LUISS

Dipartimento di Impresa e Management

Corso di laurea in Marketing – Gestione dei Processi e delle Relazioni di Marketing

Cattedra di Legal Issues in Marketing

La minaccia invisibile: l'Active Listening e la privacy digitale nell'era degli smartphone

RELATORE
Prof. Andrea Giannaccari

CORRELATORE
Prof.ssa Mirella Pellegrini

CANDIDATO
Annalisa Simone
775971

Anno Accademico 2023 - 2024

SOMMARIO

INTRODUZIONE

Nell'era dell'informazione, la tecnologia ha rivoluzionato ogni aspetto della nostra quotidianità. Gli smartphone e i dispositivi connessi sono diventati strumenti indispensabili per milioni di persone, offrendo una vasta gamma di servizi che migliorano l'efficienza e la comodità della vita moderna. Tuttavia, con questa crescente interconnessione, si è aperto uno spazio per nuove minacce alla privacy.

Un fenomeno che ha suscitato particolare preoccupazione è l'*Active Listening*, ossia l'ascolto attivo, ma anche passivo e costante delle conversazioni da parte di dispositivi tecnologici connessi a Internet, come smartphone, smart TV e assistenti vocali. Sebbene le aziende tecnologiche affermino di non registrare conversazioni senza consenso, le segnalazioni da parte degli utenti suggeriscono il contrario, alimentando paure e sospetti. Il concetto dell'*Active Listening* non si limita semplicemente alla raccolta di dati, ma ha implicazioni profonde per la privacy degli individui e il loro diritto alla protezione dei dati personali. Il termine descrive la capacità di un dispositivo di ascoltare continuamente i dialoghi dell'utente, interpretando parole chiave e rispondendo con azioni o suggerimenti basati sui dati raccolti. Questo ha sollevato dibattiti sia giuridici che etici, poiché molte delle applicazioni che utilizzano tecnologie di riconoscimento vocale accedono a dati sensibili senza che gli utenti siano pienamente consapevoli di come e quando tali dati vengano raccolti o utilizzati.

Parallelamente alla minaccia dell'*Active Listening*, un'altra pratica invasiva e pervasiva è legata all'utilizzo dei *cookie* sul web. I cookie, originariamente introdotti per migliorare l'esperienza di navigazione degli utenti, sono piccoli file di testo memorizzati sui dispositivi durante la visita a siti web. Sebbene essi abbiano una funzione legittima, come la memorizzazione delle preferenze utente o il miglioramento delle prestazioni del sito, i *cookie* di terze parti sono utilizzati per tracciare le attività degli utenti su più siti, consentendo alle aziende di creare profili dettagliati e personalizzare la pubblicità. Questo tracciamento silenzioso e spesso invisibile rappresenta un ulteriore attacco alla privacy, poiché raccoglie informazioni sugli utenti senza un consenso realmente informato.

La crescente diffusione di queste pratiche ha portato a nuove sfide per la protezione della privacy. Se da un lato la personalizzazione dei servizi

offerti tramite l'uso dei dati raccolti è percepita come un vantaggio, dall'altro lato sorge il rischio che tali tecnologie vengano impiegate per fini non trasparenti, compromettendo la sicurezza e la riservatezza degli utenti. Il diritto alla privacy, sancito da normative come il *GDPR* (General Data Protection Regulation), impone limiti rigorosi sull'uso dei dati personali, ma l'applicazione pratica di tali regolamentazioni spesso non è altrettanto rigorosa quanto la teoria. In molti casi, i consumatori accettano inconsapevolmente termini e condizioni che autorizzano pratiche di ascolto attivo o l'uso estensivo di *cookie* per il tracciamento, esponendosi a potenziali violazioni della privacy.

Di fronte a tale scenario, sorge spontanea una domanda: "*Come possono gli utenti proteggere efficacemente la propria privacy dall'Active Listening dei dispositivi tecnologici e dall'uso indiscriminato dei cookie, senza rinunciare ai benefici che questi strumenti offrono nella vita quotidiana?***"**

Questa domanda è centrale in quanto esprime la tensione tra l'innovazione tecnologica e la necessità di tutelare i diritti individuali.

Nella trattazione che segue, verranno analizzati i diversi aspetti tecnologici, legali ed etici dell'*Active Listening* e del tracciamento tramite *cookie*, con l'obiettivo di proporre soluzioni concrete per la mitigazione dei rischi legati alla privacy digitale.

L'analisi sarà strutturata in quattro capitoli principali. Il primo capitolo fornirà una panoramica del concetto di *Active Listening* e del tracciamento tramite *cookie*, esplorando come queste pratiche vengano utilizzate dalle aziende per monitorare i comportamenti degli utenti e per fini pubblicitari. Il secondo capitolo esaminerà gli aspetti tecnologici che rendono possibile l'ascolto attivo, con un focus sulla storia ed evoluzione delle tecnologie di riconoscimento vocale. Il terzo capitolo tratterà gli aspetti giuridici ed etici, esplorando le normative vigenti e analizzando casi di studio che hanno coinvolto grandi aziende tecnologiche. Infine, nel quarto capitolo, verranno proposte misure pratiche per la mitigazione dei rischi legati all'ascolto attivo e al tracciamento tramite *cookie*, con l'obiettivo di fornire agli utenti strumenti utili per proteggere la loro privacy.

Questa tesi si pone l'obiettivo di esplorare non solo le implicazioni pratiche dell'*Active Listening e* dell'uso dei *cookie*, ma anche di fornire una risposta alla domanda di ricerca iniziale, offrendo soluzioni che bilancino innovazione e protezione della privacy.

CAPITOLO I

ACTIVE LISTENING

1.1 Cos'è l'Active Listening

Uno degli strumenti più utilizzati nel mondo al giorno d'oggi è lo smartphone. Questo strumento potentissimo supporta ogni attività della nostra vita quotidiana ed è dotato di molteplici funzioni e da una grande varietà di sensori che memorizzano una elevata quantità di dati personali [1].
In parallelo con il crescente numero di funzioni e applicazioni che possono essere scaricate sugli smartphone, è aumentato significativamente anche il numero di minacce alla sicurezza degli utenti, in particolare per quanto riguarda la compromissione della privacy.
Attualmente, oltre alla privacy, ciò che preoccupa maggiormente le persone è l'introduzione di una nuova tecnologia, chiamata "*Active Listening*": "*Il termine, nel suo utilizzo più generale, viene utilizzato per fare riferimento ad una tipologia particolare di ascolto attivo*" [2].
L'ascolto attivo è una tecnica di comunicazione che implica l'ascolto consapevole e profondo nei confronti dell'interlocutore.
Questo approccio va oltre il semplice sentire le parole pronunciate; richiede un impegno mentale ed emotivo per comprendere il significato, le emozioni e le intenzioni di chi parla.
Spostando l'attenzione verso la tecnologia, l'ascolto attivo, ha valore più minaccioso in termini di privacy e di sicurezza; nel corso degli anni è cresciuta l'attenzione delle persone verso quest'ultima tematica, soprattutto verso i dispositivi tecnologici.
Negli ultimi anni è emerso un timore sempre più diffuso: gli smartphone potrebbero trasformarsi in dispositivi di intercettazione remota. Molte persone hanno riportato su internet che, dopo aver avuto una conversazione, sui loro dispositivi personali sono apparse pubblicità

[1] Kröger, J. L., & Raschke, P. (2019). Is my phone listening in? On the feasibility and detectability of mobile eavesdropping. *Journal Name*, *Volume* (Issue), 102–120.
[2] Cultur-e. (2023). Gli smartphone ci ascoltano? Ecco il fenomeno dell'active listening. *Fastweb Plus*. https://www.fastweb.it/fastweb-plus/digital-dev-security/active-listening-gli-smartphone-ci-ascoltano/

mirate. Questo ha portato molti a credere che le loro conversazioni private fossero state registrate e analizzate di nascosto [3]. Queste convinzioni hanno fatto sorgere una domanda: "*Si tratta solo di deliri paranoici o di un assaggio di qualcosa di ancora più sinistro?*" [4]

Vari tentativi di ricerca non sono riusciti a trovare prove concrete di smartphone che ascoltano e trasmettono dati vocali.

"*Google ha dichiarato di avere accesso al 70% delle transazioni con carta di credito e di debito negli Stati Uniti. Insieme a Facebook e altri, monitora anche gran parte di ciò che stiamo facendo sul web. Utilizzando tecnologie di tracciamento nascoste, le aziende possono vedere molte delle pagine che tu e le persone a te collegate state visitando, consentendo loro di personalizzare meglio i loro annunci. Secondo l'autore di uno studio, Google ha tracker sul 76% dei siti web, mentre Facebook ci guarda sul 23% dei siti*" [5].

Antonio García Martínez, ex collaboratore di *Ideas* per *WIRED*, ha affrontato il tema dell'*Active Listening* da parte di *Facebook*; numerose sono le teorie del complotto nei confronti di questa piattaforma e l'autore le ha smentite tutte. Secondo queste teorie, *Facebook* registrerebbe tutte le attività del nostro smartphone mentre è in funzione.

"Dal punto di vista funzionale, questo equivale a una telefonata sempre attiva da parte dell'utente a Facebook. La tua chiamata voice-over-internet media richiede qualcosa come 24 kbps a tratta, il che equivale a circa 3 kB di dati al secondo. Supponiamo che tu abbia il telefono acceso per metà della giornata, ovvero circa 130 MB al giorno, per utente. Ci sono circa 150 milioni di utenti attivi ogni giorno negli Stati Uniti, quindi circa 20 petabyte al giorno, solo negli Stati Uniti. Per metterlo in prospettiva, l'intero archivio dati di Facebook è "solo" di circa 300 petabyte, con un tasso di ingestione giornaliero di circa 600 terabyte. In

[3] Kröger, J. L., & Raschke, P. (2019). Is my phone listening in? On the feasibility and detectability of mobile eavesdropping. *Journal Name*, *Volume* (Issue), 102–120.

[4] Triggs, R. (2018, luglio 18). No, your phone is not always listening to you. *Android Authority*. https://www.androidauthority.com/your-phone-is-not-listening-to-you-884028/

[5] CBS News. (2023, maggio 15). Do smartphones listen to us and target us with ads? *CBS News*. https://www.cbs.com/shows/news/

altre parole, la sorveglianza audio costante produrrebbe circa 33 volte più dati al giorno di quelli che Facebook consuma attualmente" [6].
Tuttavia, questo non è possibile, ma c'è un modo più intelligente per farlo. Il dispositivo *Amazon Echo*, noto anche come "*Alexa*" per via del software che lo alimenta, è ormai una presenza comune in molte case americane. Questo dispositivo è dotato di un hardware sufficiente per rilevare alcune parole chiave, permettendo ad *Amazon* di eseguire una traduzione "*speech-to-text*" e un'elaborazione del linguaggio naturale. In sostanza, l'*Echo* funziona come un microfono, un altoparlante e un computer semplice, svolgendo efficacemente il compito di riconoscimento vocale.
L'app di *Facebook* potrebbe fare lo stesso, ma, a differenza di *Amazon*, dispone di molte più parole chiave "*targetizzabili*".
Ad esempio, se pronunciassimo parole chiave come *"Golf"*, *"Tiger Woods"* o *"The Masters"*, potremmo essere inclusi nel segmento di targeting "*Golf*". Di conseguenza, il telefono dovrebbe rilevare tutte le parole chiave associate a quel segmento.
Dato che *Facebook* non utilizza parole chiave specifiche, il telefono dovrebbe monitorare ogni singola parola target. Questa tecnica è quasi impossibile da applicare su ogni singolo smartphone esistente e quindi rappresenta una sfida straordinaria.
Dunque, è evidente che gli smartphone si siano trasformati in veri e propri computer, offrendo un'ampia gamma di applicazioni che richiedono il consenso per accedere a informazioni personali, inclusa la posizione dell'utente e, spesso, del microfono.
Le applicazioni potrebbero abusare dei permessi concessi per raccogliere dati e informazioni personali degli utenti, utilizzando questo materiale per vari scopi, fra cui quelli pubblicitari [7]. Questa pratica solleva serie preoccupazioni riguardo la condivisione di informazioni private ed è considerata una questione urgente e di primaria importanza.
Inizialmente, le registrazioni segrete non erano percepite come minacce di alto livello, bensì erano considerate solo attacchi potenzialmente possibili. Tuttavia, con il tempo e l'evoluzione della tecnologia, è diventato evidente

[6] Garcia Martinez, A. (2017, novembre 18). Facebook's not listening through your phone. It doesn't have to. *Wired*. https://www.wired.com/story/facebooks-listening-smartphone-microphone/.
[7] Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 627–638.

che tali registrazioni possono rappresentare un rischio significativo per la privacy e sicurezza degli utenti [8].

Questi cambiamenti hanno fatto crescere la preoccupazione del pubblico nei confronti dei problemi legati alla sicurezza e alla privacy, ma soprattutto è aumentato l'interesse verso la soluzione a questo problema e il modo in cui deve essere affrontato. Tuttavia, si sa ancora poco sugli approcci adottati dagli utenti per mitigare rischi di privacy e sicurezza sui propri smartphone [9].

Grazie a uno studio condotto da *Adrienne Porter Felt et al.*, è possibile comprendere l'attenzione del pubblico verso le autorizzazioni concesse durante l'installazione di nuove app sui dispositivi mobili. Questo studio si è focalizzato principalmente sul sistema di autorizzazione *Android*.

I ricercatori hanno eseguito due studi basati sull'usabilità: un sondaggio online su 308 utenti *Android* e uno studio di laboratorio con 25 utenti *Android*. Questi due studi sono stati progettati per confermarsi e validarsi reciprocamente.

Generalmente, un'applicazione deve ottenere autorizzazioni per utilizzare risorse come fotocamera, microfono, posizione o registro chiamate. Tuttavia, ogni applicazione ha un set di autorizzazioni, funzionalità e requisiti specifici. I ricercatori hanno posto varie domande agli utenti, tra cui alcune relative alle preferenze in materia di privacy. La maggior parte dei sondaggi ha rilevato che le persone sono molto protettive nei confronti dei propri dati personali, ma spesso le azioni non rispecchiano le preferenze dichiarate.

Sia nel sondaggio online che nello studio di laboratorio, solo il 17% dei partecipanti ha prestato attenzione ai permessi durante l'installazione delle applicazioni. Inoltre, il 42% dei partecipanti allo studio di laboratorio non era a conoscenza dell'esistenza delle autorizzazioni [10].

In conclusione, la crescente diffusione dello smartphone come strumento quotidiano e il costante aumento delle minacce sulla privacy hanno sollevato serie preoccupazioni riguardo la sicurezza dei dati personali.

---

[8] Krum, C. (2010). *Mobile marketing: Finding your customers no matter where they are*. Pearson Education.

[9] Kraus, L., Fiebig, T., Miruchna, V., Moller, S., & Shabtai, A. (2015). *Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy*.

[10] Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 627–638.

Il fenomeno dell'*Active Listening*, in particolare, rappresenta una minaccia emergente, molte persone temono che le loro conversazioni private possano essere intercettate e utilizzate per scopi e fini pubblicitari.
Nonostante le rassicurazioni di aziende come *Facebook* e le difficoltà tecniche di un ascolto continuo, rimane il timore che le app possano abusare delle autorizzazioni concesse per raccogliere informazioni sensibili. Gli studi appena citati di *Adrienne Porter Felt et al*. evidenziano una disconnessione tra la consapevolezza degli utenti sulla privacy e il loro comportamento pratico, con una percentuale significativa di utenti che non presta attenzione ai permessi durante l'installazione delle app.
Questo divario tra percezione e realtà pone sfide importanti per la tutela della privacy, sottolineando la necessità di una maggiore educazione e trasparenza in questo ambito.

1.2 Motivazioni dell'Active Listening e monitoraggio del comportamento online

Nel 2011, con l'introduzione di *Siri* e successivamente seguita da *Google Assistant*, *Alexa* e *Cortana*, è stato possibile servire gli utenti, supportandoli in ogni attività come, invio di sms, chiamate telefoniche o nell'aggiunta di elementi ad una lista di attività da svolgere.
Le domande che dovremmo porci sono più di una. *"Il mio telefono mi ascolta?" "Quanto mi ascolta il mio telefono?"* e *"Cosa fa il mio telefono con le conversazioni che raccoglie?"* [11].
Il primo aspetto da considerare è che lo scopo di questi assistenti vocali è proprio quello di assistere gli utenti; dunque, sarà poi normale ricevere pubblicità personalizzate dopo aver avuto una conversazione su di essi.
Un esempio pratico potrebbe essere: *"Hey Google, cerca corsi di pilates nella mia zona"*; successivamente la probabilità di ricevere pubblicità mirate su corsi di pilates sarà molto alta. Un esempio molto simile potrebbe essere legato al classico motore di ricerca. Dopo aver effettuato una ricerca su un qualsiasi argomento, ci verranno forniti tutti i risultati e pubblicità più pertinenti. Possiamo infatti immaginare il nostro smartphone come un motore di ricerca vocale.
Gli smartphone e, più in generale, qualsiasi dispositivo connesso a Internet osservano il modo in cui interagiamo con i contenuti per migliorare la nostra esperienza utente. Analizzano attentamente i nostri dati al fine di proporci servizi e prodotti più pertinenti e adatti ai nostri interessi. Questo aspetto non implica necessariamente che i nostri dati personali siano a rischio, ma è fondamentale che tutti gli utenti comprendano come e perché questi dati vengono raccolti.
In parole più semplici, questo metodo serve a studiare il nostro comportamento, ed è una pratica molto comune: il 79% dei siti web, per esempio, adotta questa strategia.
Il tracciamento dei nostri comportamenti favorisce una navigazione più rapida e comoda. Ad esempio, piattaforme come *Netflix* suggeriscono film

[11] Stouffer, C. (2023, giugno 13). Is my phone listening to me? Yes, here's why and how to stop it. *Norton*. https://us.norton.com/blog/how-to/is-my-phone-listening-to-me.

o serie TV basandosi sui contenuti che abbiamo già visto. Questo permette di analizzare i nostri gusti e interessi, offrendo suggerimenti personalizzati. Se uno spettatore guarda frequentemente serie tv o film *thriller*, *Netflix* proporrà contenuti simili, migliorando così l'esperienza di visione e rendendola più piacevole e soprattutto più mirata.
Oltre a *Netflix*, anche altri fornitori importanti di servizi come *Amazon* e *YouTube* utilizzano strategie simili per proporre prodotti e video che potrebbero interessarci.
Questo tipo di personalizzazione è reso possibile grazie alla raccolta e all'analisi dei dati sulle nostre abitudini di navigazione e preferenze. Pertanto, sebbene il tracciamento dei nostri comportamenti possa sollevare preoccupazioni riguardo alla privacy, è anche vero che porta a un'esperienza utente più efficiente e soddisfacente [12].
Recentemente, con l'evoluzione tecnologica, anche altri dispositivi sono diventati potenziali minacce per l'*Active Listening*, tra cui le *smart TV*.
Negli ultimi anni, le *smart TV* sono diventate sempre più pratiche grazie a funzionalità avanzate come gli assistenti vocali.
Nei modelli più recenti, sono integrati dispositivi come *Chromecast* e *Google Assistant*, che ne aumentano la versatilità e le potenzialità.
Le *smart TV* si connettono facilmente a Internet e, una volta abilitati gli assistenti vocali, sono in grado di tracciare ciò che cerchiamo e guardiamo. Queste informazioni possono essere utilizzate per fornire pubblicità mirate.
È importante essere consapevoli che aziende che forniscono contenuti, come *Netflix*, possono tracciare la cronologia di navigazione delle nostre *smart TV* e successivamente offrire pubblicità più in linea con i nostri interessi. Nel 2017, *Vizio*, una società statunitense che produce televisori, sound bar e altri dispositivi simili, ha affrontato seri problemi legali con la *FTC (Federal Trade Commission)* per aver monitorato le abitudini di visione e comportamento dei propri clienti tramite le sue *smart TV*.
I dati raccolti sono stati poi venduti ad aziende pubblicitarie e utilizzati per indirizzare i clienti con annunci mirati. Questo comportamento ha portato *Vizio* a dover affrontare accuse legali, risolte con il pagamento di 2,2 milioni di dollari. Il problema principale risiedeva nel fatto che la

[12] Stouffer, C. (2021, giugno 28). Internet tracking: How and why we're followed online. *Norton*. https://us.norton.com/blog/privacy/internet-tracking.

funzionalità di raccolta dati era attivata di default, mentre altri produttori consentivano agli utenti di attivarla o disattivarla [13].

Recentemente, sono emerse evidenze che alcune società di marketing stanno promuovendo software progettati per ascoltare le conversazioni degli utenti. La testata giornalistica *404 Media* ha scoperto una pagina web, successivamente rimossa, appartenente alla società *Cox Media Group*, la quale pubblicizzava un servizio denominato "*Active Listening*".

Questo servizio è in grado di identificare i consumatori in tempo reale attraverso l'utilizzo di smartphone, *smart TV* e altri dispositivi, monitorando le conversazioni e permettendo alle aziende di veicolare annunci pubblicitari mirati.

Questa notizia ha sollevato numerosi dubbi e interrogativi, soprattutto riguardo alla legalità di tali sistemi. La domanda che molti si pongono è: "*È etico e legale ascoltare le nostre conversazioni?"*

La società *Cox Media Group (CMG)* sostiene che questa pratica è legale, in quanto i consumatori acconsentono accettando i termini e le condizioni delle applicazioni e del software che scaricano.

Tuttavia, la complessità e la lunghezza spesso incomprensibile dei termini di servizio possono portare gli utenti a dare il proprio consenso senza una piena comprensione di ciò che accettano.

Rimane quindi aperto il dilemma su quali siano effettivamente le applicazioni che utilizzano questi sistemi. Tra i partner menzionati da *CMG* figurano grandi aziende come *Amazon*, *Microsoft* e *Google*. Tuttavia, queste aziende affermano di non condividere registrazioni vocali e di prevenire la raccolta di audio quando le applicazioni non sono in uso attivo.

Sebbene la presunta pratica di ascolto clandestino da parte degli smartphone sia stata ufficialmente negata, numerose evidenze suggeriscono l'esistenza di software progettati a tale scopo. Di conseguenza, molti interrogativi rimangono irrisolti.

Il sospetto comune che gli smartphone possano ascoltare le conversazioni si è quindi rafforzato, alimentando una crescente preoccupazione tra gli utenti [14].

---

[13] Norton. (2018, agosto 8). *What is a smart TV and the privacy risks of a smart TV. Norton*. https://us.norton.com/blog/iot/smart-tvs-and-risk.

[14] Galletta, M. (2023, dicembre 28). *È vero che i nostri dispositivi smartphone ci ascoltano? TecnoAndroid*.

In conclusione, l'*Active Listening*, reso possibile da assistenti vocali e dispositivi connessi a Internet come smartphone e *smart TV*, rappresenta una doppia faccia della medaglia. Da un lato, migliora l'esperienza utente attraverso la personalizzazione dei contenuti e delle pubblicità; dall'altro, solleva importanti questioni sulla privacy e sul monitoraggio dei comportamenti online.
È essenziale che gli utenti siano consapevoli di come e perché i loro dati vengono raccolti, per bilanciare i benefici di una maggiore comodità con la necessità di proteggere la propria privacy.

1.3 Strategie di Monitoraggio e Tracciamento dei Dati sui Siti Web

Gli annunci pubblicitari che vediamo online sono sempre più mirati e basati sui nostri interessi personali; di conseguenza, molte persone credono che le applicazioni installate sugli smartphone ascoltino continuamente le nostre conversazioni. Questa teoria ha trovato particolare risonanza tra coloro che diffidano di alcune delle più grandi aziende di Internet, come *Facebook*.

Come discusso nel *paragrafo 1.1*, *Facebook* ha affrontato significativi problemi riguardanti la tutela della privacy dei propri utenti. Tuttavia, è stato dimostrato che non ha bisogno di spiare le nostre conversazioni, poiché dispone già di ampie risorse per monitorare le nostre attività in qualsiasi momento.

Molte persone giungono facilmente alla conclusione che un'applicazione sullo smartphone o su altri dispositivi abbia rilevato la conversazione e utilizzato queste informazioni per mostrare pubblicità mirate.

Oltre a violare le leggi sulla privacy di molti paesi, un sistema del genere sarebbe anche tecnicamente complesso da sviluppare e implementare, oltre che estremamente costoso, soprattutto se applicato a centinaia di milioni di smartphone su cui è installata l'app di *Facebook*. Le aziende che gestiscono la pubblicità online utilizzano informazioni molto più semplici e accessibili per personalizzare gli annunci in base ai nostri interessi, spesso sfruttando dati che forniamo inconsapevolmente. Strumenti di tracciamento ormai avanzati consentono a *Facebook* e *Google* di identificare i nostri interessi anche senza che li abbiamo mai cercati sui social network o sui motori di ricerca, utilizzando dati relativi ai nostri spostamenti, alle nostre abitudini e persino alle persone che frequentiamo [15].

Per comprendere appieno il funzionamento delle strategie di monitoraggio del comportamento degli utenti e il loro potenziale utilizzo nell'*Active Listening*, è essenziale esaminare l'intera macroarea delle strategie di monitoraggio e tracciamento dei dati.

---

[15] Il Post. (2021, maggio 27). *Perché a volte ci sembra che gli smartphone ci ascoltino*. *Il Post*. https://www.ilpost.it/2021/05/27/facebook-microfono-smartphone-pubblicita/

La raccolta dei dati e le questioni relative alla privacy sono cruciali non solo per l'ascolto attivo sugli smartphone e sulle *smart TV*, ma anche per garantire la sicurezza e la privacy degli utenti durante la navigazione sui siti web. Infatti, esistono numerosi metodi per tracciare gli utenti sui siti web e analizzarne il comportamento.
Il metodo più comune e diffuso è l'uso dei cosiddetti *cookie*, di cui approfondiremo la normativa nel *Capitolo III*.
Il termine "*cookie*" è stato introdotto per la prima volta in ambito informatico negli anni '70, e nei primi anni '80 erano conosciuti come *"Magic Cookie"*. Tuttavia, i siti web hanno iniziato a utilizzare i cookie nella seconda metà degli anni '90, diffondendosi rapidamente da allora [16].
I *cookie* di tracciamento sono strumenti creati dal server per raccogliere informazioni o dati sugli utenti generati da un sito web. Questi cookie sono utili per velocizzare e semplificare gli accessi ai siti web, essendo salvati direttamente sul dispositivo utilizzato per accedere. Ad esempio, dopo essersi registrati su un sito, al ritorno sullo stesso, il sito può proporre automaticamente le credenziali precedentemente inserite.
In Italia, così come in molti altri Paesi, è obbligatorio per i siti web richiedere il consenso esplicito all'utilizzo dei *cookie* per personalizzare l'esperienza di navigazione. Il *GDPR* (*General Data Protection Regulation*) afferma che le informazioni contenute nei *cookie* devono essere trattate e gestite come dati personali. I *cookie* non sono pericolosi, poiché non contengono alcun tipo di virus, il problema riguarda il modo in cui questi dati vengono utilizzati violando la privacy degli utenti.
Esistono diverse tipologie di *cookie*, tra cui la principale distinzione è tra *cookie* di prima parte e *cookie* di terza parte.
I *cookie* di prima parte sono creati direttamente dal server del sito che l'utente sta visitando e vengono utilizzati per migliorare l'esperienza di navigazione dell'utente. Le informazioni e i dati presenti in questa tipologia di *cookie* non vengono utilizzati per pubblicità mirate e personalizzate su altri siti web [17].
I *cookie* di terza parte, invece, sono creati da domini diversi da quelli dei siti visitati dall'utente. Vengono spesso utilizzati per tracciare il comportamento degli utenti e fornire annunci personalizzati

[16] Polimeni, A. (2022). Cookie: cosa sono, come funzionano e come proteggerti. *Agenda Digitale*.
[17] Net Informatica. (2020, ottobre 14). A cosa servono i cookie. *Net Informatica*.

successivamente. Molti browser hanno bloccato il loro utilizzo poiché li considerano lesivi per la privacy degli utenti. Inoltre, i *cookie* possono variare anche in base alla loro durata[18].
Esistono i *cookie* temporanei di sessione, che rimangono sul dispositivo dell'utente fino al termine della sessione di navigazione per poi essere cancellati automaticamente. I *cookie* persistenti, invece, rimangono attivi sul dispositivo dell'utente fino alla loro data di scadenza o fino alla cancellazione da parte dell'utente stesso.
Oltre ai *cookie*, esistono numerosi altri metodi di tracciamento dei dati. Tra i più comuni troviamo:

- *Account Tracking*: questo metodo prevede il monitoraggio e la registrazione delle attività online dell'utente mentre accede a uno specifico account o piattaforma;
- *Web Beacons*: noti anche come "*web bugs*", questi strumenti controllano e tracciano i movimenti degli utenti su un sito web, inclusi i contenuti su cui cliccano;
- *Browser Fingerprinting*: questo metodo raccoglie tutte le informazioni presenti su un dispositivo e crea un identificatore univoco, utilizzato per monitorare qualsiasi attività o movimento online dell'utente [19].

L'utilizzo di questi metodi di tracciamento solleva importanti questioni riguardanti la privacy degli utenti e la necessità di un consenso informato. Le normative sulla protezione dei dati, come il *GDPR*, richiedono che gli utenti siano informati e diano il loro consenso prima che tali tecnologie possano essere utilizzate per raccogliere e trattare i loro dati personali.

[18] La Rosa, A. (2020). Cookie di prima e terza parte: Cosa sono e come funzionano. *Engage.it*.
[19] *Stouffer, C. (2021, giugno 28). Internet tracking: How and why we're followed online. Norton. https://us.norton.com/blog/privacy/internet-tracking.*

1.4 Casi Studio e Implicazioni pratiche sulla raccolta dati e analisi del comportamento del cliente

Le implicazioni pratiche del monitoraggio delle attività degli utenti e dell'utilizzo dei dati personali da parte delle aziende di marketing si riflettono chiaramente in numerosi casi studio. Questi esempi pratici mostrano come le informazioni raccolte vengano impiegate non solo per creare pubblicità mirate, ma anche per modellare i comportamenti e le scelte degli utenti.
Analizzando questi casi si possono approfondire le tecniche adottate, i rischi coinvolti e le risposte degli utenti e delle autorità di regolamentazione. Tali studi offrono una visione dettagliata delle dinamiche operative e delle conseguenze tangibili di queste pratiche sulla privacy e sulla sicurezza dei dati personali.

Google Assistant e Apple Siri

Nel *paragrafo 1.1* di questo capitolo è stato approfondito l'argomento relativo agli assistenti vocali; tuttavia, nel 2019, assistenti vocali come *Google Assistant* e *Apple Siri* hanno sollevato numerose critiche e preoccupazioni riguardo alla privacy.
Inizialmente, sembrava che gli assistenti vocali basati sull'intelligenza artificiale delle grandi aziende della *Silicon Valley* rappresentassero una novità rivoluzionaria nel settore della tecnologia. Tuttavia, questi dispositivi hanno dimostrato di avere significativi problemi legati alla privacy degli utenti.
Quando l'utente pronuncia la parola chiave "*Hey Google*", l'assistente si attiva e offre supporto, ma il problema risiede nel fatto che questi dispositivi possono ascoltare conversazioni private anche quando non sono stati chiamati. Questo può portare a ricevere pubblicità mirate immediatamente dopo una conversazione privata.
La radice del problema era che i processi di registrazione vocale e le relative funzioni erano gestiti da esseri umani.

Nel 2019, diverse registrazioni vocali di *Google Assistant* trapelate su un sito di notizie belga hanno portato l'*Agenzia per la Protezione dei Dati di Amburgo* ad agire, invocando i poteri di emergenza previsti dall'*Articolo 66* del *GDPR* per fermare la revisione manuale delle registrazioni vocali di *Google* [20].

Gli audio trapelati hanno rivelato una serie di situazioni imbarazzanti e inquietanti, come discussioni su violenza fisica, criminalità e traffico di droga. Questi incidenti mostravano anche che le persone potevano essere identificate attraverso le registrazioni.

Gli appaltatori umani che ascoltavano queste registrazioni erano spesso scioccati e impotenti di fronte a tali informazioni.

A seguito di questi eventi, *Google* ha interrotto tutte le revisioni manuali delle registrazioni degli assistenti vocali, citando che solo lo 0,2% delle registrazioni era soggetto a revisione manuale. Tuttavia, secondo i tecnologi di *Google*, queste revisioni erano essenziali per migliorare e addestrare gli algoritmi di intelligenza artificiale.

In risposta a situazioni simili, *Apple* ha annunciato che avrebbe interrotto tutte le revisioni manuali delle registrazioni vocali a livello globale. D'ora in poi, i contractor umani non avrebbero più ascoltato frammenti audio di *Siri*, l'assistente vocale dell'azienda [21].

I casi di *Google Assistant* e *Apple Siri* illustrano le sfide e le preoccupazioni legate all'uso degli assistenti vocali e dell'*Active Listening*.

Mentre la tecnologia offre grandi vantaggi in termini di funzionalità e personalizzazione, solleva anche gravi questioni etiche sulla privacy degli utenti.

È essenziale che le aziende tecnologiche trovino un equilibrio tra innovazione e protezione dei dati personali degli utenti, garantendo trasparenza e controllo agli utenti sui propri dati vocali.

---

[20] Dissent. (2019, luglio 11). Google is investigating the source of voice data leak, plans to update its privacy policies. *DataBreaches.net*. https://databreaches.net/2019/07/11/google-is-investigating-the-source-of-voice-data-leak-plans-to-update-its-privacy-policies/.

[21] Lindsey, N. (2019, agosto 14). Amazon, Google, Apple stopping human review of recordings from voice assistants. *CPO Magazine*. https://www.cpomagazine.com/data-privacy/amazon-google-apple-stopping-human-review-of-recordings-from-voice-assistants/.

Questi casi evidenziano la necessità di un uso etico e responsabile della tecnologia, un tema che sarà ulteriormente esplorato nei capitoli successivi.

Target

Target è una catena di grandi magazzini statunitense con sede a *Minneapolis, Minnesota*, e rappresenta l'ottavo rivenditore al dettaglio negli Stati Uniti.
Nel 2002, *Andrew Pole*, un giovane statistico, ha iniziato la sua carriera presso *Target*. Un giorno, due colleghi del reparto marketing gli hanno posto una domanda intrigante: *"È possibile determinare se una cliente è incinta anche contro la sua volontà?"*
Questo interrogativo nasceva dalla consapevolezza che i neogenitori rappresentavano una risorsa preziosa per i rivenditori.
Solitamente, i consumatori non acquistano tutto ciò di cui hanno bisogno in un unico negozio. Ad esempio, comprano generi alimentari al supermercato, giocattoli nei negozi specializzati, e si recano da *Target* solo per prodotti specifici come articoli per la pulizia, calzini o carta igienica. Tuttavia, *Target* offre una gamma completa di prodotti, dai generi alimentari ai peluche, dai mobili da giardino all'elettronica.
Uno degli obiettivi principali dell'azienda è convincere i clienti che *Target* è l'unico negozio di cui hanno bisogno. Realizzare questo obiettivo è complesso, poiché cambiare le abitudini di acquisto radicate è estremamente difficile.
Ci sono momenti in cui le vecchie abitudini possono cambiare, e la nascita di un bambino è sicuramente uno di questi.
I neogenitori, spesso esausti e sopraffatti, possono vedere modificati i loro modelli di acquisto, poiché diventano più vulnerabili.
Quando nasce un bambino, i certificati di nascita, essendo documenti pubblici, rendono i genitori bersagli di un bombardamento di offerte, incentivi e pubblicità da parte di varie aziende.

La chiave per *Target* era raggiungere questi clienti prima degli altri rivenditori. I responsabili del marketing hanno quindi deciso di inviare annunci pubblicitari mirati alle donne nel secondo trimestre di gravidanza, periodo in cui solitamente si acquistano prodotti come vitamine prenatali o abbigliamento per la maternità.
Riuscire a identificare le donne in questa fase aumenta significativamente la probabilità di fidelizzarle come clienti per anni.
Per decenni, *Target* ha raccolto una quantità enorme di dati sui suoi clienti attraverso un sistema di *Guest ID*, che tiene traccia di tutti gli acquisti effettuati. Ad esempio, se si utilizza una carta di credito, un coupon o si apre una e-mail inviata dall'azienda, queste informazioni vengono registrate e collegate al proprio *Guest ID*.
Al *Guest ID* sono associate anche altre informazioni demografiche. Tuttavia, tutti questi dati sarebbero inutili se non venissero analizzati. Ed è qui che entra in gioco *Andrew Pole*. Grazie all'analisi predittiva, Pole è riuscito a comprendere i comportamenti e le abitudini di acquisto dei consumatori, permettendo a *Target* di commercializzare i propri prodotti in modo più efficiente e mirato.
Con l'aumento della precisione nell'analisi dei dati, la ricerca su come le abitudini quotidiane influenzino le nostre decisioni è diventata uno dei temi più affascinanti nella ricerca clinica. Tuttavia, molti di noi non sono consapevoli dell'esistenza di questi modelli comportamentali.
Il compito di *Andrew Pole* in questa azienda era proprio quello di analizzare le abitudini comportamentali dei consumatori ed espandere le vendite. Egli aveva il compito di analizzare tutti i *"cicli di stimolo-routine-premio"* tra gli acquirenti e aiutare l'azienda a capire in che modo potesse sfruttare questi dati.
Il *ciclo di stimolo-routine-premio* è un modello di comprensione delle abitudini ed è una teoria descritta da *Charles Duhigg* nel suo libro *"The Power of Habit"*.
Questo modello fornisce una struttura di comprensione su come si sviluppano le abitudini comportamentali.
Lo stimolo rappresenta una condizione o situazione che provoca un comportamento; la routine comprende tutte le azioni e i comportamenti abituali; il premio, infine, è l'esperienza gratificante o il beneficio ottenuto al termine della routine. Quest'ultima è spesso collegata a sensazioni di

piacere, sollievo dallo stress, gratificazione sociale o altre forme di ricompensa positiva.
Il modello appena descritto può essere applicato a più ambiti, anche molto diversi fra loro, per esempio: psicologia, neuroscienze, salute, marketing e management.
Pertanto, *Andrew Pole* mettendo in pratica il modello *Ciclo di stimolo-routine-premio* è stato in grado di identificare quei momenti unici della vita in cui le abitudini delle persone diventano più flessibili e la pubblicità giusta avrebbe spinto questi a spendere il proprio denaro in modi differenti rispetto al passato, come nel caso delle donne in gravidanza.
Tutto questo è reso possibile grazie ad una eccezionale analisi dei dati, ma il problema era proprio questo.
Riuscire a comprendere i momenti di vita di una persona e suggerire soluzione attraverso una pubblicità mirata può creare disagio. *Target*, infatti, si rese conto che usare i dati personali per prevedere la gravidanza di una donna avrebbe potuto rivelarsi un disastro per le relazioni pubbliche.
La soluzione è stata quella di mescolare tutti gli annunci di oggetti che le donne in gravidanza non avrebbero mai comprato, così da far sembrare casuali gli annunci di oggetti per bambini [22].
Questo modello di *ciclo di stimolo-routine-premio* dimostra l'importanza della comprensione dei comportamenti dei consumatori per migliorare le strategie di marketing.
Applicando tale modello, *Target* ha potuto individuare momenti chiave della vita dei clienti in cui le abitudini di acquisto sono più suscettibili al cambiamento, come nel caso della gravidanza. Questa capacità di predizione, sebbene efficace, solleva importanti questioni etiche sulla privacy e sull'uso dei dati personali.
L'*Active Listening*, sebbene impiegato con scopi differenti, segue un principio simile, ossia la raccolta e l'analisi dei dati personali per fornire risposte più mirate e personalizzate.

[22] Duhigg, C. (2012, febbraio 15). How companies learn your secrets. *The New York Times Magazine*.

CAPITOLO II

ASPETTI TECNOLOGICI DELL'ACTIVE LISTENING

2.1 Tecnologie di riconoscimento vocale

Nel capitolo precedente sono stati esplorati vari aspetti cruciali per una comprensione approfondita e completa dell'*Active Listening*.
Questo tema va oltre la semplice pubblicità mirata sui nostri smartphone, poiché coinvolge molte altre dinamiche e fonti diverse. Le cause possono includere l'accettazione superficiale di *cookie*, l'analisi dei nostri comportamenti di acquisto, come dimostrato dal caso di *Target*, l'uso degli assistenti vocali su *smart TV* e smartphone, e in generale un uso non adeguato di questi dispositivi.
Una delle cause più probabili è legata all'uso del riconoscimento vocale, ossia l'attivazione continua del microfono sui nostri telefoni.
È quindi fondamentale capire a fondo questo argomento: cos' è, qual è la sua storia, come funziona e come viene applicato nel mondo reale.
Questo capitolo mira a fornire una panoramica completa non solo dal punto di vista tecnologico, ma anche su come prevenire problemi legati alla privacy e alla costante paura di essere ascoltati, che poi porta alla ricezione di pubblicità mirate, che è il focus centrale di questa tesi.
Tuttavia, le strategie e le misure per prevenire questi problemi saranno trattate nei capitoli successivi.

Il riconoscimento vocale, noto anche come "*riconoscimento vocale automatico*" (*automatic speech recognition*, *ASR*) è una tecnologia utilizzata dagli assistenti vocali per interagire con gli utenti.
I moderni assistenti vocali integrati nei nostri dispositivi mobili rappresentano delle sofisticate applicazioni software che agiscono come veri e propri intermediari tra l'utente e la tecnologia.
Questi assistenti vocali non solo facilitano l'interazione con i dispositivi, ma migliorano anche l'efficienza e la comodità dell'uso quotidiano[23].

[23] Elgan, M. (2013, agosto 31). Why are virtual assistant apps so shy? *Computerworld*. https://www.computerworld.com/article/1393993/why-are-virtual-assistant-apps-so-shy.html.

Queste applicazioni, comunemente conosciute come "*Voice Assistant*", sono progettate per eseguire una vasta gamma di attività e servizi basati sui comandi vocali degli utenti.
La loro capacità di elaborare input verbali, combinata con la loro accessibilità a una ricca varietà di fonti di dati online, consente loro di fornire risposte e assistenza in tempo reale. Tra le informazioni che possono essere recuperate e fornite ci sono notizie aggiornate, informazioni sui mercati finanziari, condizioni del traffico, prezzi dei prodotti al dettaglio e molto altro ancora. La loro funzione è particolarmente preziosa in scenari in cui l'utente ha bisogno di gestire diverse fonti di informazione simultaneamente e in modo rapido.
Come ampiamente discusso nel capitolo precedente, esempi noti di tali applicazioni includono *Google Assistant, Siri, S Voice, Cortana* e *Alexa*. Questi assistenti vocali sono progettati per rispondere a comandi vocali, permettendo così agli utenti di interagire con i loro dispositivi attraverso semplici espressioni verbali.
Ogni comando vocale può avviare una serie di azioni che, altrimenti, richiederebbero più passaggi e un intervento manuale significativo.
Questa capacità di eseguire operazioni multiple con un solo comando non solo semplifica l'interazione con i dispositivi mobili, ma offre anche un notevole vantaggio in situazioni in cui l'utente ha le mani occupate o è impegnato in altre attività.
Per esempio, quando un utente sta guidando e non può distogliere l'attenzione dalla strada, un assistente vocale può fornire indicazioni stradali, rispondere a chiamate, inviare messaggi o riprodurre musica senza che sia necessario un intervento fisico. Questo non solo aumenta la sicurezza durante la guida, riducendo la necessità di distrazioni, ma migliora anche l'efficienza delle operazioni quotidiane. Inoltre, gli assistenti vocali possono essere utilizzati per gestire e automatizzare altre funzioni, come l'accensione e lo spegnimento di dispositivi domestici intelligenti, facilitando ulteriormente la vita quotidiana degli utenti.
Gli assistenti vocali rappresentano una delle più innovative e convenienti evoluzioni nel campo delle interfacce utente, offrendo una modalità di interazione che è tanto naturale quanto efficace.
La loro capacità di semplificare compiti complessi e di rispondere alle esigenze degli utenti in modo tempestivo e personalizzato dimostra il loro

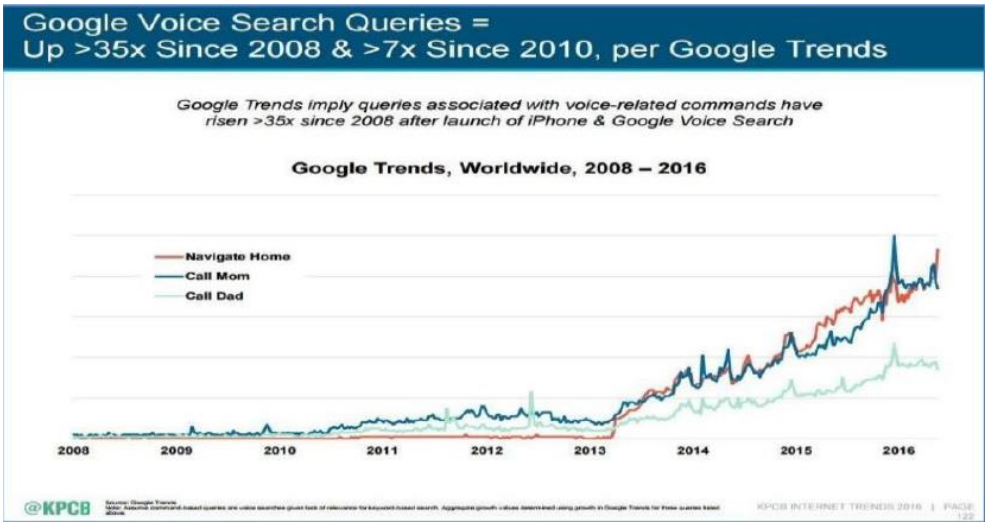
valore crescente nella nostra vita quotidiana e nell'ecosistema tecnologico moderno.
Numerose aziende di spicco nel panorama tecnologico, tra cui *Google*, *Apple* e *Microsoft*, stanno svolgendo un ruolo cruciale nello sviluppo continuo e nell'innovazione delle applicazioni di assistenza vocale.
Questi giganti della tecnologia sono costantemente impegnati a migliorare l'efficacia e la sofisticatezza delle loro soluzioni, mirando a fornire agli utenti un'esperienza sempre più fluida e intuitiva.
Le applicazioni di assistenza vocale sono progettate con l'obiettivo di implementare un'interfaccia di controllo basata sul riconoscimento vocale, che permette agli utenti di interagire con i loro dispositivi attraverso comandi verbali.
Grazie a queste applicazioni, un numero crescente di persone si sta abituando a parlare direttamente ai propri dispositivi, richiedendo loro di svolgere una varietà di attività quotidiane come inviare e-mail, effettuare telefonate, o trasmettere messaggi di testo. Gli assistenti vocali sono in grado di ricevere i comandi vocali dell'utente, processarli e, in base alle istruzioni fornite, eseguire i compiti richiesti.
Questa operazione avviene mediante l'invio delle richieste a servizi web esterni predefiniti, che elaborano e rispondono alle esigenze dell'utente[24].
Uno dei principali punti di forza di queste applicazioni è l'accesso a un vasto database di conoscenze e risorse online, che consente loro di fornire risposte precise e aggiornate a una gamma di domande e comandi. Tuttavia, tale vantaggio non è privo di limitazioni. Per funzionare in modo ottimale, gli assistenti vocali necessitano di una connessione Internet stabile e continua. Senza accesso alla rete, le loro capacità possono risultare significativamente ridotte o, in alcuni casi, l'applicazione può diventare completamente inutilizzabile[25].
Nella società odierna, caratterizzata da un ritmo di vita frenetico e dall'onnipresenza della tecnologia, le persone sono costantemente alla ricerca di soluzioni che semplifichino e velocizzino il multitasking.

---

[24] Knight, W. (2012, maggio 29). Where speech recognition is going. *MIT Technology Review*. http://www.technologyreview.com/news/427793/where-speech-recognition-is-going/.
[25] Jesdanun, A. (2013, marzo 7). Strengths and weaknesses of Apple's Siri and Google Now. *The Mercury News*. http://www.mercurynews.com/ci_22740979/strengths-and-weaknesses-apples-siri-and-google-no.

In questo contesto, l'utilizzo degli assistenti vocali si rivela una scelta ideale non solo per coloro che desiderano aumentare l'efficacia delle loro attività quotidiane, ma anche per chi trova scomodo o poco pratico digitare. Grazie ai continui progressi tecnologici, gli assistenti vocali sono ora in grado di riconoscere e trascrivere il parlato con tassi di errore molto bassi, rendendo la loro adozione sempre più diffusa.
Questa innovazione sta trasformando radicalmente il modo in cui le persone effettuano ricerche su internet. Infatti, la ricerca vocale sta emergendo come una delle modalità preferite, specialmente per le sue caratteristiche di rapidità e comodità.
Gli esperti di marketing digitale, consapevoli di queste tendenze, lavorano incessantemente per garantire che i loro siti web siano ottimizzati per tutte le forme di interazione, inclusi i comandi vocali, le domande e le query. L'aumento significativo dell'uso della ricerca vocale ha reso imperativo che i contenuti online fossero facilmente accessibili attraverso questi nuovi metodi di ricerca. In passato, l'ottimizzazione dei siti web era focalizzata prevalentemente sulle ricerche testuali. Tuttavia, con l'ascesa dei comandi vocali, è diventato essenziale adattare i criteri di ottimizzazione anche per le richieste vocali.
Le persone, infatti, stanno cambiando il loro modo di interagire con i motori di ricerca, preferendo sempre più spesso utilizzare la voce anziché la digitazione.
Da uno studio condotto da *Aditya Kumar Jh et al. (2024*), è emerso che l'utilizzo degli assistenti vocali come *Cortana*, *Siri*, *Amazon Echo* e *Google Assistant* è aumentato significativamente dal 2008 al 2016 [26].

[26] Jha, A. K., et al. (2024). Analysis of voice-based searches and how they affect digital marketing. *Educational Administration: Theory and Practice*, *30*(5), 13914-13921.



(Jha, A. K., et al. (2024). Analysis of voice-based searches and how they affect digital marketing. *Educational Administration: Theory and Practice*, *30*(5), 13914-13921).

Questa transizione comporta una serie di sfide e opportunità per i professionisti del marketing digitale. Ad esempio, le query vocali tendono a essere più conversazionali e naturali rispetto alle query testuali, il che richiede un ripensamento delle strategie SEO tradizionali. Inoltre, gli assistenti vocali come *Siri*, *Google Assistant e Alexa* stanno diventando intermediari chiave tra gli utenti e le informazioni online, influenzando in modo significativo il comportamento di ricerca e di acquisto.
Un aspetto cruciale legato all'uso degli assistenti vocali riguarda la gestione dei dati e la privacy degli utenti.
Queste tecnologie raccolgono una vasta gamma di informazioni personali, tra cui la posizione geografica, le preferenze di ricerca, le abitudini di utilizzo e molto altro. Tali dati, se da un lato permettono di fornire un servizio più personalizzato e rilevante, dall'altro sollevano importanti questioni etiche e legali relative alla privacy.
Le informazioni raccolte dagli assistenti vocali possono essere utilizzate dalle aziende per creare contenuti di marketing altamente mirati.
Ad esempio, conoscendo la posizione dell'utente, le preferenze di consumo e i comportamenti online, le aziende possono sviluppare campagne pubblicitarie su misura che rispondano in modo preciso alle esigenze e ai desideri degli utenti.

Questa capacità di personalizzazione rappresenta un potente strumento per migliorare l'efficacia delle strategie di marketing e aumentare il coinvolgimento dei clienti[27].
Oltre alle considerazioni tecniche, è fondamentale considerare anche le implicazioni legate alla privacy e alla sicurezza dei dati. Poiché gli assistenti vocali elaborano e memorizzano una quantità significativa di dati sensibili e la protezione di queste informazioni è di primaria importanza. Le aziende che sviluppano e gestiscono tali applicazioni devono garantire che i dati raccolti siano trattati con il massimo grado di riservatezza e sicurezza. Questo implica l'adozione di rigorose misure di protezione dei dati, tra cui la crittografia delle comunicazioni e l'implementazione di politiche di accesso e gestione dei dati rigorose.
In aggiunta, le normative sulla privacy, come il *Regolamento Generale sulla Protezione dei Dati (GDPR)* in Europa, impongono obblighi specifici riguardo alla raccolta, all'uso e alla conservazione delle informazioni personali.
Gli utenti devono essere informati chiaramente su come i loro dati vengono utilizzati e avere la possibilità di gestire le loro preferenze in merito alla raccolta e all'elaborazione dei dati. È cruciale che le aziende rispettino tali normative e garantiscano trasparenza e controllo agli utenti, per mantenere la loro fiducia e proteggere la loro privacy[28].
In sintesi, gli assistenti vocali rappresentano una delle più innovative e convenienti evoluzioni nel campo delle interfacce utente, offrendo una modalità di interazione tanto naturale quanto efficace.
La loro capacità di semplificare compiti complessi e di rispondere tempestivamente alle esigenze degli utenti dimostra il loro valore crescente nella nostra vita quotidiana e nell'ecosistema tecnologico moderno.
Nel prossimo paragrafo, si esploderanno due aspetti fondamentali, la storia e lo sviluppo degli assistenti vocali, analizzando come queste tecnologie si sono evolute nel tempo e come sono diventate parte integrante della nostra vita quotidiana.

---

[27] Jha, A. K., et al. (2024). Analysis of voice-based searches and how they affect digital marketing. *Educational Administration: Theory and Practice*, *30*(5), 13914-13921.
[28] Kevin, O., & Shibwabo, K. B. (2015, luglio 7). The application of real-time voice recognition to control critical mobile device operations. *Faculty of Information Technology, Strathmore University*, Nairobi, Kenya.

2.2 Storia e sviluppo

Il riconoscimento vocale, la capacità delle macchine di comprendere e interpretare il linguaggio umano, ha affascinato ingegneri e scienziati per decenni. Questo campo di ricerca ha visto progressi significativi dalle sue prime fasi negli anni '30 fino ai moderni assistenti vocali come *Siri, Google Assistant e Alexa*.

La storia del riconoscimento vocale ha origine negli anni '30, quando *Homer Dudley* dei *Bell Laboratories* propose un modello per l'analisi e la sintesi vocale.

Dudley sviluppò il *VODER* (*Voice Operating Demonstrator*), un dispositivo capace di produrre suoni simili a quelli umani, controllato manualmente da un operatore. Presentato all'*Esposizione Universale di New York* del 1939, il *VODER* rappresentò un significativo passo avanti verso la creazione di macchine parlanti.

Negli anni '50, la ricerca si concentrò sul riconoscimento di suoni e parole isolate. Un esempio notevole è il sistema sviluppato da *Davis, Biddulph* e *Balashek* dei *Bell Laboratories* nel 1952, capace di riconoscere le cifre pronunciate da un singolo parlante utilizzando le frequenze formanti dei suoni vocali. Questo approccio pionieristico influenzò le successive ricerche nel campo.

Negli anni '60 e '70, gli studi sul riconoscimento vocale si concentrarono sull'acustica e sulla fonetica. Ricercatori come *Itakura* e *Saito* in Giappone e *Vintsyuk* in Unione Sovietica svilupparono tecniche per la normalizzazione temporale e il riconoscimento dinamico dei pattern, migliorando la precisione dei sistemi di riconoscimento vocale.

Nel 1972, *l'Advanced Research Projects Agency (ARPA)* del Dipartimento della Difesa degli Stati Uniti finanziò il programma *Speech Understanding Research (SUR)*, stimolando lo sviluppo di sistemi più sofisticati.

Tra questi, il sistema *Harpy* della *Carnegie Mellon University*, capace di riconoscere oltre mille parole, rappresentò un importante avanzamento grazie all'uso di un approccio di ricerca a grafo per gestire la complessità del linguaggio.

Gli anni '80 videro l'introduzione della modellazione statistica nel riconoscimento vocale, con l'adozione dei modelli nascosti di *Markov (Hidden Markov Models, HMM)*. Questi modelli permisero di rappresentare matematicamente le variazioni intrinseche del segnale

vocale, migliorando notevolmente la precisione e la robustezza dei sistemi di riconoscimento.
IBM e AT&T Bell Laboratories furono tra i principali attori di questa rivoluzione. *IBM*, guidata da *Fred Jelinek*, sviluppò il sistema *Tangora*, un "*dattilografo vocale*" in grado di riconoscere parole e frasi pronunciate da un singolo parlante.
Tangora utilizzava un modello di linguaggio statistico basato su n-grammi, migliorando l'accuratezza del riconoscimento. *AT&T Bell Laboratories*, invece, si concentrò sul riconoscimento vocale indipendente dal parlante, sviluppando algoritmi di clustering e tecniche di modellazione acustica per gestire la variabilità dei segnali vocali provenienti da diversi parlanti.
Questi sforzi culminarono nello sviluppo di sistemi come il *Voice Recognition Call Processing (VRCP)*, che automatizzava la gestione delle chiamate telefoniche.
Gli anni '90 segnarono l'espansione commerciale del riconoscimento vocale, con l'introduzione di sistemi pratici per il grande pubblico. Tra i principali successi vi furono il sistema di informazioni sui voli *Pegasus* e il sistema di informazioni meteorologiche *Jupiter*, entrambi sviluppati al *Massachusetts Institute of Technology (MIT).*
Questi sistemi dimostrarono l'efficacia della gestione dei dialoghi, guidando gli utenti attraverso menu impliciti senza richiedere dettagli espliciti delle query.
Un'altra importante applicazione fu il sistema *"How May I Help You?" (HMIHY) di AT&T*, introdotto nel 2000, che utilizzava il riconoscimento vocale per il routing delle chiamate nei centri di assistenza clienti.
Questi sistemi dimostrarono che, sebbene il riconoscimento vocale non fosse ancora perfetto, poteva fornire valore reale agli utenti migliorando l'efficienza e l'efficacia delle interazioni uomo-macchina.

Il nuovo millennio

Con l'avvento del nuovo millennio, il riconoscimento vocale ha fatto un ulteriore balzo in avanti con l'introduzione degli assistenti vocali virtuali. *Apple* ha lanciato *Siri* nel 2011, seguito da *Google Now* (poi evoluto in *Google Assistant*) e *Amazon Alexa*.
Questi assistenti vocali hanno reso il riconoscimento vocale una parte integrante della vita quotidiana di milioni di persone, consentendo interazioni naturali con i dispositivi elettronici.
Gli assistenti vocali moderni combinano tecnologie avanzate di riconoscimento vocale con intelligenza artificiale e apprendimento automatico, permettendo alle macchine di comprendere e rispondere a una vasta gamma di comandi vocali.
L'uso di reti neurali profonde *(Deep Neural Networks, DNN)* ha ulteriormente migliorato la precisione del riconoscimento, rendendo possibili applicazioni come la trascrizione automatica, il controllo vocale dei dispositivi domestici e la ricerca vocale su internet.
Il decennio dal 2010 al 2020 ha visto miglioramenti straordinari nel riconoscimento vocale automatico. L'ascesa del deep learning ha trasformato il campo, con tassi di errore delle parole che sono scesi al di sotto di quelli dei trascrittori professionisti su alcuni benchmark.
Le tecnologie di assistenti vocali come *Siri di Apple*, *Alexa di Amazon* e *Google Home* hanno rivoluzionato il modo in cui le persone utilizzano il riconoscimento vocale quotidianamente.
Gli ingredienti chiave del successo del deep learning nel riconoscimento vocale sono stati la disponibilità di enormi set di dati trascritti, il rapido progresso nelle unità di elaborazione grafica (*GPU*) e il miglioramento degli algoritmi di apprendimento e delle architetture dei modelli. Questi fattori hanno consentito una riduzione costante e significativa dei tassi di errore delle parole, rendendo il riconoscimento vocale una tecnologia affidabile e diffusa.
Guardando al futuro, fino al 2030, possiamo aspettarci ulteriori progressi entusiasmanti nella tecnologia del riconoscimento vocale.
Sebbene i miglioramenti nella precisione generale del riconoscimento vocale non saranno drammatici come nel decennio precedente, ci sono diverse aree di sviluppo che promettono di portare innovazioni significative.

Apprendimento semi-supervisionato: L'apprendimento semi-supervisionato, in particolare i modelli pre-addestrati auto-supervisionati, diventeranno parte integrante di molte applicazioni di machine learning, incluso il riconoscimento vocale. Questi modelli possono migliorare l'accuratezza utilizzando dati non annotati, rendendo la tecnologia più accessibile anche a laboratori di ricerca più piccoli e accademici.

Riconoscimento su dispositivo: La maggior parte del riconoscimento vocale avverrà direttamente sul dispositivo o al limite della rete, migliorando la privacy dei dati, riducendo la latenza e garantendo la disponibilità del servizio anche senza connessione internet. Ciò richiederà modelli con requisiti di calcolo e memoria più piccoli, nonché un consumo energetico ridotto.

Personalizzazione: I modelli di riconoscimento vocale saranno profondamente personalizzati per gli utenti individuali, utilizzando il contesto e le preferenze personali per migliorare l'accuratezza. Questo sarà particolarmente utile per gruppi di utenti o domini che sono sottorappresentati nei dati di addestramento.

Rappresentazioni più ricche: Le trascrizioni saranno sostituite da rappresentazioni più ricche per i compiti a valle che si basano sull'output di un riconoscitore vocale. Queste rappresentazioni potrebbero includere ipotesi multiple con pesi differenti, migliorando la comprensione semantica delle interazioni vocali.

Servizi di trascrizione automatizzati: Entro il 2030, il 99% dei servizi di trascrizione vocale sarà automatizzato, con i trascrittori umani che si occuperanno del controllo di qualità e della correzione delle trascrizioni più difficili. Questo includerà la sottotitolazione di video, la trascrizione di interviste e la trascrizione di lezioni o discorsi.

Assistenti vocali migliorati: Gli assistenti vocali continueranno a migliorare, ma in modo incrementale piuttosto che fondamentale.

I principali colli di bottiglia non saranno più nel riconoscimento vocale, ma nella comprensione del linguaggio naturale, nella capacità di mantenere conversazioni e nelle risposte contestuali multiple.

La storia del riconoscimento vocale è un viaggio affascinante attraverso decenni di innovazione e progresso tecnologico.

Dalle prime macchine parlanti agli assistenti vocali intelligenti di oggi, questa tecnologia ha trasformato il modo in cui interagiamo con le macchine e ha aperto nuove possibilità per l'automazione e l'efficienza. Sebbene ci siano ancora molte sfide da affrontare, i continui avanzamenti nella ricerca e nello sviluppo promettono un futuro in cui le macchine saranno in grado di comprendere e rispondere al linguaggio umano con una precisione e una naturalezza sempre maggiori.

Le previsioni per il decennio 2020-2030 indicano che il riconoscimento vocale continuerà a evolversi, diventando più integrato nella nostra vita quotidiana e migliorando l'interazione uomo-macchina.

Con l'adozione di tecniche di apprendimento semi-supervisionato, la personalizzazione avanzata e l'implementazione su dispositivi, possiamo aspettarci che il riconoscimento vocale diventi ancora più preciso, accessibile e utile in una varietà di applicazioni[29] [30].

[29] Hannun, A. (2021, agosto 3). The history of speech recognition to the year 2030.

[30] Juang, B. H., & Rabiner, L. R. (2004, agosto 10). Automatic speech recognition: A brief history of the technology development. *Georgia Institute of Technology, Atlanta; Rutgers University; University of California, Santa Barbara*.

2.3 Funzionamento del riconoscimento vocale

Come discusso nel paragrafo precedente, la tecnologia di riconoscimento vocale ha avuto inizio con un vocabolario limitato, ma oggi trova applicazione in numerosi settori e il suo mercato è destinato a crescere considerevolmente, raggiungendo un valore stimato di 24,9 miliardi di USD entro il 2025.
Attualmente, il mercato offre una vasta gamma di dispositivi e applicazioni di riconoscimento vocale. Le soluzioni più avanzate fanno uso di intelligenza artificiale (AI) e apprendimento automatico (machine learning). Queste tecnologie sono in grado di integrare elementi come grammatica, sintassi e la struttura dei segnali audio e vocali per comprendere il linguaggio umano.
Il processo di riconoscimento vocale inizia con l'acquisizione dell'audio, che avviene tramite il microfono del dispositivo. Successivamente, si procede con la fase di preelaborazione, durante la quale il segnale audio viene pulito eliminando i rumori di fondo e normalizzando il volume.
In seguito, il sistema analizza l'audio pre-elaborato ed estrae caratteristiche chiave come tono, frequenza e intonazione. Queste caratteristiche vengono quindi confrontate con pattern vocali memorizzati in un database per identificare le parole pronunciate.
Il programma valuta anche la biometria vocale dell'utente, esaminando elementi come la frequenza, il tono, l'accento e l'intonazione del parlante.
L'ultima fase del processo coinvolge la conversione del parlato in testo, seguita dall'interpretazione del significato attraverso algoritmi di elaborazione del linguaggio naturale *(NLP)*.
La tecnologia di riconoscimento vocale viene valutata principalmente in base alla sua accuratezza, misurata attraverso il tasso di errore delle parole *(WER)*, e alla sua velocità di risposta.
Il riconoscimento vocale, dunque, si basa su una varietà di algoritmi e tecniche di calcolo per convertire il parlato in testo scritto e migliorare l'accuratezza della trascrizione. Uno degli strumenti fondamentali in questo campo è l'elaborazione del linguaggio naturale (*NLP*), che consente ai computer di comprendere e interpretare il linguaggio umano.
Diversi algoritmi sono impiegati nel riconoscimento vocale per migliorare la precisione e l'efficacia delle trascrizioni.

Tra questi, i modelli di linguaggio come gli *N-grammi* e le reti neurali profonde (*deep learning*) sono particolarmente utili.
Gli *N-grammi* rappresentano una tecnica utilizzata per modellare le probabilità di sequenze di parole in un linguaggio. Un *N-gramma* è una sequenza di *N* parole consecutive. Ad esempio, "*ordina la pizza*" è un trigramma o *3-gramma*, mentre "*per favore ordina la pizza*" è un *4-gramma*. I modelli di *N-grammi* assegnano probabilità alle frasi o alle locuzioni basandosi sulla frequenza con cui appaiono in un corpus di testo. Questo approccio utilizza la grammatica e le probabilità di determinate sequenze di parole per migliorare la precisione del riconoscimento vocale. Più precisamente, aiuta il sistema a predire quale parola è più probabile che segua in una data sequenza, riducendo così gli errori di trascrizione.
Le *Reti Neurali* sono sfruttate principalmente per algoritmi di apprendimento profondo (*deep learning*). Queste reti elaborano i dati di addestramento imitando l'interconnettività del cervello umano attraverso strati di nodi. Ogni nodo è composto da input, pesi, un *bias* e un output. Se il valore di output supera una determinata soglia, "*attiva*" il nodo, passando i dati allo strato successivo nella rete.
Le reti neurali apprendono questa funzione di mappatura attraverso l'apprendimento supervisionato, regolandosi in base alla funzione di perdita attraverso il processo di discesa del gradiente. Sebbene le reti neurali tendano a essere più accurate e possano gestire grandi quantità di dati, richiedono un tempo maggiore per l'addestramento rispetto ai modelli linguistici tradizionali, comportando un costo in termini di efficienza delle prestazioni.
Gli algoritmi di *Speaker Diarization (SD)* identificano e segmentano il parlato in base all'identità dell'oratore. Questa tecnica è particolarmente utile per distinguere tra diversi individui in una conversazione. Viene spesso applicata nei call center per distinguere tra clienti e agenti di vendita, migliorando così l'efficacia del servizio clienti e fornendo una trascrizione accurata delle interazioni multiple[31].
L'adozione di tecnologie come il riconoscimento vocale offre numerosi vantaggi che ne fanno strumenti sempre più indispensabili nella nostra vita quotidiana e professionale.

[31] *IBM (International Business Machines Corporation). (n.d.). What is speech recognition? IBM. https://www.ibm.com/topics/speech-recognition.*

Multitasking e utilizzo a mani libere: Il riconoscimento vocale permette di eseguire più attività contemporaneamente senza l'uso delle mani, migliorando notevolmente l'efficienza operativa. Questo è particolarmente utile in contesti dove l'uso delle mani è limitato, come durante la guida, la cucina o nel corso di interventi chirurgici. Gli utenti possono gestire dispositivi, inviare messaggi o cercare informazioni semplicemente parlando, senza interrompere altre attività.

Velocità di interazione*:* Parlare e impartire comandi vocali è intrinsecamente più veloce che digitare. La velocità della voce umana consente di formulare e trasmettere comandi in una frazione del tempo necessario per scriverli, rendendo i processi più rapidi e snelli. Questo risulta particolarmente vantaggioso in situazioni dove la velocità è cruciale, come nel caso di risposte rapide durante riunioni o nella gestione di emergenze.

Espansione dei casi d'uso*:* I casi d'uso del riconoscimento vocale si stanno ampliando grazie ai progressi nell'apprendimento automatico e nelle reti neurali profonde. Queste tecnologie avanzate migliorano costantemente l'accuratezza e l'efficacia del riconoscimento vocale, permettendo applicazioni sempre più sofisticate. Ad esempio, l'uso di assistenti virtuali come *Siri, Alexa e Google Assistant* è in continua crescita, supportando un'ampia gamma di funzioni che vanno dalla gestione della casa intelligente all'assistenza personale, dalla traduzione in tempo reale alla navigazione stradale. Come tutte le tecnologie, il riconoscimento vocale presenta anche alcuni svantaggi oltre ai numerosi vantaggi.

Possibilità di errori*:* Sebbene la tecnologia di riconoscimento vocale stia progredendo rapidamente, non è ancora perfetta e può commettere errori. La precisione del sistema può variare a seconda delle condizioni di utilizzo e della qualità del segnale audio. Questo può portare a malintesi e trascrizioni errate, soprattutto in situazioni in cui la pronuncia è poco chiara o quando vengono utilizzate parole omofone.

Interferenza del rumore di fondo: Uno dei maggiori problemi del riconoscimento vocale è l'interferenza causata dal rumore di fondo. Ambienti rumorosi possono compromettere l'accuratezza del sistema, rendendo difficile per l'algoritmo distinguere tra la voce dell'utente e i rumori circostanti. Questa interferenza può ridurre l'affidabilità del

riconoscimento vocale, soprattutto in luoghi pubblici o durante eventi affollati.

***Preoccupazioni per la riservatezza dei dati**:* La riservatezza dei dati registrati è una preoccupazione significativa con l'uso del riconoscimento vocale. I dati vocali raccolti possono contenere informazioni sensibili che, se non adeguatamente protette, potrebbero essere vulnerabili a violazioni della privacy. L'archiviazione e l'elaborazione di questi dati sollevano questioni etiche e legali riguardo alla protezione delle informazioni personali degli utenti[32].

Le sfide tecnologiche ed etiche che questa tecnologia deve affrontare sono principalmente due. La prima riguarda la sicurezza dei dati: le aziende devono adottare misure di sicurezza solide per proteggere i dati vocali degli utenti. La seconda sfida è il consenso informato: è fondamentale che gli utenti siano pienamente informati su come i loro dati vocali vengono raccolti, utilizzati e protetti. Inoltre, è essenziale ottenere il consenso esplicito degli utenti prima di procedere con la raccolta e l'utilizzo delle loro informazioni vocali.

[32] Shaip. (2024, luglio 16). Leveraging voice – Overview and applications of voice recognition technology. *Shaip*. https://www.shaip.com/blog/voice-recognition-overview-and-applications/

2.4 Applicazione dei sistemi di riconoscimento vocale nel mondo reale

La tecnologia di riconoscimento vocale ha avuto inizio con un vocabolario limitato, ma oggi trova applicazione in numerosi settori e il suo mercato è destinato a crescere considerevolmente, raggiungendo un valore stimato di 24,9 miliardi di USD entro il 2025.
Le soluzioni avanzate sfruttano l'intelligenza artificiale e il *machine learning* per migliorare la comprensione del linguaggio umano.
In questo paragrafo esploreremo nel dettaglio le applicazioni del riconoscimento vocale nel mondo reale e le implicazioni di questa tecnologia sulla nostra vita quotidiana.
Il riconoscimento vocale ha rapidamente trasformato il modo in cui interagiamo con i nostri dispositivi. Dispositivi come *Amazon Echo, Google Home e Apple Siri* rappresentano solo l'inizio di questa trasformazione, offrendo funzionalità che spaziano dalla gestione delle attività quotidiane alla fornitura di supporto emotivo.
Questa tecnologia, che inizialmente poteva sembrare difficile da realizzare, è ora parte integrante della vita quotidiana di molti utenti in tutto il mondo. *Amazon Echo* e *Google Home* possono controllare altri dispositivi intelligenti, rispondere a domande, fornire aggiornamenti sul traffico e sulle condizioni meteorologiche, e persino leggere storie ai bambini. Questi dispositivi stanno evolvendo per diventare il centro dei sistemi smart home, con capacità sempre più avanzate.
Ad esempio, *Google Home* è ora in grado di riconoscere fino a sei voci diverse, permettendo a ciascun membro della famiglia di avere un'esperienza personalizzata. Inoltre, la capacità di interfacciarsi con altri dispositivi smart, come luci e termostati, rende questi assistenti vocali strumenti indispensabili per la gestione domestica.
Nel settore automobilistico, il riconoscimento vocale è utilizzato per migliorare la sicurezza e la comodità dei conducenti. Ad esempio, l'integrazione di *Alexa* nelle automobili *Ford* permette ai conducenti di ottenere indicazioni stradali e creare liste della spesa senza dover distogliere le mani dal volante.
La capacità di *Alexa* di integrarsi con i sistemi di navigazione e di fornire informazioni in tempo reale sul traffico è un esempio di come il

riconoscimento vocale possa migliorare significativamente l'esperienza di guida.
Per le persone anziane, i dispositivi a riconoscimento vocale possono rappresentare un aiuto significativo.
Questi dispositivi possono fornire promemoria per l'assunzione di farmaci, aiutare con le chiamate di emergenza e offrire compagnia attraverso interazioni vocali. Questo può ridurre il carico cognitivo per i *caregiver* e migliorare la qualità della vita degli anziani. Ad esempio, un semplice comando vocale può ricordare agli anziani di prendere i loro farmaci o di controllare i livelli di zucchero nel sangue, migliorando la gestione delle condizioni di salute croniche. Inoltre, la capacità di questi dispositivi di rispondere a comandi vocali permette agli anziani di accedere facilmente a informazioni e servizi senza dover utilizzare interfacce complicate.
I dispositivi di riconoscimento vocale sono utilizzati anche nel campo dell'educazione, fornendo risorse didattiche e rispondendo a domande complesse che possono stimolare l'apprendimento dei bambini. Allo stesso tempo, offrono funzionalità di intrattenimento come la riproduzione di musica, la gestione dei dispositivi di streaming e l'interazione con giochi vocali.
Ad esempio, *Google Home* può rispondere a domande di matematica, spiegare concetti scientifici e persino aiutare con la pronuncia di parole straniere, diventando un prezioso strumento educativo. Inoltre, la capacità di questi dispositivi di interagire con piattaforme di streaming musicale e di controllare la riproduzione di video li rende anche strumenti di intrattenimento completi.
L'antropomorfizzazione dei dispositivi di riconoscimento vocale, ovvero l'attribuzione di caratteristiche umane a questi dispositivi, è un fenomeno comune.
Le persone tendono a sviluppare un attaccamento emotivo verso questi dispositivi, trattandoli come membri della famiglia o amici intimi.
Questo può essere potenziato dalla capacità dei dispositivi di rispondere con intonazioni umane e di adattarsi alle preferenze personali dell'utente. Ad esempio, *Alexa* di *Amazon* utilizza una voce femminile con intonazioni calde e accoglienti, che può creare un senso di comfort e familiarità negli utenti. Le persone possono iniziare a vedere questi dispositivi non solo come strumenti tecnologici, ma come compagni che possono fornire supporto emotivo e assistenza.

L'abitudine all'uso di dispositivi a riconoscimento vocale può portare a cambiamenti nelle norme comportamentali. Gli utenti possono diventare meno consapevoli della presenza di questi dispositivi, fidandosi implicitamente della loro capacità di agire nel loro migliore interesse. Tuttavia, questa fiducia può esporli a rischi di privacy e sicurezza.

Ad esempio, ci sono stati casi in cui i dispositivi di riconoscimento vocale hanno registrato conversazioni non intenzionalmente, sollevando preoccupazioni sulla possibile violazione della privacy domestica.

La capacità di questi dispositivi di ascoltare costantemente l'ambiente circostante per rilevare comandi vocali significa che potrebbero potenzialmente registrare informazioni sensibili senza il consenso esplicito degli utenti[33].

La tecnologia di riconoscimento vocale ha fatto passi da gigante negli ultimi anni, trovando applicazione in una vasta gamma di dispositivi e settori. *Amazon Echo*, introdotto nel 2014, è diventato rapidamente un simbolo di questa rivoluzione tecnologica, integrandosi nelle case di milioni di utenti. *Google Home e Apple Siri* hanno seguito l'esempio, offrendo funzionalità simili e migliorando costantemente le loro capacità grazie ai progressi nell'intelligenza artificiale (*AI*) e nell'apprendimento automatico (*machine learning*). Tuttavia, come dimostra il caso del 2015 in cui un *Echo* di *Amazon* è stato implicato in un'indagine per omicidio, le implicazioni di privacy e sicurezza di questi dispositivi sono diventate un argomento di grande preoccupazione.

Nel 2015, alcune testate giornalistiche hanno riportato che la polizia è riuscita a estrarre l'audio da un dispositivo, sebbene non sia stato specificato il tipo di informazioni contenute. Dispositivi come *Alexa*, insieme ad altri simili, si attivano tramite specifiche parole chiave. Tuttavia, non è insolito che si attivino accidentalmente, registrando frammenti di conversazione. In uno dei dispositivi presenti nella casa del

[33] Kevin, O., & Shibwabo, K. B. (2015, luglio 7). The application of real-time voice recognition to control critical mobile device operations. *Faculty of Information Technology, Strathmore University*, Nairobi, Kenya.

sospettato, è stato registrato un utilizzo di 140 litri d'acqua durante la notte in cui la vittima è stata trovata nella vasca idromassaggio del sospettato[34].
La capacità di questi dispositivi di "*ascoltare*" è un passo avanti verso la realizzazione di una interfaccia senza soluzione di continuità.
La tecnologia di riconoscimento vocale è destinata a evolversi ulteriormente, integrando sempre più funzioni e migliorando la sua accuratezza. Le future generazioni di dispositivi ad attivazione vocale saranno probabilmente in grado di riconoscere e rispondere a una gamma ancora più ampia di comandi vocali, migliorando l'interazione *uomo-macchina*.
L'adozione diffusa dei dispositivi ad attivazione vocale avrà anche un impatto significativo sul comportamento sociale e sulle norme. L'antropomorfizzazione di questi dispositivi, ossia l'attribuzione di caratteristiche umane alle macchine, potrebbe influenzare il modo in cui le persone percepiscono e interagiscono con la tecnologia. Ad esempio, molti utenti si riferiscono ai loro assistenti vocali con nomi umani e li trattano come se fossero parte della famiglia. Questo fenomeno può portare a un maggiore attaccamento emotivo ai dispositivi e a un aumento della fiducia nei loro confronti.
Tuttavia, questa fiducia potrebbe essere sfruttata in modo improprio. L'abitudine a interagire con assistenti vocali potrebbe ridurre la capacità degli utenti di distinguere tra comunicazioni con esseri umani e macchine, aumentando il rischio di manipolazione e frode. Inoltre, la dipendenza crescente da questi dispositivi potrebbe ridurre le interazioni sociali tra le persone, portando a una maggiore isolamento sociale.
Il riconoscimento vocale rappresenta una delle tecnologie più promettenti e in rapida evoluzione del nostro tempo, con applicazioni che spaziano dalla domotica alla sanità, dall'*Automotive* alla sicurezza. Tuttavia, la sua diffusione solleva anche importanti questioni etiche e di privacy che devono essere affrontate per garantire un uso sicuro e responsabile. Le aziende tecnologiche, i legislatori e i consumatori devono collaborare per sviluppare normative e pratiche che proteggano la privacy degli utenti e prevenire l'uso improprio dei dati.

[34] Parlangeli, D. (2016, dicembre 28). La polizia americana vuole sentire Echo di Amazon per un caso di omicidio. *Wired Italia*. https://www.wired.it/gadget/accessori/2016/12/28/polizia-echo-amazon-omicidio/

Il futuro del riconoscimento vocale è luminoso, ma richiede un equilibrio tra innovazione e tutela dei diritti degli utenti. Solo attraverso un approccio etico e responsabile possiamo garantire che questa tecnologia continui a migliorare la nostra vita quotidiana senza compromettere la nostra privacy e sicurezza [35].

Nel prossimo capitolo verranno esaminati gli aspetti legali dei dispositivi di riconoscimento vocale, includendo alcuni casi concreti di violazione della privacy legati al loro utilizzo. Inoltre, si affronteranno le questioni legali relative alla raccolta e all'uso dei dati personali tramite i cookie, nonché le misure di tutela dei consumatori nell'intera macroarea della protezione dei dati.

[35] Hui, J. Y., & Leong, D. (2017). The era of ubiquitous listening: Living in a world of speech-activated devices. *Asian Journal of Public Affairs*, *10*(1), e5.

CAPITOLO III

ASPETTI LEGALI ED ETICI DELL'ACTIVE LISTENING

Nei primi due capitoli della tesi, è stato esplorato il concetto di "*Active Listening*" nel contesto del marketing digitale, ponendo maggiore attenzione sulle implicazioni tecnologiche e sui casi studio che illustrano come questa pratica venga utilizzata per raccogliere e analizzare le conversazioni degli utenti. È stata evidenziata l'evoluzione delle tecnologie di riconoscimento vocale e la diffusione degli assistenti vocali e come questi abbiano sollevato preoccupazioni significative riguardo alla privacy degli utenti, particolarmente in relazione alla personalizzazione della pubblicità.

Successivamente, è stato approfondito il funzionamento delle tecnologie alla base dell'*Active Listening*, con un'analisi dettagliata dei sistemi di riconoscimento vocale, della loro evoluzione storica, e delle loro applicazioni nel mondo reale. Si è discusso su come queste tecnologie possano migliorare l'esperienza utente, ma al contempo come possono sollevare questioni cruciali sulla gestione dei dati personali e sulla sicurezza.

In un'epoca in cui la privacy digitale è costantemente minacciata, è fondamentale comprendere il quadro normativo che regola l'uso delle tecnologie di ascolto attivo e come le aziende possono operare all'interno dei confini legali. Questo capitolo esplorerà le normative esistenti, ponendo maggior enfasi sulle normative europee, e analizzerà il concetto di consenso informato, nonché la trasparenza delle pratiche di raccolta dei dati. Inoltre, verrà discussa l'importanza della responsabilità etica nel marketing e la crescente attenzione dei consumatori verso la protezione dei propri dati.

3.1 Il Regolamento dell'Unione Europea: Gestione e Protezione dei Dati Personali

Negli anni Novanta, l'Unione Europea attribuiva grande importanza al rispetto dei diritti fondamentali, tra cui il diritto alla privacy. Tuttavia, mancava una regolamentazione uniforme tra gli Stati membri in materia di protezione dei dati personali. Durante questo periodo, esisteva già un insieme complesso di principi fondamentali relativi alla privacy. Di conseguenza, il legislatore europeo decise di introdurre la direttiva "*95/46/CE*", mirata a proteggere le persone fisiche riguardo al trattamento dei dati personali e a facilitare la libera circolazione di tali dati.
Questa direttiva entrò in vigore il 24 ottobre 1995, stabilendo che tutti gli Stati membri avrebbero dovuto adeguare la propria legislazione entro il 31 dicembre 1996.
In Italia, la situazione era particolare; la direttiva venne recepita con la *legge n. 675 del 31 dicembre 1996*, la prima normativa italiana in materia di protezione dei dati personali.
Questa legge sanciva che la riservatezza delle persone, sia fisiche che giuridiche, costituisse un diritto assoluto e inviolabile, degno di tutela mediante sanzioni penali, civili e amministrative. La direttiva perseguiva due obiettivi principali: da un lato, proteggere il diritto alla privacy dei dati personali, e dall'altro, garantire la libera circolazione dei dati personali tra gli Stati membri dell'UE, noto come "*free flow of data*".
L'Unione Europea ha deciso di passare da una direttiva a un regolamento come strumento legislativo, poiché la direttiva non garantiva un'applicazione uniforme dei principi tra gli Stati membri, cosa che invece il regolamento assicura. Secondo l'Articolo 288 del *TFUE*, il regolamento è un atto di portata generale, vincolante in tutti i suoi elementi e direttamente applicabile in tutti gli Stati membri [36].
A differenza della direttiva, il regolamento entra immediatamente in vigore negli ordinamenti nazionali, con disposizioni che sono obbligatorie e prevalgono anche su eventuali norme nazionali contrastanti.

[36] Unione Europea. (2007). Trattato sul funzionamento dell'Unione Europea, art. 288. *Gazzetta ufficiale dell'Unione Europea*, 13 dicembre 2007

In seguito, è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il *Regolamento UE 2016/679*, noto come *GDPR* (*General Data Protection Regulation*) [37].

Il presente Regolamento sostituisce la precedente direttiva *95/46/CE* con l'intento di armonizzare le normative riguardanti la protezione dei dati personali all'interno dell'Unione Europea.

Il Regolamento *UE 2016/679*, entrato ufficialmente in vigore il 25 maggio 2018, mira a soddisfare un'esigenza particolarmente sentita nell'era della globalizzazione in cui ci troviamo [38]. Quest'ultimo dichiara che: «*La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano*» [39].

Negli ultimi anni, infatti, la globalizzazione e l'innovazione tecnologica hanno portato a un notevole aumento nella raccolta e condivisione dei dati personali, esponendo gli individui a un maggior rischio di essere tracciati. Il diritto alla protezione dei dati personali è un diritto autonomo e distinto rispetto alla riservatezza della privacy, in quanto amplia la tutela dell'individuo oltre la sua sfera privata, estendendola alle interazioni sociali. Questo diritto garantisce all'individuo il controllo sulla diffusione dei propri dati, offrendo la possibilità di richiederne la cancellazione o la rettifica.

[37] Sgobbi, M. (2022). *Il trattamento dei dati personali e gli strumenti di raccolta dei dati online: Cookies e Big Data* [Tesi di laurea magistrale, Università degli Studi di Padova, Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali].

[38] Locoratolo, B. (2021). *Il trattamento dei dati personali e la privacy*. Napoli: Simone.

[39] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR*).

Il concetto di diritto alla privacy ha origini che risalgono al 15 dicembre 1890, quando l'avvocato *Warren Samuel* e il giudice *Louis Brandeis* pubblicarono un articolo sulla rinomata rivista dell'epoca "*Harvard Law Review*", intitolato "*The Right to Privacy*" [40].

In questo scritto, la privacy veniva descritta come il diritto dell'individuo di decidere quali informazioni personali condividere con gli altri e in quali contesti.

Il Regolamento, dunque, ha un obiettivo ben preciso: fornire un elevato livello coerente di protezione delle persone fisiche e giuridiche e di eliminare qualsiasi ostacolo rivolto alla circolazione dei dati nell'Unione Europea [41].

Per quanto concerne l'applicazione delle norme previste dal GDPR, gli Articoli 1 e 2 delineano chiaramente due ambiti distinti: quello materiale e quello territoriale.

L'*Articolo 3* del Regolamento introduce il principio di stabilimento, il quale stabilisce che deve esistere una presenza effettiva di un luogo all'interno del territorio europeo, attraverso uno stabilimento, un titolare o un responsabile dello stesso. Ciò significa che i dati possono essere trasferiti all'estero, a condizione che l'entità che li gestisce abbia una sede all'interno del territorio nazionale; questo è uno dei principi adottati dall'*Agenzia delle Entrate* italiana.

Inoltre, questo articolo si applica al trattamento dei dati personali svolto nell'ambito delle attività di uno stabilimento da parte di un titolare o responsabile del trattamento all'interno dell'Unione Europea, indipendentemente dal luogo in cui avviene effettivamente il trattamento, sia esso all'interno o al di fuori dell'Unione.

Nel GDPR, i dati personali sono definiti come "*qualsiasi informazione che riguardi una persona fisica identificata o identificabile*". Una persona è considerata identificabile se può essere riconosciuta attraverso un nome, un numero di identificazione, dati di localizzazione o qualsiasi

[40] Corona, F. (2018). Diritto alla riservatezza: riconoscimento ed evoluzione normativa. *Legaldesk.it*.

[41] Data Protection Manager. (2021). Nascita del diritto alla privacy e sua evoluzione come diritto alla riservatezza e alla protezione dei dati. *Privacymanager.eu*

caratteristica specifica legata alla sua identità fisica, fisiologica, genetica, psicologica, economica, culturale o sociale [42].

È evidente che i dati personali costituiscono informazioni relative a un individuo.

Per comprendere appieno cosa si intende per "*informazione*", è utile distinguere tra "*informazione sintattica*", "*informazione semantica*" e "*informazione strutturale*".

L'informazione semantica si riferisce a contenuti dotati di significato, l'informazione sintattica riguarda i dati rappresentati attraverso una specifica serie di segni, mentre l'informazione strutturale si riferisce alla configurazione fisica di un oggetto. *Herbert Zech*, autore di una *classificazione complessa*, sottolinea come questa distinzione si manifesti anche nella vita quotidiana: quando parliamo del contenuto di una notizia o di un libro, ci riferiamo all'aspetto semantico; quando discutiamo della composizione di un testo o di un file, ci riferiamo all'aspetto sintattico; infine, quando trattiamo di un CD o di un libro stampato, ci riferiamo all'aspetto strutturale. Questi tre livelli sono interconnessi: il significato può essere contenuto in un testo, il testo può essere composto attraverso segni, e quest'ultimo può essere materializzato su un supporto fisico. Pertanto, lo strato fisico supporta quello sintattico, e lo strato sintattico veicola quello semantico [43] [44] [45].

Da un punto di vista semantico, i dati personali possono essere definiti come quelle informazioni che possiedono un significato specifico e descrivono qualcosa di riferibile a una persona fisica, indipendentemente dalla forma sintattica o dal supporto materiale utilizzato per trasmettere e conservare tali informazioni[46].

---

[42] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), art. 4, comma 1*.

[43] Zech, H. (2015). Information as a property. *JIPITEC, 6*, 192, par. 1.

[44] Zech, H. (2016). A legal framework for a data economy in the European Digital Single Market: Rights to use data. *Journal of Intellectual Property Law & Practice*, *11*(6), 460 ss.

[45] Zech, H. (2016). Data as a tradeable commodity. In A. De Franceschi (Ed.), *European contract law and the digital single market* (pp. 51 ss). Cambridge: Intersentia.

[46] Floridi, L. (2009). Data is a description of something that allows it to be recorded, analyzed, and reorganized. In G. Sommaruga (Ed.), *Formal theories of information: From Shannon to semantic information theory and general concepts of information* (pp. 13 ss). Springer.

La dottrina definisce il dato personale come un "*bene giuridico di secondo livello*", considerandolo il mezzo tecnico-giuridico utilizzato dai legislatori nazionali e comunitari per proteggere l'insieme dei diritti legati all'identità personale [47].

L'*Articolo 4* del Regolamento Generale sulla Protezione dei Dati (GDPR) distingue chiaramente tra "*dati personali*" e "*dati identificativi*". I dati personali comprendono tutte le informazioni che permettono di riconoscere una persona fisica, sia in modo diretto che indiretto.

Questo significa che qualsiasi dato che, preso singolarmente o in combinazione con altri, può portare all'identificazione di un individuo, rientra nella categoria dei dati personali.

D'altra parte, i dati identificativi sono una sottocategoria di dati personali, che consentono di identificare una persona fisica esclusivamente in modo diretto. Tra questi rientrano informazioni come l'indirizzo di residenza, l'indirizzo e-mail, il numero di telefono, o la targa del veicolo.

Questi elementi sono sufficienti, da soli, a stabilire l'identità della persona a cui si riferiscono.

Il GDPR approfondisce ulteriormente queste dinamiche nei suoi Considerando. Innanzitutto, viene sottolineato che, per valutare se una persona è identificabile, è necessario considerare tutti i mezzi ragionevolmente disponibili al titolare del trattamento o a terzi, che possano essere utilizzati per identificare direttamente o indirettamente la persona fisica in questione [48]. Questo principio è fondamentale per garantire una protezione completa e rigorosa dei dati personali.

In aggiunta, il GDPR riconosce che le persone fisiche possono essere associate a identificativi online generati dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli che utilizzano, come gli indirizzi IP, i cookies, o altri identificativi digitali come i tag a radiofrequenza.

Queste identificative digitali possono lasciare tracce, che, se combinate con altre informazioni o identificativi univoci, possono essere utilizzate per creare profili dettagliati delle persone fisiche, consentendo così di

---

[47] Locoratolo, B. (2021). *Il trattamento dei dati personali e la privacy* (p. 46). Napoli: Simone.

[48] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Considerando n. 26*.

identificarle [49]. Questo aspetto del regolamento evidenzia la complessità e la pervasività della raccolta e dell'uso dei dati personali nell'era digitale, richiedendo una particolare attenzione e protezione da parte dei legislatori e delle aziende.

Una sentenza significativa della *Corte di Giustizia* dell'Unione Europea, emessa il *19 ottobre 2016*, nel caso "*Patrick Breyer contro la Repubblica Federale Tedesca*", ha fornito chiarimenti cruciali in merito alla protezione dei dati personali[50].

Il caso riguardava la pratica della *Repubblica Federale* di Germania di raccogliere gli indirizzi IP degli utenti che visitavano i siti web governativi. *Patrick Breyer*, un cittadino tedesco, aveva intentato una causa contro il governo tedesco, sostenendo che la raccolta di indirizzi IP senza il consenso degli utenti violava il diritto alla protezione dei dati personali, poiché considerava l'indirizzo IP un dato personale.

Il governo tedesco, dal canto suo, ha difeso la propria pratica, argomentando che la raccolta degli indirizzi IP era necessaria per motivi di sicurezza, in particolare per prevenire attacchi informatici e individuare potenziali aggressori.

La *Corte di Giustizia Europea*, nella sua decisione, ha stabilito che un indirizzo IP, anche se dinamico, può essere considerato un dato personale qualora l'utente sia identificabile tramite ulteriori informazioni in possesso del fornitore di servizi internet.

Questa sentenza ha avuto un impatto rilevante, confermando che anche dati che non identificano direttamente un individuo possono essere classificati come dati personali se, attraverso altri mezzi, è possibile risalire all'identità dell'utente.

Questa decisione si inserisce nel più ampio contesto di protezione dei dati personali sancito dal Regolamento del GDPR, che riconosce l'importanza di tutelare ogni informazione che, direttamente o indirettamente, possa portare all'identificazione di una persona fisica. Il GDPR, infatti, definisce chiaramente i dati personali come qualsiasi informazione relativa a una persona fisica identificata o identificabile, ampliando la protezione a

---

[49] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Considerando n. 30.*

[50] InfoCuria - Giurisprudenza. (n.d.). *Sentenza della Corte di giustizia dell'Unione Europea, Causa C-434/16.*

un'ampia gamma di dati che includono anche identificativi online come gli indirizzi IP.
Tuttavia, il dato anonimo, ossia quel dato che non può essere associato a ad una persona fisica identificata o identificabile, non è considerato un dato personale [51].
Ad oggi si ritengono valide per il diritto interno le definizioni fornite dall'*Art. 4* del GDPR. Tali definizioni non contemplano i "*dati anonimi*" né la "*anonimizzazione*", così oggi ci ritroviamo senza una nozione formale di questi concetti. A tal proposito l'*Articolo 26* del GDPR prevede che i principi riguardanti la protezione dei dati personale non deve applicarsi a informazioni anonime, ossia a tutte quelle informazioni che non fanno alcun tipo di riferimento ad una persona fisica [52].
L'*Art. 4* del *Regolamento 2016/679* fa riferimento anche alla cosiddetta "*pseudonimizzazion*e" dei dati.
Quest'ultima è una tecnica utilizzata per proteggere la privacy delle informazioni personali, rendendo i dati meno identificabili.
Consiste nel sostituire gli identificatori diretti che possono essere ricondotti a una persona come, nome e cognome, numero di telefono, etc. con pseudonimi o altri identificatori che non rivelano l'identità originale.
Questo sotto intende che l'utilizzo di informazioni aggiuntive possono portare all'identificazione degli individui, motivo per cui i dati pseudonimi sono dei dati personali a tutti gli effetti [53].
Il Regolamento, nell'*Articolo 4*, *comma 2*, offre una definizione ampia di trattamento dei dati personali, descrivendolo come "*qualsiasi operazione o insieme di operazioni eseguite con o senza l'utilizzo 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*

[51] Italia. (2003). *Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 4*. Gazzetta Ufficiale della Repubblica Italiana, abrogato dal Decreto legislativo 10 agosto 2018, n. 101.
[52] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Considerando n. 26.*
[53] Massimini, M. (2021, maggio 11). Anonimizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR. *Privacy.it*.

forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".
Per comprendere meglio questa definizione, è utile approfondire i vari termini utilizzati.
La raccolta dei dati rappresenta la fase iniziale del trattamento, in cui si acquisiscono le informazioni. La registrazione implica la memorizzazione di questi dati su un supporto fisico o digitale. L'organizzazione si riferisce alla classificazione dei dati secondo criteri specifici. La conservazione riguarda il mantenimento di queste informazioni su un supporto, garantendo la loro disponibilità nel tempo. La consultazione consiste nel processo di lettura o accesso ai dati memorizzati.
Una distinzione importante è quella tra *comunicazione* e *diffusione dei dati*. La comunicazione prevede il trasferimento dei dati personali a specifici destinatari, diversi dall'interessato, dal rappresentante del titolare nello Stato, dal responsabile e dagli incaricati. In questo caso, i dati vengono condivisi con terzi. La diffusione, invece, riguarda la divulgazione dei dati a una platea indeterminata di soggetti, indipendentemente dalla modalità utilizzata, inclusa la pubblicazione su internet, come nel caso di una fotografia postata su un social network. Senza il consenso dell'interessato, la diffusione dei dati è da considerarsi illecita.
L'*Articolo 6* par. 1 del GDPR stabilisce le condizioni di liceità e dispone che il trattamento è lecito solo se e nella misura in cui occorra almeno una delle seguenti condizioni:

1. L'interessato ha espressamente acconsentito al trattamento dei propri dati personali per qualsiasi finalità [54].
2. Il trattamento è necessario per rispettare un obbligo legale a cui il titolare è vincolato;
3. Il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica.

Questa base giuridica può essere applicata secondo quanto stabilito nel *Considerando n. 46* del GDPR, che afferma:
"*Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali*

[54] Corona, F. (2022). Consenso privacy: le nuove regole del GDPR. *Legaldesk.it*.

fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana" [55].

In sintesi, la transizione dall'uso di una direttiva al GDPR è stata cruciale per uniformare la protezione dei dati personali in tutta l'Unione Europea, garantendo un'applicazione diretta e armonizzata delle norme.
Questo cambiamento ha permesso di superare le carenze della direttiva precedente, rispondendo in maniera più efficace alle sfide poste dalla globalizzazione e dalla tecnologia. Con l'introduzione del GDPR, è necessario ora esaminare come queste nuove normative abbiano influenzato il panorama delle politiche sulla privacy online e se le aziende siano effettivamente conformi alle nuove disposizioni, come sarà discusso nel prossimo paragrafo.

[55] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Considerando n. 46.*

3.2 L’impatto sulle aziende dopo l’entrata in vigore del GDPR

Il GDPR dell’Unione Europea è una delle normative più rigorose e complete mai adottate in materia di privacy e protezione dei dati personali. Come menzionato nel paragrafo precedente, la sua entrata in vigore il *25 maggio 2018* ha inevitabilmente avuto un impatto significativo.
Un anno dopo l'entrata in vigore del GDPR, *Thomas Linden* e altri autori, nel loro studio "*The Privacy Policy Landscape After the GDPR*," hanno analizzato l'impatto di questa normativa sulle politiche di privacy online. Il GDPR impone a tutti i responsabili del trattamento dei dati, in ogni settore, di essere trasparenti e chiari riguardo le loro pratiche di privacy, con l'obiettivo principale di superare le lacune delle normative precedenti. Subito dopo l'introduzione della normativa, le aziende e i fornitori di servizi si sono precipitati ad aggiornare le loro informative sulla privacy per rispettare i nuovi requisiti, mentre gli utenti si sono interrogati sull'effetto del GDPR sul panorama delle politiche di privacy online.
In risposta, i ricercatori hanno iniziato a studiare il comportamento delle aziende in relazione al GDPR.
Il GDPR è stato ideato per rafforzare e armonizzare la protezione dei dati per tutti gli individui nell'UE, nonché per dare alle persone un maggiore controllo sui propri dati personali. Questa normativa ha imposto una serie di requisiti stringenti alle aziende e le ha obbligate a rivedere le loro politiche di privacy per conformarsi ai nuovi requisiti di trasparenza e responsabilità.
Le politiche sulla privacy non solo sono diventate più lunghe e dettagliate, ma hanno anche dovuto essere redatte in un linguaggio che fosse chiaro e comprensibile per il consumatore medio. Questo è stato particolarmente importante, poiché il GDPR richiede che le informazioni fornite agli utenti siano facilmente accessibili e comprensibili, evitando l'uso di un

linguaggio tecnico o giuridico complesso che potrebbe confondere gli utenti[56] [57] [58].

Un'indagine condotta poco dopo l'entrata in vigore del GDPR ha rilevato che molte aziende hanno ampliato le loro politiche sulla privacy per includere dettagli specifici su come i dati vengono raccolti, utilizzati, condivisi e protetti.

Questo cambiamento ha comportato un aumento significativo del numero di parole e frasi nelle politiche di privacy delle aziende con sede nell'UE, con un incremento medio del 35% nel numero di parole e del 33% nel numero di frasi. Tuttavia, nonostante queste modifiche, alcune aziende hanno faticato a garantire che le loro politiche fossero non solo conformi, ma anche facilmente comprensibili per gli utenti, evidenziando una tensione tra l'esigenza di fornire informazioni complete e quella di mantenere la chiarezza e la semplicità.

Il GDPR ha introdotto una serie di obblighi di conformità che le aziende devono rispettare per evitare pesanti sanzioni finanziarie.

Le sanzioni per il mancato rispetto del GDPR possono raggiungere i 20 milioni di euro o il 4% del fatturato globale annuo dell'azienda.

Questo alto livello di rischio finanziario ha spinto molte aziende a investire in misure di conformità più rigorose, come l'adozione di nuove tecnologie per la protezione dei dati e la formazione del personale sulla gestione sicura dei dati personali [59] [60].

---

[56] Lin, X., Liu, H., Li, Z., & Xiong, G. (2022). Privacy protection of China's top websites: A multi-layer privacy measurement via network behaviours and privacy policies. *Computers & Security*, *114*(1), 102606.

[57] Measuring the GDPR's impact on web privacy. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*, San Diego, California, USA, February 24-27, 2019.

[58] Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. In *Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association.

[59] Kim, Y. (2014). Convolutional neural networks for sentence classification. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP 2014)*, October 25-29, Doha, Qatar (pp. 1746–1751). Association for Computational Linguistics (ACL).

[60] Kohlschütter, C., Fankhauser, P., & Nejdl, W. (2010). Boilerplate detection using shallow text features. In *Proceedings of the third ACM international conference on Web search and data mining* (pp. 441–450). ACM.

Oltre alle sanzioni finanziarie, il GDPR impone alle aziende di notificare le violazioni dei dati alle autorità di controllo competenti entro settantadue ore dalla loro scoperta. Questo requisito ha portato molte aziende a migliorare i loro sistemi di rilevamento e risposta agli incidenti, implementando nuove procedure per garantire una rapida identificazione e gestione delle violazioni dei dati.
Questo obbligo di notifica ha anche creato una cultura della trasparenza e della responsabilità, in cui le aziende devono essere pronte a rispondere rapidamente a qualsiasi violazione dei dati per proteggere sia gli interessati che la propria reputazione aziendale [61].
L'adozione del GDPR ha richiesto alle aziende di rivedere e adattare le loro pratiche operative e le loro strategie aziendali per garantire la conformità continua. Un aspetto fondamentale del GDPR è il principio della "*Privacy by design*" e della "*Privacy by default*", che richiede alle aziende di integrare la protezione dei dati in tutte le fasi di progettazione dei prodotti e dei servizi. Questo ha portato molte aziende a ripensare i loro approcci alla raccolta e al trattamento dei dati, assicurando che questi processi fossero allineati con i requisiti normativi e che i dati personali fossero protetti fin dalla fase di progettazione [62].
Inoltre, molte aziende hanno dovuto creare nuove funzioni di governance della privacy, come la nomina di un *Responsabile della Protezione dei Dati (DPO*) e la creazione di gruppi dedicati alla gestione della privacy e della conformità.
Questi cambiamenti organizzativi sono stati necessari per garantire che le aziende avessero le competenze e le risorse necessarie per rispettare i requisiti del GDPR e per rispondere rapidamente a eventuali questioni relative alla privacy e alla protezione dei dati [63].
Le aziende sono state spinte a implementare nuove soluzioni tecnologiche per la protezione dei dati, come la crittografia avanzata, i sistemi di

[61] Lebanoff, L., & Liu, F. (2018). Automatic detection of vague words and sentences in privacy policies. *arXiv preprint*, arXiv:1808.06219.
[62] Lindgaard, G., Fernandes, G., Dudek, C., & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! *Behaviour & Information Technology*, *25*(2), 115–126.
[63] Lippi, M., Palka, P., Contissa, G., Lagioia, F., Micklitz, H.-W., Sartor, G., & Torroni, P. (2018). Claudette: An automated detector of potentially unfair clauses in online terms of service.

gestione del consenso, gli strumenti di pseudonimizzazione e le tecnologie di monitoraggio della conformità. Questi strumenti sono stati cruciali per garantire che i dati personali fossero protetti in ogni fase del loro ciclo di vita, dal momento della raccolta fino alla loro eliminazione [64].

Tuttavia, l'implementazione di queste nuove tecnologie ha anche presentato diverse sfide.

Le aziende hanno dovuto affrontare problemi di integrazione con i sistemi esistenti, la necessità di formare il personale sull'uso delle nuove tecnologie e l'esigenza di garantire che queste soluzioni fossero sufficientemente robuste per affrontare un panorama di minacce in continua evoluzione. Alcune aziende, in particolare quelle di piccole e medie dimensioni, hanno trovato difficoltà a adattare i loro modelli di business all'interno dei nuovi requisiti del GDPR, poiché le risorse e le competenze necessarie per farlo possono essere significative [65].

L'adozione del GDPR ha comportato costi significativi per molte aziende. Questi costi sono stati associati a consulenze legali, aggiornamenti tecnologici, formazione del personale e altre iniziative necessarie per garantire la conformità. Le piccole e medie imprese hanno spesso faticato a trovare le risorse necessarie per rispettare i requisiti del GDPR, il che ha creato potenzialmente un divario competitivo tra le grandi aziende e le PMI.

Le grandi aziende, con maggiori risorse finanziarie e capacità di adattamento, hanno potuto investire rapidamente in misure di conformità e sfruttare il GDPR come un'opportunità per rafforzare la loro posizione competitiva sul mercato [66].

Al contrario, molte PMI hanno dovuto affrontare difficoltà economiche nel tentativo di conformarsi al GDPR. La necessità di investire in nuove tecnologie, formazione e consulenza legale ha rappresentato una sfida significativa per queste aziende, spesso con risorse limitate.

Di conseguenza, alcune PMI potrebbero essere state costrette a ridurre altre spese operative o a rivedere i loro modelli di business per far fronte ai costi

---

[64] Litman-Navarro, K. (2019). We read 150 privacy policies. They were an incomprehensible disaster. *The New York Times*.

[65] Liu, C., & Arnett, K. P. (2002). Raising a red flag on global www privacy policies. *Journal of Computer Information Systems*, *43*(1), 117–127.

[66] Loiacono, E. T., Watson, R. T., & Goodhue, D. L. (2002). Webqual: A measure of website quality. *Marketing Theory and Applications*, *13*(3), 432–438.

della conformità, mettendo potenzialmente a rischio la loro competitività sul mercato [67].

Un effetto positivo dell'entrata in vigore del GDPR è stato il rafforzamento delle relazioni tra le aziende e i loro clienti. Le aziende che hanno saputo dimostrare un forte impegno per la protezione dei dati personali e la trasparenza nelle loro pratiche di privacy hanno visto un aumento della fiducia e della lealtà dei clienti. I consumatori, consapevoli delle maggiori protezioni offerte dal GDPR, si sono sentiti più sicuri nel condividere le loro informazioni personali con aziende che rispettano rigorosamente le normative sulla privacy [68].

Tuttavia, il GDPR ha anche reso le aziende più vulnerabili alle conseguenze reputazionali in caso di violazioni dei dati o di mancata conformità. Le aziende che non sono riuscite a conformarsi al GDPR o che sono state coinvolte in incidenti di violazione dei dati hanno affrontato non solo sanzioni finanziarie, ma anche danni significativi alla loro reputazione e una perdita di fiducia da parte dei clienti. Questo ha reso la protezione dei dati un elemento critico nella gestione delle relazioni con i clienti e nella costruzione di una solida reputazione aziendale [69].

Nonostante i numerosi benefici, il GDPR ha anche ricevuto critiche riguardo alla sua efficacia.

Alcuni studi hanno indicato che, sebbene le politiche sulla privacy fossero diventate più dettagliate e lunghe, ciò non sempre si traduce in una maggiore comprensione da parte degli utenti.

Le politiche dettagliate possono essere difficili da comprendere, specialmente per chi non ha familiarità con i termini legali o tecnici, portando a una potenziale confusione piuttosto che a una maggiore trasparenza [70].

Inoltre, alcune aziende hanno adottato un approccio minimale alla conformità, implementando solo le misure di base necessarie per evitare

---

[67] Lomas, N. (2019). Privacy policies are still too horrible to read in full. *TechCrunch*.

[68] Lui, M., & Baldwin, T. (2012). langid.py: An off-the-shelf language identification tool. In *Proceedings of the ACL 2012 system demonstrations* (pp. 25–30). Association for Computational Linguistics.

[69] Marotta-Wurgler, F. (2016). Self-regulation and competition in privacy policies. *The Journal of Legal Studies*, *45*(S2), S13–S39.

[70] Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US web surveys. *The Information Society*, *18*(5), 345–359.

sanzioni, piuttosto che impegnarsi in una vera protezione della privacy degli utenti. Questo atteggiamento ha sollevato preoccupazioni circa l'effettiva efficacia del GDPR nel migliorare la protezione dei dati personali e ha evidenziato la necessità di ulteriori azioni da parte delle autorità di controllo per garantire una conformità sostanziale piuttosto che formale [71]. Sebbene il GDPR sia una normativa dell'UE, il suo impatto si è esteso ben oltre i confini europei.

Le aziende globali che operano in Europa o che trattano i dati dei cittadini europei sono tenute a rispettare le regole del GDPR, il che ha portato molte di loro a adottare pratiche di privacy più rigorose anche nei loro mercati di origine.

Questo fenomeno ha contribuito ad elevare gli standard globali di privacy dei dati e ha stimolato il dibattito sulla necessità di normative simili in altre regioni del mondo. La capacità del GDPR di influenzare le pratiche di privacy globale ha dimostrato la forza del regolamento nel promuovere un approccio più uniforme e coerente alla protezione dei dati personali a livello internazionale [72].

L'entrata in vigore del GDPR ha rappresentato un punto di svolta nella protezione dei dati personali, imponendo nuovi obblighi alle aziende e ridefinendo il modo in cui i dati vengono gestiti.

Sebbene abbia creato sfide significative in termini di conformità e abbia comportato costi elevati, ha anche stimolato miglioramenti nella gestione della privacy e ha promosso una cultura di maggiore rispetto per i diritti degli individui.

Il GDPR continuerà ad evolversi e il suo impatto a lungo termine sulle aziende e sulla società rimarrà un argomento chiave di discussione negli anni a venire [73].

---

[71] Napierala, M. A. (2012). What is the Bonferroni correction. *AAOS Now*, *6*(4), 40.

[72] Ramanath, R., Liu, F., Sadeh, N. M., & Smith, N. A. (2014). Unsupervised alignment of privacy policies using hidden markov models. In *Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (ACL 2014), Volume 2: Short Papers* (pp. 605–610).

[73] Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2019, giugno 24). The privacy policy landscape after the GDPR.

3.3 Differenza fra GDPR e CCPA

Fino ad ora, l'attenzione è stata focalizzata sulla sicurezza e la protezione della privacy all'interno dell'Unione Europea. Questo studio si propone di esaminare le leggi che regolano il mercato europeo e proteggono i consumatori dalle violazioni della loro privacy. Sebbene sia essenziale stabilire delle priorità, data la complessità e la molteplicità delle normative, l'analisi è stata circoscritta al contesto europeo. Tuttavia, è altrettanto importante comprendere le differenze rispetto alle leggi che, in altre giurisdizioni, affrontano problemi simili in materia di privacy.
Un esempio significativo è il CCPA, la normativa statunitense che protegge la privacy dei consumatori.
Il *GDPR (General Data Protection Regulation)* e il *CCPA (California Consumer Privacy Act)* rappresentano due delle normative più rilevanti in materia di protezione dei dati personali, rispettivamente nell'Unione Europea e negli Stati Uniti, ma presentano notevoli differenze in termini di scopo, applicazione e requisiti.
Mentre il GDPR mira a un approccio completo e uniforme alla protezione dei dati personali in tutta l'UE, il CCPA è stato concepito come una legge statale più limitata che si applica principalmente ai consumatori della California, ma con effetti potenzialmente globali data l'importanza del mercato californiano e la natura globale del commercio digitale. Analizzare queste differenze è fondamentale per comprendere le implicazioni normative per le aziende e i diritti dei consumatori.

Ambito di Applicazione
Una delle principali differenze tra il GDPR e il CCPA riguarda l'ambito di applicazione.
Il GDPR si applica a qualsiasi organizzazione che tratta dati personali di individui nell'UE, indipendentemente dalla localizzazione dell'organizzazione stessa. Questo significa che un'azienda con sede fuori

dall'UE deve comunque rispettare il GDPR se offre beni o servizi a, o monitora il comportamento di, individui nell'UE [74].
In contrasto, il CCPA si applica solo alle aziende che operano in California o che raccolgono dati personali di residenti in California e che soddisfano determinate soglie di reddito o attività, come avere un fatturato lordo annuo superiore a 25 milioni di dollari, trattare i dati di cinquantamila o più consumatori o dispositivi, o ricavare almeno il 50% dei propri introiti dalla vendita di dati personali [75].
Questo limita l'applicabilità del CCPA a un sottoinsieme di aziende, sebbene molte grandi società globali rientrino comunque nell'ambito della legge.

Requisiti di Consenso e Base Legale per il Trattamento

Il GDPR richiede una base legale per qualsiasi trattamento di dati personali, che può includere il consenso esplicito dell'individuo, la necessità per l'esecuzione di un contratto, l'adempimento di un obbligo legale, la protezione di interessi vitali, l'esecuzione di un compito di interesse pubblico o legittimo interesse del titolare del trattamento [76].
Questo approccio basato sul consenso e sulla base legale è molto più stringente rispetto al CCPA, che non richiede una giustificazione simile per il trattamento dei dati. Il CCPA, invece, permette ai consumatori di optare per il "*Do Not Sell My Personal Information*", cioè il diritto di rinunciare alla vendita dei loro dati, un meccanismo che indica un approccio più orientato all'*opt-out* piuttosto che all'*opt-in*.

[74] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), art. 3*.
[75] California Civil Code. (n.d.). §1798.140(c)(1). *California Consumer Privacy Act (CCPA)*.
[76] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), art. 6*.

Diritti degli Interessati

Il GDPR conferisce agli individui una serie di diritti, inclusi il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e opposizione al trattamento [77].

Questi diritti sono intesi a fornire un controllo significativo agli individui sui loro dati personali. Il CCPA, pur conferendo alcuni diritti simili, come il diritto di accesso e di cancellazione dei dati, non offre un diritto equivalente alla portabilità dei dati o alla limitazione del trattamento nella stessa misura del GDPR. Inoltre, mentre il GDPR garantisce questi diritti a tutti i soggetti i cui dati vengono trattati, il CCPA li limita ai residenti in California, il che rappresenta una differenza significativa in termini di protezione globale dei dati.

Categorie di Dati Sensibili

Il GDPR riconosce categorie specifiche di dati personali come "*dati sensibili*", che includono informazioni su origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici trattati per identificare univocamente una persona fisica, dati relativi alla salute, o dati relativi alla vita sessuale o all'orientamento sessuale di una persona [78].

Questi dati sono soggetti a norme di protezione più rigorose.

Il CCPA, invece, non distingue esplicitamente tra categorie di dati personali, sebbene offra protezione per alcune informazioni sensibili attraverso vari meccanismi, come il diritto di conoscere e di cancellare.

[77] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), artt. 12-22*.

[78] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), art. 9*

Trasferimenti di Dati Transfrontalieri

Un'altra differenza cruciale riguarda i trasferimenti di dati transfrontalieri. Il GDPR impone restrizioni rigorose sul trasferimento di dati personali al di fuori dell'UE, richiedendo che tali trasferimenti avvengano solo verso paesi che garantiscono un livello adeguato di protezione dei dati o attraverso meccanismi di salvaguardia approvati, come clausole contrattuali standard o norme vincolanti d'impresa [79].

In contrasto, il CCPA non impone requisiti specifici per i trasferimenti di dati al di fuori degli Stati Uniti, il che può riflettere le differenze fondamentali nei quadri normativi e nelle priorità di politica pubblica tra l'UE e gli Stati Uniti.

Sanzioni e Applicazione

Come citato nel *paragrafo 3.1* di questo capitolo, le sanzioni previste dal GDPR per il mancato rispetto delle sue disposizioni sono significativamente più severe rispetto a quelle del CCPA.

Il GDPR consente multe fino a venti milioni di euro o il 4% del fatturato globale annuo dell'azienda, qualunque sia il maggiore, per le violazioni più gravi [80].

Al contrario, il CCPA prevede sanzioni civili che possono arrivare fino a 7.500 dollari per violazione intenzionale e 2.500 dollari per violazione non intenzionale, con la possibilità per i consumatori di intentare cause private in caso di violazioni della sicurezza dei dati [81].

Questa differenza nelle potenziali sanzioni riflette l'approccio più rigoroso dell'UE rispetto alla protezione dei dati personali.

In sintesi, mentre il GDPR e il CCPA condividono l'obiettivo comune di proteggere la privacy e i dati personali, si distinguono per la loro portata,

---

[79] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), artt. 44-50.*

[80] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), art. 83*.

[81] California Civil Code. (n.d.). §1798.150. *California Consumer Privacy Act (CCPA)*.

requisiti di conformità, diritti degli interessati e meccanismi di *enforcement*.
Le aziende che operano in entrambi i contesti giuridici devono navigare attentamente queste differenze per garantire la conformità ed evitare sanzioni. Capire sia le somiglianze che le differenze tra queste due normative è cruciale per sviluppare strategie di conformità efficaci e per proteggere i diritti dei consumatori in un panorama digitale sempre più globale e regolamentato [82].

[82] Voss, W. G. (2021, gennaio). The CCPA and the GDPR are not the same: Why you should understand both. *TBS Business School*, Toulouse, France.

3.4 Normativa sui cookies

Nel *Capitolo I, paragrafo 1.3*, intitolato "*Strategie di Monitoraggio e Tracciamento dei Dati sui Siti Web*", è stato presentato un argomento di grande rilevanza per comprendere come funzionano le strategie di monitoraggio degli utenti e il loro potenziale utilizzo nell'*Active Listening*: *l'utilizzo dei cookie*.

Il problema principale legato all'utilizzo dei dati degli utenti per la pubblicità mirata, e in particolare nell'*Active Listening*, si manifesta a posteriori. La raccolta dei dati può avvenire in molti modi diversi, molti dei quali sono regolamentati dal GDPR all'interno dell'Unione Europea. In particolare, una delle strategie comunemente utilizzate da tutti i siti web è l'impiego dei cookie.

All'inizio degli anni Novanta, i siti web hanno cominciato a utilizzare i cookie, che da allora si sono diffusi ampiamente nel mondo digitale.

I cookie, creati dal server, sono utilizzati per raccogliere informazioni sugli utenti e vengono salvati su un disco locale di un dispositivo mobile o computer.

Come menzionato in precedenza, i cookie hanno una funzione specifica: facilitare e velocizzare l'accesso degli utenti ai siti web. Tuttavia, la normativa italiana, così come altre normative internazionali, impone ai siti web di ottenere un consenso esplicito da parte degli utenti per l'utilizzo dei cookie. Solitamente, i siti web chiariscono per quali scopi vengono utilizzati i cookie, come ad esempio per personalizzare l'esperienza di navigazione degli utenti. Poiché i cookie raccolgono informazioni specifiche sugli utenti, il nuovo regolamento GDPR stabilisce che i dati degli utenti contenuti nei cookie devono essere trattati e gestiti come dati personali [83].

Per questo motivo, i cookie sono da sempre oggetto di particolare attenzione da parte dei *Garanti della privacy* europei, un'attenzione che è ulteriormente aumentata con l'entrata in vigore del GDPR nel 2018.

Questo argomento rientra nel contesto delle comunicazioni elettroniche, disciplinate dalla direttiva *2002/58/CE* del Parlamento Europeo.

La direttiva impone ai gestori dei siti web di ottenere il consenso informato degli utenti prima di installare i cookie sui loro dispositivi.

---

[83] Net Informatica. (n.d.). A cosa servono i cookies. *Net Informatica*.

Nota anche come "*Cookie Law*", la direttiva non specifica esattamente come questi obblighi debbano essere attuati, lasciando così a ciascuno Stato membro la possibilità di adottare diverse modalità di applicazione.
Molte autorità nazionali specializzate nella protezione dei dati personali hanno allineato le loro disposizioni a quelle del GDPR. Ad esempio, hanno stabilito l'obbligo di mantenere sempre un registro dei consensi, applicando anche ai cookie la regola che richiede il consenso preventivo dell'utente per determinati trattamenti dei dati personali. Secondo il GDPR, questo consenso deve essere libero, specifico, inequivocabile, revocabile e dimostrabile.
In Italia, la normativa che regola l'uso dei cookie è contenuta *nell'Art. 122 del D. Lgs 196/2003* [84] e stabilisce che i cookie tecnici possono essere utilizzati senza il consenso dell'utente. Tuttavia, i cookie non tecnici, poiché possono invadere la privacy degli utenti quando usati per scopi di marketing, possono essere installati solo se gli utenti sono adeguatamente informati e danno un consenso valido [85].
L'attuazione corretta di questi principi è attentamente monitorata dalle autorità per la privacy europee, che non esitano a imporre multe significative in caso di violazioni.
Guardando alla situazione in Europa, in Francia nel 2020, la *Commissione Nazionale per l'Informatica e la Libertà (CNIL)* ha sanzionato *Google* e *Amazon* con multe di cento e trentacinque milioni di euro rispettivamente. Queste sanzioni sono state inflitte per aver utilizzato cookie di marketing e profilazione sui dispositivi di milioni di utenti senza ottenere il loro consenso esplicito, in violazione dell'*Articolo 82* della legge francese sull'informatica e la libertà [86].
Nel luglio 2019, l'*Information Commissioner's Office (ICO)*, l'ente britannico per la protezione dei dati personali, ha dichiarato nel suo rapporto annuale 2018-2019 di aver emesso ventitré multe per violazioni della normativa sulla privacy e sulle comunicazioni elettroniche (*PECR*). Questa legge disciplina l'uso dei cookie e il marketing elettronico nel

[84] Italia. (2003). *Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 122*. Gazzetta Ufficiale della Repubblica Italiana.
[85] I cookie sotto la lente dei garanti privacy: Lo stato dell'arte in Italia e UE. *Agenda Digitale*.
[86] Francia. (1978). *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 82*. Journal Officiel de la République Française.

Regno Unito. Secondo il rapporto, l'ammontare complessivo delle sanzioni è stato di poco più di due milioni di sterline.
Un altro problema rilevante era quello legato ai cosiddetti "*Cookie Wall*".
Un *cookie wall* è una pratica adottata da alcuni siti web che impedisce agli utenti di accedere al contenuto del sito a meno che non acconsentano all'uso di tutti i cookie, inclusi quelli non essenziali, al momento dell'apertura della pagina iniziale. In queste situazioni, l'utente non ha l'opzione di rifiutare selettivamente i cookie e può solo accettare tutti o lasciare il sito.
L'*Information Commissioner's Office (ICO)* del Regno Unito ha dichiarato che i *cookie wall* sono problematici perché non si può subordinare l'accesso generale al sito all'accettazione di cookie non necessari.
Secondo il *Considerando 25 del GDPR*, due elementi chiave devono essere rispettati:

1. *Contenuto specifico del sito web:* l'accesso al sito non deve essere condizionato all'accettazione di cookie non essenziali. Tuttavia, è possibile limitare l'accesso a contenuti specifici se l'utente rifiuta i cookie;
2. *Scopo legittimo:* questo riguarda la fornitura di un servizio online richiesto esplicitamente dall'utente, escludendo l'uso di cookie di terze parti per scopi di pubblicità o tracciamento online.

Questi requisiti garantiscono che il consenso dell'utente sia realmente libero e informato, come richiesto dal GDPR [87] [88].
Il 4 maggio del 2020 sono state emanate dal *Comitato Europeo per la protezione dei dati (EDPB)* nuove linee guida europee in materia di consenso dei cookie che differiscono da quelle precedenti per aspetti più formali [89].

---

[87] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Considerando n. 25*.
[88] What is a cookie wall? *Mandatly*. https://mandatly.com/cookie-compliance/what-is-cookie-wall
[89] Consenso e cookie: Nuove linee guida europee EDPB, cosa cambia. *Agenda Digitale*. https://www.agendadigitale.eu/sicurezza/privacy/consenso-e-cookie-nuove-linee-guida-europee-edpb-cosa-cambia/.

Queste nuove linee guida si erano concentrate su come il consenso doveva essere ottenuto per l'utilizzo dei cookie e altre tecnologie di tracciamento, stabilendo criteri rigorosi per garantire che il consenso degli utenti fosse valido. I punti principali erano:

a) *Consenso Libero e Informato*: Il consenso per l'uso dei cookie deve essere ottenuto in modo che gli utenti possano prendere una decisione libera e informata. Ciò significa che non si può condizionare l'accesso a un sito web all'accettazione di cookie non essenziali.
b) *Scelta Granulare*: Gli utenti devono avere la possibilità di selezionare quali tipi di cookie accettare. Questo implica che non è sufficiente un'unica opzione "*accetta tutti i cookie*" senza permettere agli utenti di rifiutare o accettare solo determinate categorie.
c) *Trasparenza*: Le informazioni riguardanti i cookie devono essere presentate in modo chiaro e facilmente comprensibile. Gli utenti devono sapere quali dati vengono raccolti, per quale scopo e per quanto tempo saranno conservati.
d) *Revocabilità del Consenso:* Gli utenti devono poter revocare il loro consenso in qualsiasi momento con la stessa facilità con cui l'hanno dato. Questo significa che le impostazioni dei cookie devono essere facilmente accessibili e modificabili.
e) *Cookie Walls:* Le linee guida hanno chiarito che i *cookie wall*, che bloccano l'accesso a un sito se l'utente non accetta i cookie, non soddisfano i requisiti di "*consenso libero*" perché non danno all'utente una vera scelta [90].

Nel novembre del 2023 sono state introdotte nuove linee guida sui cookie da parte dell'*EDPB* volte a chiarire ulteriormente l'*Articolo 5* della Direttiva *e-Privacy* [91]. Questo articolo richiede esplicitamente che gli utenti

[90] European Data Protection Board (EDPB). (n.d.). *European Data Protection Board*.
[91] Unione Europea. (2002). *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva ePrivacy), art. 5*.

diano il consenso informato prima che le informazioni vengano registrate sui propri dispositivi.
I siti web sono tenuti a chiedere il permesso prima di utilizzare i cookie non necessari per il funzionamento del sito. Tutto ciò avviene attraverso un banner cookie in cui l'utente accetta o meno il consenso.
Tuttavia, oltre che richiedere esplicitamente il consenso, il sito web deve assolutamente comunicare e fornire agli utenti tutte le informazioni chiare su come vengono utilizzati i cookie e l'utente deve avere sempre la possibilità di accettare o rifiutare i cookie che non sono essenziali per il funzionamento il sito.
Le linee guida *2/2023* dell'*EDPB* in oggetto forniscono analisi molto dettagliate e specifiche sulle tecnologie e metodi di tracciamento come, *URL* e *pixel tracking*, *elaborazione locale*, *tracciamento sull' IP* e altri [92].
L'*URL tracking* implica l'inserimento di parametri speciali nell'*URL* per tracciare l'interazione dell'utente con il link [93].
Quando un utente clicca su un link in una newsletter via e-mail, il sito web di destinazione può riconoscere da quale e-mail proviene l'utente.
Il *Pixel Tracking* invece, utilizza piccoli pixel invisibili incorporati in e-mail o pagine web. Quando quest'ultimi vengono caricati, trasmettono informazioni come l'ora di apertura dell'e-mail o la visita di una pagina web, permettendo il tracciamento dettagliato del comportamento dell'utente.
L'*elaborazione locale* fa riferimento a dati che vengono elaborati direttamente sul dispositivo dell'utente, senza trasmettere ad una rete di comunicazione elettronica. Questi posso essere dati memorizzati da applicazioni installate sul dispositivo e che possono essere utilizzati per vari scopi, incluso il tracciamento e anche la personalizzazione dell'esperienza utente, classico obiettivo delle strategie di marketing.
In sintesi, le *Linee Guida 2/2023 dell'EDPB* sottolineano la necessità di considerare una varietà di tecnologie e metodi di tracciamento per proteggere la privacy online.

[92] European Data Protection Board (EDPB). (2023). *Linee guida 2/2023 sull'interpretazione e l'applicazione del Regolamento generale sulla protezione dei dati (GDPR).*
[93] LegalBlink. (2023). *Linee guida 2023 sull'uso dei cookie*.

È fondamentale che sia gli utenti che le aziende adottino un approccio consapevole per assicurare che la raccolta e l'utilizzo dei dati personali siano eseguiti in modo responsabile e nel rispetto delle normative vigenti.

3.5 Il Consenso Informato

Il consenso informato è un principio cruciale nella gestione dei dati personali e nella tutela della privacy, specialmente nell'ambiente digitale. Questo concetto affonda le sue radici nella medicina e nella ricerca, dove serve a garantire che i partecipanti comprendano pienamente i rischi, i benefici e le implicazioni di un trattamento o di una procedura prima di accettarli.

Nella sfera digitale, il consenso informato si applica alla raccolta e all'utilizzo dei dati personali da parte di aziende e piattaforme online. Secondo il GDPR, il consenso deve essere "*libero, specifico, informato e inequivocabil*e" [94] il che significa che gli utenti devono avere una comprensione chiara di ciò a cui stanno acconsentendo e devono essere in grado di ritirare il loro consenso facilmente e senza penalità.

Nel contesto digitale, il consenso informato protegge i diritti degli utenti garantendo che essi siano pienamente consapevoli di come i loro dati verranno utilizzati e condivisi. Questo è essenziale non solo per conformarsi alle normative come il GDPR, ma anche per mantenere la fiducia degli utenti e promuovere pratiche etiche nella gestione dei dati.

Ad esempio, quando una piattaforma chiede il consenso per raccogliere dati tramite cookie o altri strumenti di tracciamento, deve fornire informazioni chiare su quali dati saranno raccolti, per quale scopo e con chi saranno condivisi.

Gli utenti devono ricevere informazioni dettagliate su ciò che implica il consenso. Questo include la descrizione dei dati che verranno raccolti, il motivo della raccolta, come verranno utilizzati e per quanto tempo saranno conservati. È fondamentale che le informazioni fornite siano comprensibili per gli utenti, devono essere evitate terminologie tecniche o giuridiche che potrebbero confondere gli utenti, rendendo invece il linguaggio accessibile e diretto.

Il consenso deve essere fornito liberamente, senza alcuna forma di pressione o manipolazione e questo significa che l'utente deve avere la

[94] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Articolo 4(11).*

scelta di acconsentire o rifiutare senza subire conseguenze negative. Inoltre, gli utenti devono avere il diritto di revocare il loro consenso in qualsiasi momento, e tale revoca deve essere facile da effettuare come l'atto di dare il consenso iniziale.

In uno studio condotto da *Burkhardt et al. (2022)* ed intitolato "*Privacy Behaviour: A Model for Online Informed Consent"* il consenso informato dovrebbe anche considerare la "*autorizzazione autonoma*" dell'individuo e il "*controllo comportamentale percepito*", riconoscendo l'importanza delle percezioni degli utenti sulla propria capacità di gestire il controllo sui propri dati [95].

Una delle sfide principali nell'implementazione del consenso informato online è la complessità delle informative sulla privacy, che spesso sono troppo lunghe e difficili da capire per l'utente medio. Questo porta a situazioni in cui il consenso è tecnicamente "informato" ma non veramente compreso, il che può sollevare questioni etiche sulla validità del consenso ottenuto. Altra sfida è l'uso di "*modelli oscuri*" (*dark patterns*) nelle interfacce utente, che possono manipolare gli utenti a dare il consenso senza una vera comprensione o scelta. Tali pratiche violano lo spirito del consenso informato e possono minare la fiducia degli utenti nelle piattaforme digitali [96].

L'*Autorizzazione Autonoma* di *Burkhardt et al*. (*2022*) è fondata sul principio dell'autonomia individuale, sostenendo che per essere veramente informato, il consenso deve essere dato senza coercizione e con una chiara comprensione delle implicazioni del trattamento dei dati personali [97].

Questo modello si collega strettamente ai requisiti del GDPR, che richiede che il consenso sia libero, informato e specifico [98].

---

[95] Burkhardt, et al. (2022). Privacy behaviour: A model for online informed consent.

[96] Obar, J. A., & Oeldorf-Hirsch, A. (2020). *The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services*. *Information, Communication & Society, 23*(1), 128-147.

[97] Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford University Press.

[98] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), Articolo 4(11).*

La *Teoria del Comportamento Pianificato*, d'altro canto, spiega le intenzioni degli individui basandosi su atteggiamenti, norme soggettive e controllo percepito [99].

Nel contesto del consenso informato, il *TPB* può essere utilizzato per comprendere come le convinzioni degli utenti sul trattamento dei loro dati influenzano la loro decisione di fornire o meno il consenso.

L'integrazione di questi due modelli teorici, come suggerito dagli autori, offre un approccio più olistico ed etico alla gestione del consenso informato online, enfatizzando la necessità di rispettare i diritti degli utenti e di evitare pratiche manipolative [100].

Spesso, molti utenti non comprendono completamente ciò che significa fornire il loro consenso, a causa della complessità delle informative sulla privacy o di un design che li spinge ad accettare automaticamente senza piena consapevolezza [101].

Per affrontare questo problema, il modello comportamentale descritto suggerisce che le organizzazioni dovrebbero non solo fornire informazioni chiare e accessibili, ma anche considerare il contesto psicologico e sociale in cui gli utenti prendono le loro decisioni [102].

Le pratiche di marketing che non rispettano il consenso informato rischiano di compromettere la fiducia degli utenti e di violare le normative sulla privacy, con conseguenze potenzialmente gravi per la reputazione aziendale e la sostenibilità a lungo termine [103][104].

---

[99] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

[100] Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford University Press.

[101] Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26-33.

[102] Obar, J. A., & Oeldorf-Hirsch, A. (2020). *The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services*. *Information, Communication & Society*, *23*(1), 128-147.

[103] Hajli, N., Wang, Y., Tajvidi, M., & Hajli, M. S. (2017). People, technologies, and organizations interactions in a social commerce era. *IEEE Transactions on Engineering Management*, *64*(4), 594-604.

[104] Obar, J. A. (2020). *The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services*. *Information, Communication & Society*, *23*(1), 128-147.

Questo approccio non solo si conforma alle normative come il GDPR, ma rafforza anche la fiducia tra le aziende e i consumatori, creando un ambiente più sicuro e rispettoso per la gestione dei dati personali [105][106].

Il *modello comportamentale* per il consenso informato rappresenta un passo avanti verso la creazione di pratiche di gestione dei dati personali che siano più etiche e orientate alla privacy.

Integrando i principi dell'*Autorizzazione Autonoma* e della *Teoria del Comportamento Pianificato*, le organizzazioni possono migliorare il loro approccio al consenso, garantendo che le decisioni degli utenti siano veramente informate e libere. Questo non solo aiuta a rispettare le normative vigenti, come il GDPR, ma promuove anche una cultura di trasparenza e rispetto nei confronti degli utenti nell'ambiente digitale.

Il testo è chiaro e ben strutturato, delineando in modo esaustivo il concetto di consenso informato nel contesto della gestione dei dati personali e della privacy digitale. Viene spiegato come il consenso, per essere valido, debba essere libero, informato e specifico, e si enfatizza l'importanza di evitare pratiche manipolative che potrebbero compromettere la validità di tale consenso. L'integrazione dei modelli teorici dell'*Autorizzazione Autonoma* e della *Teoria del Comportamento Pianificato* offre un quadro completo e olistico per la gestione del consenso informato online, ponendo l'accento sulla necessità di pratiche etiche e trasparenti.

In sintesi, un approccio etico e trasparente al consenso informato è essenziale non solo per conformarsi alle normative come il GDPR, ma anche per mantenere la fiducia degli utenti e promuovere una gestione responsabile dei dati personali. Le organizzazioni che adottano tali pratiche possono costruire relazioni più solide e durature con i propri utenti, basate sulla trasparenza e sul rispetto della privacy.

Passando ora al trattamento dei dati per finalità di marketing, è fondamentale che le aziende non solo ottengano il consenso informato degli utenti, ma lo facciano in un modo che rispetti le loro aspettative e i loro diritti.

---

[105] Romanou, A. (2018). The necessity of the implementation of big data analytics in auditing. *International Journal of Accounting Information Systems, 28*, 1-10.

[106] Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, *16*(2), 171-182.

Il marketing basato sui dati può essere estremamente efficace, ma deve essere condotto in modo da garantire che gli utenti comprendano come i loro dati verranno utilizzati e abbiano il pieno controllo su di essi.

3.6 Utilizzo dei dati personali per scopi di marketing

Come discusso nei capitoli precedenti, il "*Direct marketing*" è uno degli strumenti principali che le aziende utilizzano per informare i clienti sulla propria attività e sui prodotti o servizi offerti. In un contesto tecnologico in continua evoluzione, le aziende devono affrontare la sfida di adattare le loro strategie di marketing ai nuovi strumenti digitali, mantenendo al contempo un approccio etico e conforme alle normative sulla privacy per quanto riguarda l'utilizzo dei dati personali a fini di marketing.
I dati degli utenti, infatti, sono spesso utilizzati per creare campagne pubblicitarie mirate, che possono risultare invasive o indesiderate se non gestite correttamente [107].
In passato, le attività di marketing erano principalmente limitate a metodi tradizionali come l'affissione di cartelloni pubblicitari. Oggi, invece, è fondamentale comprendere come il marketing si sia evoluto con l'avvento delle nuove tecnologie digitali e quali opportunità e sfide queste rappresentano [108].
L'obiettivo del marketing è sempre stato quello di identificare, e talvolta di creare, i bisogni dei clienti attuali o potenziali. Tuttavia, mentre un tempo era più complesso raccogliere informazioni precise su questi bisogni, oggi, grazie allo sviluppo di nuove figure professionali e all'uso dell'intelligenza artificiale, è diventato molto più semplice acquisire una vasta quantità di dati sui clienti. Questi dati possono essere utilizzati non solo per personalizzare le campagne pubblicitarie, ma anche per ottimizzare le strategie di marketing, migliorando così l'efficacia complessiva delle campagne stesse. Inoltre, l'analisi delle tendenze di mercato e del comportamento dei consumatori gioca un ruolo chiave nel migliorare la precisione e il successo delle iniziative di marketing [109].
Di conseguenza, le aziende devono bilanciare l'uso avanzato dei dati con il rispetto delle normative sulla privacy, assicurando che le loro pratiche di

---

[107] Legaldesk.it. *Marketing e GDPR: Cosa c'è da sapere*. https://legaldesk.it/blog/marketing-gdpr/
[108] Altalex. (2021, aprile 20). *Dati utilizzati a fini di marketing: cosa c'è da sapere*. https://www.altalex.com/documents/news/2021/04/20/dati-utilizzati-a-fini-di-marketing
[109] PMI.it. *Regole privacy per siti e-commerce*. https://www.pmi.it/impresa/normativa/esperto/314500/regole-privacy-per-siti-e-commerce.html

marketing non solo rispettino la legge, ma siano anche trasparenti e rispettose dei diritti degli utenti.
Il raggiungimento di questi scopi è diventato più accessibile grazie ai progressi tecnologici, in particolare nell'ambito dell'intelligenza artificiale e della personalizzazione dei contenuti. Molto del marketing digitale, infatti, si basa sulla dettagliata profilazione degli utenti.
Secondo l'*Articolo 4* del GDPR, la profilazione è definita come "*qualunque trattamento automatizzato di dati personali volto a valutare aspetti personali di una persona fisica*" [110].
In termini di marketing, questo implica l'analisi dei dati di clienti o utenti per raggrupparli in segmenti con caratteristiche comuni, come preferenze, interessi e comportamenti [111] [112]. Nonostante ciò, l'*Articolo* 22 del GDPR afferma che gli individui hanno il diritto di non essere soggetti a decisioni basate unicamente su processi automatizzati.
Anche se chi si occupa di marketing cerca di raccogliere il maggior numero di dati possibile, il trattamento deve comunque essere limitato al minimo necessario, in linea con il principio di minimizzazione dei dati dell'*Articolo 5* del GDPR [113]. Inoltre, quando la profilazione è basata esclusivamente su processi automatizzati, è indispensabile ottenere un consenso specifico per ogni finalità.
Per inviare messaggi pubblicitari a scopo promozionale utilizzando strumenti automatizzati, è necessario ottenere il consenso dell'utente. Tuttavia, il *Codice Privacy* stabilisce che, se un utente ha precedentemente effettuato un acquisto presso il mittente del messaggio o ha mostrato un interesse specifico per i prodotti o servizi offerti, non è richiesto il consenso

---

[110] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), art. 4, comma 1*.
[111] Altalex. (2021, aprile 20). *Dati utilizzati a fini di marketing: cosa c'è da sapere*. https://www.altalex.com/documents/news/2021/04/20/dati-utilizzati-a-fini-di-marketing.
[112] European Commission. (n.d.). *Can data received from a third party be used for marketing?* European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing_it.
[113] Unione Europea. (2016). *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 e alla libera circolazione di tali dati (GDPR), artt. 5 e 22.*

esplicito dell'interessato [114]. Questo è valido a condizione che il destinatario del messaggio sia un cliente attuale o lo sia stato in passato e che la comunicazione riguardi prodotti o servizi simili a quelli acquistati in precedenza.

Un altro requisito essenziale è che l'utente sia stato chiaramente informato tramite un'informativa sulla privacy che i suoi dati potrebbero essere utilizzati per attività di *soft spam* [115]. Inoltre, è necessario rispettare il principio di *OPT-IN*, che prevede che l'azienda che invia il messaggio promozionale abbia ottenuto il consenso per utilizzare un indirizzo e-mail raccolto in modo legittimo direttamente dal cliente, e che questo consenso sia stato fornito per finalità commerciali [116].

Spesso, i responsabili del trattamento dei dati richiedono ai clienti, tramite moduli cartacei o *form* online, di fornire il consenso per l'uso dei loro dati personali non solo per scopi promozionali propri, ma anche per quelli di terze parti, a cui poi i dati vengono comunicati o ceduti.

Il problema sorge quando questa prassi viene attuata senza una chiara e specifica identificazione di queste terze parti, né nell'informativa sulla privacy né nel modulo di raccolta del consenso. A volte, non viene neppure specificata la categoria economica o merceologica a cui appartengono i destinatari dei dati, contravvenendo chiaramente alle disposizioni della normativa sulla privacy [117].

La condivisione o il trasferimento di dati personali a terzi per scopi di marketing richiede che l'informativa sulla privacy fornita dal titolare del trattamento, come previsto dall'*Art. 13* del GDPR, specifichi almeno le categorie economiche o merceologiche dei terzi che riceveranno e

---

[114] CF News. (2023, marzo 15). *La Cassazione delimita il perimetro del soft spam*. https://www.cfnews.it/diritto/la-cassazione-delimita-il-perimetro-del-soft-spam/#:~:text=7555%20del%2015%20marzo%202023,al%20trattamento%20dei%20dati%20personali

[115] Italia. (2003). *Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 130, comma 4*. Gazzetta Ufficiale della Repubblica Italiana.

[116] Gli Stati Generali. (n.d.). *Opt-in e opt-out nelle newsletter*. https://www.glistatigenerali.com/app-software_innovazione/opt-in-e-opt-out-newsletter/

[117] DGRS. (n.d.). *La comunicazione dei dati personali a terzi per finalità promozionali: Gli ultimi provvedimenti del Garante tra conferme e novità*. https://www.dgrs.it/la-comunicazione-dei-dati-personali-a-terzi-per-finalita-promozionali-gli-ultimi-provvedimenti-del-garante-tra-conferme-e-novita/.

utilizzeranno i dati per le loro finalità di marketing. Inoltre, per l'uso dei dati a fini promozionali da parte di questi terzi, è necessario ottenere un consenso specifico dall'interessato, distinto da quello che potrebbe essere stato precedentemente richiesto dal titolare per le proprie campagne promozionali.

Il terzo che riceve i dati è anche obbligato a fornire all'interessato un'informativa sulla privacy successiva, come stabilito dall'*Art. 14* del GDPR, nella quale deve chiarire da chi ha ottenuto i dati personali [118] [119].

Il *Garante della protezione dei dati personali* ha recentemente imposto una sanzione significativa a *Fastweb*, pari a quasi cinque milioni e mezzo di euro, a causa di pratiche di telemarketing considerate troppo invasive.

Questa decisione è parte di un impegno continuo del Garante per contrastare il fenomeno delle chiamate promozionali indesiderate, che rappresentano una violazione delle normative sulla privacy e una fonte di disturbo per molti cittadini.

L'azienda è stata penalizzata per non aver rispettato le disposizioni del *Regolamento generale sulla protezione dei dati* (GDPR) e per aver gestito in modo inappropriato i consensi degli utenti. In particolare, il Garante ha riscontrato che *Fastweb* aveva effettuato chiamate promozionali senza il consenso esplicito degli interessati, o in alcuni casi, nonostante l'opposizione espressa dagli stessi. Inoltre, è emerso che *Fastweb* aveva utilizzato dati personali provenienti da terzi senza verificare adeguatamente la validità dei consensi raccolti, aggravando così la situazione.

Questo intervento fa parte di una più ampia azione di vigilanza che mira a ridurre le pratiche di telemarketing aggressivo e a garantire che le aziende operino nel rispetto dei diritti alla privacy degli individui.

La sanzione imposta a *Fastweb* serve da lezione per altre aziende che ricorrono a tecniche simili, ricordando l'importanza di rispettare le

---

[118] Altalex. (2018, aprile 12). *Articolo 13 GDPR: Dati personali raccolti presso l'interessato, informazioni da fornire*. https://www.altalex.com/documents/news/2018/04/12/articolo-13-gdpr-dati-personali-raccolti-presso-interessato-informazioni-da-fornire.

[119] Altalex. (2018, aprile 12). *Articolo 14 GDPR: Dati personali non ottenuti presso l'interessato, informazioni da fornire*. https://www.altalex.com/documents/news/2018/04/12/articolo-14-gdpr-dati-personali-non-ottenuti-presso-interessato-informazioni-da-fornire

normative sulla protezione dei dati personali e di garantire un trattamento etico e trasparente delle informazioni degli utenti [120].

In conclusione, è fondamentale che le aziende bilancino l'uso innovativo delle tecnologie digitali con il rispetto delle normative sulla privacy, garantendo che le pratiche di marketing siano etiche e trasparenti.

Come si è visto nel caso di *Fastweb*, le conseguenze di non rispettare le norme sulla protezione dei dati possono essere severe, con sanzioni significative che servono da monito per altre aziende.

Nel *Capitolo II* è stato esaminato l'aspetto tecnologico dei dispositivi di riconoscimento vocale come *Siri*, *Alexa*, e altri, evidenziando le potenzialità e i rischi associati all'*Active Listening*. In questo capitolo, invece, ci siamo concentrati sulle tutele legali e sulle normative progettate per proteggere i dati personali degli utenti.

Nel paragrafo successivo, approfondiremo ulteriormente questo tema, analizzando casi studio specifici che illustrano come l'utilizzo non appropriato di questi dispositivi possa portare a violazioni della privacy, esaminando le implicazioni legali e le misure di protezione necessarie per prevenire tali abusi.

[120] Garante Privacy. *Telemarketing aggressivo: Il Garante privacy sanziona Fastweb per quattro milioni di euro.*

3.7 Pubblicità mirata attraverso i dispositivi di riconoscimento vocale

Come discusso in precedenza, l'intelligenza artificiale (AI) continua a evolversi rapidamente, e con il tempo viene integrata all'interno di vari dispositivi e macchine.
Quando si parla di AI, si tende spesso a immaginare le forme più comuni e riconoscibili, ma in realtà essa si manifesta in molteplici modalità, una delle quali è la tecnologia di riconoscimento vocale.
Nel *Capitolo II* è stato approfondito l'aspetto tecnologico dell'*Active Listening*, esaminando come questa capacità si manifesta. La forma più diffusa di tale fenomeno è proprio il riconoscimento vocale. Queste tecnologie offrono un'interazione umanizzata e interattiva, con esempi noti come *Siri* di *iPhone* e *Alexa* di *Amazon*.
Nel 2018, *Amazon* ha ottenuto un nuovo brevetto per il suo assistente vocale *Alexa*, che consente al dispositivo di determinare le emozioni degli utenti basandosi sul tono della loro voce. Questo permette di rilevare lo stato d'animo degli utenti e fornire loro pubblicità mirate. Il principale rischio di questo brevetto è legato alla possibile riduzione dell'autonomia dell'utente, poiché questi non ha modo di evitare che le proprie emozioni vengano rilevate dal dispositivo.
Nonostante ciò, l'intelligenza artificiale è stata concepita e sviluppata con l'obiettivo di supportare l'umanità nei compiti quotidiani, dai più semplici ai più complessi.
Può essere definita come un insieme di tecniche che cercano di riprodurre la cognizione umana o animale attraverso le macchine [121].
Questa tecnologia è capace di riconoscere immediatamente una voce, associarla a un individuo già identificato e memorizzare le informazioni nella sua memoria interna [122].
Con l'introduzione del nuovo brevetto, *Alexa* è in grado di memorizzare rappresentazioni dei dati vocali e combinarle con altre caratteristiche dell'utente. Quando riceve nuovi input vocali, determina lo stato emotivo

[121] Calo, R. (2017). AI policy: A primer and roadmap. *UCLA Law Review*, *51*(5), 1265-1335.
[122] Mann, V. A., Diamond, R., & Carey, S. (1979). Development of voice recognition: Parallels with face recognition. *Journal of Experimental Child Psychology*, *27*(2), 153-165.

dell'utente basandosi su tono e volume della voce, permettendo di presentare pubblicità mirate in base all'umore rilevato [123].
Tuttavia, questa tecnologia può avere un impatto ambivalente sull'autonomia degli utenti: da un lato, può aumentarla migliorando la capacità di fare scelte informate, mentre dall'altro può ridurla quando interferisce o anticipa le scelte, imponendo preferenze all'utente [124].
Le leggi a tutela dei consumatori mirano costantemente a riequilibrare il rapporto di potere tra aziende e consumatori, proteggendo questi ultimi da pratiche commerciali sleali che possono compromettere o minacciare la loro autonomia. I consumatori, infatti, possono essere considerati vulnerabili per vari motivi, tra cui limiti mentali o fisici, o semplicemente per la mancanza di adeguate informazioni sui prodotti.
Amazon è soggetta a obblighi normativi legati alla protezione dei dati, ma il GDPR non fa esplicito riferimento alle emozioni o alla loro raccolta[125].
Tuttavia, l'uso della voce degli utenti da parte di *Alexa* per il riconoscimento delle emozioni potrebbe far rientrare tali informazioni nella categoria dei dati biometrici, regolati dall'*Art. 9* del GDPR.
Il riconoscimento biometrico, infatti, consente di identificare una persona basandosi non solo su caratteristiche fisiche, ma anche comportamentali, attraverso processi completamente automatizzati.
L'emozione può essere definita come una risposta fisiologica agli stimoli esterni, e nel campo della pubblicità, i ricercatori hanno imparato a misurare l'impatto delle emozioni sul successo complessivo di una campagna pubblicitaria [126].
Oggi, grazie al calcolo affettivo, l'intelligenza artificiale è in grado di riconoscere e interpretare le emozioni umane. Questo approccio si basa sull'idea che i sistemi informatici possano essere progettati per elaborare, interpretare e simulare l'affetto umano, migliorando così l'interazione tra uomo e macchina [127].

---

[123] Kinsella, B. (2018). Amazon files for patent to detect user illness and emotional state by analyzing voice data.
[124] Mik, E. (2016). The erosion of autonomy in online consumer transactions. *Law, Innovation and Technology*, *8*(1), 1-38.
[125] McStay, A. (2017). *Privacy and the media* (p. 142). SAGE Publications.
[126] Mehta, A., & Purvis, S. C. (2006). Reconsidering recall and emotion in advertising. *Journal of Advertising*, *46*, 49-56.
[127] Costa, H., & Macedo, L. (n.d.). Affective computing. *ATCM State of the Art, Theoretical Report*.

Il primo passo per addestrare un sistema a riconoscere le emozioni degli utenti consiste nel raccogliere due tipi di input: primari e secondari. Gli input primari includono registrazioni di persone che esprimono diverse emozioni leggendo lo stesso testo, mentre gli input secondari utilizzano database esistenti sviluppati da altri ricercatori [128].

Successivamente, la macchina estrae informazioni dalle voci registrate per identificare correlazioni statistiche tra caratteristiche vocali specifiche e stati emotivi.

Un metodo alternativo per riconoscere le emozioni è la categorizzazione, che può avvenire in due forme: discreta o continua. La categorizzazione discreta si limita a rilevare emozioni come rabbia, gioia o paura, mentre quella continua descrive lo stato emotivo su uno spettro più ampio e dettagliato [129].

Questo sistema, basato sull'apprendimento automatico, mira a migliorare l'accuratezza delle risposte di *Alexa*, adeguando suggerimenti e raccomandazioni in base allo stato emotivo dell'utente [130].

Alexa potrebbe così proporre contenuti sponsorizzati in modo mirato, come ad esempio consigliare musica o prodotti farmaceutici in risposta a specifiche emozioni percepite [131].

In pratica, quando un utente fa una richiesta ad *Alexa*, il dispositivo invia l'audio al cloud, dove viene analizzato per individuare schemi vocali ed emozioni. Questo processo è cruciale per la generazione di pubblicità personalizzate, poiché gli inserzionisti partecipano a un'asta per offrire annunci pertinenti basati sugli stati emotivi rilevati [132].

La tecnologia comporta sia vantaggi che svantaggi: può codificare il mondo e influenzare le modalità con cui le persone utilizzano corpo e

---

[128] Lugovic, S., Horvat, M., & Dunder, I. (2016). Techniques and applications of emotion recognition in speech. In *Proceedings of the 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2016)*.

[129] Dai, W., Yang, P., Chen, L., & Li, Z. (2015). Emotion recognition and affective computing on vocal social media. *Information & Management*, *52*(7), 777-788.

[130] Barrett, B. (2018). The year Alexa grew up. *WIRED*. https://www.wired.com/story/amazon-alexa-2018-machine-learning/

[131] Cook, J. (2018). Amazon patents new Alexa feature that knows when you're ill and offers you medicine.

[132] Marr, B. (2018). Machine learning in practice: How does Amazon's Alexa really work? *Forbes*.

mente, trascurando le loro inclinazioni emotive e intellettuali. Il brevetto di *Amazon Alexa* per il riconoscimento delle emozioni rivoluzionerà il modo in cui gli inserzionisti valutano il comportamento degli utenti per misurare la compatibilità dei prodotti con il mercato di riferimento. Tuttavia, il marketing mirato ha ricevuto critiche a causa della percezione del danno arrecato al consumatore e della vulnerabilità percepita degli utenti a cui è rivolto [133].

La vulnerabilità dei consumatori si manifesta soprattutto nella mancanza di controllo personale.

Quando un consumatore non è in grado di gestire attenzione, comportamento o emozioni, le sue reazioni diventano incontrollabili e fanno parte della sua esperienza di vulnerabilità. Il grado di vulnerabilità può variare a seconda delle caratteristiche demografiche o dello stato personale del consumatore, e dipende fortemente dalle percezioni di stimoli specifici nel contesto del marketing.

I consumatori vulnerabili sono più suscettibili all'influenza degli inserzionisti, il che può portare a comportamenti d'acquisto impulsivi, consumo eccessivo e ostentazione [134].

La Commissione Europea ha definito i criteri per identificare i consumatori vulnerabili in base a caratteristiche sociodemografiche, comportamentali, situazioni personali e ambiente di mercato.

Un consumatore vulnerabile è considerato tale quando si trova ad affrontare un alto rischio di esiti negativi sul mercato, ha difficoltà a reperire o assimilare informazioni, e risulta maggiormente influenzabile da determinate pratiche di marketing.

Esiste un'intersezione tra la normativa sulla protezione dei dati e quella a tutela dei consumatori, poiché entrambe mirano a proteggere l'autonomia dei soggetti interessati e dei consumatori stessi. Il GDPR si prefigge di tutelare le persone fisiche in merito al trattamento dei dati personali.

---

[133] Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. *Journal of Macromarketing*, *25*(2), 128-139.

[134] Shi, H. Y., Wang, H., & Huang, Z. (2019). The concept of consumer vulnerability: Scale development and validation. *Journal of Consumer Affairs*, *53*(3), 1-22.

Nel corso degli anni, il diritto alla protezione dei dati personali si è evoluto, trasformandosi da uno strumento per il mercato a un diritto fondamentale, talvolta visto come un diritto di cittadinanza de facto [135].
La pubblicità mirata si basa sulla raccolta di informazioni dettagliate sui consumatori e sulle loro preferenze online o tramite altri media, con l'obiettivo di proporre annunci personalizzati. L'aggregazione di dati può condurre alla creazione di profili, il che comporta rischi legati all'uso di dati personali.
Le aziende, che possiedono una vasta quantità di informazioni sui consumatori, possono sfruttare questi dati per influenzare il processo decisionale.
L'incertezza resta sulla possibilità che i dati emotivi possano essere considerati una categoria specifica di dati meritevole di protezione. Tuttavia, il processo di riconoscimento delle emozioni di *Amazon Alexa* si basa sull'input vocale dell'utente, e ciò potrebbe richiamare la normativa sui dati biometrici.
Nel 2018 le emozioni non erano regolamentate e non rientravano nel campo di applicazione del GDPR, ma oggi non è più così.
Oggi, il *Regolamento Generale sulla Protezione dei Dati* (GDPR) stabilisce chiaramente che ogni tipo di informazione che possa essere associata a un individuo identificabile è soggetta alla protezione.
Questo include i dati biometrici e le informazioni derivate, come le emozioni, se queste possono essere utilizzate per identificare direttamente o indirettamente una persona.
Le emozioni possono essere considerate dati personali se, attraverso il loro trattamento, è possibile risalire all'identità dell'individuo. Per esempio, nel caso in cui le emozioni siano dedotte da parametri biometrici come la voce, e questi dati siano utilizzati in combinazione con altre informazioni per identificare una persona, rientrano sotto la protezione del GDPR.
Pertanto, oggi il trattamento delle emozioni, in quanto potenzialmente riconducibile a un soggetto identificabile, può essere regolato dal GDPR, specialmente se si configura come trattamento di dati biometrici o sensibili.
L'*Articolo 5(3*) della *Direttiva ePrivacy* considera informazioni memorizzate nei dispositivi terminali degli utenti, indipendentemente dal

[135] McStay, A. (2016). Empathic media and advertising: Industry, policy, legal and citizen perspectives (The case for intimacy). *Big Data & Society*, *3*(2), 1-11.

fatto che si tratti di dati personali, al fine di proteggere gli utenti dai rischi derivanti dall'uso di identificatori nascosti[136].

Pertanto, è possibile categorizzare le emozioni come dati personali alla luce di questi precedenti [137][138].

La *Direttiva sulle pratiche commerciali sleali (UCP)* è finalizzata a regolare tutte le pratiche commerciali che possono avere un impatto sugli interessi economici dei consumatori. L'obiettivo principale di questa direttiva è migliorare il funzionamento del mercato interno per i consumatori, eliminando le differenze normative nazionali che ostacolano il libero accesso ai beni e servizi all'interno del mercato comunitario [139].

Questa direttiva pone l'accento sull'autonomia del consumatore, intendendo che i consumatori dovrebbero essere in grado di prendere decisioni informate. Tuttavia, la direttiva riconosce anche che esistono gruppi di consumatori che potrebbero avere difficoltà nel prendere decisioni informate. Questi gruppi vulnerabili sono tutelati *dall'Articolo 5(3)* della *Direttiva UCP*.

Secondo la Commissione Europea, i consumatori possono affrontare vulnerabilità in diverse situazioni, come di fronte a materiali di marketing complessi o quando hanno minori possibilità di scelta o di acquisto. Di conseguenza, una pratica commerciale può essere considerata sleale se valutata dal punto di vista dei consumatori particolarmente vulnerabili a tale pratica.

Nel 2019 l'Unione Europea ha adottato una nuova direttiva sui contratti per la fornitura di contenuti e servizi digitali, nota come *Direttiva 2019/770 (Direttiva sui Contenuti Digitali*)[140]. L'obiettivo di questa direttiva è garantire un elevato livello di protezione sia per i consumatori che pagano

---

[136] Unione Europea. (2002). *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva ePrivacy), Articolo 5(3).*

[137] Gonzalez Cabanas, J., Cuevas, R., & Guerrero, C. D. (2018). Facebook use of sensitive data for advertising in Europe.

[138] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 1-21.

[139] Anagnostaras, G. (2010). The Unfair Commercial Practices Directive in context: From legal disparity to legal complexity? *Common Market Law Review*, *47*, 147-174.

[140] Unione Europea. (2019). *Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali*.

per un servizio, sia per coloro che forniscono dati in cambio dello stesso, come accade per prodotti con elementi digitali, ad esempio frigoriferi intelligenti. Inoltre, la *Direttiva sui Contenuti Digitali* ha cercato di armonizzare le leggi contrattuali come parte del quadro di protezione dei consumatori.

Il riconoscimento emotivo di *Amazon Alexa* può essere classificato come "*bene con elementi digitali*" ai sensi dell'*Articolo 2(3)* della *Direttiva sui Contenuti Digitali* [141].

Il concetto di "*bene con elementi digitali*" si riferisce a beni che incorporano o sono interconnessi con contenuti digitali o servizi digitali in modo tale che, in assenza di tali contenuti o servizi digitali, i beni non sarebbero in grado di svolgere le loro funzioni.

L'assenza di contenuti digitali, come l'input audio dell'utente, impedirebbe al sistema di riconoscimento vocale di funzionare correttamente [142][143].

Il riconoscimento vocale di *Amazon Alexa*, che implica l'analisi della voce dell'utente per dedurre il suo stato emotivo, solleva interrogativi sulla classificazione di tali dati. La voce, come dato biometrico, può essere utilizzata per stabilire l'identità di una persona in modo automatico o semi-automatico, in base alle sue caratteristiche fisiche o comportamentali. Per questo motivo, l'analisi delle emozioni potrebbe essere soggetta alle disposizioni dell'*Articolo 9* del GDPR, che richiede condizioni specifiche per il trattamento di dati biometrici [144][145].

Il GDPR protegge i dati personali senza riguardo alla tecnologia utilizzata per trattarli, essendo il regolamento neutrale rispetto alla tecnologia e applicabile sia al trattamento automatizzato che manuale. Se i dati non possono essere ricondotti a una persona identificabile, essi non rientrano nella definizione di dati personali prevista dal GDPR.

---

[141] Unione Europea. (2019). *Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, Articolo 2(3)*.

[142] Huertas Cerdeira, V. (2019). EU adopts new rules on sales contracts for goods and digital content. *Consilium.europa.eu*

[143] Sadet, R. (2019). EU adopts new rules on sales contracts for goods and digital content. *Consilium.europa.eu.*

[144] European Commission. (2019). What is personal data? *European Commission*. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[145] Sedenberg, E., & Chuang, J. (2017). Smile for the camera: Privacy and policy implications of emotion AI.

In conclusione, l'uso del riconoscimento vocale da parte di *Amazon Alexa* per dedurre lo stato emotivo degli utenti solleva importanti questioni riguardanti la classificazione dei dati biometrici e il rispetto delle disposizioni del GDPR. Poiché la voce può essere considerata un dato biometrico, il suo trattamento richiede condizioni giuridiche specifiche, come il consenso esplicito dell'utente, per garantire una protezione adeguata della privacy.

CASO AMAZON: VIOLAZIONE DELLA PRIVACY

Come riportato il 1° giugno 2023 da *Network Digital 230* nella sezione *Data Protection*, è emerso che *Amazon* è stata multata per oltre trenta milioni di dollari a seguito di due azioni legali avviate dalla *FTC (Federal Trade Commission*) per violazioni della privacy. Queste informazioni sono state rese pubbliche grazie a documenti processuali divulgati dalla stampa americana.
La più grave delle due cause riguarda l'accusa secondo cui *Amazon* avrebbe raccolto e conservato i dati personali di minori che interagivano con l'assistente vocale *Alexa*, senza eliminare le registrazioni delle loro conversazioni o i dati di geolocalizzazione. Questa condotta è stata considerata una violazione delle normative statunitensi sulla protezione della privacy online dei minori, e per questo *Amazon* dovrà pagare una multa di venticinque milioni di dollari.
La seconda causa riguarda il dispositivo di sorveglianza domestica *Ring*. Si accusa *Amazon* di non aver limitato adeguatamente l'accesso dei dipendenti ai video registrati dal sistema e di non aver implementato adeguate misure di sicurezza per prevenire attacchi hacker.
La *FTC* ha inoltre accusato l'azienda di aver utilizzato i dati degli utenti per migliorare i propri algoritmi senza ottenere il consenso.
Per queste violazioni, *Amazon* è stata multata per 5,8 milioni di dollari. In base all'accordo, *Ring* dovrà cancellare tutti i video dei clienti e i "*face embeddings*" (dati biometrici del volto) raccolti prima del 2018, nonché eliminare qualsiasi prodotto sviluppato utilizzando questi dati.
L'accusa secondo cui *Amazon* avrebbe violato sia il *FTC Act* che il *Children's Online Privacy Protection Act (COPPA)*, conservando

illegalmente i dati personali di minori tramite l'assistente *Alexa*, è stata portata avanti dal Dipartimento di Giustizia, che ha presentato una denuncia e un accordo transattivo per conto della *FTC*.
Il governo ha sostenuto che *Amazon* avrebbe conservato per anni i dati vocali e di geolocalizzazione di giovani utenti, ostacolando i genitori nel far valere i loro diritti di cancellazione dei dati, come previsto dal *COPPA*.
In base all'accordo proposto, *Amazon* dovrà eliminare gli account inattivi dei bambini, così come alcune registrazioni vocali e dati di geolocalizzazione. Inoltre, sarà vietato utilizzare questi dati per addestrare gli algoritmi dell'azienda.
La *FTC* ha dichiarato che le voci dei bambini rappresentano un set di dati prezioso per *Amazon*, poiché le caratteristiche vocali dei minori differiscono significativamente da quelle degli adulti. Questo avrebbe permesso all'azienda di ottimizzare l'algoritmo di *Alexa* per interagire meglio con i giovani utenti. Il governo ha inoltre accusato *Amazon* di non aver implementato un sistema efficace per garantire la cancellazione dei dati su richiesta.
Se l'accordo sarà approvato dal tribunale, oltre alla sanzione civile di venticinque milioni di dollari, ad *Amazon* sarà vietato utilizzare le registrazioni vocali e i dati di geolocalizzazione dei bambini per migliorare i propri prodotti. L'azienda dovrà inoltre cancellare gli account *Alexa* dei minori inattivi e informare gli utenti riguardo le azioni legali e le nuove pratiche di gestione e cancellazione dei dati. *Amazon* sarà infine tenuta a sviluppare un programma specifico per garantire la corretta gestione della privacy in relazione ai dati di geolocalizzazione.
Emma Daniels, portavoce di *Amazon*, ha dichiarato in un comunicato: *"I nostri dispositivi e servizi sono progettati per proteggere la privacy dei clienti e dare loro pieno controllo sulla propria esperienza. Sebbene non siamo d'accordo con le affermazioni della FTC su Alexa e Ring, e neghiamo di aver violato la legge, questi accordi ci permettono di chiudere definitivamente la questione"* [146].
La questione della violazione della privacy attraverso l'uso dei nostri dati, della nostra voce e delle nostre emozioni non riguarda solo *Alexa*. Come

[146] Corriere Comunicazioni. Violazione della privacy per Amazon: Stangata da 30 milioni di dollari. *Corriere Comunicazioni*. https://www.corrierecomunicazioni.it/privacy/violazione-della-privacy-per-amazon-stangata-da-30-milioni-di-dollari/

discusso nei capitoli precedenti, esistono molti dispositivi in grado di ascoltarci, tra cui *smart TV*, smartphone e altre tecnologie di intelligenza artificiale. Anche se *Alexa* rappresenta uno dei casi più emblematici, situazioni simili sono state documentate anche con assistenti vocali come *Apple Siri* o *Google Assistant*, come già analizzato. Di fatto, si parla di una gamma diversificata di dispositivi che sembrano essere in grado di ascoltarci, il che ha portato a discutere del fenomeno noto come l*'Active Listening.*

Tuttavia, nessuna azienda ha ancora confermato ufficialmente che questi dispositivi ascoltino costantemente le nostre conversazioni. Al momento, la nostra preoccupazione riguarda soprattutto la raccolta e l'uso improprio dei dati personali, probabilmente ottenuti da conversazioni private, dalle attività online come la navigazione su siti web, il download di app e altri comportamenti digitali.

Di recente, però, il *4 settembre 2024*, *Corriere.it* ha pubblicato un articolo in cui è stato riportato alla luce il fenomeno dell'*Active Listening*, suggerendo per la prima volta che i nostri dispositivi potrebbero effettivamente ascoltarci.

L'idea che i nostri telefoni ci ascoltino è profondamente radicata ed è facile capirne il motivo. È comune vedere annunci pubblicitari di prodotti o servizi che sembrano collegati a conversazioni avute di recente. Ad esempio, dopo aver discusso a cena di comprare un nuovo divano, può capitare di vedere banner pubblicitari di divani sui social media o su altri siti web, inducendoci a pensare che i nostri dispositivi ci stiano ascoltando. Questa sensazione è rafforzata dalla presenza di microfoni intorno a noi, che si trovano non solo negli smartphone, ma anche negli smart speaker, come quelli con *Amazon Alexa*, *Google Assistant* o *Apple Siri*, nelle telecamere di sicurezza, in molti modelli di *smart TV* e in vari dispositivi connessi alla rete.

Nonostante queste percezioni, molti esperti di sicurezza informatica considerano l'idea che gli smartphone ci registrino in continuazione una leggenda metropolitana. Diverse ricerche hanno tentato di indagare sulla questione.

Nel 2018, un gruppo di ricercatori della *Northeastern University* ha esaminato oltre 17.000 delle app più diffuse per verificare se alcune di esse utilizzassero il microfono del telefono per registrare segretamente l'audio.

Il risultato dello studio non ha fornito alcuna prova a sostegno dell'ipotesi che queste app ascoltassero attivamente gli utenti.
Allora, la domanda sorge spontanea: *"Perché se ne parla di nuovo?"*
Grazie ad una inchiesta condotta da *404 Media*, un sito americano di giornalismo investigativo, sono tornate alla ribalta le dichiarazioni di *Cox Media Group (CMG)*, un conglomerato mediatico che include emittenti radiofoniche e concessionarie pubblicitarie.
CMG ha affermato di avere accesso alle conversazioni private delle persone, raccolte tramite i microfoni di dispositivi come telefoni, TV e altri gadget connessi. Queste conversazioni verrebbero utilizzate per creare pubblicità mirata, riaccendendo così il dibattito sull'*Active Listening* e la sorveglianza digitale [147].

[147] Corriere.it. I cellulari ci spiano con il microfono? Le affermazioni di Cox Media Group che riaprono il caso. *Corriere della Sera*.

CAPITOLO IV

MITIGAZIONE DEI RISCHI E SUGGERIMENTI

Nei capitoli precedenti, è stato esaminato come l'*Active Listening* sia diventato una delle principali preoccupazioni legate alla privacy digitale, soprattutto con l'aumento dell'uso di dispositivi come smartphone, assistenti vocali e altre tecnologie in grado di raccogliere dati sensibili. Questi strumenti, spesso presenti nelle nostre vite quotidiane, utilizzano tecnologie avanzate per riconoscere comandi vocali e migliorare l'esperienza utente. Tuttavia, tale raccolta di dati può essere sfruttata per finalità non sempre trasparenti, mettendo a rischio la privacy dell'utente. In questo capitolo, saranno esplorate e suggerite alcune delle principali strategie per mitigare tali rischi e garantire una gestione più sicura dei dati personali.

Una delle soluzioni principali per proteggere la privacy consiste nella gestione attenta delle autorizzazioni concesse alle applicazioni installate sui dispositivi mobili. Molte applicazioni richiedono accesso a funzioni sensibili, come il microfono o la posizione, anche quando tali permessi non sono strettamente necessari per il loro funzionamento.

Secondo lo studio condotto da *Felt et al. (2011)*, solo una piccola parte degli utenti presta effettivamente attenzione ai permessi richiesti durante l'installazione delle applicazioni, aumentando così i rischi di accesso improprio ai propri dati personali [148]. Per questo motivo, è essenziale che gli utenti revisionino regolarmente le autorizzazioni attraverso le impostazioni del sistema operativo dei loro dispositivi.

Disabilitare l'accesso a funzioni sensibili, come il microfono, per applicazioni che non ne hanno un reale bisogno può ridurre notevolmente il rischio di ascolto passivo.

In particolare, piattaforme come *Android* e *iOS* permettono agli utenti di monitorare quali applicazioni hanno accesso a determinati permessi e di revocarli se non necessari. Questo approccio è fondamentale per prevenire la raccolta non autorizzata di informazioni vocali e altre forme di sorveglianza involontaria.

[148] Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. *Proceedings of the 18th ACM Conference on Computer and Communications Security* (pp. 627–638). ACM.

Gli assistenti vocali, come *Amazon Alexa, Google Assistant e Apple Siri*, sono strumenti potenti che, però, rappresentano un rischio significativo per la privacy. Questi dispositivi, progettati per essere attivati da comandi vocali specifici, possono essere attivati involontariamente da suoni di fondo o da parole che somigliano ai comandi predefiniti.
Questo può portare a una raccolta accidentale di dati personali [149].
L'uso continuo di questi dispositivi senza un adeguato controllo può aumentare il rischio di esposizione dei propri dati, poiché i dispositivi potrebbero trasmettere informazioni ai server delle aziende produttrici per migliorare le prestazioni e fornire pubblicità mirata [150].
Per mitigare tali rischi, gli utenti dovrebbero disabilitare l'attivazione vocale continua e configurare gli assistenti vocali affinché si attivino solo manualmente, tramite il tocco di un pulsante. Inoltre, molti dispositivi permettono di disattivare fisicamente il microfono, impedendo così qualsiasi ascolto accidentale.
In merito al tema dei cookie di tracciamento, specialmente quelli di terze parti, rappresentano una minaccia significativa per la privacy online. Questi piccoli file vengono utilizzati per tracciare le attività di navigazione degli utenti attraverso diversi siti web, creando profili dettagliati delle preferenze e abitudini di navigazione per finalità pubblicitarie.
Molte persone ignorano i rischi legati ai cookie e non configurano adeguatamente i loro browser per bloccare quelli di terze parti, esponendosi così al tracciamento online [151].
Per proteggersi dal tracciamento invasivo, gli utenti possono adottare diverse misure, tra cui:

1. *Bloccare i cookie di terze parti:* Alcuni browser, come Mozilla Firefox e Brave, offrono protezioni integrate contro il tracciamento, bloccando automaticamente i cookie di terze parti;
2. *Navigazione in modalità privata:* Questa modalità impedisce ai siti web di memorizzare cookie una volta terminata la sessione di navigazione;

[149] Stouffer, C. (2023). Is my phone listening to me? Yes, here's why and how to stop it. *Norton*
[150] Triggs, R. (2018). No, your phone is not always listening to you. *Android Authority*.
[151] Polimeni, A. (2022). Cookie: cosa sono, come funzionano e come proteggerti. *Agenda Digitale*.

3. *Estensioni per il blocco dei tracker:* Strumenti come *uBlock Origin* e *Privacy Badger* aiutano a bloccare i tentativi di tracciamento durante la navigazione.

Un'altra tecnica efficace per proteggere la privacy durante la navigazione online e le comunicazioni vocali è l'uso della *crittografia end-to-end* e delle *VPN (Virtual Private Network).*
La crittografia end-to-end garantisce che solo il mittente e il destinatario di una comunicazione possano accedere ai contenuti scambiati, impedendo a terze parti di intercettare i dati. Applicazioni di messaggistica come *WhatsApp* utilizzano questo tipo di crittografia, proteggendo le conversazioni degli utenti da eventuali intercettazioni.
Inoltre, l'utilizzo di una *VPN* offre un ulteriore livello di protezione.
Le *VPN* criptano tutto il traffico internet dell'utente e nascondono il suo indirizzo IP, riducendo significativamente il rischio di tracciamento da parte di inserzionisti e altre entità. Questo è particolarmente utile quando si utilizzano reti Wi-Fi pubbliche, che spesso presentano vulnerabilità di sicurezza [152].
Infine, uno degli aspetti più importanti nella mitigazione dei rischi legati alla privacy è la consapevolezza da parte degli utenti.
È fondamentale che gli utenti leggano attentamente i termini di servizio e le politiche sulla privacy delle applicazioni e dei dispositivi che utilizzano, evitando di concedere autorizzazioni indiscriminatamente. Inoltre, gli utenti dovrebbero integrare nella propria routine tecnologica l'abitudine di mantenere i propri dispositivi aggiornati per garantire che le vulnerabilità di sicurezza possano essere risolte tempestivamente.
Un utilizzo consapevole e una gestione attiva delle impostazioni di privacy, insieme a misure tecnologiche avanzate, possono ridurre significativamente i rischi legati alla raccolta e all'utilizzo dei dati personali, permettendo agli utenti di mantenere un controllo maggiore sulla propria privacy digitale.

[152] Stouffer, C. (2021). Internet tracking: How and why we're followed online. *Norton.*

CONCLUSIONE

Nell'ambito di questo elaborato, si è indagato sul fenomeno dell'*Active Listening* e dell'uso indiscriminato dei *cookie*, analizzando in che modo queste pratiche tecnologiche abbiano un impatto significativo sulla privacy digitale degli utenti. Attraverso l'esplorazione dei fondamenti tecnici e delle implicazioni legali ed etiche di queste tecnologie, è emerso come la raccolta e il monitoraggio dei dati vocali e delle attività online abbiano profondamente trasformato il modo in cui gli individui interagiscono con i loro dispositivi e con l'ambiente digitale.

Rispondere alla domanda di ricerca iniziale: "*Come possono gli utenti proteggere efficacemente la propria privacy dall'Active Listening dei dispositivi tecnologici e dall'uso indiscriminato dei cookie, senza rinunciare ai benefici che questi strumenti offrono nella vita quotidiana?"* richiede una strategia articolata e multilivello.

La protezione della privacy può essere migliorata grazie all'adozione di misure pratiche di mitigazione, molte delle quali già esplorate nel corso della trattazione. Tra queste, l'utilizzo di strumenti per bloccare il tracciamento, come i *cookie blockers* e le *VPN*, e una maggiore consapevolezza riguardo ai termini e alle condizioni d'uso delle applicazioni sono essenziali. Gli utenti dovrebbero inoltre sfruttare le opzioni di gestione delle autorizzazioni sui propri dispositivi, limitando l'accesso alle informazioni sensibili come il microfono e la posizione, e optare per browser più rispettosi della privacy, come quelli che non permettono l'installazione di *cookie* di terze parti senza consenso esplicito.

Dal punto di vista tecnico, la sfida è duplice: proteggere i dati sensibili mentre si continua a beneficiare delle funzionalità avanzate offerte dalle moderne tecnologie vocali e digitali. Le aziende, dal canto loro, devono migliorare la trasparenza riguardo alle pratiche di raccolta dati e fornire agli utenti un controllo maggiore e più semplice da esercitare sui propri dati personali. Le normative vigenti, come il *GDPR*, sono un importante passo avanti, ma l'applicazione pratica deve essere ulteriormente perfezionata per garantire una protezione più efficace.

Resta ancora molto da esplorare. La ricerca futura potrebbe approfondire come nuove tecnologie, come l'intelligenza artificiale e l'*Internet of Things* (IoT), influenzeranno ulteriormente il concetto di *Active Listening* e la

privacy. Sarà fondamentale comprendere in che modo la personalizzazione basata sui dati possa evolversi per conciliare le esigenze di marketing e la tutela della riservatezza degli utenti. Inoltre, ulteriori studi potrebbero investigare l'efficacia di nuove normative più severe o il ruolo delle tecnologie emergenti, come la crittografia avanzata e i sistemi di intelligenza artificiale distribuita, nel prevenire l'abuso della raccolta dei dati personali.

In conclusione, la protezione della privacy nell'era digitale rimane un obiettivo complesso ma imprescindibile. La tensione tra il progresso tecnologico e la tutela dei diritti individuali continuerà a rappresentare una sfida. Solo attraverso un approccio combinato che includa innovazione, consapevolezza degli utenti e un quadro normativo solido, sarà possibile garantire che i benefici offerti dalle tecnologie moderne non avvengano a scapito della privacy e della sicurezza personale.

RIFERIMENTI

Articoli di giornale

1. Kröger, J. L., & Raschke, P. (2019). Is my phone listening in? On the feasibility and detectability of mobile eavesdropping. Journal Name, Volume (Issue), 102–120.
2. Duhigg, C. (2012, febbraio 15). How companies learn your secrets. The New York Times Magazine.
3. Litman-Navarro, K. (2019). We read 150 privacy policies. They were an incomprehensible disaster. The New York Times.

Sitologia

4. Cultur-e. (2023). Gli smartphone ci ascoltano? Ecco il fenomeno dell'active listening. Fastweb Plus. https://www.fastweb.it/fastweb-plus/digital-dev-security/active-listening-gli-smartphone-ci-ascoltano/
5. Triggs, R. (2018, luglio 18). No, your phone is not always listening to you. Android Authority. https://www.androidauthority.com/your-phone-is-not-listening-to-you-884028/
6. CBS News. (2023, maggio 15). Do smartphones listen to us and target us with ads? CBS News. https://www.cbs.com/shows/news/
7. Garcia Martinez, A. (2017, novembre 18). Facebook's not listening through your phone. It doesn't have to. Wired. https://www.wired.com/story/facebooks-listening-smartphone-microphone/
8. Stouffer, C. (2023, giugno 13). Is my phone listening to me? Yes, here's why and how to stop it. Norton. https://us.norton.com/blog/how-to/is-my-phone-listening-to-me
9. Stouffer, C. (2021, giugno 28). Internet tracking: How and why we're followed online. Norton. https://us.norton.com/blog/privacy/internet-tracking
10. Norton. (2018, agosto 8). What is a smart TV and the privacy risks of a smart TV. Norton. https://us.norton.com/blog/iot/smart-tvs-and-risk
11. Galletta, M. (2023, dicembre 28). È vero che i nostri dispositivi smartphone ci ascoltano? TecnoAndroid.
12. Polimeni, A. (2022). Cookie: cosa sono, come funzionano e come proteggerti. Agenda Digitale.
13. Net Informatica. (2020, ottobre 14). A cosa servono i cookie. Net Informatica.
14. La Rosa, A. (2020). Cookie di prima e terza parte: Cosa sono e come funzionano. Engage.it.
15. Dissent. (2019, luglio 11). Google is investigating the source of voice data leak, plans to update its privacy policies. DataBreaches.net. https://databreaches.net/2019/07/11/google-is-investigating-the-source-of-voice-data-leak-plans-to-update-its-privacy-policies/.
16. Lindsey, N. (2019, agosto 14). Amazon, Google, Apple stopping human review of recordings from voice assistants. CPO Magazine. https://www.cpomagazine.com/data-privacy/amazon-google-apple-stopping-human-review-of-recordings-from-voice-assistants/.
17. Elgan, M. (2013, agosto 31). Why are virtual assistant apps so shy? Computerworld. https://www.computerworld.com/article/1393993/why-are-virtual-assistant-apps-so-shy.html.

18. Knight, W. (2012, maggio 29). Where speech recognition is going. MIT Technology Review. http://www.technologyreview.com/news/427793/where-speech-recognition-is-going/.
19. Jesdanun, A. (2013, marzo 7). Strengths and weaknesses of Apple's Siri and Google Now. The Mercury News. http://www.mercurynews.com/ci_22740979/strengths-and-weaknesses-apples-siri-and-google-no.
20. IBM (International Business Machines Corporation). What is speech recognition? IBM. https://www.ibm.com/topics/speech-recognition.
21. Shaip. (2024, luglio 16). Leveraging voice – Overview and applications of voice recognition technology. Shaip. https://www.shaip.com/blog/voice-recognition-overview-and-applications/.
22. Parlangeli, D. (2016, dicembre 28). La polizia americana vuole sentire Echo di Amazon per un caso di omicidio. Wired Italia. https://www.wired.it/gadget/accessori/2016/12/28/polizia-echo-amazon-omicidio/.
23. Corona, F. (2018). Diritto alla riservatezza: riconoscimento ed evoluzione normativa. Legaldesk.it.
24. Data Protection Manager. (2021). Nascita del diritto alla privacy e sua evoluzione come diritto alla riservatezza e alla protezione dei dati. Privacymanager.eu.
25. Massimini, M. (2021, maggio 11). Anonimizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR. Privacy.it.
26. Corona, F. (2022). Consenso privacy: le nuove regole del GDPR. Legaldesk.it.
27. Lomas, N. (2019). Privacy policies are still too horrible to read in full. TechCrunch.
28. Net Informatica. A cosa servono i cookies. Net Informatica.
29. I cookie sotto la lente dei garanti privacy: Lo stato dell'arte in Italia e UE. Agenda Digitale.
30. Mandatly. What is a cookie wall? Mandatly. https://mandatly.com/cookie-compliance/what-is-cookie-wall
31. LegalBlink. (2023). Linee guida 2023 sull'uso dei cookie.
32. Legaldesk.it. Marketing e GDPR: Cosa c'è da sapere. https://legaldesk.it/blog/marketing-gdpr/
33. Altalex. (2021, aprile 20). Dati utilizzati a fini di marketing: cosa c'è da sapere. https://www.altalex.com/documents/news/2021/04/20/dati-utilizzati-a-fini-di-marketing
34. PMI.it. Regole privacy per siti e-commerce. https://www.pmi.it/impresa/normativa/esperto/314500/regole-privacy-per-siti-e-commerce.html
35. CF News. (2023, marzo 15). La Cassazione delimita il perimetro del soft spam. https://www.cfnews.it/diritto/la-cassazione-delimita-il-perimetro-del-soft-spam/#:~:text=7555%20del%2015%20marzo%202023,al%20trattamento%20dei%20dati%20personali
36. Gli Stati Generali. (n.d.). Opt-in e opt-out nelle newsletter. https://www.glistatigenerali.com/app-software_innovazione/opt-in-e-opt-out-newsletter/
37. DGRS. (n.d.). La comunicazione dei dati personali a terzi per finalità promozionali: Gli ultimi provvedimenti del Garante tra conferme e novità. https://www.dgrs.it/la-comunicazione-dei-dati-personali-a-terzi-per-finalita-promozionali-gli-ultimi-provvedimenti-del-garante-tra-conferme-e-novita/
38. Altalex. (2018, aprile 12). Articolo 13 GDPR: Dati personali raccolti presso l'interessato, informazioni da fornire. https://www.altalex.com/documents/news/2018/04/12/articolo-13-gdpr-dati-personali-raccolti-presso-interessato-informazioni-da-fornire

39. Altalex. (2018, aprile 12). Articolo 14 GDPR: Dati personali non ottenuti presso l'interessato, informazioni da fornire. https://www.altalex.com/documents/news/2018/04/12/articolo-14-gdpr-dati-personali-non-ottenuti-presso-interessato-informazioni-da-fornire
40. Barrett, B. (2018). The year Alexa grew up. WIRED. https://www.wired.com/story/amazon-alexa-2018-machine-learning/
41. Cook, J. (2018). Amazon patents new Alexa feature that knows when you're ill and offers you medicine.
42. Marr, B. (2018). Machine learning in practice: How does Amazon's Alexa really work? Forbes.
43. Huertas Cerdeira, V. (2019). EU adopts new rules on sales contracts for goods and digital content. Consilium.europa.eu
44. Sadet, R. (2019). EU adopts new rules on sales contracts for goods and digital content. Consilium.europa.eu.
45. European Commission. (2019). What is personal data? European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
46. Corriere Comunicazioni. (n.d.). Violazione della privacy per Amazon: Stangata da 30 milioni di dollari. Corriere Comunicazioni. https://www.corrierecomunicazioni.it/privacy/violazione-della-privacy-per-amazon-stangata-da-30-milioni-di-dollari/
47. Corriere.it. I cellulari ci spiano con il microfono? Le affermazioni di Cox Media Group che riaprono il caso. Corriere della Sera.
48. Stouffer, C. (2023). Is my phone listening to me? Yes, here's why and how to stop it. Norton
49. Triggs, R. (2018). No, your phone is not always listening to you. Android Authority.
50. Stouffer, C. (2021). Internet tracking: How and why we're followed online. Norton.

Documenti scientifici

51. Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. Proceedings of the 18th ACM Conference on Computer and Communications Security, 627–638.
52. Kraus, L., Fiebig, T., Miruchna, V., Moller, S., & Shabtai, A. (2015). Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy.
53. Jha, A. K., et al. (2024). Analysis of voice-based searches and how they affect digital marketing. Educational Administration: Theory and Practice, 30(5), 13914-13921.
54. Kevin, O., & Shibwabo, K. B. (2015, luglio 7). The application of real-time voice recognition to control critical mobile device operations. Faculty of Information Technology, Strathmore University, Nairobi, Kenya.
55. Hannun, A. (2021, agosto 3). The history of speech recognition to the year 2030.
56. Juang, B. H., & Rabiner, L. R. (2004, agosto 10). Automatic speech recognition: A brief history of the technology development. Georgia Institute of Technology, Atlanta; Rutgers University; University of California, Santa Barbara.
57. Hui, J. Y., & Leong, D. (2017). The era of ubiquitous listening: Living in a world of speech-activated devices. Asian Journal of Public Affairs, 10(1), e5.
58. Sgobbi, M. (2022). Il trattamento dei dati personali e gli strumenti di raccolta dei dati online: Cookies e Big Data [Tesi di laurea magistrale, Università degli Studi di Padova, Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali].
59. Zech, H. (2015). Information as a property. JIPITEC, 6, 192, par. 1.

60. Zech, H. (2016). A legal framework for a data economy in the European Digital Single Market: Rights to use data. Journal of Intellectual Property Law & Practice, 11(6), 460 s.
61. Lin, X., Liu, H., Li, Z., & Xiong, G. (2022). Privacy protection of China's top websites: A multi-layer privacy measurement via network behaviours and privacy policies. Computers & Security, 114(1), 102606.
62. Measuring the GDPR's impact on web privacy. In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019), San Diego, California, USA, February 24-27, 2019.
63. Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18). USENIX Association.
64. Kim, Y. (2014). Convolutional neural networks for sentence classification. In Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP 2014), October 25-29, Doha, Qatar (pp. 1746–1751). Association for Computational Linguistics (ACL).
65. Kohlschütter, C., Fankhauser, P., & Nejdl, W. (2010). Boilerplate detection using shallow text features. In Proceedings of the third ACM international conference on Web search and data mining (pp. 441–450). ACM.
66. Lebanoff, L., & Liu, F. (2018). Automatic detection of vague words and sentences in privacy policies. arXiv preprint, arXiv:1808.06219.
67. Lindgaard, G., Fernandes, G., Dudek, C., & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! Behaviour & Information Technology, 25(2), 115–126.
68. Lippi, M., Palka, P., Contissa, G., Lagioia, F., Micklitz, H.-W., Sartor, G., & Torroni, P. (2018). Claudette: An automated detector of potentially unfair clauses in online terms of service.
69. Liu, C., & Arnett, K. P. (2002). Raising a red flag on global www privacy policies. Journal of Computer Information Systems, 43(1), 117–127.
70. Loiacono, E. T., Watson, R. T., & Goodhue, D. L. (2002). Webqual: A measure of website quality. Marketing Theory and Applications, 13(3), 432–438.
71. Lui, M., & Baldwin, T. (2012). langid.py: An off-the-shelf language identification tool. In Proceedings of the ACL 2012 system demonstrations (pp. 25–30). Association for Computational Linguistics.
72. Marotta-Wurgler, F. (2016). Self-regulation and competition in privacy policies. The Journal of Legal Studies, 45(S2), S13–S39.
73. Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US web surveys. The Information Society, 18(5), 345–359.
74. Napierala, M. A. (2012). What is the Bonferroni correction. AAOS Now, 6(4), 40.
75. Ramanath, R., Liu, F., Sadeh, N. M., & Smith, N. A. (2014). Unsupervised alignment of privacy policies using hidden markov models. In Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (ACL 2014), Volume 2: Short Papers (pp. 605–610).
76. Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2019, giugno 24). The privacy policy landscape after the GDPR.
77. Voss, W. G. (2021, gennaio). The CCPA and the GDPR are not the same: Why you should understand both. TBS Business School, Toulouse, France.
78. Burkhardt, et al. (2022). Privacy behaviour: A model for online informed consent.
79. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.
80. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26-33.

81. Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147.
82. Hajli, N., Wang, Y., Tajvidi, M., & Hajli, M. S. (2017). People, technologies, and organizations interactions in a social commerce era. IEEE Transactions on Engineering Management, 64(4), 594-604.
83. Romanou, A. (2018). The necessity of the implementation of big data analytics in auditing. International Journal of Accounting Information Systems, 28, 1-10.
84. Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. Ethics and Information Technology, 16(2), 171-182.
85. Calo, R. (2017). AI policy: A primer and roadmap. UCLA Law Review, 51(5), 1265-1335.
86. Mann, V. A., Diamond, R., & Carey, S. (1979). Development of voice recognition: Parallels with face recognition. Journal of Experimental Child Psychology, 27(2), 153-165.
87. Kinsella, B. (2018). Amazon files for patent to detect user illness and emotional state by analyzing voice data.
88. Mik, E. (2016). The erosion of autonomy in online consumer transactions. Law, Innovation and Technology, 8(1), 1-38
89. Mehta, A., & Purvis, S. C. (2006). Reconsidering recall and emotion in advertising. Journal of Advertising, 46, 49-56.
90. Costa, H., & Macedo, L. (n.d.). Affective computing. ATCM State of the Art, Theoretical Report.
91. Lugovic, S., Horvat, M., & Dunder, I. (2016). Techniques and applications of emotion recognition in speech. In Proceedings of the 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2016).
92. Dai, W., Yang, P., Chen, L., & Li, Z. (2015). Emotion recognition and affective computing on vocal social media. Information & Management, 52(7), 777-788.
93. Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. Journal of Macromarketing, 25(2), 128-139.
94. Shi, H. Y., Wang, H., & Huang, Z. (2019). The concept of consumer vulnerability: Scale development and validation. Journal of Consumer Affairs, 53(3), 1-22.
95. McStay, A. (2016). Empathic media and advertising: Industry, policy, legal and citizen perspectives (The case for intimacy). Big Data & Society, 3(2), 1-11.
96. Gonzalez Cabanas, J., Cuevas, R., & Guerrero, C. D. (2018). Facebook use of sensitive data for advertising in Europe.
97. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1-21.
98. Anagnostaras, G. (2010). The Unfair Commercial Practices Directive in context: From legal disparity to legal complexity? Common Market Law Review, 47, 147-174.
99. Sedenberg, E., & Chuang, J. (2017). Smile for the camera: Privacy and policy implications of emotion AI.
100. Krum, C. (2010). Mobile marketing: Finding your customers no matter where they are. Pearson Education.
101. Locoratolo, B. (2021). Il trattamento dei dati personali e la privacy. Napoli: Simone.
102. Zech, H. (2016). Data as a tradeable commodity. In A. De Franceschi (Ed.), European contract law and the digital single market (pp. 51 ss). Cambridge: Intersentia.
103. Floridi, L. (2009). Data is a description of something that allows it to be recorded, analyzed, and reorganized. In G. Sommaruga (Ed.), Formal theories of information: From Shannon to semantic information theory and general concepts of information (pp. 13 ss). Springer.
104. Faden, R. R., & Beauchamp, T. L. (1986). A history and theory of informed consent. Oxford University Press.
105. McStay, A. (2017). Privacy and the media (p. 142). SAGE Publications

Documenti legali

106. Unione Europea. (2007). Trattato sul funzionamento dell'Unione Europea, art. 288. Gazzetta ufficiale dell'Unione Europea, 13 dicembre 2007.
107. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR).
108. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), art. 4, comma 1.
109. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), Considerando n. 26.
110. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), Considerando n. 30.
111. InfoCuria - Giurisprudenza. Sentenza della Corte di giustizia dell'Unione Europea, Causa C-434/16.
112. Italia. (2003). Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 4. Gazzetta Ufficiale della Repubblica Italiana, abrogato dal Decreto legislativo 10 agosto 2018, n. 101.
113. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), Considerando n. 46.
114. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), art. 3.
115. California Civil Code. (n.d.). §1798.140(c)(1). California Consumer Privacy Act (CCPA).
116. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), art. 6.
117. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), artt. 12-22.
118. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), art. 9.
119. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), art. 83.
120. California Civil Code. (n.d.). §1798.150. California Consumer Privacy Act (CCPA).

121. Italia. (2003). Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 122. Gazzetta Ufficiale della Repubblica Italiana.
122. Francia. (1978). Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 82. Journal Officiel de la République Française.
123. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), Considerando n. 25.
124. European Data Protection Board (EDPB). (n.d.). European Data Protection Board.
125. Unione Europea. (2002). Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva ePrivacy), art. 5.
126. European Data Protection Board (EDPB). (2023). Linee guida 2/2023 sull'interpretazione e l'applicazione del Regolamento generale sulla protezione dei dati (GDPR).
127. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), Articolo 4(11).
128. European Commission. (n.d.). Can data received from a third party be used for marketing? European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing_it
129. Unione Europea. (2016). 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 e alla libera circolazione di tali dati (GDPR), artt. 5 e 22.
130. Italia. (2003). Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, art. 130, comma 4. Gazzetta Ufficiale della Repubblica Italiana.
131. Unione Europea. (2002). Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva ePrivacy), Articolo 5(3)
132. Unione Europea. (2019). Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.
133. Unione Europea. (2019). Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, Articolo 2(3).

Libri

134. Krum, C. (2010). *Mobile marketing: Finding your customers no matter where they are*. Pearson Education.
135. Locoratolo, B. (2021). *Il trattamento dei dati personali e la privacy*. Napoli: Simone.
136. Zech, H. (2016). Data as a tradeable commodity. In A. De Franceschi (Ed.), *European contract law and the digital single market* (pp. 51 ss). Cambridge: Intersentia.
137. Floridi, L. (2009). Data is a description of something that allows it to be recorded, analyzed, and reorganized. In G. Sommaruga (Ed.), *Formal theories of information: From*

Shannon to semantic information theory and general concepts of information (pp. 13 ss). Springer.
138. Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford University Press.
139. McStay, A. (2017). *Privacy and the media* (p. 142). SAGE Publications.