UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

European Digital Law of the Person, of the Contract

***and of the Technological Marketplace* - EUDILA**

Cattedra Jean Monnet del Progetto ERASMUS +

Tecnologia e Privacy:

Il Caso degli Smart Assistant

Mirko Cortina

0356931

Anno accademico 2023/2024

INDICE

Abstract

In questo lavoro analizzeremo l'evoluzione del diritto digitale e il suo impatto sugli smart assistant, esplorando le sfide legate alla protezione dei dati personali e alla regolamentazione di questa tecnologia in rapida crescita. Nel Capitolo 1, verranno introdotti i dati personali, definendoli e analizzando le principali criticità legate alla loro raccolta e trattamento nell'era digitale. Il Capitolo 2 offrirà una panoramica sugli smart assistant, dalla loro nascita alla diffusione attuale, esaminando come questi dispositivi stiano influenzando vari aspetti della vita quotidiana, dalla gestione delle attività domestiche all'interazione con servizi online. Nel Capitolo 3, l'attenzione sarà posta sulle implicazioni giuridiche degli smart assistant, con un approfondimento sul diritto alla riservatezza, alla privacy e sulla protezione dei dati personali e verranno analizzati due articoli del GDPR rilevanti rispetto al tema. Nel Capitolo 4 ci concentreremo poi sull'impatto del Data Act sugli smart assistant, evidenziando le nuove opportunità e le sfide che questa normativa porterà, specialmente in termini di trasferimento e uso dei dati personali tra dispositivi connessi. Infine, nel Capitolo 5 proporremo delle linee guida per un uso consapevole e sicuro degli smart assistant, con l'obiettivo di proteggere i propri dati personali e di garantire un'interazione responsabile con queste tecnologie.

CAPITOLO 1 – Il Diritto Digitale

Prima di affrontare il caso specifico, è utile introdurre il contesto in cui esso si inserisce: il mondo digitale, con le sue regole e peculiarità legate alla diffusione dei dati. Il diritto digitale è un ambito in costante evoluzione, che copre tutte le questioni legali inerenti all'uso delle tecnologie digitali e di Internet. In un'epoca in cui la tecnologia è diventata parte integrante della nostra quotidianità, il diritto digitale assume un ruolo fondamentale nel garantire la tutela e il rispetto dei diritti sia degli individui sia delle organizzazioni.

Proprio in seguito a questa espansione è sorto il problema del dover dare un inquadramento giuridico a tutto ciò, con l'obiettivo di definire cosa è lecito e cosa non lo è, cosa è consentito, dove si deve fermare la tecnologia, cosa può fare e cosa non può fare. Si pensi ad esempio al fatto che in questo settore si va ad alterare uno dei concetti fondamentali del diritto civile, ovvero il bisogno di affiancare ad un generico evento il luogo in cui esso si è manifestato e la relativa data, quando invece con Internet non è più così immediato assegnare tali dati all'evento in esame, essendo esso un mezzo di comunicazione che rende difficile collocare nello spazio chi se ne avvale. Inoltre, il sempre maggior utilizzo di queste tecnologie ha portato ad una graduale dissoluzione dei confini che ci possono essere tra la vita online e quella offline, fino al fatto che, se in passato l'accesso alla rete era un evento sporadico, oggi costituisce un elemento fondamentale di integrazione e di sviluppo personale. Internet non è più solo uno strumento, ma uno spazio parallelo e complementare alla vita reale, in cui l'individuo ha il diritto di accedere in qualsiasi momento per partecipare pienamente alla società contemporanea.

Pertanto, è ormai diventato sempre più cruciale estendere la regolamentazione giuridica esistente alle nuove aree emerse con l'avvento del digitale, inclusi tutti gli aspetti legati agli smart assistant, come approfondiremo nel prosieguo di questa trattazione.

1.1 I dati personali

1.1.1 Cosa sono

Prima di trattare le tematiche che riguardano gli assistenti digitali, è importante introdurre un aspetto cruciale legato alla diffusione di informazioni che riguardano un determinato individuo, ovvero quello dei cosiddetti dati personali. Con questa espressione si intende quell'insieme di informazioni che permettono di identificare o di rendere identificabile una persona fisica e che permettono di comprendere aspetti riguardanti il proprio carattere, il proprio stile di vita, la relativa situazione economica, etc.

È possibile raggruppare i vari dati in una serie di categorie:

- tra i più rilevanti ci sono quelli che permettono di ottenere un'*identificazione diretta*, come il nome e il cognome o il numero della carta d'identità, la foto profilo, etc.;
- i dati che permettono un'*identificazione indiretta*, come il codice fiscale, l'indirizzo IP o il numero di targa del proprio veicolo;
- i "*dati sensibili*", ovvero quell'insieme di dati che dichiarano l'origine etnica dell'individuo, le sue convinzioni religiose e le opinioni politiche, oltre che dati relativi alla propria salute;
- i "*dati giudiziari*", ovvero quelli relativi a condanne penali o reati. Sono quindi quei dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari, come il divieto di soggiorno o lo stato di libertà condizionata.

Un'eccezione è data da quei dati che vengono resi anonimi, facendo in modo che la persona non sia più identificabile tramite di essi, per i quali tale dato non è più considerato personale (a patto che l'anonimizzazione di tali dati sia irreversibile).

Con l'evoluzione delle nuove tecnologie, si è via via ampliato quell'insieme di dati personali che assumono un ruolo significativo per l'identificazione della persona, come quelli relativi alle comunicazioni elettroniche e quelli che consentono la geolocalizzazione, fornendo importanti informazioni sulle abitudini dell'individuo rispetto ai luoghi più frequentati e ai suoi spostamenti.

1.1.2 Criticità

I dati personali costituiscono una delle risorse più critiche e vulnerabili dell'era digitale. La raccolta, l'elaborazione e la conservazione di questi dati da parte di aziende, piattaforme online e governi solleva questioni rilevanti in termini di privacy e sicurezza. In particolare, la protezione dei dati personali è regolamentata da normative specifiche in molte giurisdizioni, con il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea che rappresenta uno degli standard più avanzati a livello globale. Il

GDPR impone obblighi rigorosi ai titolari del trattamento, come la necessità di ottenere il consenso esplicito degli utenti, garantire la trasparenza sulle modalità di utilizzo dei dati e fornire agli individui il diritto di accesso, rettifica e cancellazione dei propri dati. La protezione dei dati personali è tuttavia complessa, soprattutto in un contesto in cui la tecnologia evolve rapidamente e le frontiere digitali sono globali. Le aziende devono bilanciare la necessità di utilizzare i dati per migliorare i loro servizi con l'obbligo di proteggere la privacy degli utenti. Le violazioni della sicurezza dei dati e gli utilizzi impropri possono comportare gravi conseguenze, non solo in termini di sanzioni legali, ma anche di danni alla reputazione e perdita di fiducia da parte dei consumatori. La crescente consapevolezza degli individui riguardo ai propri diritti sulla protezione dei dati personali sta inoltre spingendo le aziende a implementare pratiche più rigorose di gestione dei dati, rendendo la protezione dei dati personali un tema centrale nel diritto digitale contemporaneo.

Un altro aspetto molto rilevante da considerare in quest'ottica, oltre al già citato rispetto della privacy e della sicurezza, è il valore economico che può avere un dato. Infatti, ad oggi, sempre più aziende utilizzano i dati personali per veicolare le scelte e gli acquisti dei consumatori. Accedendo ai loro dati personali hanno la possibilità di conoscere le loro preferenze o i loro gusti, e quindi possono capire cosa potrebbe essere interessato ad acquistare quel determinato individuo e regolarsi di conseguenza. Spesso non ci si rende neanche conto di quanti dati personali condividiamo, anche inconsciamente, ogni giorno, visitando un sito web ed accettando termini accessori riguardo il trattamento dei nostri dati o acquistando prodotti e servizi online o in negozio. È diventato quindi fondamentale studiare l'argomento dal punto di vista giuridico, al fine di comprendere questo nuovo sistema che sta diventando sempre più predominante nelle vite di ogni cittadino e di giungere alle modalità attraverso le quali sia possibile tutelare ogni individuo sotto questo punto di vista.

E ancora il tema della responsabilità delle piattaforme digitali è un altro punto cruciale. Le grandi aziende tecnologiche, come i social media e i motori di ricerca, giocano un ruolo significativo nella diffusione delle informazioni. Le questioni relative alla disinformazione, ai contenuti illegali e all'incitamento all'odio online sollevano domande

su come queste piattaforme debbano essere regolamentate e su chi debba essere ritenuto responsabile per i contenuti che ospitano.

CAPITOLO 2 – Smart Assistant

2.1 Cosa sono

Un assistente digitale (o smart assistant) consiste in uno strumento che, attraverso l'intelligenza artificiale avanzata, la comprensione e l'elaborazione del linguaggio naturale e il machine learning, è in grado di dialogare con l'interlocutore con l'obiettivo di rispondere ad una generica domanda che gli viene posta o di eseguire un suo determinato comando. Gli smart assistant in generale sono costituiti da più elementi fondamentali:

- una componente *hardware*, in cui è installato l'assistente virtuale (ad esempio uno smartphone o una smart TV);
- una componente *software*, ovvero un programma che, attraverso l'utilizzo di complessi algoritmi, è in grado di raggiungere alti livelli di interazione uomo-macchina elaborando ed interpretando la richiesta che gli viene posta dall'utente;
- le *risorse*, ovvero i dati esterni che alimentano il database degli smart assistant, grazie ai quali il dispositivo è in grado di rispondere alle domande che gli vengono poste (ad esempio "dimmi che ore sono") e di eseguire azioni su richiesta (ad esempio "spegni le luci in cucina").

Tra gli smart assistant più noti e diffusi sul mercato dobbiamo citare Siri di Apple, Alexa di Amazon, Google Assistant di Google e Bixby di Samsung. Questi dispositivi ascoltano il mondo che li circonda e nel momento in cui ricevono uno specifico comando di attivazione (che di solito consiste in una parola chiave, la cosiddetta *wake-up word*) predefinito dalla relativa casa produttrice, si collega al server per decodificare la richiesta che le è stata impartita, ed in seguito, elaborando una consistente mole di dati, interpreta la realtà e giunge ad una decisione (la risposta che fornisce all'utente).

Una particolare declinazione degli assistenti digitali è rappresentata dai chatbot, strumenti di assistenza che vengono integrati in molti e-commerce con l'obiettivo di offrire supporto ai clienti attraverso un'apposita chat. Questi sistemi intelligenti confrontano le richieste degli utenti con un database di informazioni di cui sono dotati e da cui estrapolano la risposta alla particolare richiesta. Da qui, adoperandosi di alcune capacità cognitive umane possono interagire in modo naturale, rispondendo alle domande e guidando il cliente nel processo di acquisto in modo simile a come farebbe una persona reale. A livello di differenze rispetto ai classici smart assistant diciamo che i chatbot sono progettati per conversazioni testuali, spesso hanno un campo d'azione limitato e operano in spazi circoscritti (sui quali tuttavia sono molto specializzati). Al contrario gli smart assistant come Siri o Alexa sono dispositivi molto più versatili che possono offrire un'esperienza più ricca e dinamica se vengono adoperati in un contesto più generale di vita quotidiana.

2.2 Evoluzione degli smart assistant

La tecnologia ubiqua (concetto che descrive la presenza pervasiva e integrata della tecnologia nella vita quotidiana, al punto che essa diventa quasi invisibile e completamente integrata nell'ambiente circostante) ha travolto le nostre abitudini quotidiane, portandoci a delegare la maggior parte delle attività domestiche e lavorative all'intelligenza artificiale. In particolare, gli smart assistant hanno subito una straordinaria evoluzione nel corso degli ultimi due decenni, trasformandosi da semplici strumenti di automazione a sofisticati sistemi di intelligenza artificiale capaci di interagire con gli esseri umani in modi sempre più naturali e intuitivi. Le prime versioni degli assistenti digitali risalgono agli anni '90, quando i software di automazione e di elaborazione del linguaggio naturale iniziarono a svilupparsi. Tuttavia, erano strumenti rudimentali, capaci di rispondere a semplici comandi predefiniti. Il vero punto di svolta è avvenuto con l'integrazione del riconoscimento vocale nei dispositivi. Negli anni 2000, aziende come Google hanno iniziato a sviluppare tecnologie in grado di comprendere e rispondere alle domande attraverso il linguaggio naturale. Il lancio di Siri da parte di Apple nel 2011 ha segnato un momento cruciale: per la prima volta, un assistente

digitale era integrato direttamente in un dispositivo mobile, in grado di comprendere e rispondere a comandi vocali in tempo reale. Con l'avanzare della tecnologia, altri giganti del settore tecnologico hanno seguito l'esempio di Apple. I più importanti sono stati Amazon Alexa (2014) e Google Assistant (2016), i quali hanno ampliato le possibilità degli assistenti digitali, integrandoli in dispositivi domestici come gli smart speaker. Questi sistemi non solo rispondono a domande, ma controllano anche dispositivi intelligenti in casa, come luci, termostati e sistemi di sicurezza. Inoltre, grazie alle evoluzioni più recenti (legate all'uso di algoritmi di apprendimento automatico, ovvero il machine learning, e all'intelligenza artificiale) questi assistenti sono anche in grado di apprendere dai comportamenti e dalle preferenze degli utenti per offrire risposte e servizi sempre più personalizzati. Ad esempio, Google Assistant utilizza i dati raccolti dai vari servizi Google per fornire suggerimenti proattivi e rilevanti, come avvisi sul traffico o promemoria personalizzati.

Notiamo anche che, al giorno d'oggi, il mondo degli smart assistant si sta espandendo in maniera significativa in un nuovo settore, quello delle automobili. Si parla sempre più spesso di *smart car*, o auto intelligenti, per indicare veicoli dotati di sistemi avanzati che, grazie alla connessione costante, sono in grado di comunicare informazioni in tempo reale al conducente e agli altri utenti della strada. Questi sistemi consentono non solo lo scambio di dati tra veicoli, ma anche la connessione con il sistema circostante, migliorando la sicurezza stradale attraverso la prevenzione e la rilevazione degli incidenti. Inoltre, offrono nuovi modelli assicurativi personalizzati e informazioni geo-referenziate sulla viabilità, rendendo l'esperienza di guida più sicura e intelligente. Un aspetto molto rilevante di questa potenziale nuova tecnologia è legato all'arrivo dei cosiddetti *smart speaker* o assistenti vocali intelligenti, in grado di dialogare con gli utenti e permettere loro di gestire tutto tramite la voce: dalle indicazioni stradali alle informazioni sulla situazione del traffico, fino alla gestione della musica e dell'entertainment a bordo veicolo.

Dobbiamo quindi immaginarci un futuro non così lontano in cui l'assistente vocale accompagnerà l'utente sia quando è a casa sia quando è in macchina, rendendo

disponibile la tecnologia direttamente nell'abitacolo, senza che sia necessario utilizzare lo smartphone.

2.3 Impatto sulla vita di ogni giorno

Come già detto, l'integrazione degli smart assistant nella vita quotidiana ha trasformato profondamente il modo in cui interagiamo con la tecnologia, influenzando vari aspetti della nostra esistenza: per alcune cose ha avuto un impatto positivo ma bisogna sempre fare attenzione anche a quelli negativi. Sicuramente hanno reso molte attività più *rapide* ed *efficienti*, infatti, con un semplice comando vocale, è possibile inviare messaggi, impostare promemoria, gestire calendari e cercare informazioni, eliminando la necessità di interagire manualmente con i dispositivi. Questo consente alle persone di gestire meglio il proprio tempo, delegando compiti ripetitivi o semplici agli assistenti. Con l'espansione dei dispositivi connessi, gli smart assistant sono diventati il centro di controllo delle smart home (*automazione domestica*). Attraverso assistenti come Alexa o Google Assistant, è possibile gestire l'illuminazione, il riscaldamento, la sicurezza e persino elettrodomestici come lavatrici o frigoriferi, contribuendo ad incrementare le possibili comodità che si ritrovano all'interno della propria abitazione. Per le persone con disabilità, gli assistenti digitali rappresentano un supporto fondamentale, infatti, la capacità di interagire con i dispositivi tramite comandi vocali offre un livello di accessibilità senza precedenti. Ad esempio, chi ha difficoltà motorie può controllare la propria casa o comunicare con altre persone senza dover utilizzare dispositivi fisici complessi. Anche nel contesto degli e-commerce, gli assistenti digitali e i già citati chatbot hanno migliorato l'esperienza di acquisto online: rispondendo a domande in tempo reale, suggerendo prodotti o risolvendo problemi tecnici, questi strumenti migliorano la soddisfazione del cliente e semplificano il processo di acquisto. Gli smart assistant stanno rivoluzionando anche il modo in cui fruiamo dell'intrattenimento, tanto che possiamo parlare di *intrattenimento personalizzato*. Che si tratti di riprodurre musica, suggerire film o programmare la visione di serie TV, gli smart assistant possono personalizzare l'esperienza in base ai gusti e alle abitudini degli utenti. Ad esempio,

Alexa e Google Assistant possono interagire con piattaforme come Spotify, Netflix o YouTube per offrire contenuti su richiesta.

Nonostante i numerosi vantaggi che abbiamo elencato, bisogna tenere conto anche dell'altro lato della medaglia, infatti, l'adozione diffusa degli assistenti digitali solleva anche molte preoccupazioni, con la privacy in primo piano. Questi assistenti raccolgono una grande quantità di dati personali, sollevando interrogativi su come tali informazioni vengano utilizzate e protette. Combinando dati storici come le preferenze di acquisto, la proprietà della casa, la posizione geografica e la dimensione del nucleo familiare, gli algoritmi sono in grado di costruire modelli dettagliati che identificano schemi di comportamento. Man mano che nuovi dati vengono aggiunti, questi modelli si perfezionano, permettendo agli assistenti digitali di apprendere abitudini e preferenze degli utenti. In questo modo, possono rispondere a domande complesse, offrire consigli personalizzati, fare previsioni e persino avviare conversazioni in modo proattivo. Tuttavia, è proprio questa capacità di raccogliere e utilizzare informazioni così dettagliate che rende la protezione della privacy un tema di grande importanza. Inoltre, alcuni dispositivi non si limitano ad essere in connessione con la rete, bensì sono anche in grado di dialogare con altri dispositivi e tale capacità agevola la possibilità di raccolta, di incrocio dei dati e di diffusione di informazioni personali.

L'eccessiva dipendenza da questi strumenti potrebbe ridurre la capacità di eseguire autonomamente alcune attività o limitare le interazioni sociali dirette. Va anche detto che al giorno d'oggi tali tecnologie non sono ancora intelligenti strictu sensu, non essendo dotati della capacità di sviluppare una coscienza autonoma, e quindi è fondamentale utilizzare le nuove tecnologie con il giusto occhio critico.

Pertanto, possiamo concludere che, seppur questa tecnologia abbia reso molte attività quotidiane più semplici e accessibili, è altrettanto essenziale bilanciare tali vantaggi con la consapevolezza delle sfide legate alla privacy e all'uso etico di queste tecnologie.

CAPITOLO 3 – Implicazioni giuridiche degli Smart Assistant

3.1 Riservatezza, Privacy e Protezione dei dati personali

L'evoluzione tecnologica ha portato il legislatore europeo a rivedere la normativa sulla protezione dei dati personali. La tradizionale idea di "sfera privata" necessita oggi di una rivisita, in risposta alla continua rivoluzione digitale e alle nuove forme di intrusione che essa introduce, considerando il costante flusso di interazioni e integrazioni con il mondo virtuale che caratterizza sempre di più la nostra vita quotidiana. Questo cambiamento richiede una riflessione approfondita non solo sul concetto di riservatezza, ma anche su quello più ampio di privacy, entrambi strettamente collegati ma con implicazioni diverse nella tutela della persona nell'era digitale.

Il *diritto alla riservatezza* si riferisce alla tutela della vita privata e intima di una persona, proteggendo informazioni personali e aspetti della propria esistenza che si desidera mantenere al riparo da sguardi o interferenze esterne. Questo diritto copre principalmente la vita privata delle persone, garantendo che certi aspetti personali non vengano divulgati senza il consenso dell'individuo e può essere considerato come il diritto all'inviolabilità della propria quotidianità, dei propri spazi e delle proprie relazioni. Esempi includono la protezione di segreti personali, la riservatezza delle conversazioni, e la protezione contro intrusioni indebite nella vita domestica o privata. Ha radici storiche profonde ed è stato uno dei primi diritti a essere riconosciuto come fondamentale per la dignità umana.

Mentre il *diritto alla privacy* è un concetto più ampio rispetto alla riservatezza e riguarda la protezione generale della sfera personale di un individuo. Include il diritto ad essere lasciati in pace, a controllare l'accesso alle proprie informazioni personali e a decidere su come queste informazioni vengano raccolte, utilizzate e condivise. Riguarda la sfera personale, familiare, e professionale, estendendosi anche al diritto di controllare la propria immagine pubblica.

L'articolo 2 della Costituzione Italiana sancisce i diritti inviolabili dell'uomo, fornendo le basi per la protezione della privacy. Sebbene non espliciti direttamente questo diritto, esso è stato interpretato come comprensivo della tutela della vita privata e della riservatezza, essenziali per l'espressione della libertà individuale. A differenza del diritto alla riservatezza, non è stato considerato fin da subito come fondamentale, ma nel tempo lo è divenuto anch'esso, in quanto rappresenta una garanzia essenziale per la dignità della persona e per la sua libertà, pertanto, merita di particolare tutela tanto che una violazione dei dati personali potrebbe provocare, letteralmente, danni fisici, materiali o immateriali dell'individuo stesso. Questo concetto si è ampliato, evolvendosi per far fronte alle nuove sfide poste dalla digitalizzazione e dal trattamento dei dati personali. Oggi, il diritto alla privacy è riconosciuto come un pilastro centrale per garantire il rispetto dell'individuo, non solo nella sua dimensione privata ma anche nella vita pubblica e digitale.

Infine, parliamo del *diritto alla protezione dei dati personali*, una specifica declinazione del diritto alla privacy che riguarda la regolamentazione della raccolta, gestione, conservazione e utilizzo dei dati personali da parte di terzi, inclusi enti pubblici e privati. Questo diritto si applica principalmente al trattamento dei dati personali e protegge informazioni come nome, indirizzo, informazioni finanziarie, dati medici e qualsiasi altro dato che possa identificare una persona. È un concetto relativamente recente, emerso con l'avvento della società dell'informazione e della digitalizzazione.

3.2 Il GDPR

La perdita del controllo dei dati personali o una limitazione dei diritti della persona nei confronti dei propri dati, la discriminazione, il furto o l'usurpazione d'identità, le perdite finanziarie, i pregiudizi alla reputazione e la perdita di riservatezza dei dati protetti da segreto professionale sono solo alcuni dei danni riferibili ad una cattiva o incauta gestione dei dati dei propri utenti, clienti o collaboratori. Proprio per questi motivi, a fronte di un sempre maggior utilizzo di tecnologie come gli smart assistant, ovvero di dispositivi in grado di raccogliere, memorizzare e condividere una molteplicità di dati

sensibili, è diventato sempre più necessario regolamentare e gestire questo nuovo mondo. Al giorno d'oggi, uno dei principali riferimenti in materia è il già citato Regolamento Generale sulla Protezione dei Dati (GDPR, dall'inglese General Data Protection Regulation), un regolamento dell'Unione Europea che disciplina il modo in cui le aziende e le altre organizzazioni trattano i dati personali. Il GDPR ha influenzato significativamente altre normative sulla privacy dei dati in tutto il mondo e richiede la conformità di qualsiasi organizzazione che acceda ai dati personali delle persone nell'UE. È divenuto pienamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018 ed è anche noto come Regolamento Ue 2016/679. Il GDPR nasce da precise esigenze, come indicato dalla stessa Commissione Ue, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo. Si tratta poi di una risposta, necessaria ed urgente, alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini Ue. A preoccupare sono, però, gli spazi di autonomia che permangono in capo ai singoli Stati Membri nel disciplinare in maniera più specifica rispetto al GDPR alcuni aspetti non ricompresi nella competenza dell'UE in base al principio di attribuzione. Tale circostanza potrebbe far sorgere contrasti tra le diverse Autorità di controllo nazionali che si trovino a disciplinare nello specifico e applicare in concreto a livello nazionale le disposizioni del GDPR. Senza entrare troppo nel dettaglio in merito a quest'argomento, ci concentreremo ora sul trattare uno dei 99 articoli del GDPR, ovvero l'articolo 5.

3.2.1 Articolo 5 - Principi applicabili al trattamento di dati personali

L'Articolo 5 del GDPR stabilisce i principi fondamentali per il trattamento dei dati personali che sono essenziali per garantire la protezione e la riservatezza dei dati degli individui. Questo articolo funge da base per tutte le altre disposizioni del GDPR e guida il trattamento dei dati personali in modo che sia conforme alle norme di protezione dei dati.

Andiamo quindi ad approfondire i principali aspetti che tale articolo tratta:

- la *liceità*, poiché il trattamento dei dati personali deve essere basato su una base giuridica valida, come il consenso dell'interessato, l'adempimento di un contratto, gli obblighi legali, la protezione degli interessi vitali, i compiti di interesse pubblico o i legittimi interessi perseguiti dal titolare del trattamento;
- la *correttezza*, essendo che i dati devono essere trattati in modo equo e giusto rispetto all'interessato, evitando pratiche ingannevoli o dannose;
- la *trasparenza*, attraverso cui gli interessati devono essere informati chiaramente e in modo comprensibile su come i loro dati saranno trattati, inclusi gli scopi del trattamento e le eventuali conseguenze;
- la *limitazione della finalità*, con cui i dati personali devono essere raccolti per scopi determinati, espliciti e legittimi e non devono essere trattati ulteriormente in modi incompatibili con tali scopi. Questa limitazione assicura che i dati non siano utilizzati per scopi diversi da quelli per cui sono stati raccolti inizialmente;
- la *minimizzazione dei dati che bisogna raccogliere*, dove in particolare devono essere raccolti e conservati solo i dati personali che sono adeguati, pertinenti e limitati a quanto necessario rispetto agli scopi per i quali sono trattati. Questo principio promuove la raccolta e l'uso di dati solo nella misura necessaria per raggiungere gli obiettivi prefissati;
- l'*esattezza*, infatti i dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per garantire che i dati inaccurati, rispetto agli scopi per i quali sono trattati, siano rettificati o cancellati senza indugi;
- la *limitazione della conservazione*, ovvero che i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario per gli scopi per i quali i dati personali sono trattati. Una volta raggiunto lo scopo del trattamento, i dati devono essere cancellati o anonimizzati;
- l'*integrità* e la *riservatezza*, secondo cui i dati personali devono essere trattati in modo da garantire una sicurezza adeguata, inclusa la protezione contro il

trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danneggiamento accidentale. Questo principio richiede l'adozione di misure tecniche e organizzative adeguate per proteggere i dati personali;

- ultimo ma non meno importante è l'aspetto legato alla *responsabilità*, per la quale il titolare del trattamento è responsabile dell'osservanza dei principi stabiliti e deve essere in grado di dimostrare tale conformità. Questo principio implica che i titolari del trattamento devono adottare e mantenere misure adeguate per garantire il rispetto dei principi e che devono poter dimostrare la loro conformità alle autorità di controllo.

L'Articolo 5 del GDPR stabilisce quindi i principi guida per il trattamento dei dati personali e assicura che i dati siano trattati in modo giusto e trasparente. Questi principi sono fondamentali per la protezione dei diritti e delle libertà degli individui e costituiscono la base su cui si fondano altre disposizioni del GDPR. Adottare e rispettare questi principi è essenziale per garantire che il trattamento dei dati personali sia conforme alle normative e per costruire la fiducia tra le organizzazioni e gli individui i cui dati vengono trattati.

3.2.2 Articolo 7 - Condizioni per il consenso

Prima di approfondire le modalità con cui gli smart assistant raccolgono, utilizzano e conservano i dati, è utile esaminare brevemente un altro articolo del GDPR, che tratta una questione cruciale nell'era delle tecnologie e della condivisione dei dati, ovvero il consenso che l'utente deve fornire per permettere al sito di raccogliere specifici dati personali. Questo articolo stabilisce le modalità e i requisiti che devono essere soddisfatti affinché il consenso sia considerato valido ai sensi del Regolamento ed è diviso in quattro paragrafi:

1. *Modalità di ottenimento del consenso*: libero, specifico, informato ed inequivocabile. In particolare, deve essere dato liberamente, senza coercizione o pressione indebita (una scelta consapevole dell'interessato). Deve essere chiaro e preciso riguardo agli scopi per i quali i dati verranno trattati (non è

accettabile un consenso generico per tutte le possibili finalità). Inoltre, gli interessati devono essere adeguatamente informati su cosa comporta il trattamento dei loro dati (finalità del trattamento, durata della conservazione dei dati e diritti dell'interessato). Deve essere espresso in modo chiaro e non ambiguo, ad esempio tramite una dichiarazione scritta o una chiara azione positiva.

2. *Documentazione del consenso*. Il titolare del trattamento è tenuto a dimostrare che l'interessato ha dato il consenso e questo significa che devono essere mantenute prove concrete del consenso ottenuto, come registrazioni di quando e come il consenso è stato fornito.
3. *Diritto di revoca*. L'interessato ha il diritto di revocare il consenso in qualsiasi momento, con l'accorgimento che l'eventuale revoca deve essere trattata con la stessa facilità con cui è stato dato il consenso. Inoltre, la revoca del consenso non influisce sulla liceità del trattamento basato sul consenso prima della revoca, tuttavia, una volta revocato, il trattamento futuro dei dati non è più lecito basato su quel consenso.
4. *Condizioni per i minori*. Per i minori di età inferiore ai 16 anni, il consenso deve essere dato o autorizzato da un genitore o tutore legale, anche se in generale gli Stati membri possono stabilire un'età inferiore, seppur non inferiore ai 13 anni.

L'Articolo 7 risulta quindi cruciale per garantire che il consenso al trattamento dei dati personali sia ottenuto in modo conforme e rispettoso dei diritti degli individui. Stabilisce chiaramente che il consenso deve essere un atto positivo, informato e consapevole, e prevede meccanismi per la documentazione e la revoca, che assicurano trasparenza e controllo da parte dell'interessato.

3.3 Protezione dei dati e Smart Assistant

Secondo un recente studio, condotto congiuntamente dalla Northeastern University of Boston e dall'Imperial College di Londra, molti dati personali degli utenti raccolti dai dispositivi intelligenti sarebbero trasmessi a terze parti (come Spotify e Microsoft) senza

alcuna autorizzazione, anche nei casi in cui l'utente non abbia sottoscritto alcun abbonamento. Netflix, ad esempio, potrebbe rilevare la presenza dell'utente nella propria abitazione. L'indagine sull'Internet of Things (IoT) condotta dalla Global Privacy Enforcement Network (GPEN) nel 2016 "ha rivelato che le società del settore non hanno ancora posto sufficiente attenzione alla protezione dei dati personali, con il rischio, peraltro, di generare sfiducia nei consumatori. Alcune aziende, ad esempio, non si rendono conto che non solo il nome e il cognome, ma anche i dettagli sul consumo elettrico di una persona o i suoi stessi parametri vitali, sono dati personali da proteggere. Così come non è ancora sufficientemente garantita neppure la possibilità per i consumatori di cancellare i dati raccolti da questi dispositivi. Il Garante italiano insieme alle altre Autorità del Global Privacy Enforcement Network monitorerà con attenzione questi prodotti e servizi, al fine di verificare che la realizzazione di strumenti innovativi come elettrodomestici intelligenti, braccialetti per il controllo dei cicli del sonno o dell'indice glicemico, oppure le stesse automobili connesse a Internet, non avvenga a danno della riservatezza dei dati personali, spesso anche sensibili, degli utenti". All'esito dell'indagine, oltre il 60% dei dispositivi IoT non ha superato l'esame di affidabilità dei Garanti Privacy di 26 diversi Paesi.

In generale possiamo dire che, quando un evento interrompe l'equilibrio di un sistema, si verifica inevitabilmente una fase di disordine. In tali circostanze, è compito del diritto intervenire per ristabilire l'ordine e garantire che tutto torni sotto controllo. Pertanto, dopo aver esaminato i diritti degli utenti e a fronte degli esiti di tali indagini è bene approfondire come gli smart assistant raccolgano e gestiscano i dati.

Innanzitutto, anche quando non volontariamente attivati, gli smart assistant restano in ascolto passivo (il cosiddetto *passive listening*), una sorta di stato di dormiveglia da cui escono quando recepiscono la parola di attivazione e quindi sono sempre potenzialmente in grado di registrare suoni e immagini.

Come abbiamo già detto, gli smart assistant funzionano raccogliendo input vocali dall'utente, dati contestuali (come la cronologia delle ricerche) e dati da dispositivi collegati (come smart speaker) elaborandoli e fornendo risposte personalizzate o eseguendo azioni. Tutto ciò deve avvenire in conformità con i principi dell'Articolo 5 del

GDPR e ad esempio il trattamento deve essere lecito, devono essere raccolti solo i dati strettamente necessari per le finalità dichiarate, inoltre devono garantire la trasparenza riguardo al trattamento, informando l'utente in modo chiaro su quali dati vengono raccolti (a fronte del quale devono ottenere il consenso, come trattato nell'Articolo 7) e come vengono utilizzati, rispettando il diritto alla privacy.

Il trattamento dei dati personali negli smart assistant avviene per una serie di finalità, che devono essere esplicitamente comunicate all'utente, come l'esecuzione dei comandi, la personalizzazione o il miglioramento del servizio. Queste finalità devono essere in linea con il principio della limitazione delle finalità previsto dall'Articolo 5, e l'utente deve essere sempre informato in modo trasparente su come verranno utilizzati i suoi dati, in ottemperanza all'Articolo 7.

Un aspetto cruciale per gli smart assistant riguarda la protezione della riservatezza dei dati personali e la sicurezza del trattamento. Questi dispositivi devono implementare adeguate misure tecniche e organizzative per proteggere i dati da accessi non autorizzati o perdite e ciò include una crittografia delle comunicazioni tra il dispositivo e i server remoti, un'autenticazione sicura dell'utente per prevenire l'accesso ai comandi da parte di terzi non autorizzati e una limitazione della conservazione dei dati a quelli strettamente necessari.

L'Articolo 7 del GDPR sottolinea l'importanza di ottenere un consenso libero, informato e specifico per il trattamento dei dati. Nel caso degli smart assistant, ciò significa che l'utente deve essere chiaramente informato, prima della raccolta dei dati, su come verranno trattati e per quali scopi, deve avere la possibilità di revocare il consenso in qualsiasi momento e deve ricevere aggiornamenti su eventuali modifiche alle politiche di trattamento dei dati. Un problema comune è che spesso gli utenti non sono pienamente consapevoli della quantità e del tipo di dati raccolti dagli smart assistant, sollevando preoccupazioni sulla trasparenza. Per questo motivo, molte aziende stanno lavorando per rendere più chiare le loro politiche sulla privacy e fornire strumenti che permettano agli utenti di controllare meglio i propri dati.

Il mancato rispetto delle norme sul consenso o dei principi di protezione dei dati (come quelli sanciti dall'Articolo 5) può portare a gravi conseguenze legali per le aziende che sviluppano e gestiscono smart assistant. Oltre alle sanzioni amministrative previste dal GDPR, come le multe che possono arrivare fino al 4% del fatturato globale, le violazioni possono anche danneggiare la fiducia degli utenti, con gravi ripercussioni sulla reputazione dell'azienda.

La rapida diffusione degli smart assistant e la continua innovazione tecnologica stanno spingendo i legislatori a rivedere costantemente le normative esistenti per garantire che questi dispositivi rispettino il diritto alla privacy. Le normative europee, come il GDPR, rappresentano un punto di riferimento globale per la protezione dei dati, ma si prevede che in futuro ci saranno ulteriori sviluppi normativi per affrontare sfide specifiche legate alle nuove tecnologie, come il crescente uso dell'intelligenza artificiale negli smart assistant. Pertanto, la sfida per il futuro sarà continuare a innovare nel campo delle tecnologie intelligenti mantenendo un alto livello di protezione dei dati.

CAPITOLO 4 – Impatto del Data Act sugli smart assistant

4.1 Il Data Act

Il Data Act è una proposta legislativa dell'Unione Europea che fa parte del pacchetto di regolamentazione dei dati, volto a promuovere un mercato europeo dei dati equo e competitivo. Il suo obiettivo principale è di facilitare l'accesso, la condivisione e l'uso dei dati tra le imprese e i cittadini, per stimolare l'innovazione e la concorrenza, mantenendo al contempo elevati standard di protezione e sicurezza dei dati. È una proposta molto recente, pubblicata nel dicembre del 2023 ed entrata in vigore l'11 gennaio 2024.

L'idea alla base del Data Act è di sfruttare al meglio il potenziale dei dati generati da diversi settori e dispositivi (dall'Internet of Things alle piattaforme digitali), creando

condizioni che permettano a tutti gli attori economici di trarre vantaggio da questa risorsa, tenendo conto del fatto che in molti casi i dati sono in realtà controllati da poche grandi imprese, che limitano la possibilità di accesso da parte di altre aziende e individui. Il Data Act punta a rimuovere questi ostacoli, creando un ambiente in cui i dati possano circolare in modo più fluido, promuovendo l'innovazione e la concorrenza. Gli obiettivi principali sono:

- *accessibilità dei dati*, facilitandone l'accesso per le imprese, le pubbliche amministrazioni e i cittadini. Ciò significa che le aziende che generano dati devono metterli a disposizione di altre imprese o individui a condizioni eque;
- *neutralità nei confronti del trattamento dei dati*, nel senso che nessun attore, grande o piccolo, dovrebbe avere un vantaggio ingiusto nell'accesso ai dati;
- *promozione dell'innovazione*, infatti, la possibilità di accedere e condividere i dati consente alle imprese (soprattutto a quelle piccole e medie (PMI)) di innovare più facilmente e di sviluppare nuovi servizi e prodotti;
- *interoperabilità e portabilità* introducendo meccanismi per rendere più semplice la portabilità dei dati tra servizi e piattaforme, riducendo i costi di transizione e limitando la dipendenza da un unico fornitore;
- *uso dei dati da parte del settore pubblico* attraverso delle disposizioni che consentono alle amministrazioni pubbliche di accedere ai dati delle imprese in situazioni di emergenza (come le pandemie) o per scopi di pubblico interesse;
- infine, come vedremo nel prossimo paragrafo, la *tutela dei dati personali*, secondo cui qualsiasi uso o condivisione di dati deve rispettare le normative esistenti in materia di protezione dei dati personali (in primis il GDPR).

L'introduzione del Data Act può avere diverse ripercussioni sui settori economici e sulla società. Innanzitutto, può stimolare l'economia dei dati nell'UE, creando nuove opportunità di business per aziende di tutti i settori. Le PMI potrebbero beneficiare in particolare dall'accesso a dati che altrimenti sarebbero esclusi a causa del controllo da parte di grandi attori tecnologici. D'altro canto, vi sono anche sfide significative legate alla sua attuazione. Alcune grandi aziende potrebbero essere riluttanti a condividere i loro dati, soprattutto se ciò riduce il loro vantaggio competitivo. Inoltre,

l'interoperabilità tra sistemi e piattaforme diverse richiede standard tecnici comuni che devono ancora essere sviluppati e applicati. Infine, c'è il rischio che il Data Act possa entrare in conflitto con le normative internazionali sulla protezione dei dati, come quelle statunitensi o cinesi, creando potenziali barriere commerciali.

Il Data Act rappresenta quindi un passo cruciale nella strategia europea per la creazione di un'economia digitale sostenibile e innovativa. Se attuato correttamente, potrebbe rivoluzionare il modo in cui i dati vengono gestiti, utilizzati e condivisi, ponendo l'Unione Europea come un pioniere nell'economia dei dati.

4.2 Data Act e GDPR messi a confronto

In generale possiamo dire che il Data Act integra il GDPR, in quanto i due regolamenti operano su livelli diversi. Il GDPR garantisce che i dati personali siano protetti e trattati in modo lecito, mentre il Data Act si concentra sulla promozione dell'uso di dati non personali per stimolare l'innovazione. Anche se il Data Act riguarda principalmente i dati non personali, può coinvolgere i dati personali in alcune circostanze ed in questi casi è bene sapere che il Data Act non può sovrascrivere il GDPR: qualsiasi trattamento di dati personali deve rispettare le regole di protezione imposte dal GDPR. Questo significa che, se le aziende vogliono condividere o utilizzare dati personali, devono ottenere il consenso degli individui coinvolti o rispettare altre basi legali previste dal GDPR.

Inoltre, possiamo dire che il Data Act promuove la condivisione dei dati e la portabilità, il che implica che gli individui o le aziende possono trasferire i propri dati da un fornitore di servizi all'altro in modo facile e sicuro. Questo principio si collega con l'Articolo 20 del GDPR, che riconosce il *diritto alla portabilità dei dati personali*, permettendo agli utenti di trasferire i propri dati personali da un servizio all'altro. Tuttavia, mentre il GDPR limita questo diritto ai dati personali, il Data Act lo estende ai dati non personali.

In sintesi, il Data Act espande le opportunità di accesso ai dati, ma non va a discapito della privacy personale garantita dal GDPR. Le due normative lavorano insieme per

bilanciare l'accessibilità dei dati e la protezione della privacy, sostenendo l'innovazione senza compromettere i diritti individuali.

4.3 Implicazioni del Data Act sugli Smart Assistant

Con l'introduzione del Data Act, le normative europee hanno compiuto un ulteriore passo verso la regolamentazione della gestione dei dati nel contesto dell'Internet of Things e dei dispositivi intelligenti come gli smart assistant. Come abbiamo detto, il Data Act (che si affianca al GDPR) si focalizza principalmente sulla portabilità e la condivisione dei dati, imponendo requisiti specifici per la trasparenza e l'accesso ai dati personali. Per gli smart assistant, che raccolgono e trattano una vasta gamma di dati dagli utenti, ciò comporta una serie di implicazioni significative:

- innanzitutto, il Data Act prevede che i dati raccolti dai dispositivi intelligenti possano essere trasferiti tra diversi fornitori di servizi senza ostacoli indebiti, promuovendo una *maggiore interoperabilità* e consentendo agli utenti di spostare i propri dati tra diverse piattaforme e servizi. Ciò rappresenta una sfida per gli smart assistant, che devono garantire non solo la conformità alle disposizioni di portabilità dei dati, ma anche la sicurezza e l'integrità dei dati durante tali trasferimenti.
- inoltre, il Data Act introduce il principio della *trasparenza nella gestione dei dati*, che obbliga le aziende a fornire agli utenti informazioni chiare su come i loro dati vengono trattati, condivisi e utilizzati, andando oltre le disposizioni del GDPR in termini di chiarezza e dettaglio. Per gli smart assistant, ciò implica una maggiore responsabilità nella comunicazione con gli utenti, inclusa la fornitura di opzioni per il controllo e la gestione dei dati raccolti.
- un altro aspetto cruciale è l'*accesso e la gestione dei dati*, poiché il Data Act conferisce agli utenti il diritto di accedere ai propri dati in modo diretto e di richiederne la cancellazione o la modifica, imponendo alle aziende di implementare meccanismi efficaci per soddisfare tali richieste.

- infine, il Data Act prevede misure specifiche per garantire la *sicurezza dei dati* durante la raccolta, l'archiviazione e la trasmissione degli stessi, rispetto ai quali, seppur il GDPR rimanga fondamentale per assicurarne la protezione e il rispetto della privacy, il Data Act permette di bilanciare la possibilità di accesso ai dati con la necessità di proteggere la privacy degli utenti e di garantire che qualsiasi condivisione di dati non comprometta la sicurezza delle informazioni sensibili.

In conclusione, mentre il GDPR ha gettato solide basi per la protezione dei dati personali, il Data Act amplia queste normative per affrontare le sfide emergenti della tecnologia e dell'uso diffuso degli smart assistant. Questo nuovo regolamento impone un livello superiore di responsabilità e trasparenza nella gestione dei dati, creando un ambiente più aperto e competitivo. Gli utenti beneficeranno di un maggiore controllo sui propri dati, mentre le aziende avranno l'opportunità di innovare grazie all'accesso a informazioni precedentemente limitate. Tuttavia, sarà fondamentale mantenere un equilibrio tra l'accesso ai dati e la protezione della privacy, per garantire che la sicurezza e i diritti degli utenti siano sempre tutelati in un contesto di crescente condivisione e interoperabilità dei dati.

CAPITOLO 5 – Linee guida per un corretto utilizzo di tale tecnologia

Come abbiamo più volte detto in questo lavoro, per migliorare il livello di servizio e per fornire un'esperienza più personalizzata, gli assistenti digitali raccolgono e memorizzano costantemente una vasta quantità di dati personali non solo sugli utenti diretti, ma anche su chiunque si trovi nelle vicinanze, dalle preferenze e le abitudini di vita ai consumi e agli interessi, così come la posizione e i percorsi abituali o il numero e caratteristiche delle persone presenti nell'ambiente. Pertanto, è essenziale utilizzare questi strumenti in modo informato e consapevole per proteggere adeguatamente i dati personali degli utenti e di chiunque entri nel campo di azione di un qualsiasi assistente digitale.

1) Se per attivare l'assistente digitale è necessario registrarsi fornendo alcuni dati personali, è fondamentale leggere attentamente l'informativa sul trattamento dei dati, disponibile sul sito dell'azienda o nella confezione del dispositivo, con l'obiettivo di verificare:

- il *tipo di dati* che vengono *raccolti* (ad esempio tramite microfono o videocamera);
- *l'utilizzo* che se ne fa dei dati e l'eventuale *trasferimento a terzi*;
- a chi viene estesa la possibilità di *accesso ai dati*;
- dove e per quanto tempo i dati vengono *conservati*.

2) Quando si attiva uno smart assistant, è consigliabile fornire solo le informazioni strettamente necessarie per la registrazione e l'uso dei servizi. Si può anche scegliere di usare pseudonimi, soprattutto per account legati a minori. Meglio evitare di memorizzare informazioni sensibili, come dati di salute, password o numeri di carte di credito, inoltre, è importante valutare attentamente i rischi legati all'accesso dello smart assistant ai dati del dispositivo, come foto, contatti o calendario.

3) Come detto precedentemente, quando lo smart assistant è acceso ma non utilizzato, rimane in uno stato di "passive listening", pronto ad attivarsi appena rileva la parola scelta. In queste situazioni, l'assistente è potenzialmente in grado di captare suoni o immagini, che possono eventualmente essere memorizzati o inviati a server esterni, pertanto, per proteggere la privacy, è consigliabile disattivare il microfono o la videocamera quando non si utilizza l'assistente, o spegnere direttamente il dispositivo per evitare acquisizioni indesiderate di dati.

4) Se lo smart assistant può eseguire attività particolari come inviare messaggi, pubblicare sui social o fare acquisti online, è consigliabile selezionare quelle che si ritengono essere necessarie e disattivare tutte le altre oppure, se possibile, di proteggerle con una password (decidere quali funzioni mantenere attive). Inoltre, essendo parte dell'Internet of Things, gli assistenti possono interagire con altri dispositivi connessi, come elettrodomestici e sistemi di sicurezza, aumentando la raccolta di dati personali, per cui è importante capire come vengono gestiti tali dati.

5) Per limitare il trattamento dei dati personali raccolti dallo smart assistant, è possibile cancellare periodicamente la cronologia delle informazioni registrate, o eliminare solo i dati più sensibili. Questa operazione può essere effettuata tramite il sito web, l'app di gestione o le impostazioni del dispositivo su cui è installato l'assistente digitale.

6) Per un uso sicuro dello smart assistant, è consigliato impostare password complesse e aggiornate, verificare che la rete Wi-Fi utilizzi il protocollo di sicurezza WPA 2 e mantenere aggiornati i sistemi di protezione anti-virus (fare attenzione alla sicurezza). Inoltre, è importante regolare le impostazioni di privacy del dispositivo o dell'app di gestione sui livelli desiderati.

7) Qualora si decidesse di vendere, regalare o dismettere il dispositivo su cui è installato lo smart assistant, è consigliabile disattivare gli account personali creati, cancellare tutti i dati registrati nel dispositivo o nella app di gestione, e richiedere la cancellazione dei dati conservati nei database dell'azienda produttrice o di terze parti.

Conclusioni

Quest'analisi legata al tema degli smart assistant evidenzia quindi l'importanza crescente della protezione dei dati personali in un'epoca di rapida innovazione tecnologica. La sempre più rapida espansione delle funzionalità di tali dispositivi ha trasformato le modalità di interazione con la tecnologia, integrandosi profondamente nella vita quotidiana e modificando il modo in cui gestiamo e condividiamo le nostre informazioni personali. L'approfondimento sui dati personali e le loro criticità ha messo in luce la complessità della protezione delle informazioni in un contesto digitale. Con l'aumento dell'uso di dispositivi intelligenti, le sfide legate alla privacy e alla sicurezza dei dati si sono amplificate, rendendo essenziale un quadro normativo robusto e adattabile.

Il GDPR ha rappresentato un passo fondamentale nella tutela dei dati personali, stabilendo principi chiave per la loro gestione e protezione. Tuttavia, l'evoluzione della tecnologia richiede un continuo adeguamento delle norme per affrontare nuove

problematiche e garantire che le pratiche di trattamento dei dati rimangano conformi agli standard di sicurezza e trasparenza. L'introduzione del Data Act promette di rafforzare ulteriormente la protezione dei dati, in particolare riguardo al trasferimento e all'uso delle informazioni personali. Questa normativa, insieme al GDPR, può contribuire a creare un ambiente più sicuro e trasparente per l'utilizzo delle tecnologie intelligenti.

In sintesi, l'adozione di smart assistant e la continua evoluzione delle tecnologie connesse sottolineano la necessità di un equilibrio tra innovazione e protezione della privacy. È cruciale adottare pratiche di utilizzo consapevole e garantire che le normative in vigore rispondano adeguatamente alle nuove sfide per garantire la sicurezza e la riservatezza delle informazioni personali.

BIBLIOGRAFIA E SITOGRAFIA

- https://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali
- https://www.oracle.com/it/chatbots/what-is-a-digital-assistant
- https://www.cyberlaws.it/2021/smart-assistant/
- https://blog.osservatori.net/it_it/smart-speaker-e-smart-car
- https://blog.osservatori.net/cos-e-smart-car-come-funziona
- https://www.carra-gaini.it/privacy-e-riservatezza-che-differenza-ce-e-perche-e-importante-che-le-aziende-comprendano/
- https://protezionedatipersonali.it/diritto-alla-protezione-dei-dati-personali
- https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/
- https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf
- https://www.altalex.com/documents/news/2024/01/20/data-act-rivoluzione-trattamento-dati
- https://www.agendadigitale.eu/sicurezza/privacy/data-act-e-gdpr-una-convivenza-difficile-i-nodi-su-diritto-alla-portabilita-e-accesso/