STUDIO LEGALE SLB BROGLIA

SMART SPEAKERS

ASSISTENTI DIGITALI (VIRTUAL ASSISTANT)
I CONSIGLI DELLE AUTORITÀ PER UN USO CONSAPEVOLE

Gli assistenti digitali sono programmi che interpretano il nostro linguaggio e interagiscono con noi e con il web mediante algoritmi.

Un assistente virtuale è dotato di un software che riceve un input mediante la voce, identifica un comando o una domanda, interagisce, se necessario, con altri programmi o servizi e "risponde" vocalmente alla richiesta.

Gli assistenti digitali possono raccogliere e memorizzare una grande quantità di dati personali, anche delle persone che si trovano nel loro raggio di azione (preferenze, abitudini, consumi, caratteristiche biometriche, posizione, percorsi abituali o frequenti, indirizzi, età, sesso, stati emotivi e molto altro).

E' opportuno farne un uso informato e consapevole.

COME FUNZIONANO

Gli attuali assistenti vocali hanno caratteristiche costruttive che consentono loro, una volta attivati, di cercare informazioni su internet, suonare musica, fare telefonate e gestire diversi compiti, come per esempio pubblicare contenuti sui social o effettuare acquisti.

Essi sono anche in grado di essere utilizzati per ulteriori compiti e funzionalità, come controllare altri apparecchi collegati alla rete (una porta "smart", l'impianto di riscaldamento, il frigorifero) oppure installare ulteriori programmi o funzionalità.

Gli assistenti più conosciuti:

Vendor	Device	Virtual Assistant
Amazon	Amazon Echo, Echo plus and Dot	Alexa
Google	Google Home	Google Assistant
Alibaba	AliGenie XL	Genie AI
Baidu	Raven H and R, Xiaodu Zijia	DuerOS
Xiaomi	Mi AI speaker	Xiao AI
Apple	Homepod	Siri

E' possibile disattivare alcune funzionalità e, spesso, inserire una password per autorizzare l'uso solo su specifica richiesta dell'utilizzatore.

Google, per esempio, ha recentemente introdotto alcune modifiche.

ATTENZIONE ALLE FUNZIONALITÀ ATTIVE

E' bene informarsi attentamente su come e da chi vengano raccolti, elaborati, conservati ed eventualmente a chi vengano resi accessibili, i dati personali e considerare il possibile impatto sulla riservatezza domestica.

Occorre inoltre valutare se disattivare alcune funzioni di controllo domotico e inserire apposite password per controllare l'attivazione o la disattivazione dei sistemi, in modo da poter utilizzare lo smart assistant con maggiore sicurezza.

Le Autorità per la protezione dei dati personali (si veda quanto pubblicato dall'European Data Protection Supervisor) evidenziano alcune problematiche che un uso disattento o superficiale possono far emergere.

MANCANZA DI TRASPARENZA

Può essere difficoltoso rendere pienamente consapevoli tutti i soggetti i cui dati potrebbero essere raccolti durante l'uso degli assistenti, anche in relazione alle diverse tipologie di dati trattati.

MANCANZA DI UN ADEGUATO CONSENSO

Gli assistenti potrebbero raccogliere i dati vocali delle persone senza che queste ne siano pienamente consapevoli e, pertanto, senza il loro consenso.

PROFILAZIONE

Il riutilizzo dei dati raccolti può consentire forme particolarmente invasive di profilazione e targettizzazione dei soggetti coinvolti.

SICUREZZA

Gli smart speaker più diffusi non consentono un adeguato controllo e un pieno accesso ai dati. E' talvolta possibile, da parte di malintenzionati, manipolare gli apparecchi, agendo da remoto, perché essi sono connessi alla rete. In tal modo è anche possibile modificare i parametri di settaggio, all'insaputa del proprietario.

CONSERVAZIONE NON NECESSARIA

Molti assistenti digitali consentono una conservazione dei dati ben al di là delle effettive necessità degli utenti e delle case produttrici e, spesso, non è possibile intervenire autonomamente per effettuare la cancellazione o la distruzione dei dati conservati.

TRATTAMENTI NON CONSENTITI

E' possibile, in seguito a errori di interpretazione degli apparecchi, che si effettuino trattamenti non adeguatamente consentiti dagli utenti, anche a seguito di attivazioni non consapevoli.

POTENZIALE SORVEGLIANZA MASSIVA

Sebbene non progettati per registrare più di pochi comandi, i sistemi potrebbero dare accesso da remoto a programmi di sorveglianza massiva.

CARENZA DI PRIVACY BY DESIGN E BY DEFAULT

Come risulta evidente dai cenni di cui sopra, gli attuali sistemi non sembrano perfettamente conformi agli attuali principi in materia di protezione dei dati, che fanno della c.d. *privacy by design* e della *privacy by default* due principi cardine in tema di sicurezza e protezione delle persone fisiche nonché delle loro libertà fondamentali.

LA SCHEDA DEL GARANTE ITALIANO

Anche il Garante Italiano ha pubblicato interessanti e utili consigli in una apposita scheda informativa.

Vediamo in sintesi, rimandando alla pagina indicata per l'approfondimento, cosa ci viene suggerito.

INFORMARSI SEMPRE

su quali e quante informazioni saranno acquisite dall'apparecchio, senza dimenticare di verificare quali e quanti dati saranno trasferiti a società terze per il funzionamento dell'assistente o per altre finalità. Importante anche verificare il luogo e la durata della conservazione.

NON FORNIRE TROPPE INFORMAZIONI

quando si attiva per la prima volta l'apparecchio ed evitare di fornire dettagli sui propri dati finanziari o particolari, ossia "sensibili" (stato di salute, password, altre credenziali).

DISATTIVARE L'ASSISTENTE

quando non lo si usa e prevedere un comando di attivazione "specifico", non di uso comune o che potrebbe essere "frainteso" dallo speaker. Gli assistenti, mediante la funzione di c.d. "*passive listening*" (ascolto passivo) potrebbero infatti attivare il microfono ed eventualmente anche la telecamera se attivati inconsapevolmente.

Appare pertanto opportuno, anche se talvolta un po' scomodo, prevedere particolari meccanismi di attivazione e, possibilmente, spegnerlo del tutto.

Va ricordato che ormai gli assistenti si trovano anche nei telecomandi del televisore, oltre che in tanti altri oggetti (basti pensare alle vetture)!

UTILIZZARE SOLO SPECIFICHE FUNZIONI

Spesso gli assistenti consentono molteplici azioni anche online, come abbiamo visto. Per evitare, per esempio, acquisti non desiderati, magari effettuati per sbaglio da minori che giocano con gli assistenti, è opportuno decidere con attenzione quali funzionalità attivare e, laddove possibile, utilizzare password o credenziali specifiche.

CANCELLARE LA CRONOLOGIA

Al fine di limitare invasioni della nostra riservatezza, è consigliabile cancellare periodicamente, mediante il sito del produttore, la cronologia delle informazioni conservate.

UTILIZZARE SISTEMI SICURI

Dalle password di accesso ai sistemi di protezione anti virus fino alla eventuale crittografia, è consigliabile, vista la possibile invasività e pericolosità della circolazione incontrollata delle nostre informazioni, rendere il sistema operativo dell'assistente digitale o la applicazione per il suo utilizzo, i più sicuri possibile, rivolgendosi a tecnici professionisti.

CANCELLARE I DATI

Quando si vende il dispositivo sul quale è installato lo smart assistant, sia esso un cellulare, un apparecchio o una vettura, è bene cancellare o chiedere al produttore la cancellazione di tutti i dati eventualmente conservati!

Avv. ANDREA BROGLIA
info@studiolegalebroglia.com
VIA DELLA BRUNELLA 4
21100 VARESE

STUDIO LEGALE
SLB BROGLIA