [online], about.fb.com, 4.04.18 <www.about.fb.com>.

Simonetta, B., *Scandalo Cambridge Analytica. Così i nostri dati su Facebook finiscono nel mercato delle app,* [online], ilsole24ore.com, 20.03.18 <www.ilsole24ore.com>

Tabacchi, E*., Perché i Social Network sono gratuiti?*, [online], larixstudio.com, 25.05.17, <www.larixstudio.com>.

The Guardian, *The Cambridge Analytica Files*, 2018 [video file] https://www.youtube.com/watch?v=FXdYSQ6nu-M.

Tiani, V., *Le domande del Parlamento europeo a cui Zuckerberg non ha risposto*, [online], wired.it, 22.05.18 <www.wired.it>.

*Scandalo dati, prima multa a Facebook: 500mila sterline*, [online], rainews.it, 11.07.18 <www.rainews.it>.