La relazione fa riferimento alla Bottega del Sapere tenutasi sabato 1 giugno 2019 presso la Libreria Friuli. I docenti coinvolti, Pier Luca Montessoro, del Dipartimento di Scienze Giuridiche dell’Università degli Studi di Udine e Federico Costantini, del Dipartimento Politecnico di Ingegneria e Architettura, hanno sostenuto un incontro con la popolazione, trattando il tema: “Senti chi parla!”, sulla riservatezza degli assistenti virtuali tra informatica e diritto.

**SENTI CHI PARLA!**

**Il problema della riservatezza degli “assistenti virtuali” tra informatica e diritto**

Luca Montessoro – DPIA

Federico Costantini – DISG

La domotica non rappresenta il futuro, è il presente. Ciò che cinquanta anni fa era solo fantascienza, oggi è parte dell’esperienza quotidiana.

Gli assistenti virtuali sono innegabilmente utili, presto i dispositivi impareranno tutte le lingue e sapranno captare le nostre emozioni, con risultati davvero imprevedibili ma….. ma vi sono insidie e non sono sempre evidenti.

Oggigiorno è possibile gestire gli impianti di una casa anche attraverso semplici comandi vocali. Questi dispositivi, per essere comandati, devono ascoltarci ma possono anche trasformarsi in “orecchie indiscrete”, creando situazioni imbarazzanti ….in un caso il dispositivo ha consigliato a un utente di uccidere i suoi parenti adottivi, mentre in un altro ha usato un linguaggio particolarmente scurrile….. Negli Stati Uniti, in un caso di omicidio, è stato richiesto ad Amazon di riprodurre le registrazioni di Alexa, tenendo conto della voce registrata durante i comandi vocali.

I dispositivi “smart” e gli “smart speaker”

Grazie alle smart home, le smart cities, lo smart world e all’Internet of things, i nostri dati viaggiano molto e vanno lontano. Ma di quali dati stiamo parlando? Azioni più o meno esplicite? Comandi espliciti? Normali conversazioni? Ma soprattutto, quando, come e chi processa i nostri dati?

Per poter monitorare i dati generati dagli smart speaker dobbiamo creare una rete ad hoc che ci permette di monitorare il traffico. È stato sfruttato un apparato di rete denominato HUB che inoltra i dati in ingresso da una qualsiasi delle sue porte su tutte le altre. L’HUB replica tutti i pacchetti a tutte le porte prima di immetterli in internet: possiamo quindi visualizzare anche il traffico dati dello smart speaker. Questa procedura viene chiamata «sniffing».

Possiamo conoscere il traffico generato e quello ricevuto usando un dispositivo associato ad un account Amazon. Interessante è anche misurare il tempo di ascolto del dispositivo: dopo il comando di accensione «Alexa», se non viene pronunciato nessun comando, il dispositivo rimane in ascolto e connesso al server per circa 6 secondi. Lo smart speaker comunica con il server anche se l’audio è muto. E possiamo osservare che il dispositivo si connette ai server di Amazon non solo quando viene chiamato, ma anche in ulteriori intervalli regolari per scambiare delle informazioni. Non è però possibile risalire al dettaglio di queste informazioni perché restano crittografate.

Molto spesso l’acquisto di uno smart speaker richiede almeno un abbonamento. Ad esempio un abbonamento ad Amazon Prime, un abbonamento ad un servizio musicale, un abbonamento ad un servizio streaming video, oppure anche un abbonamento per l’acquisto di dispositivi “Amazon Certified”. Per fare acquisti direttamente tramite Alexa è richiesto l’abbonamento ad Amazon Prime. Per ascoltare musica è necessario un abbonamento ad Amazon Music, anche se si volesse utilizzare Spotify, Deezer, Napster è necessario avere un account premium. Sia che io ascolti musica tramite Amazon Music che con un servizio di terze parti, Alexa (Amazon) può potenzialmente risalire ai miei gusti e preferenze musicali. Lo stesso discorso vale per lo streaming di film e serie tv. Se chiedo ad Alexa di farmi vedere qualcosa su Prime Video (incluso con Amazon Prime), Netflix o altri servizi, Amazon potenzialmente può essere a conoscenza dei miei gusti e preferenze riguardo a film e serie tv. Dunque Amazon potenzialmente sa che facendo uno spot personalizzato con una determinata canzone e determinati soggetti può ottenere molto più facilmente la mia attenzione.

Tutti i dispositivi smart possono essere collegati agli assistenti vocali grazie ad una applicazione aggiuntiva; non tutti i dispositivi smart infatti sono nati con un’integrazione di assistenti vocali. Questo ha portato alla creazione di terze parti per interfacciare i dispositivi smart di qualche anno fa con gli assistenti vocali. In questi casi i nostri dati diventano noti anche a terzi.

Controllo dei dati: criticità

Un altro aspetto negativo dell’uso degli smart speaker è dato dall’impossibilità di cambiare la cronologia: tutto è già pronto e configurato.

Nel caso di Amazon, la cronologia audio delle registrazioni è imposta, posso solo eliminarla in seguito. Nel frattempo ci sono delle persone che ascoltano ogni giorno migliaia di ricerche vocali di utenti di tutto il mondo, per migliorare la qualità dell’assistente vocale, insegnandogli a rispondere correttamente alle diverse richieste. Lo smart speaker viene fornito così com’è, già preconfigurato: lo si accende, si imposta l’account e tutto funziona. Se smette di funzionare, sarà possibile riavviarlo staccando la spina. Non è possibile fare una diagnostica per capire il problema e le cause del malfunzionamento, inoltre non è possibile verificare se la configurazione scelta sia impostata correttamente: si tratta di una scatola chiusa con cui possiamo interagire soltanto con la voce. Dobbiamo fidarci che un oggetto «abbastanza stupido» capisca correttamente ciò che gli diciamo ed esegua quindi ciò che gli era stato chiesto.

Circa il 70% delle persone utilizza un sistema di blocco sul proprio smartphone, ma nessuno di questi può impostare un sistema di blocco sul proprio smart speaker.

Non si è mai totalmente al sicuro.

Che cosa possiamo fare con l’acquisto di Alexa?

La licenza per l’accesso ai servizi di Amazon è esclusivamente per uso personale e non commerciale. Non ci è consentito fare un uso derivato dei Servizi Amazon o dei loro contenuti, effettuare qualsiasi tipo di download o copia di informazioni dell’account a vantaggio di un altro rivenditore o utilizzare data mining, robots o simili dispositivi di acquisizione e estrazione dati. Attraverso l’uso commerciale quindi, i servizi di Amazon vengono utilizzati in maniera impropria.

Che cosa sanno di me?

Amazon raccoglie i nostri dati personali per fornire e migliorare costantemente i prodotti e i servizi. Tutti i contenuti presenti o resi disponibili attraverso i Servizi Amazon sotto forma di file audio, raccolta dati, sono proprietà di Amazon o dei suoi fornitori di contenuti.

Il dispositivo è capace di riconoscimento vocale di noti comandi di attivazione. I dati vengono inviati solo dopo la pronuncia della parola di attivazione. I dati non vengono elaborati in locale e il dispositivo interrompe la comunicazione con il server solo dopo aver terminato una specifica richiesta. I dati, durante il percorso dall’utente al server di Amazon, anche se intercettati, non possono essere letti. Ma tutti i dati e le informazioni sono condivisi con gli operatori di Amazon al fine di migliorare il servizio. Quindi, che cosa sanno di me? Come vengono usati i miei dati? Che diritti ho? Come posso interagire con il sistema ed esercitare i miei diritti?

Il GDPR (Regolamento generale sulla protezione dei dati) ha rivoluzionato la materia della protezione dei dati personali, ponendo l’accento sui doveri del Titolare e del Responsabile del trattamento, in ossequio al principio di «accountability», o responsabilizzazione.

Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato) rappresenta i dati personali della persona a cui si riferiscono.

Amazon è a conoscenza di tutti i dati da noi forniti, come età, indirizzo, nome e numero di telefono. Anche tutte le informazioni relative al pagamento, all’affidabilità creditizia, numero di partita IVA. È a conoscenza anche della nostra posizione, dei nostri indirizzi e-mail, dei nostri amici e anche di altre persone. Inoltre tutte le registrazioni vocali di Alexa appartengono ad Amazon, comprese le immagini e video conservati in relazione ai Servizi Amazon e configurazioni del dispositivo, comprese le credenziali del Wi-Fi.

Chi offre il servizio, inoltre, è a conoscenza di ulteriori dati raccolti, come ad esempio: Indirizzo IP, login, indirizzo e-mail e password; informazioni sul computer, sul dispositivo e sulla connessione; informazioni relative all’interazione con i contenuti, quali il download, lo streaming e i dettagli di riproduzione; metriche dei dispositivi e del Servizio Amazon; cronologia degli acquisiti e dell'utilizzo dei contenuti; i prodotti e/o i contenuti visualizzati o cercati e anche i numeri di telefono utilizzati per chiamare il numero del servizio clienti.

I nostri dati vengono usati per l’acquisto e la consegna di prodotti e servizi, per migliorare i Servizi Amazon, per fornire servizi locali, adempiere ad obblighi di legge, comunicare con il cliente. Inoltre per la pubblicità, per la prevenzione di frodi e rischi relativi al credito e per specifiche finalità per le quali si richiede consenso.

Quali sono i nostri diritti?

Noi abbiamo il diritto di essere informati, il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati e il diritto di opposizione. Possiamo interagire con il sistema ed esercitare i nostri diritti rivolgendoci al Servizio Clienti preposto, contattando il Data Protection Officer per ottenere informazioni dettagliate sui dati personali ed inoltrando una segnalazione all’Autorità di Controllo competente nel caso si sospetti un’irregolarità nel trattamento dei dati personali. Si può inoltre verificare l’aggiornamento dell’informativa e dei dati, inserendo, modificando o eliminando le informazioni che riteniamo più opportune.