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 +

IL MONDO DELL'INTERNET OF THINGS: GLI ASSISTENTI DIGITALI E LA PROTEZIONE DEI DATI PERSONALI

Federico Cesini

0345638

Anno accademico 2023/2024

Indice

Abstract

Nel contesto mondiale odierno, il continuo progresso delle tecnologie digitali applicate alla quotidianità ha portato ad un enorme sviluppo nel campo dell'Internet of Things (IoT).

Con il termine IoT ci si riferisce ad una rete di dispositivi intelligenti, capaci di raccogliere e scambiare informazioni tra loro.

In questo lavoro ci si sofferma sugli Assistenti Digitali, dispositivi IoT ormai presenti nella vita di miliardi di individui per migliorarne la quotidianità, possono infatti essere utilizzati per soddisfare diversi tipi di richieste o per compiere determinate azioni.

Agli enormi vantaggi che da essi scaturiscono, si accompagnano però notevoli rischi in ambito di sicurezza digitale e di privacy.

Si tratta infatti di strumenti che, grazie al Machine Learning e all'Intelligenza Artificiale, possono raccogliere e diffondere i dati personali dell'utilizzatore e di tutti coloro che entrano nel loro raggio d'azione, indipendentemente dalla piena consapevolezza dei soggetti.

Lo scenario tecnologico attuale lancia al diritto e all'etica un guanto di sfida, in quanto richiede di individuare un giusto compromesso tra le opportunità che la scienza offre e il rispetto dei diritti fondamentali dell'individuo.

A tal fine, intervengono le Autorità di controllo, le quali, attraverso l'introduzione delle linee guida proposte dall'EDPB e delle regolamentazioni introdotte dal GDPR e dall'AI Act, hanno dimostrato negli ultimi anni un ruolo estremamente attivo nella protezione dei diritti dei cittadini dell'Unione Europea. Tali norme mirano infatti a promuovere l'innovazione e lo sviluppo delle nuove tecnologie in modo responsabile e sostenibile.

Anche le norme tecniche possono svolgere un ruolo sempre più importante, come lo standard ISO/IEC 27400:2022, atto a garantire la sicurezza informatica e la privacy dei sistemi IoT.

Fondamentale risulta innanzitutto rendere gli utenti consapevoli dei rischi che corrono, a tal proposito interviene il Garante della Privacy attraverso una scheda informativa contenente una serie di accortezze e suggerimenti da seguire per tutelare la propria privacy.

Il punto chiave delle regolamentazioni sta però nel concetto di accountability, ossia di responsabilizzazione di produttori e fornitori di tali servizi, i quali sono tenuti ad adottare comportamenti proattivi e trasparenti nei confronti degli utenti, al fine di tutelarli.

Questi strumenti andrebbero infatti progettati per rispettare la privacy dell'utente, il quale idealmente non dovrebbe preoccuparsi di comprendere l'incidenza del dispositivo acquistato sulla protezione dei propri dati personali.

1 Introduzione

Nel corso degli ultimi anni, si è assistito ad una costante accelerazione nell'ambito della ricerca e del progresso tecnologico.

Una tecnologia di cui si sente sempre più spesso parlare, grazie al suo continuo sviluppo e alla sua crescente diffusione, è quella dell'Internet of Things (IoT). Si tratta in breve di tutti quei dispositivi che attraverso Internet sono capaci di connettersi tra loro e scambiare informazioni.

Nell'ambito IoT, una tipologia di strumenti che sicuramente merita attenzione sono gli Assistenti Digitali, utilizzati ormai quotidianamente sia in ambito domestico che aziendale. Essi, infatti, sono dotati di una tecnologia che, attraverso un semplice comando scritto o vocale, permette di soddisfare le richieste più varie degli utenti. Tuttavia, per poter funzionare, tali dispositivi raccolgono in continuazione un'enorme quantità di dati. Ciò espone gli utilizzatori ad importanti rischi di sicurezza per quanto riguarda la loro privacy e la protezione dei loro dati personali.

In questo lavoro si vuole innanzitutto fornire una panoramica generale sull'Internet of Things e sulle sue possibili applicazioni.

Successivamente ci si sofferma in particolare sugli Assistenti Digitali, a partire dal loro funzionamento e dalle tecnologie che essi sfruttano, fino ad arrivare alle opportunità che questi offrono ed ai possibili rischi derivanti dal loro utilizzo.

Si vuole poi andare ad esaminare il quadro normativo attuale e le soluzioni che questo offre nell'ambito della privacy. Si fa in particolare riferimento all'European Data Protection Board (EDPB), al General Data Protection Regulation (GDPR) e all'Artificial Intelligence Act (AI Act), nonché alla normativa tecnica ISO/IEC 27400:2022.

Si riportano inoltre i consigli e le best practice messe a disposizione dal Garante per la Protezione dei Dati Personali (GPDP), al fine di promuovere un utilizzo più sicuro e consapevole degli Assistenti Digitali.

Per concludere si affrontano i possibili sviluppi degli Assistenti Digitali, con particolare attenzione all'Intelligenza Artificiale. Viene inoltre fornito un quadro generale degli interventi giuridici in materia e di quello che ci aspetta in futuro.

2 L'Internet of Things

L'Internet of Things, stando alla definizione formulata dall'International Organization for Standardization (ISO) e dall'International Electrotechnical Commission (IEC), è descritto come "un'infrastruttura di entità, persone, sistemi e risorse di informazione interconnesse insieme a servizi che elaborano e reagiscono alle informazioni dal mondo fisico e dal mondo virtuale".

Il termine IoT, che tradotto letteralmente significa Internet delle Cose, si riferisce dunque ad una rete di dispositivi fisici connessi tra loro, anche detti oggetti intelligenti o smart objects. Tali strumenti, sono infatti dotati di sensori, software e altre tecnologie che permettono loro di raccogliere ed elaborare informazioni e dati che verranno poi scambiati e condivisi con altri dispositivi e sistemi intelligenti, in modo autonomo, attraverso Internet.

Lo scopo di queste tecnologie è quello di monitorare, controllare e trasferire informazioni in tempo reale per poi rispondere con azioni adeguate. Aspetto fondamentale dell'IoT è che i dispositivi possono essere controllati a distanza, ossia da remoto. Essi sono inoltre capaci di trasmettere dati che contengono informazioni circa l'interazione tra questi oggetti e chi gli utilizza, ossia i consumatori. Proprio su questo aspetto nascono le critiche relative alla privacy e alla protezione dei dati personali in relazione con l'IoT.

Del concetto di connessione tra dispositivi si parlava già da molto tempo, a partire dalla nascita di Internet, avvenuta più di cinquant'anni fa. Tuttavia, l'espressione IoT venne utilizzata per la prima volta nel 1999 dall'ingegnere inglese Kevin Ashton, ricercatore del MIT (Massachussetts Institute of Technology) e cofondatore dell'Auto-ID Center del MIT. Proprio al MIT è stato individuato lo standard per RFId (Radio Frequency Identification) e per altri sensori in stretta relazione con l'IoT. Il termine Internet of Things inizia tuttavia a prendere piede soltanto nel 2010, anno in cui diviene noto il servizio StreetView di Google.

L'Internet of Things è un paradigma tecnologico potenzialmente illimitato, in cui l'oggetto stesso acquista una sua identità nel mondo digitale, basti pensare al QR code. L'oggetto è definito intelligente per il fatto che interagisce con il mondo circostante reperendo e condividendo informazioni tra rete e mondo reale. Inoltre, il fatto che tutti questi oggetti possano essere collegati in rete permette di creare una mappa intelligente di tutte le cose.

Una videocamera, ad esempio, potrà inviare dati e immagini in modo intelligente, in funzione ad esempio delle immagini riprese, della temperatura o della luminosità. In questo modo sarà in grado di adattare il proprio comportamento in funzione di parametri di interesse che possono evolvere nel corso del tempo.

Dal frigorifero, al forno, al semaforo, fino all'orologio, tutti i dispositivi possono essere considerati IoT, basta che siano connessi ad Internet e capaci di ricevere e trasmettere dati.

Questi dispositivi possono quindi essere oggetti di uso quotidiano, come ad esempio un frigorifero intelligente che ordina automaticamente un alimento appena si accorge che è finito, o i riscaldamenti che si accendono quando rilevano che l'utente sta per arrivare a casa.

In ambito cittadino potremmo avere, ad esempio, dei lampioni con un sensore ottico che permette la regolazione della luce in base alle condizioni di visibilità o dei rilevatori che danno informazioni sulla qualità dell'aria. Fino ad arrivare ai più complessi strumenti utilizzati in ambito industriale o di trasporto, come dei semafori che si sincronizzano per creare un'onda verde per il passaggio di un mezzo di soccorso.

Questi sono soltanto alcuni tra i possibili esempi che dimostrano come, il futuro descritto da Orwell e dai romanzi distopici, non sia tanto lontano dal presente. Ci troviamo infatti in un mondo in cui gli oggetti "prendono vita" e possono collegarsi tra loro e con la vita reale di tutti i giorni.

2.1 I soggetti implicati

L'Internet of Things, nel contesto odierno, ha un ampio impatto su una moltitudine di soggetti ed organizzazioni, a partire dal miglioramento della vita quotidiana delle singole persone, fino ad incidere in maniera sostanziale sulla competitività delle imprese.

Questa tecnologia è infatti in grado di influenzare notevolmente la vita e il lavoro degli esseri umani. Essa permette infatti di sfruttare le macchine per compiere le mansioni più pesanti o noiose, rendendo quindi la vita più sana, produttiva e confortevole. Ad esempio, i dispositivi IoT potrebbero semplificare notevolmente la routine. Premere il pulsante della sveglia, potrebbe attivare automaticamente la macchina del caffè e aprire le serrande delle finestre. La dispensa potrebbe rilevare automaticamente che un prodotto stia per finire e ordinarlo in modo autonomo. Un forno intelligente potrebbe fornire un menù del giorno e potrebbe addirittura preparare il pranzo. Lo smartwatch, invece, potrebbe pianificare le riunioni, mentre la Smart Car imposta automaticamente le coordinate GPS per arrivare a destinazione.

Anche le imprese stanno sfruttando notevolmente le potenzialità che l'IoT può offrire. A partire dai dati IoT si può migliorare la gestione del business, nonché creare nuovi modelli di business e flussi di ricavi tramite il collegamento tra il mondo del business fisico e digitale. Di forte interesse è anche la gestione da remoto di asset e dispositivi smart, attivandone servizi e funzionalità avanzate. Fondamentali sono inoltre temi come sostenibilità, sicurezza e gestione delle risorse. Il tutto porta chiaramente ad un aumento della produttività e dell'efficienza delle operazioni aziendali.

2.2 Il funzionamento

Un dispositivo intelligente cattura dati dall'ambiente circostante o input dall'utente attraverso dei sensori. Sfruttando le connessioni di rete esistenti, questo comunica tali informazioni a un sistema cloud e alla propria applicazione IoT. Un'applicazione IoT è un'applicazione software-as-a-service (SaaS) in grado di integrare i dati ricevuti dai vari dispositivi IoT, in grandi quantità tali dati prendono il nome di Big Data. Grazie all'uso di algoritmi di Machine Learning e dell'Intelligenza Artificiale, le applicazioni IoT elaborano ed analizzano questi dati.

Vengono poi prese delle decisioni intelligenti e consapevoli che saranno ritrasmesse al dispositivo IoT, in modo che questo possa rispondere agli input in modo intelligente ed automatico. L'utilizzatore ha accesso a un'interfaccia utente grafica per gestire il dispositivo IoT, ad esempio un'applicazione mobile o un sito Web.

2.3 Le tecnologie utilizzate

La crescente diffusione ed evoluzione dell'IoT è tuttora possibile grazie allo sviluppo di un insieme specifico di tecnologie che, ad un costo accessibile, consentono la raccolta e la condivisione di dati con un intervento umano minimo, permettendo la connessione tra mondo fisico e mondo digitale.

- I sensori sono dispositivi capaci di rilevare cambiamenti nell'ambiente, quali ad esempio temperatura, umidità, luce, pressione, movimento o suoni. Gli attuatori sono invece dispositivi che possono provocare cambiamenti fisici nell'ambiente. Con la crescita della domanda, il mercato dei sensori è passato da pochi e costosi fornitori a una produzione industriale a prezzi competitivi.
- La connettività Internet, per trasmettere i dati IoT da sensori e attuatori fino al cloud, è ad oggi sufficientemente veloce e stabile da consentire l'invio e la ricezione di enormi volumi di dati e sostenere la crescita esponenziale dell'IoT.
  Tradizionalmente la connettività è associata soprattutto alla fibra e alle reti Wi-Fi. Tuttavia, oggi merita attenzione il 5G che, grazie alle sue caratteristiche, consente l'interconnessione di un numero di dispositivi molto elevato, oltre alla possibilità di gestire ampi set di dati in modo rapido, affidabile e senza vincoli di spazio, cosa che prima non era possibile.
- L'Edge computing è una tecnologia utilizzata per aumentare la potenza di calcolo di una rete IoT, riducendo la latenza di comunicazione e migliorando il tempo di risposta. Questo perché consente di elaborare e analizzare i dati più vicino alla fonte, anziché in un data center centralizzato.
- Il Cloud computing è quella tecnologia che permette di archiviare, elaborare ed analizzare volumi elevati di dati, generati dai dispositivi IoT, con una potenza elevata, su sistemi di elaborazione gestiti in cloud. Sul cloud i dati possono essere reperiti senza la necessità di trovarsi su un dispositivo fisico, sono quindi accessibili da più dispositivi nella rete, in qualsiasi parte del mondo si trovino.
- I Big Data consistono in enormi quantità di dati raccolti e messi a disposizione da varie fonti, tra cui i dispositivi IoT. Negli ultimi decenni i dati generati nel mondo sono cresciuti in modo esponenziale. Per poter raccogliere ed elaborare grandi quantità di dati, le aziende devono quindi utilizzare strumenti di analisi avanzati e con un'adeguata potenza di calcolo. Le imprese di qualsiasi settore possono oggi raccogliere tantissime informazioni sul funzionamento dei dispositivi e sulle persone che li utilizzano. I Big Data diventano quindi una vera e propria merce di valore e non sfruttarli per le aziende vorrebbe dire sprecare un'occasione di guadagno economico e ulteriore sviluppo tecnologico. Questo tema in particolare solleva dubbi sulla sicurezza derivante dall'IoT, e su temi quali privacy e trattamento dei dati personali sensibili.
- L'AI e il Machine Learning sono tecnologie in grado non solo di gestire ed elaborare grandi quantità di dati IoT, ma anche di analizzarli e apprendere il più possibile da essi. I Big Data stessi alimenteranno queste tecnologie, e quanto più vasti e diversificati saranno i dati, tanto più robusti, accurati e sofisticati saranno gli output e gli insight che l'analisi avanzata supportata dall'AI potrà fornire. I progressi nelle reti neurali hanno portato il Natural Language Processing (NLP) ai dispositivi IoT, come ad esempio negli Assistenti Digitali, rendendoli molto interessanti per l'uso domestico.

- Anche l'integrazione tra il mondo IoT e quello Blockchain ha grandi potenzialità, quest'ultima potrebbe essere usata per migliorare la sicurezza e la privacy nell'IoT. La blockchain potrebbe essere utilizzata per creare reti sicure e decentralizzate per i dispositivi IoT, riducendo al minimo le vulnerabilità dei dati. Essa, infatti può fungere da garante dell'identità dei diversi nodi della rete e da ente certificante della provenienza e dell'integrità dei dati raccolti di dispositivi IoT. Tuttavia, c'è da dire che tra queste due tecnologie ci sono ancora tante difficoltà di integrazione non trascurabili.

2.4 I campi di applicazione

Le potenziali applicazioni dell'IoT sono varie e il suo impatto si fa sentire in un'ampia gamma di settori.

- Le Smart Homes, o case intelligenti, sono tecnologie IoT ormai molto diffuse e conosciute, esse vengono utilizzate per gestire in automatico o da remoto gli oggetti connessi dell'abitazione. I dispositivi intelligenti per la casa possono essere utilizzati per monitorare e azionare l'illuminazione, la climatizzazione, i sistemi di sicurezza o gli elettrodomestici, o ad esempio per spegnere automaticamente i dispositivi quando non sono utilizzati, per trovare oggetti smarriti o per automatizzare attività quotidiane. Lo scopo principale è quello di migliorare l'efficienza, il comfort e la sicurezza dell'abitazione, e allo stesso tempo ridurne i consumi energetici. Le Smart Homes trovano un ampio campo di applicazione nella domotica, vale a dire un ecosistema in cui tutti i dispositivi IoT comunicano e si coordinano tra loro e con il proprietario della casa per ottenere una gestione energetica il più efficiente possibile.
- Gli Smart Building, o edifici intelligenti, estendono il concetto applicato dalle Smarth Homes, che si rivolgono principalmente ai consumatori e alle loro abitazioni, alla realizzazione ed ottimizzazione di palazzi ed uffici intelligenti.
- La Smart City, o città intelligente, secondo lo Smart City Index (SCI) è "un ambiente urbano che applica la tecnologia per esaltare i vantaggi e attenuare gli inconvenienti dell'urbanizzazione". Si tratta quindi di applicazioni IoT che hanno reso più efficienti la gestione e la manutenzione urbana per affrontare i problemi in modo proattivo, il tutto per migliorare la qualità di vita in città, e cercare di soddisfare le esigenze e i bisogni dei cittadini. Questo tipo di tecnologia intelligente può essere utilizzata per misurare la qualità dell'aria e i livelli di radiazioni, gestire e smaltire in modo efficiente i rifiuti, ridurre i costi energetici con sistemi di illuminazione intelligenti, gestire in modo efficiente i parcheggi o individuare le necessità di manutenzione per infrastrutture quali strade, ponti e condotti. Possono essere utilizzati anche per alleviare la congestione del traffico e ottimizzare i percorsi, ad esempio gestendo i mezzi pubblici, in questi casi parliamo di Smart Mobility. Un esempio sono i semafori intelligenti che diventano verdi quando vedono che c'è una macchina al semaforo e non passano macchine dal senso opposto, oppure gli autobus connessi tra loro e con i display delle fermate, in modo tale da mantenere aggiornati gli utenti sui tempi di attesa.
- Ad oggi, la maggior parte delle auto prodotte sono collegabili ad Internet. Le Smart Cars, o automobili intelligenti, sono automobili con un sistema IoT capaci di dialogare costantemente con l'ambiente circostante, possono guidare da sole o assistere il guidatore

aumentando comodità e sicurezza. Tali sistemi raccolgono dati a partire dall'acceleratore, dai freni, dal tachimetro, dal contachilometri, dalle ruote e dai serbatoi del carburante. Le Smart Cars possono avere vari utilizzi, ad esempio, gestire il traffico, aumentare l'efficienza del carburante, ridurre i costi, migliorare la sostenibilità, chiamare i soccorsi ed avvisare amici e familiari automaticamente in caso di incidente, prevenire gli incidenti, effettuare manutenzione predittiva sui veicoli o utilizzare funzionalità da remoto, ad esempio preriscaldare l'auto o farla arrivare automaticamente dove ci si trova.

- La Smart Agricolture, anche detta Agricolture 4.0, è uno dei settori con la più elevata opportunità di sviluppo in ambito digitale. La sensoristica ambientale può essere utilizzata per controllare le condizioni ambientali, la crescita delle colture, la salute del bestiame, le condizioni e l'umidità del terreno, garantendo che le colture siano irrigate al momento giusto, oltre alla gestione di acqua, fertilizzanti e concimi. Il tutto al fine di migliorare la qualità dei prodotti e di ridurre le risorse utilizzate e l'impatto ambientale. Inoltre, i dispositivi a basso consumo o ad energia solare possono essere controllati anche da remoto.
- L'Industrial IoT (IIoT) è un'evoluzione della tecnologia Internet of Things applicata al settore industriale, essa si riferisce ai dispositivi intelligenti utilizzati nei settori della produzione, della vendita al dettaglio, della sanità e di imprese di altro tipo per migliorare l'efficienza delle attività. IIoT viene spesso usato come sinonimo di Industry 4.0, ossia la quarta ondata della rivoluzione industriale. I dispositivi IoT industriali forniscono informazioni e dati dettagliati e in tempo reale per monitorare le prestazioni delle macchine, rilevare i guasti, gestire l'inventario, controllare la qualità dei prodotti, gestire le catene di fornitura e di distribuzione e ottimizzare i processi di produzione. Il settore dell'IIoT è quello con la crescita più rapida e anche quello che produce ogni anno la maggior quantità di dati, gran parte dei quali proviene da circa un miliardo di videocamere di sorveglianza installate in tutto il mondo. Dai dati della ricerca dell'Osservatorio Smart Manufacturing della School of Management del Politecnico di Milano è emerso che il mercato dell'Industry 4.0 in Italia stia crescendo a un ritmo del 20% annuo e rappresenti una spinta concreta per il Made in Italy.
- La Smart Health consiste nell'utilizzo di tutti quei dispositivi medici connessi alla rete che permettono ai dottori di monitorare i pazienti da remoto e raccogliere dati in tempo reale sui loro segni vitali. Inoltre, con strumenti chirurgici smart, i medici possono collegarsi da remoto con i migliori chirurghi al mondo ed effettuare interventi chirurgici guidati.
- L'IoT è sempre più impiegato anche nel settore del retail, ossia della vendita al dettaglio, ad esempio attraverso le casse automatiche, gli sconti personalizzati e gli scaffali intelligenti, i quali avvertono il negoziante quando sta per terminare un articolo e consentono di ottimizzare il posizionamento dei prodotti. Tali dispositivi possono essere utilizzati per monitorare il comportamento dei clienti, gestire i livelli di inventario e ottimizzare i layout dei negozi.

2.5 Sostenibilità

La Smart Energy rappresenta l'integrazione e il coordinamento efficace dei principi dell'Internet of Things nel settore energetico, adeguandosi pienamente al concetto di Sostenibilità Ambientale. Questo consente un vero e proprio miglioramento dell'efficienza energetica di case, edifici e impianti. La Smart Energy dimostra di essere un terreno fertile per le innovazioni, infatti, oltre a promuovere un futuro più intelligente ed efficiente, si propone di migliore il comfort degli utenti e ridurre i costi per i consumi energetici. Oltre agli ambiti già discussi questo concetto abbraccia il monitoraggio dei consumi, attraverso lo Smart Metering, e l'ottimizzazione della distribuzione elettrica, tramite lo Smart Grid.

Lo Smart Metering è l'ambito applicativo dell'IoT che si occupa degli Smart Meter, o contatori connessi, ossia dei dispositivi IoT che consentono la telelettura e la telegestione dei consumi di energia elettrica, gas e acqua. Gli Smart Meter sono dispositivi sempre più diffusi, soprattutto a causa di obblighi normativi in ambito energetico, ma anche grazie ai vantaggi che essi offrono. Questi dispositivi intelligenti, infatti, forniscono informazioni dettagliate sui consumi, utili non sono agli utenti che possono ottimizzare i costi, ma anche ai distributori di energia che possono intervenire in caso di necessità. Questa tecnologia porta ad un aumento complessivo dell'efficienza energetica.

Le Smart Grids, o reti intelligenti, nascono come evoluzione del sistema elettrico tradizionale e possono essere considerate la spina dorsale della transizione energetica e digitale, in particolare dell'Europa, per il raggiungimento di precisi obiettivi di sviluppo sostenibile. Esse consistono in un insieme di reti elettriche e di tecnologie che, grazie allo scambio di informazioni, permettono di gestire e monitorare la distribuzione di energia elettrica tra produttori e consumatori, soddisfacendo le diverse richieste degli utenti collegati in modo efficiente, razionale e sicuro.

2.6 L'IoT in Italia e nel mondo

In Italia, come nel resto del mondo, l'IoT sta vivendo una crescita costante. Da una ricerca condotta dall'Osservatorio Internet of Things del Politecnico di Milano è stimata una crescita del mercato del 13% annuo, portando l'Italia a raggiungere gli 8,3 miliardi di euro nel 2022, per un totale di oltre 124 milioni di connessioni IoT attive, vale a dire 2,1 per abitante. Tale crescita è evidente in settori chiave come Agricolture 4.0, Industry 4.0, Smart Building, Smart Homes e Smart Cars. Questo anche grazie al PNRR che continua a offrire opportunità per il mercato IoT, questo prevede infatti un investimento complessivo di 29,78 miliardi di euro dedicati direttamente o indirettamente a questo settore. Tra tutti spiccano gli investimenti nella Smart Energy, in particolare in Smart Grid, Smart Cars, Smart Building e Smart City. Appare dunque evidente come l'Internet of Things sia un punto focale per la digitalizzazione della società, questo lo pone al centro dell'interesse della politica economica dell'Italia e dell'Unione Europea.

2.7 Il futuro dell'IoT

L'IoT negli anni sta passando da un approccio in cui ogni dispositivo ha una funzione, ad esempio uno per gestire la temperatura, un altro per controllare l'umidità e un altro ancora invece si occupa della sicurezza, ad un approccio integrato in cui i diversi apparecchi collaborano tra loro per fornire una risposta ottimale. Il nuovo IoT si sta indirizzando verso un approccio System Integrator, in cui si passa da singoli dispositivi con uno scopo ben definito e con una funzionalità specifica ad un sistema che permette di orchestrare obiettivi diversi, con dati che hanno una provenienza diversa, in maniera coordinata. Il tutto cercando di integrare aspetti quali sicurezza, risparmio energetico, comfort, costi e sostenibilità. Come si è visto infatti, il tema della sostenibilità sta diventando sempre più importante per l'IoT, poiché le aziende cercano in tutti i modi di ridurre l'impatto ambientale.

Un altro sviluppo che ci si può aspettare in futuro è un'integrazione sempre maggiore tra tecnologia ed esperienza umana. Tecnologie come la realtà virtuale avanzata, le sensazioni aptiche e la personalizzazione in tempo reale supportata dall'AI lasciano intendere che la nostra interazione con i dispositivi IoT renderà possibili esperienze sensoriali sempre più reali.

Nel corso degli ultimi anni il numero di dispositivi connessi a Internet continua a crescere, grazie anche ai costi di produzione in continua riduzione. Secondo le previsioni di IDC, entro il 2025 i dati generati a livello globale supereranno i 73mila miliardi di gigabyte. E nonostante non sia possibile quantificare i dati digitali in termini fisici, per rendere l'idea si può dire che se tutti questi dati fossero copiati in floppy disk degli anni '90 e fossero posti uno accanto all'altro, questi coprirebbero il percorso di andata e ritorno tra la Terra e la Luna per 5000 volte. In conclusione, si può dire che l'IoT svolgerà nei prossimi anni un ruolo sempre più importante nel plasmare e trasformare il modo e il mondo in cui viviamo.

3 Gli Assistenti Digitali

Lo sviluppo delle tecnologie digitali applicate alla quotidianità, ed in particolare dei dispositivi IoT, ha portato negli ultimi anni ad una crescita sempre maggiore del mercato degli Assistenti Digitali, o Smart Assistant. Secondo le stime questi dovrebbero essere così diffusi da aver superato il numero della popolazione mondiale, ciò sta a significare che mediamente ce ne è più di uno a persona.

L'Assistente Digitale è un software avanzato che, grazie al Machine Learning, ovvero processi di auto-apprendimento che utilizzano algoritmi di Intelligenza Artificiale (AI), è in grado di riconoscere e interpretare il linguaggio naturale, scritto o orale che sia, degli esseri umani e di interagire con loro. Questa interazione consente agli utenti di soddisfare diversi tipi di richieste, come ad esempio, rispondere a richieste di informazioni, fare ricerche su Internet, fornire previsioni meteo e di traffico, riprodurre un brano musicale, leggere un messaggio ricevuto su WhatsApp o impostare sveglie, timer e promemoria. Tali programmi possono anche essere utilizzati per compiere determinate azioni, quali fare acquisti online o, nel caso di una Smart Home, regolare la temperatura di casa, accendere e spegnere la luce, attivare gli elettrodomestici o aprire e chiudere le serrature, svolgendo un ruolo di coordinamento tra i dispositivi IoT.

Gli Smart Assistant attualmente più noti e diffusi sul mercato sono Alexa (Amazon), Google Assistant (Google), Siri (Apple), Bixby (Samsung), XiaoAI (Xiaomi) e Cortana (Microsoft).
Questo tipo di tecnologia, essendo ormai molto diffusa, viene installata su vari tipi di dispositivi, primi fra tutti gli smartphone, ma anche nelle auto o nelle case, sotto forma di altoparlanti intelligenti, ossia gli Smart Speaker.

La grande diffusione degli Smart Assistant si deve probabilmente al loro facile utilizzo, al loro costo contenuto, ma soprattutto alla loro capacità di rispondere in modo semplice ed immediato alle richieste degli utenti. Agli enormi vantaggi che da essi scaturiscono, si accompagna però la loro estrema pervasività nella vita delle persone, essendo appunto strumenti trasversali, utilizzati in diverse attività quotidiane. Infatti, queste tecnologie si basano sulla raccolta dei dati personali dell'utente e sulle informazioni captate dall'ambiente circostante. Questo può rappresentare un enorme problema in ambito di privacy e sicurezza digitale che non sempre viene immediatamente percepito dagli utilizzatori. Possiamo quindi affermare che se da un lato è innegabile che tali dispositivi migliorino la qualità della vita, rendendo una serie di operazioni più semplici e veloci, dall'altro espongono gli utenti e, in particolare la loro privacy, ad una serie di rischi. Al momento è difficile stabilire se questa tecnologia comporti più rischi o vantaggi, tuttavia il forte senso di comodità che essa trasmette ha portato ad un crescente entusiasmo nei suoi confronti e di conseguenza ad una sua rapida diffusione. Da qui nasce un tema di particolare rilevanza in ambito sia digitale che giuridico, vale a dire l'esigenza di conciliare l'uso degli Assistenti Digitali in modo sicuro, protetto e consapevole, con il rispetto della privacy e della protezione dei dati personali degli utenti.

3.1 Il funzionamento

Per comprendere meglio il funzionamento di questa tecnologia, può essere particolarmente utile conoscerne i passaggi funzionali.

1. L'Assistente Digitale, se non attivo, si trova in standby, seppur in ascolto costante, e fino a quando non viene rilevata un'espressione o un comando specifico che lo svegli, il dispositivo non emetterà alcun segnale vocale e non eseguirà nessun'altra operazione.
2. Appena l'utente immette l'espressione di risveglio, l'assistente aprirà un canale di ascolto e la richiesta verrà immediatamente trasmessa al provider.
3. Gli Assistenti Digitali possono utilizzare tecnologie NLP (Natural Language Processing), ossia di elaborazione del linguaggio naturale, per interpretare il comando e fornire la risposta appropriata alla richiesta dell'utente. Nel caso in cui lo Smart Assistant non sia in grado di interpretare correttamente la richiesta, allora fornirà risposte standard come "non so come aiutarti"; invece, nel caso in cui vi riesca, sarà creata una frase di risposta o verrà eseguita un'azione specifica.
4. Infine, pronunciando l'espressione di spegnimento, l'assistente torna in standby.

3.2 Interoperabilità tra dispositivi

Nell'ambito dell'Internet of Things, e in particolare degli Smart Assistant, diventa cruciale il concetto non solo di interconnessione, ma anche di interoperabilità fra i sistemi informatici. Ad oggi, la tendenza in atto è infatti quella di sviluppare multipiattaforme che puntano al controllo di oggetti smart di fornitori e marche diverse da un unico punto di contatto.

Di particolare rilevanza appare l'accordo siglato recentemente da alcuni tra i più grandi colossi in ambito digitale, quali Amazon, Apple, Google e altre aziende della Zigbee Alliance, tra cui Ikea e Samsung SmartThings. Tale accordo riguarderebbe proprio il mondo della domotica, per la creazione di un protocollo unitario per la Smart Home, grazie al quale tutti i dispositivi potranno essere controllati con uno qualsiasi tra Alexa, Siri o Google Assistant.

Il frutto di questa alleanza è il progetto CHIP (Project Connected Home over IP), noto come Matter, il cui obiettivo è quello di semplificare lo sviluppo per i produttori che potranno realizzare prodotti compatibili con i tre noti assistenti vocali, ma anche quello di creare un ecosistema in cui i consumatori non si dovranno più preoccupare della compatibilità tra dispositivi IoT. Il fatto che solitamente queste aziende non siano propense ad alleanze tra loro è solo un'ulteriore conferma del grande interesse che il mercato della domotica ad oggi stia suscitando, specialmente se messo in relazione con il mercato dei dati personali.

3.3 I chatbot

Gli Assistenti Digitali acquisisco un'importanza crescente non solo per i singoli utenti, ma anche per le aziende, che li utilizzano per migliorare il servizio di assistenza clienti, arrivando anche a sostituire gli operatori con questi strumenti. Qui entrano in gioco i chatbot, vale a dire una particolare declinazione degli Smart Assistant che simulano conversazioni umane, sia scritte

che parlate, forniscono supporto agli utenti attraverso risposte rapide e precise alle loro domande tramite semplici app di messaggistica.

I chatbot, inoltre, consentono alle aziende di avere un unico e comodo punto di contatto per gestire le comunicazioni in entrata con i clienti. Con un chatbot si può anche risparmiare tempo e denaro, infatti le attività ridondanti possono essere facilmente automatizzate e rese contemporaneamente disponibili a milioni di consumatori, liberando così i dipendenti, in modo che questi possano svolgere attività più critiche.

Inoltre, utilizzando algoritmi di machine learning, gli Assistenti Digitali, possono raccogliere insight in tempo reale, che le aziende utilizzano per migliorare continuamente la users experience, conoscendo le preferenze e le abitudini di clienti e dipendenti. Tuttavia, si osserva che anche in questo caso si tratta spesso di dati personali e ciò potrebbe mettere a rischio la privacy degli utenti.

3.4 I processi

Di particolare rilevanza risulta l'utilizzo degli Smart Assistant nei processi giudiziari, questo grazie alla loro peculiarità di registrare tutto ciò che avviene nell'ambiente circostante. Negli Stati Uniti, ad esempio, dal 2015 Alexa è stata più volte interrogata come possibile testimone di omicidio.

Per quanto riguarda l'Italia si può dire che, a linee generali, nel nostro Ordinamento la registrazione di una conversazione da parte di un soggetto presuppone di norma il consenso anche degli altri interlocutori. Tuttavia, è possibile prescindere dal consenso nel caso in cui la raccolta dei dati sia utilizzata per far valere o difendere un diritto in sede giudiziale o stragiudiziale. Inoltre, fatto salvo il divieto di divulgazione, la registrazione di una conversazione effettuata da uno degli interlocutori all'insaputa dell'altro non è classificabile come intercettazione.

4 I rischi per la privacy

Gli Smart Assistant sembrano essere dispositivi estremamente utili e versatili, tuttavia non bisogna sottovalutare i rischi relativi alla privacy e alla sicurezza a cui espongono gli utenti.

4.1 Big Data

Lo sviluppo dei software di assistenza digitale è strettamente collegato ai progressi ottenuti nel campo dell'intelligenza artificiale. Infatti, come si è visto, rivolgersi agli Smart Assistant, significa fornire loro input che le macchine intelligenti sfrutteranno per imparare da sé stesse con il machine learning, o addirittura per elaborare nuovi percorsi di apprendimento attraverso l'uso di reti neurali, cercando di trarre ispirazione dalla struttura della mente umana, con il deep learning. In questo modo tali dispositivi potranno diventare sempre più precisi in fase di ascolto, di comprensione della domanda e di elaborazione della risposta, riducendo progressivamente il margine di errore.

Questo permette agli Smart Assistant di comprendere l'utente a partire dalle sue azioni passate, per fare previsioni sul suo comportamento futuro. In questo modo, l'Assistente Digitale si potrà adattare all'utilizzatore, creando contenuti personalizzati appositamente per lui in base ai suoi gusti e preferenze.

Questa sempre maggiore precisione degli Smart Assistant, si spiega alla luce del fatto che questi raccolgono e memorizzano una grande mole di dati personali nei Big Data, i quali non sono relativi solo all'utilizzatore diretto, ma a chiunque si trovi nell'ambiente circostante. Tali dati possono riguardare, ad esempio, preferenze, scelte di acquisto, abitudini di vita ed interessi, ma anche informazioni biometriche, come la voce e le caratteristiche del volto. Attraverso la geolocalizzazione si può inoltre risalire alla posizione, al domicilio e ai percorsi abituali. Infine, si hanno tutta una serie di caratteristiche personali, quali sesso, età, religione, abitudini sessuali e perfino le emozioni.

La mole di tali dati raccolti cresce ancora di più considerando il fatto che gli Assistenti Digitali sono dispositivi IoT. Gli Smart Assistant, infatti, come tutti i dispositivi IoT, non si limitano a essere in connessione con la rete, ma sono anche capaci di dialogare con altri dispositivi intelligenti, come smartwatch, Smart TV o sistemi di videosorveglianza. Ad esempio, gli Assistenti Digitali con funzioni domotiche possono essere collegati con oggetti e servizi presenti nelle Smart Homes, come gli elettrodomestici, le Smart TV, le luci o i sistemi di sicurezza e videosorveglianza. Si tratta di funzioni che semplificano notevolmente la vita quotidiana, complice anche il controllo a distanza col solo uso della voce o addirittura da remoto, senza neanche il bisogno di essere a casa.

Tuttavia, tale capacità agevola anche la possibilità di raccolta, di incrocio e di diffusione dei dati personali. I vari aspetti discussi pongono in primo piano l'esigenza di tutelare la privacy delle persone che vengono a contatto con tali dispositivi.

4.2 Passive listening

Lo Smart Assistant, quando è acceso ma non viene utilizzato, si trova in uno stato di ascolto passivo, detto passive listening, ossia una sorta di dormiveglia da cui esce non appena sente la parola di attivazione, o wake-up word. In questa fase, l'Assistente Digitale resta potenzialmente sempre in grado di sentire e vedere tutto quello che viene detto e fatto nell'ambiente circostante, tramite il microfono e la videocamera su cui esso è installato. Ciò significa che, anche quando lo Smart Assistant non è in utilizzo, questo trasmetterà ogni accadimento che percepisce a tutti gli altri dispositivi IoT a cui esso è collegato.

Bisogna notare che l'apparecchio registra non solo le conversazioni e le azioni del proprietario, ma anche quelle di altri soggetti che si trovano nello stesso ambiente, i quali potrebbero addirittura essere inconsapevoli dell'esistenza di tali dispositivi. Questi dati possono inoltre essere memorizzati e inviati a terzi, o comunque possono essere conservati su server esterni al dispositivo o sul cloud.

La funzionalità del passive listening è necessaria, in quanto tali dispositivi quando sono accesi, seppur non utilizzati, devono poter rilevare costantemente ciò che le persone nell'ambiente circostante dicono, altrimenti non potrebbero attivarsi quando la frequenza captata risulterà simile alla parola di attivazione dello stesso.

4.3 Attivazioni indesiderate

Gli Assistenti Digitali di norma dovrebbero attivarsi solo quando viene dato loro un esplicito comando vocale o testuale. Tuttavia, alcuni studi pratici hanno dimostrato che molti assistenti non si risvegliano soltanto attraverso parole chiave ben definite, bensì rispondono anche ad una serie di ulteriori stimoli vocali foneticamente simili. Da qui il rischio, non poco frequente, di attivare involontariamente lo Smart Assistant durante normali conversazioni.

A tal proposito si riporta un recente studio condotto dalla Northeastern Univesity di Boston e dall'Imperial College di Londra, dal quale emerge come l'attivazione involontaria degli Assistenti Digitali non sia affatto un evento sporadico. In particolare, la parola chiave predefinita di Amazon Echo, ossia Alexa, sembrerebbe essere spesso innescata erroneamente da molte altre parole. Ad esempio, si attiverebbe con una generica frase che inizia con "I like" più una qualsiasi parola che inizia con la s, come ad esempio "I like Shrek". Solitamente il dispositivo riconosce le false attivazioni, tuttavia questo avviene solo dopo aver inviato al server l'intera frase, e quindi dopo che questa sia stata memorizzata in modo più o meno permanente.

Sempre in questo studio, i dispositivi smart sarebbero stati sottoposti a svariate ore di ascolto di episodi di serie TV, dimostrando come questi si attivassero quando non avrebbero dovuto fino a 19 volte al giorno, semplicemente ascoltando la televisione e non la voce del loro proprietario.

Inoltre, è emerso come molti dati personali degli utenti raccolti dagli Assistenti Digitali sarebbero trasmessi a terze parti, come ad esempio Spotify e Microsoft, senza alcuna autorizzazione, nonostante l'utente non abbia sottoscritto alcun abbonamento con essi.

Di tutta risposta sulla questione privacy, Amazon non si sbilancia, ma si limita a dire che le informazioni personali ottenute sono semplicemente trasmesse al cloud per permettere ad Alexa di imparare e diventare sempre più intelligente, il tutto al fine di rispondere in maniera sempre più accurata alle esigenze degli utenti.

Da un'altra indagine in ambito IoT, condotta dalla Global Privacy Enforcement Network (GPEN) nel 2016, è emerso che molte aziende non ponessero ancora abbastanza attenzione sui dati personali, come commentato da Antonello Soro, all'epoca Presidente del Garante per la protezione dei dati personali. Ad esempio, non rendendosi conto che non soltanto il nome e il cognome, ma anche i dati biometrici, sono dati personali da proteggere. Allo stesso modo non era ancora sufficientemente garantita la possibilità per i consumatori di cancellare i dati raccolti da questi dispositivi. La stessa indagine avrebbe rivelato che oltre il 60% dei dispositivi IoT non avesse superato il test di affidabilità dei Garanti della privacy di ben 26 diversi Paesi.

Grazie alla crescente diffusione di questi dispositivi, si prospetta un rischio sempre maggiore che una notevole quantità di informazioni personali vengano raccolte e diffuse senza la piena consapevolezza dei loro proprietari. In tale contesto, risulta determinante un maggior interessamento da parte delle Autorità di controllo al fine di limitare i potenziali rischi collegati alla privacy che queste tecnologie portano con loro.

5 Il quadro normativo

Al giorno d'oggi, gli Smart Assistant sono strumenti ormai presenti nella quotidianità di milioni, se non miliardi, di individui che, per via delle loro funzionalità, li utilizzano per i motivi più disparati. Spesso però, ci si dimentica dei rischi che l'utilizzo di questi strumenti comporta, si tratta infatti di dispositivi che registrano ogni parola che ascoltano e ogni azione che vedono. Appare inoltre a questo punto evidente che gli Assistenti Digitali abbiano una spiccata capacità di raccogliere e diffondere grandi volumi di dati personali, a partire dal proprio utilizzatore, fino ad arrivare a tutti quei soggetti che, consapevoli o no, entrano nel loro raggio d'azione.

5.1 L'EDPB e il GDPR

Per tali ragioni, negli ultimi anni, le Autorità nazionali e sovranazionali, preposte alla tutela della privacy, hanno posto un'attenzione sempre maggiore su queste tecnologie, che è aumentata di pari passo con la loro diffusione. A tal proposito, il 9 marzo 2021 il Comitato Europeo per la Protezione dei Dati Personali, ossia l'European Data Protection Board (EDPB), è intervenuto sul tema, pubblicando le Linee Guida 02/2021 sugli assistenti vocali virtuali.

Il Comitato ha ritenuto che il framework normativo di riferimento dell'intervento sia costituito dal Regolamento (UE) 2016/679, noto come GDPR (General Data Protection Regulation), o Regolamento Europeo per la Protezione dei Dati Personali, e dalla Direttiva 2002/58/CE, ossia la Direttiva e-Privacy.

Prima di proseguire è opportuno soffermarsi un momento sull'appena citato GDPR. Si tratta di un Regolamento adottato a partire dal 27 aprile 2016, e divenuto operativo nei singoli Stati soltanto il 25 maggio 2018, abrogando la precedente Direttiva 46/95 CE sul trattamento dei dati personali, divenendo così la nuova legge di riferimento in materia. Il GDPR pone come suo fondamento la "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati".

Esso nasce con l'obiettivo di disciplinare il modo in cui le aziende trattano i dati personali degli utenti, in modo tale da dare ad ogni individuo il controllo sull'utilizzo dei propri dati, a tal fine vengono stabiliti precisi requisiti per il trattamento degli stessi.

Altro motivo che ha spinto nella direzione di una regolamentazione UE unica è stata la proliferazione di legislazioni nazionali in materia di privacy molto differenti tra loro. Con i suoi 173 Considerando e 99 Articoli, il Regolamento si applica non solo all'Unione Europea, ma anche a tutte quelle aziende situate al di fuori di essa che però offrono servizi o prodotti all'interno del mercato UE. Questo significa che la maggior parte delle organizzazioni dovranno rispettare tali regole, in caso contrario sono previste pesanti sanzioni.

Il motivo principale dell'intervento del Comitato Europeo per la Protezione dei Dati Personali è stato proprio quello di risolvere alcune criticità legate all'applicazione del GDPR in questo nuovo contesto tecnologico. Il tutto per fare in modo che gli operatori del settore e i responsabili del trattamento dei dati si impegnino a rispettare le normative vigenti, a tutela degli utilizzatori. L'EDPB fornisce inoltre agli stessi utenti una guida sui loro diritti e su tutto quello che dovrebbero sapere per proteggere i loro dati personali.

La complessa natura di questi dispositivi, infatti, porta ad una netta asimmetria informativa tra il fornitore e l'utente, il quale molto spesso non possiede le competenze necessarie per comprendere il funzionamento di tecnologie che utilizzano algoritmi di AI. A maggior ragione, considerando il fatto che tra i fruitori del servizio possono figurare soggetti vulnerabili, come bambini o anziani, ma anche utenti accidentali. È infatti richiesto ai fornitori di rispettare determinati requisiti, riconducibili al concetto di trasparenza per il trattamento dei dati.

Sarebbe inoltre opportuno definire i principi di ingegneria necessari affinché i sistemi IoT siano progettati con funzioni di sicurezza informatica e di controllo sulla privacy annesse. Secondo l'EDBP, alcune misure atte a garantire una maggior trasparenza, sono ad esempio la presenza di un comando vocale specifico o l'installazione di una spia che indichi se il dispositivo è acceso o spento. Intervenire a livello progettuale consentirebbe infatti di immettere sul mercato un prodotto o un servizio già testato, che non sia solo efficiente e sicuro, ma anche conforme alla normativa. Da ciò deriverebbe anche un significativo incoraggiamento verso i produttori ad adottare un atteggiamento di tipo proattivo, nell'ottica di prevenire potenziali danni agli utenti. Sono varie le problematiche e gli argomenti su cui il Comitato si sofferma, tra queste si cercherà di esplorare le più rilevanti.

5.2 Il consenso nel trattamento dei dati

Le linee guida dell'EDPB ribadiscono che alla base giuridica del trattamento dei dati personali, da parte degli Smart Assistant, debba esserci il consenso preventivo dell'utente, come espresso dall'art. 6 del GDPR. Il consenso è definito come "l'indicazione inequivocabile dei desideri dell'interessato". Ai sensi dell'articolo 5, paragrafo 3, della Direttiva e-Privacy, ciò significa che, quando il titolare del trattamento chiede il consenso per ottenere l'accesso e per memorizzare i dati dell'utilizzatore, questi dovrà anche informarlo sulle finalità del trattamento, vale a dire su come i suoi dati personali saranno utilizzati successivamente. Pertanto, il consenso costituisce la base giuridica sia per l'archiviazione e l'accesso dei dati ottenuti che per il loro utilizzo futuro.

Secondo il Board, gli utenti hanno il diritto di ricevere, da parte del provider del servizio, un'informativa sul trattamento dei loro dati personali, in forma semplice, chiara ed esaustiva, nel rispetto dell'art. 13 del GDPR e dei principi contenuti nel Considerando 58. Tali informazioni dovrebbero teoricamente essere rilasciate anche a chi non è registrato al servizio e agli utenti accidentali, condizione chiaramente molto difficile da rispettare nella pratica.

Tuttavia, come è stato anticipato, gli Assistenti Digitali potrebbero rilevare la parola chiave del risveglio anche per errore e quindi attivarsi involontariamente, quando invece non vi era intenzione di farlo. In tal caso, l'acquisizione dei dati avverrebbe in assenza di un valido consenso. Secondo le linee guida, gli Assistenti Digitali dovrebbero essere in grado di rilevare l'errore e procedere alla conseguente distruzione delle informazioni accidentalmente raccolte. Nel caso in cui ciò non avvenga, tali dati dovranno essere cancellati non appena il fornitore verrà a conoscenza dell'errore.

Amazon, per far fronte a questo problema, avendo riconosciuto la possibilità di attivazioni involontarie di Alexa, ha impostato un sistema di doppio controllo sulle parole di attivazione, al fine di minimizzare la quantità dei dati raccolti. In questo modo, gli sviluppatori non potranno analizzare la voce dell'utente per ricavare informazioni senza un suo specifico consenso.

L'EDPB fa inoltre una distinzione sulle diverse tipologie di dati trattati, tra questi si hanno i primary data, ossia le registrazioni vocali e la cronologia delle richieste, gli observed data, quindi i dati del dispositivo e dell'attività online, e gli inferred or derived data, che sono i dati dedotti dalla profilazione dell'utente.

5.3 I principi fondamentali: privacy by design e privacy by default

Gli Smart Assistant, trattandosi di dispositivi intelligenti, sono spesso interconnessi con altri dispositivi o servizi offerti da terze parti, da qui nasce un'ulteriore problematica relativa alla diffusione dei dati personali. Il trattamento dei dati, infatti, può avvenire anche da parte di altri soggetti esterni al fornitore dell'Assistente Digitale utilizzato. Essendo molteplici gli attori coinvolti nella supply chain, dai programmatori ai produttori, secondo l'EDPB, emerge la necessità di normare le attività svolte, in tema di privacy, da ogni singolo stakeholder coinvolto nel processo.

L'EDPB evidenzia quindi la necessità di implementare misure di sicurezza e di garanzia adeguate nei dispositivi che ospitano gli Smart Assistant, come espresso dai principi di privacy by design e di privacy by default, ricorrendo agli strumenti di accountability espressamente previsti dal GDPR. L'accountability consiste nella responsabilità da parte dei fornitori ad adottare comportamenti proattivi nei confronti degli utenti, al fine di tutelarli. I principi di privacy by design e di privacy by default sono tra i fondamenti ispiratori del GDPR, il quale nell'art. 25 stabilisce che le misure di protezione dei dati personali debbano essere incorporate nei sistemi e nei dispositivi utilizzati per trattare i dati, e soprattutto che queste tecnologie siano progettate in modo tale da ridurre al minimo la raccolta e il trattamento di dati personali.

Il principio di privacy by design si basa sul fatto che la tutela dei dati personali degli utenti deve iniziare a partire dalle prime fasi di progettazione del dispositivo o del servizio, questo in modo tale da prevenire, invece che curare, i rischi legati alla privacy e alla sicurezza. Queste accortezze andranno inoltre mantenute per tutto il ciclo di vita dello strumento. Tale principio prevede inoltre che i titolari del trattamento dei dati riconoscano la centralità dell'utente, verso il quale è necessaria la massima trasparenza rispetto al trattamento dei dati personali.

Il principio di privacy by default, invece, prevede che la tutela della privacy sia appunto un'impostazione di default, incorporata nel servizio. Le misure di protezione dei dati personali dovrebbero essere infatti attive a priori e non disattivabili. Inoltre, i fornitori del servizio dovrebbero di default trattare i dati personali soltanto nella misura necessaria per le finalità previste e per il periodo di tempo strettamente necessario per il funzionamento del dispositivo.

Nell'art. 5 del GDPR vengono infatti discussi tre concetti fondamentali, precedentemente citati, che regolano il trattamento dei dati personali, i quali sono strettamente connessi fra loro. Si ha innanzitutto la minimizzazione dei dati trattati, come già discusso, si hanno poi la limitazione delle finalità del trattamento e del periodo di conservazione dei dati. Nonostante questo, si assiste spesso a raccolte di dati personali in quantità sicuramente eccessive rispetto alle finalità del trattamento, oltre al fatto che questi vengono conservati più tempo del dovuto.

La questione riguardante il periodo di conservazione dei dati personali raccolti dagli Smart Assistant viene affrontata con dettaglio nell'art. 13 del GDPR. Per risolvere questo problema, Alexa, Google Assistant e Siri, lasciano all'utilizzatore la scelta di cancellare le proprie registrazioni audio tramite un comando vocale o attraverso la relativa App. Quindi è l'utente stesso a determinare il periodo di conservazione delle proprie informazioni personali. Allo stesso tempo, l'Assistente Digitale potrebbe comunque conservare registrazioni relative ad esempio ad acquisti online, avvisi o allarmi, al fine di continuare a fornire determinati servizi.

Un altro tema sviscerato dal Board è quello relativo alle finalità del trattamento dei dati personali, il quale trova applicazione nell'art. 5 della Direttiva e-Privacy. Per utilizzare un Assistente Digitale è necessario fornire il consenso iniziale, dopodiché questo non sarà più necessario nei casi in cui il trattamento venga effettuato nella misura strettamente necessaria a fornire il servizio esplicitamente richiesto dall'utente. Gli obblighi contrattuali del fornitore sono l'acquisizione, l'elaborazione, l'interpretazione e la trascrizione del comando vocale dell'utilizzatore. Ogni altra finalità, come ad esempio il miglioramento della macchina attraverso tecniche di machine learning, l'identificazione biometrica o la profilazione per contenuti e pubblicità personalizzate, sarà legittima solo previa autorizzazione dell'utente attraverso un consenso specifico.

5.4 Dati biometrici, profilazione e discriminazione

I dati biometrici sono una tipologia di dati personali, quali ad esempio la voce o le caratteristiche del volto, che contengono informazioni specifiche dell'individuo, tanto da consentire un'identificazione univoca della persona. Un utilizzo illegittimo o inappropriato di tali dati può comportare notevoli rischi e pericoli, come il controllo non autorizzato di dispositivi intelligenti, il furto d'identità ed apre alla profilazione, la quale può diventare la base per trattamenti discriminatori.

La profilazione, espressamente definita dall'art. 4 e regolata nell'art. 22 del GDPR, costituisce lo strumento di cui le aziende si servono per raccogliere dati personali da utilizzare per fini commerciali, fornendo servizi personalizzati o inviando pubblicità comportamentali. Con gli Smart Assistant, la profilazione risulta potenzialmente molto più dettagliata rispetto a quella di una normale navigazione su un motore di ricerca. In questo contesto, neanche l'anonimizzazione, risulta particolarmente efficace, dal momento che l'incrocio di dati consente in ogni caso di identificare l'individuo. In ambito di profilazione risulta determinante il diritto di opposizione, trattato nell'art. 21 del GDPR, il quale consente all'utente di contestare la decisione automatizzata che produca effetti giuridici nei suoi riguardi, nonché di poter richiedere l'intervento umano in qualsiasi momento.

Come accennato, uno dei rischi è che le decisioni prese da sistemi di AI, a partire dai dati biometrici, presentino bias discriminatori, basati sul genere, sull'etnia o su altre caratteristiche personali. Essi svantaggiano sistematicamente alcuni individui o gruppi di individui, favorendone altri, ad esempio negando opportunità o generando risultati inappropriati. Tuttavia, il principio di non discriminazione non è esplicitamente sancito dal GDPR, è invece presente come principio generale a fondamento delle carte europee, in particolare nel Considerando n. 71 delle stesse. In quest'ultimo si stabilisce che debba essere il titolare del trattamento dei dati a

mettere in atto misure adeguate che tengano conto dei potenziali rischi per gli utenti e che impediscano effetti discriminatori, al fine di tutelare i diritti degli stessi. Emerge allora che il problema di fondo si riscontri sul piano della programmazione degli algoritmi di AI, il che lo rende complesso da risolvere.

5.5 Cyber attacchi

I dati biometrici, come detto, posseggono caratteristiche intrinseche che rendono il corpo umano uno strumento per la sua identificazione univoca. Vengono infatti spesso utilizzati come chiave di protezione per dispositivi intelligenti, dagli smartphone ai sistemi di sicurezza delle Smart Homes o Smart Cars.

Questo aspetto apre le porte a dei rischi enormi nel caso in cui lo Smart Assistant, o qualsiasi altro dispositivo dove questi dati biometrici sono immagazzinati, venisse violato attraverso un cyber attacco. Uno sconosciuto potrebbe infatti prendere il controllo della Smart Car mentre si è a bordo o di un dispositivo Smart Health, come ad esempio un pacemaker. Nel caso di una Smart Home sarebbe inoltre possibile sbloccare i sistemi di sicurezza della casa, spiare cosa avviene al suo interno, o prenderne il controllo dei dispositivi, il tutto semplicemente accedendo al computer che gestisce i comandi della casa, violando così sia la privacy che la sicurezza degli utenti.

In questo contesto, la cybersecurity rischia di esserne il tallone d'Achille dell'Internet of Things. Basti considerare che tra il 2018 e il 2021 sono stati contati ben 45 cyber attacchi globali di pubblico dominio incentrati sull'IoT, con una media di quasi uno al mese.

Agli attacchi informatici si aggiungono anche le violazioni commesse dai fornitori dei servizi, prendiamo come esempio Amazon che successivamente alla violazione dei dati di un utente non ha provveduto alla segnalazione entro 72 ore dall'accadimento, né alle autorità competenti né all'interessato, il quale è rimasto inconsapevole che tutti i suoi dati sensibili erano nelle mani di un altro soggetto.

Nella progettazione di molti di questi dispositivi intelligenti non viene ancora posta sufficiente attenzione agli aspetti di sicurezza. Sarebbe quindi necessario che i produttori si dimostrino più propensi a risolvere tali lacune, poiché con l'evolvere della tecnologia si evolvono anche le strategie degli attacchi informatici.

Sicuramente una strategia pratica che diminuirebbe le conseguenze di un cyber attacco è una configurazione efficiente, infatti separando i dispositivi intelligenti della casa dagli altri, si potrebbe segmentare il rischio. Se invece fossero tutti connessi tra loro, l'attacco di uno causerebbe la violazione di tutti gli altri.

Tra le raccomandazioni tecniche per gli utenti vi è l'adozione di un server VPN (Virtual Private Network) all'interno della propria rete locale. La VPN permette di nascondere il proprio indirizzo IP attraverso la creazione di un canale di comunicazione privato, il quale consente il transito di informazioni in modo invisibile a soggetti non autorizzati.

5.6 ISO/IEC 27400:2022 e certificazioni

Fino ad ora si sono analizzate le norme e i regolamenti internazionali da un punto di vista giuridico. Tuttavia, al fine di mitigare i rischi in ambito di sicurezza dei dispositivi IoT e dei dati da essi trattati, ci si può affidare anche a norme tecniche.

A giugno del 2022, la International Organization for Standardization ha pubblicato la prima versione della norma tecnica ISO/IEC 27400:2022. Si tratta di uno standard internazionale, che include misure tecniche e organizzative volte a fornire delle linee guida utili a garantire la sicurezza informatica e la privacy dei sistemi IoT. Tale standard si integra nella più vasta famiglia delle ISO 27000 sulla sicurezza delle informazioni.

La ISO 27400, a partire dai rischi a cui sono sottoposti i sistemi IoT, individua 45 controlli raccomandati per la sicurezza e la privacy che sono applicabili durante l'intero ciclo di vita del sistema IoT. Questi controlli sono identificati in relazione al dominio o alle competenze delle parti interessate. Infatti, non sono indirizzati solo ai fornitori e agli sviluppatori di sistemi IoT, ma anche agli utenti che usufruiscono di tali sistemi.

L'applicazione dello standard ISO 27400 non risulta obbligatoria, tuttavia porterebbe dei vantaggi alle aziende che lo rispettino. Infatti, oltre a permettere di raggiungere obiettivi di sicurezza e di protezione dei dati personali, volti a tutelare i propri utenti e il mercato IoT nel suo insieme, migliorerebbe anche la reputazione dell'azienda agli occhi di eventuali stakeholders, rendendola più competitiva sul mercato.

Nel contesto odierno, risulta altamente probabile ed auspicabile che le certificazioni assumano un ruolo operativo sempre più importante. Il GDPR stesso nell'art. 42 attribuisce un ruolo fondamentale alle certificazioni, attribuisce inoltre agli Stati membri dell'Unione Europea, alle Autorità di controllo, al Comitato e alla Commissione, il compito di incoraggiare meccanismi di certificazione della protezione dei dati, allo scopo di conformarsi al Regolamento. Con l'avvento del GDPR, il ruolo delle Autorità di controllo, non si limita più al semplice controllo che le norme siano rispettate, diventa invece un ruolo proattivo nella protezione dei diritti dei soggetti coinvolti.

Le certificazioni vengono inoltre considerate veri e propri strumenti di accountability, esse infatti potrebbero svolgere un ruolo importante al fine di responsabilizzare i fornitori nei confronti degli utenti. In un futuro, le certificazioni potrebbero essere rilasciate direttamente dal Comitato Europeo, nell'ottica di pervenire ad un vero e proprio "sigillo Europeo per la protezione dei dati".

5.7 AI e ChatGPT

Gli Assistenti Digitali, come si è visto, sfruttano algoritmi di AI e di machine learning per il proprio funzionamento. L'intelligenza artificiale è una disciplina scientifica che nasce con lo scopo di sviluppare macchine in grado di simulare i processi di intelligenza umana. Ad oggi, l'AI offre moltissime opportunità per migliorare la vita di tutti i giorni, a partire dai singoli individui, fino alle grandi aziende. Essa è anche usata per favorire il progresso scientifico, oltre a fornire un aiuto nella lotta al cambiamento climatico. Nonostante sia divenuto un tema così discusso soltanto negli ultimi anni, quello dell'AI è un percorso iniziato più di 60 anni fa.

Quando si pensa all'intelligenza artificiale, una tra le prime tecnologie che viene in mente è ChatGPT, dove GPT è l'acronimo di Generative Pretrained Transformer. Si tratta di un chatbot sviluppato da OpenAI, che sfrutta l'intelligenza artificiale generativa e l'apprendimento automatico per rispondere agli input degli utenti. Essa utilizza algoritmi di machine learning e deep learning per creare un modello conversazionale del linguaggio umano, attraverso il quale può rispondere in forma scritta ad utilizzatori umani, in modo grammaticalmente perfetto su qualsiasi argomento.

Tuttavia, nonostante abbia un ottimo modello del linguaggio umano, non possiede un modello del mondo, e non è stata progettata per conoscere valori importanti per gli umani. Questo significa che i rischi di ChatGPT non si limitano a quelli legati alla privacy e al trattamento dei dati personali. Potrebbe infatti generare risposte non corrette o pericolose, ad esempio dal linguaggio aggressivo o dal contenuto razzista, mettendo a repentaglio i diritti fondamentali della persona.

5.8 Il provvedimento del Garante su ChatGPT

Con la diffusione di ChatGPT è aumentata anche l'attenzione posta dalle Autorità garanti europee sul trattamento dei dati personali da parte di questa piattaforma.

A tal proposito, il primo ad intervenire è stato proprio il Garante della Privacy italiano attraverso il provvedimento n.112, attuato il 30 marzo 2023 con l'obiettivo di bloccare ChatGPT, ai sensi dell'art. 58 del Regolamento (UE) 2016/679, almeno fino a quando questa non avrebbe rispettato la privacy degli utenti. Per quanto riguarda il trattamento dei dati personali, sarebbero infatti stati violati gli art. 5, 6, 8, 13 e 25 del GDPR.

Il Garante avrebbe aperto un'istruttoria, oltre a disporre, con effetto immediato, la limitazione provvisoria del trattamento dei dati degli utenti italiani da parte di OpenAI. ChatGPT, infatti, il precedente 20 marzo avrebbe subito un data breach, ossia una perdita dei dati degli utenti, in particolare circa le conversazioni e le informazioni relative al pagamento degli abbonati.

Nel provvedimento viene evidenziata la mancanza di un'informativa per gli utenti sulla raccolta dei dati da parte di OpenAI. Un tema cruciale rilevato è inoltre quello relativo ai Big Data, mancherebbe infatti una base giuridica che giustifichi la raccolta e la conservazione di una così ampia quantità di dati personali, utilizzati per addestrare gli algoritmi di ChatGPT. Il Garante ha poi verificato che il trattamento dei dati personali risultasse spesso inesatto, in quanto le informazioni fornite da ChatGPT non sempre corrispondono al dato reale. Per concludere, si evidenziava che non fosse presente un filtro idoneo a verificare l'età degli utenti, nonostante secondo i termini di OpenAI il servizio sarebbe rivolto ai maggiori di 13 anni.

A seguito del provvedimento, OpenAI avrebbe dovuto comunicare entro 20 giorni le misure intraprese, altrimenti sarebbe stata sottoposta ad una sanzione fino a 20 milioni di euro o fino al 4% del fatturato globale annuo.

Il 5 aprile 2023 si è svolto un incontro, in videoconferenza, tra il Collegio del Garante ed i vertici di OpenAI, durante il quale quest'ultima, pur ribadendo di essere convinta di rispettare le norme per la privacy, avrebbe confermato la volontà di collaborare per arrivare ad una soluzione del problema.
Si sarebbe a tal fine impegnata a rafforzare la trasparenza nei confronti degli utenti per quanto riguarda le finalità del trattamento dei dati personali, oltre a fornire la possibilità agli utilizzatori di esercitare i propri diritti sui dati e ad aumentare le garanzie per i minori di 13 anni.

I Garanti della Privacy europei, riuniti nell'EDPB avrebbero inoltre deciso di lanciare una task force su ChatGPT, con l'obiettivo di promuovere la cooperazione e lo scambio di informazioni sulle possibili azioni di controllo condotte dalle Autorità di protezione dei dati dell'UE.

Successivamente agli avvenimenti descritti, il 29 gennaio 2024, il Garante ha notificato a OpenAI l'atto di contestazione per la violazione della normativa in materia di protezione dei dati personali. Infatti, a seguito del provvedimento del 30 marzo 2023 e all'esito dell'istruttoria, il Garante avrebbe ritenuto che siano stati commessi uno o più illeciti rispetto a quanto stabilito dal GDPR, avendo così gli elementi per poter procedere con delle sanzioni amministrative nei confronti di OpenAI.

I vantaggi dell'Intelligenza Artificiale sono chiari, bisogna tuttavia riconoscere i rischi che porta con sé. È qui che l'innovazione tecnologica si scontra con i principi etici, caratteristici dell'essere umano. Proprio dall'etica dell'AI emergono importanti preoccupazioni circa la privacy e la sicurezza dei dati, nonché sulla trasparenza e la spiegabilità delle decisioni prese dagli algoritmi, senza contare i temi legati alla giustizia e all'equità.

5.9 L'AI Act

Appare a questo punto evidente la necessità di una qualche forma di regolamentazione sull'Intelligenza Artificiale, proprio qui entra in gioco una normativa piuttosto recente, vale a dire l'AI Act. Il 12 luglio 2024 è finalmente uscito sulla Gazzetta Ufficiale Europea il testo ufficiale del Regolamento (UE) 2024/1689 del 13 giugno 2024, noto come Artificial Intelligence Act, o semplicemente AI Act. Il quale è entrato in vigore venti giorni dopo la sua pubblicazione, mentre per la sua piena applicazione bisognerà aspettare il 2 agosto 2026. Si tratta di una legge proposta per la prima volta in Commissione il 21 aprile 2021 ed approvata solo il 13 marzo 2024, con l'obiettivo di creare un quadro normativo armonizzato e un mercato unico per l'intelligenza artificiale nell'Unione Europea. È inoltre il primo Regolamento al mondo che stabilisca delle regole sull'intelligenza artificiale.

L'AI Act si basa sul principio che l'intelligenza artificiale debba essere sviluppata e utilizzata in modo sicuro, etico e rispettoso dei diritti fondamentali dell'individuo. Esso stabilisce un

insieme di norme, in linea con la strategia digitale dell'UE, che mirano a promuovere l'innovazione, la competitività e lo sviluppo responsabile e sostenibile del settore dell'AI, anche attraverso incentivi e finanziamenti per la ricerca, assicurando così all'Europa un ruolo guida nel settore. Il tutto garantendo al tempo stesso la protezione dei consumatori, dei lavoratori e dei cittadini.

Per fare ciò, l'AI Act stabilisce una serie di requisiti e obblighi sia per i fornitori, ossia tutti coloro che sviluppano sistemi di AI, sia per gli operatori, cioè coloro che utilizzano tali sistemi.

Inoltre, per promuovere lo sviluppo, uno degli obiettivi è quello di aumentare la fiducia nell'AI, assicurando che tali sistemi siano sicuri, affidabili e soddisfino alcuni particolari requisiti di trasparenza. La trasparenza rappresenta un punto fondamentale, infatti è necessario che i produttori forniscano una chiara comprensione dei sistemi di AI adottati.

Oltre a questo, dovranno rispettare i principi etici e i diritti fondamentali, il testo prevede infatti la tutela di diversi diritti, quali il diritto alla dignità, alla non discriminazione, alla privacy, alla protezione dei dati, alla libertà di espressione e di informazione, al processo equo e alla presunzione di innocenza.

Il Regolamento segue un approccio basato sul rischio derivante dai sistemi di AI, al fine di prevenirlo e mitigarlo, questo viene classificato in rischio minimo, rischio limitato, rischio alto e rischio inaccettabile. Vengono ad esempio considerate ad alto rischio, le tecnologie di sorveglianza con riconoscimento facciale che si trovano all'interno degli aeroporti. Infatti, queste permetterebbero di raccogliere i dati biometrici di migliaia di persone, che potrebbero essere utilizzati in maniera inappropriata, senza che i proprietari ne siano consapevoli, quindi violando la loro privacy. Tra le pratiche proibite invece, si hanno ad esempio quelle legate al riconoscimento delle emozioni in ambienti lavorativi o scolastici, oppure quelle che utilizzano sistemi di categorizzazione biometrica in tempo reale, le quali potranno essere utilizzate dalle forze dell'ordine, solo in alcune specifiche situazioni previste dalla legge, come ad esempio la ricerca di una persona scomparsa o la prevenzione di un attacco terroristico.

A seconda del livello di rischio cambiano chiaramente le restrizioni e gli obblighi per le imprese che realizzano o fanno uso di tali sistemi, con relative sanzioni.

Il Regolamento non si applicherà a quei sistemi di AI utilizzati per scopi di ricerca scientifica e di sviluppo, o per scopi militari, di difesa e di sicurezza nazionale.

Per concludere, si riporta quanto dichiarato dal correlatore della commissione per il mercato interno Brando Benifei (S&D, Italia), durante il dibattito in merito all'approvazione del Regolamento: "Dopo due anni intensi di lavoro siamo finalmente riusciti ad approvare la prima legge vincolante al mondo sull'intelligenza artificiale, volta a ridurre i rischi e aumentare opportunità, combattere la discriminazione e portare trasparenza. Grazie al Parlamento europeo, le pratiche inaccettabili di IA saranno proibite in Europa. Tuteliamo i diritti dei lavoratori e dei cittadini. Dovremo ora accompagnare le aziende a conformarsi alle regole prima che entrino in vigore. Siamo riusciti a mettere gli esseri umani e i valori europei al centro dello sviluppo dell'IA".

6 Consigli del Garante e best practice

Appare a questo punto evidente come un uso incontrollato degli Assistenti Digitali possa esporre l'utente a seri rischi sulla protezione della sua privacy e dei suoi dati personali. È quindi opportuno cercare di fare un uso informato e consapevole di questi strumenti, per tutelare in modo adeguato i dati personali, non solo di chi li utilizza, ma anche di tutti coloro che entrano, volontariamente o meno, nel loro campo d'azione.

A tal fine, il GPDP, ossia il Garante per la Protezione dei Dati Personali, mette a disposizione sul proprio sito una scheda informativa contenente una serie di buone pratiche, accortezze e suggerimenti da seguire per un corretto utilizzo di queste tecnologie.

Nel caso in cui per attivare l'Assistente Digitale o le eventuali app di gestione sia necessario registrarsi fornendo i propri dati personali, è bene leggere con attenzione l'informativa sul trattamento dei dati personali. Questa per legge deve sempre essere disponibile, ad esempio sul sito dell'azienda che offre il servizio o nella confezione del dispositivo.

In particolare, è importante cercare di comprendere quali e quante informazioni saranno acquisite direttamente dallo Smart Assistant e come queste potrebbero essere utilizzate o se verranno trasferiti a terzi, ossia capire se saranno impiegate soltanto per far funzionare il dispositivo o anche per altre finalità. Bisogna quindi essere a conoscenza di chi e come potrebbe ricevere i dati raccolti, dove saranno conservati e per quanto tempo.

Nel momento in cui l'Assistente Digitale viene attivato per la prima volta, sarebbe opportuno fornire solo le informazioni specificamente necessarie per la registrazione e l'attivazione dei servizi, oltre ad utilizzare eventualmente pseudonimi per gli account, soprattutto se appartenenti a minori. Si può anche valutare la possibilità di impostare un sistema di sicurezza che limita l'accesso al servizio solo a specifici utenti.

Meglio inoltre non fornire informazioni delicate, come ad esempio quelle relative alla propria salute, le password o i numeri delle carte di credito. Occorre valutare poi i rischi e i benefici nel permettere allo Smart Assistant di accedere ai dati conservati sul dispositivo su cui è installato, come ad esempio l'archivio fotografico, la rubrica, le note o il calendario dello smartphone.

Come si è visto, quando l'Assistente Digitale è acceso ma non viene utilizzato, si trova nello stato di passive listening, in cui è potenzialmente in grado di sentire e vedere tutto quello succede intorno ad esso, stato da cui esce quando sente la parola di attivazione. I dati così raccolti possono anche essere memorizzati su server esterni e inviati a terzi. Se consentito è allora opportuno scegliere con cura l'espressione di risveglio, evitando parole di uso frequente, brevi o fraintendibili, queste potrebbero infatti causare attivazioni involontarie dello Smart Assistant.

Nei momenti in cui non si usa l'Assistente Digitale, ad esempio la notte o quando non si è in casa, al fine di interrompere il passive listening e quindi evitare ogni possibile acquisizione e trasmissione non desiderata dei dati, si potrebbe, se possibile, disattivare il microfono, la videocamera o entrambi, oppure disattivare l'Assistente Digitale dalle impostazioni, o altrimenti spegnere direttamente il dispositivo che lo ospita.

Se lo Smart Assistant è in grado di svolgere azioni particolari, come inviare messaggi, pubblicare contenuti sui social o effettuare acquisti online, sarebbe opportuno disattivare tali

funzioni superflue e mantenere attive solo quelle realmente utili, o almeno inserire, dove possibile, una password per autorizzarne l'uso solo su specifica richiesta dell'utente.

Le stesse raccomandazioni valgono sulle funzioni di controllo domotico, utili per controllare l'attivazione o la disattivazione dei sistemi della Smart Home. Si pensi, ad esempio, all'eventuale rischio che la voce dell'utente venga in qualche modo clonata ed utilizzata per controllare i sistemi di protezione della casa, oppure per spiare l'interno dell'abitazione utilizzando microfoni e videocamere.

Come descritto in precedenza, gli Assistenti Digitali, essendo dispositivi IoT, sono anche in grado di dialogare con altri dispositivi intelligenti. Essendo questa una capacità che amplifica la possibilità di diffusione dei dati personali, è sempre bene informarsi su come e da chi vengono raccolti, elaborati, conservati ed eventualmente a chi vengono resi accessibili questi dati, oltre a considerare il possibile impatto sulla privacy domestica.

Per limitare il trattamento dei dati personali raccolti dallo Smart Assistant, si può cancellare periodicamente la cronologia, o almeno eliminare dalla cronologia i dati ritenuti più delicati.

Una regola fondamentale è impostare password complesse, che andrebbero cambiate periodicamente, sia per l'uso dell'Assistente Digitale che per la sua connessione a Internet.

Altra importante precauzione è verificare che la crittografia della rete Wi-Fi sia impostata sul protocollo di sicurezza WPA 2, ovvero quello attualmente più sicuro e adatto a proteggere i dati sensibili da eventuali attacchi.

Oltre a questo, è opportuno verificare che sul dispositivo su cui è installato l'Assistente Digitale siano presenti sistemi di protezione antivirus e tenerli costantemente aggiornati.

Nel caso in cui il dispositivo su cui è installato l'Assistente Digitale venga ceduto, è bene disattivare gli eventuali account personali, le password e le credenziali di accesso memorizzate, oltre a provvedere alla cancellazione di tutti i dati registrati al suo interno. Inoltre, se i dati raccolti sono stati trasmessi e conservati nei database dell'azienda produttrice o di altri soggetti è opportuno chiederne la cancellazione.

Bisogna anche considerare il fatto che non sempre risulta facile verificare che gli standard imposti dal Regolamento Europeo siano rispettati. Per questo motivo, nel caso in cui ci siano dubbi sull'effettivo rispetto di tali norme o sul corretto trattamento dei propri dati personali, il Garante ha messo a disposizione un servizio di comunicazione, con il quale i cittadini possono segnalare la presenza di eventuali violazioni all'indirizzo e-mail urp@gpdp.it.

Per concludere, si può dire che gli Assistenti Digitali offrono enormi possibilità agli utenti, tuttavia per utilizzarli in maniera corretta è necessaria una buona dose di consapevolezza e di accortezza per evitare la dispersione di dati sensibili.

7 Conclusione

Gli Assistenti Digitali fanno ad oggi parte della vita quotidiana della maggior parte delle persone, complice soprattutto l'incondizionata diffusione degli smartphone e altri dispositivi IoT. A questo si aggiunge l'utilizzo che ne fanno le aziende, al fine di essere sempre più competitive sul mercato.

Questi dispositivi, infatti, possono svolgere le attività più banali e ridondanti, permettendo agli esseri umani di avere maggior tempo libero e di poter impiegare più energie in idee strategiche, creative ed innovative.

Inoltre, i continui progressi dell'AI e del Machine Learning lasciano presupporre che gli Smart Assistant del futuro diventeranno ancora più intelligenti, potranno infatti fornire conversazioni più naturali, rispondere a domande più complesse e offrire consigli più approfonditi.

L'intelligenza artificiale può infatti trasformare profondamente il mondo in cui viviamo, portando con sé importanti benefici per la società e per l'economia. Allo stesso tempo però, si tratta di tecnologie che presentano dei rischi per la sicurezza e per i diritti fondamentali degli individui, grazie alle loro capacità di raccogliere ed elaborare una grande mole di dati personali.

Lo scenario tecnologico odierno lancia al diritto e all'etica un guanto di sfida, in quanto richiede di individuare un giusto compromesso tra le opportunità che la scienza offre e il rispetto dei diritti fondamentali dell'individuo.

A tal fine, è quindi necessario il continuo supporto da parte delle Autorità di controllo, le quali, attraverso l'introduzione delle linee guida proposte dall'EDPB e delle regolamentazioni introdotte dal GDPR e dall'AI Act, hanno dimostrato negli ultimi anni un ruolo estremamente attivo nella protezione dei diritti dei cittadini dell'Unione Europea.

Tali norme, infatti, mirano a promuovere l'innovazione e lo sviluppo di queste nuove tecnologie in modo responsabile e sostenibile, vale a dire garantendo la protezione dei diritti fondamentali dei consumatori. Questo è possibile attraverso un processo di responsabilizzazione dell'utente e di tutti gli stakeholder coinvolti nel processo.

In primo luogo, resta di fondamentale importanza rendere gli utenti consapevoli delle potenzialità di questi strumenti, nonché dei rischi che corrono, rendendoli quindi in grado di attuare le giuste contromisure e cautele, in maniera tale da tutelare la propria sicurezza e il trattamento dei propri dati personali.

Tuttavia, il punto chiave sta nel concetto di accountability, ossia di responsabilizzazione dei produttori e dei fornitori di prodotti e servizi di assistenza digitale, i quali sono tenuti ad adottare comportamenti proattivi e trasparenti nei confronti degli utenti, al fine di tutelarli.

In quest'ambito, anche le norme tecniche possono svolgere un ruolo sempre più importante, ad esempio, rendendo alcuni standard e certificazioni obbligatori, come la norma tecnica ISO/IEC 27400:2022, atta a garantire la sicurezza informatica e la privacy dei sistemi IoT.

Nella direzione ad oggi individuata, il concetto di sicurezza informatica e di protezione dei dati personali si collegano direttamente al rispetto dei diritti e delle libertà fondamentali della persona. Quindi, risulta fondamentale fornire un prodotto o un servizio sicuro e che rispetti la privacy dell'utente, il quale idealmente non dovrebbe preoccuparsi di comprendere l'incidenza del dispositivo acquistato sulla protezione dei suoi dati personali, in piena ottica privacy by design e privacy by default.

Per concludere, si riporta l'intervento del correlatore della commissione per le libertà civili Dragos Tudorache (Renew, Romania), in occasione del dibattito conclusivo del 12 marzo 2024 sull'approvazione dell'AI Act, avvenuta poi con la votazione del giorno successivo, durante il quale ha dichiarato: "L'UE ha mantenuto la promessa. Abbiamo collegato per sempre al concetto di intelligenza artificiale i valori fondamentali che costituiscono la base delle nostre società. Ci aspetta molto lavoro che va oltre la legge sull'intelligenza artificiale. L'intelligenza artificiale ci spingerà a ripensare il contratto sociale che sta alla base delle nostre democrazie. Insieme ai nostri modelli educativi, ai nostri mercati del lavoro, al modo in cui conduciamo le guerre. La legge sull'IA non è la fine del viaggio, ma piuttosto il punto di partenza per un nuovo modello di governance basato sulla tecnologia. Ora dobbiamo concentrarci per trasformarla da legge sui libri a realtà sul campo".

Sitografia

https://www.internet4things.it/iot-library/internet-of-things-gli-ambiti-applicativi-in-italia/

https://www.oracle.com/it/internet-of-things/

https://aws.amazon.com/it/what-is/iot/

https://www.sap.com/italy/products/artificial-intelligence/what-is-iot.html#:~:text=L'Internet%20of%20Things%20(IoT)%20è%20una%20rete%20di,è%20sinonimo%20di%20Industry%204.0

https://www.ibm.com/it-it/topics/internet-of-things

https://blog.osservatori.net/it_it/cos-e-internet-of-things

https://www.arera.it/area-operatori/smartmetering

https://www.lumi4innovation.it/smart-grid-cose-e-come-funziona/

https://www.cyberlaws.it/2021/smart-assistant/

https://www.cyberlaws.it/2020/smart-assistant-privacy/

https://www.altalex.com/documents/news/2021/04/13/assistenti-vocali-virtuali-privacy-nuove-linee-guida-edpb

https://www.medialaws.eu/wp-content/uploads/2020/12/RDM-3-2020-Vizzoni-107-120.pdf

https://ilsalvagente.it/2022/12/29/come-utilizzare-gli-assistenti-digitali-in-modo-corretto/

https://www.oracle.com/it/chatbots/what-is-a-digital-assistant/

http://www.bblex.it/articolo/assistenti-virtuali-validi-aiuti-o-pericoli-per-la-privacy-intervengono-le-nuove-linee-guida/

https://www.utopiathesoftware.com/blog-post/privacy-smart-assistant-dati-personali

https://www.federprivacy.org/informazione/punto-di-vista/smart-assistant-testimoni-di-un-crimine

https://www.federprivacy.org/informazione/primo-piano/cosa-c-e-dietro-le-sbadataggini-degli-assistenti-digitali-che-minacciano-la-nostra-privacy

https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/

https://www.agendadigitale.eu/sicurezza/le-norme-tecniche-e-la-privacy-per-la-sicurezza-nelliot-cosa-sapere-per-evitare-rischi/

https://www.agendadigitale.eu/sicurezza/rischi-iot-cybersecurity/

https://www.agendadigitale.eu/sicurezza/cybersecurity-nelliot-come-si-individuano-le-vulnerabilita-e-si-limitano-i-rischi/

https://www.cybersecurity360.it/legal/iso-iec-274002022-perche-e-importante-per-la-sicurezza-e-la-protezione-dati-delliot/

https://www.esg360.it/governance/intelligenza-artificiale-ed-etica-perche-e-importante-anche-per-lesg/

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9872832

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9875657

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020

https://www.agendadigitale.eu/cultura-digitale/unai-etica-e-responsabilita-di-tutti-le-basi-per-realizzarla/

https://www.agendadigitale.eu/cultura-digitale/ai-act-ci-siamo-ecco-come-plasmera-il-futuro-dellintelligenza-artificiale-in-europa/

https://www.cybersecurity360.it/news/ai-act-pubblicato-in-gazzetta-ufficiale-europea-non-ci-sono-piu-scuse-per-adeguarsi/

https://www.cybersecurity360.it/legal/privacy-dati-personali/ai-act-quadro-normativo-europeo/

https://www.europarl.europa.eu/news/it/press-room/20240308IPR19015/il-parlamento-europeo-approva-la-legge-sull-intelligenza-artificiale

https://www.garanteprivacy.it/temi/assistenti-digitali

https://www.edpb.europa.eu/system/files/2022-02/edpb_guidelines_202102_on_vva_v2.0_adopted_it.pdf

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401689