Smart Assistant: Testimoni di un crimine

Il 25 Maggio del 2018 è entrato in vigore il *GDPR* in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali. Il legislatore ha voluto evidenziare l'esigenza, più che necessaria, di far fronte ai continui e potenziali rischi derivanti dall'uso non responsabile di quelle nuove tecnologie che oggi invadono l'ambiente reale, oltre che digitale.
Stiamo facendo riferimento soprattutto al "*Internet of Things*", massima espressione delle "cose" connesse alla rete che permettono le interazioni tra più utenti, con relativo scambio di informazioni. In maniera quasi inconsapevole l'utente viene violato, basti pensare alla profilazione e al trattamento illecito di dati. Questi sono tutti aspetti negativi, appartenenti alla stessa faccia della medaglia che le più grandi aziende presentano per invogliare l'acquisto di dispositivi Smart, dotati di Intelligenza Artificiale.
Si sta sempre di più espandendo l'allarme di un "*crimine*", che si commette o che si subisce, come la violazione di Privacy e Security e siccome queste sono la più grande vittoria dell'umanità, bisognerebbe tutelarle da violazioni o qualsivoglia azione illecita.
La tecnologia del riconoscimento vocale, per quanto possa sembrare giovane, discende da studi molto più antichi. Infatti già in epoca Medioevale Bacone, filosofo e scienziato inglese del tempo, prevedeva la tecnologia al servizio dell'uomo, come ricordato anche dal celebre aforisma tratto dall'opera "*I segreti dell'arte e della natura e confutazione della magia*": ***"Arriveremo a costruire macchine capaci di spingere grandi navi a velocità più forti che un'intera schiera di rematori e bisognose soltanto di un pilota che le diriga. Arriveremo a imprimere ai carri incredibili velocità senza l'aiuto di alcun animale. Arriveremo a costruire macchine alate, capaci di sollevarsi nell'aria come gli uccelli"***.
Non sempre i successi sperati sono giunti in tempi brevi, ma grazie all'incrollabile passione dei più grandi studiosi, e oggi tecnici e informatici si è giunti ai risultati ottenuti da colossi come Amazon con il suo progetto denominato Alexa. Le difficoltà che hanno dovuto affrontare i ricercatori dell'epoca erano legati al linguaggio, alla pronuncia, ai tempi di apprendimento poiché spesso la macchina era in grado di comprendere solo parole isolate o parole pronunciate in una determinata sequenza. Questo vero e proprio ostacolo allo sviluppo del Riconoscimento Vocale, è rappresentato da un limite *Hardware e Software* legato alla scarsa potenza computazionale, e da programmi informatici non ottimizzati o acerbi, se confrontati con quelli attuali.
Arrivati a questa consapevolezza, ci chiediamo: **perché l'intelligenza artificiale non si è mai sviluppata prima?**
Semplice appare la sua risposta: perché non esistevano computer con la potenza, la velocità e la quantità di dati come quelli odierni. Ed è solo grazie ai facilitatori dell'Intelligenza Artificiale che oggi i dispositivi hanno raggiunto questo livello di "Intelligenza".
Il primo facilitatore è rappresentato dalla legge di Gordon Moore[1], secondo la quale una maggiore velocità dà luogo ad una prestanza più intelligente. Il secondo facilitatore è la nuova legge di Moore, che segna la nostra era, secondo la quale maggiore sarà la digitalizzazione delle informazioni, maggiore sarà la quantità di dati disponibili all'interno del dispositivo e ciò rende più intelligente la macchina, giacché i dati forniscono agli algoritmi informazioni in modo tale da mantenerli allenati. Il

[1]Gordon Moore è uno dei fondatori della Intel. Nel 1965 osservò che la microelettronica si sviluppava con una velocità esponenziale ed elaborò questa legge che porta il suo nome. Secondo l'ipotesi di Moore il numero di transitori nei microprocessori sarebbe raddoppiato ogni 12 mesi e così fu.

terzo fattore è rappresentato dal **cloud computing**. Ci sono miriadi di definizioni per classificare questa nuvola informatica, ma per capire di cosa si tratta, basta soffermarsi sul perché della sua nascita. Quando nacquero i primi Personal Computer, l'utente aveva piena autonomia di elaborare tutto quello di cui necessitava, però si è compreso che il sistema informatico non poteva da solo portare a termine tutte queste mansioni. Per questo sono state elaborate delle reti LAN (Local Area Network) interne, alle quali erano collegati diversi dispositivi che venivano gestiti in maniera centralizzata. Cosa che accade quando usiamo Google Drive o Dropbox, che permettono, con la semplice connessione ad Internet, di avere sempre a portata di mano file e documenti su cui si lavora. Sono davvero tantissimi i progetti presentati già nel lontano 1846 da Joseph Faber, seguito dal VOCODER di Homer Dudley fino ad arrivare ai giorni nostri con **ALEXA**, lanciata da Amazon in Italia nel 2018.

Quindi è ben noto che la vera rivoluzione arriva con il **Machine Learning** e **l'Intelligenza Artificiale**, con i quali si passa da semplici sistemi di riconoscimento vocale a dei veri e propri assistenti vocali. La prima azienda fu Apple, la quale lanciò sul mercato nel 2011 Siri, suscitando nelle altre aziende una certa curiosità sulla realizzazione di simili dispositivi. Non passò molto tempo e sul mercato s'iniziò a respirare aria di concorrenza data dall'Assistente Google, da Amazon con Alexa, da Microsoft con Cortana e dalla Samsung con il suo Bixby. Per quanto intelligenti, questi assistenti vocali presentano ancora molti limiti che riguardano il confronto tra ciò che il dispositivo è in grado di ascoltare e quello che è presente nel database e questo rende spesso tali dispositivi inefficienti perché magari il comando vocale viene pronunciato con accenti diversi o con cadenze dialettali non conosciute allo smart speaker.

Gli orizzonti di applicazione dell'AI sono stati nettamente ampliati dall'ormai diffusa tecnologia dell'**Internet Of Things** che ha la capacità di raccogliere e di utilizzare dati provenienti sia da dispositivi di comune utilizzo quali il Personal Computer o Smartphone e sia da qualsiasi altro dispositivo oggi classificato come strumento quotidiano, a partire dai veicoli come la Classe A della Mercedes sino alla domotica della casa Smart.

Dall'analisi della terminologia si evince che qualsiasi oggetto e in maniera indiretta anche soggetto può essere predisposto ad una connessione che favorisce lo scambio di tante informazioni: basti pensare alla novità del braccialetto impiegato come anti-smarrimento dei bambini. Il bambino in questo caso sarà un "oggetto" dell'Internet, giacché il dispositivo *GPS* (Global Positioning System) contenuto all'interno del braccialetto consente la connessione tra l'oggetto fisico, ovvero il bambino, e l'oggetto digitale, ovvero l'applicazione sullo smartphone che riceve i segnali.

Questo è il caso della **tecnologia *RFID*** (Radio-Frequency Identification) che prevede oggetti dotati di un microchip con numero di serie, utile per l'identificazione. Queste etichette intelligenti, che possono essere sia attive che passive, ovvero legate o meno ad un'alimentazione, trasmettono segnali e risulta utile il loro impiego per la prevenzione della criminalità, per i vari tracciamenti e per le attività aziendali. È noto, quindi, che sono predisposti a questo tipo di connessione oggetti digitali che generano e trasmettono dati e oggetti fisici che, invece, non sono destinati a tale tipo di funzionalità, fuorché non vengono modificati mediante l'inserimento di tag o chip, diventando per tanto digitali com'è noto nell'identificazione a radiofrequenza sopraccitato. Però per poter parlare di connessione è necessario che un determinato oggetto abbia sia un proprio indirizzo *IP* (Internet Protocol address) utile all'identificazione in rete, sia la capacità di scambiare dati con altri oggetti dello spazio virtuale. In altri termini tale "cosa" deve abitare l'ambiente digitale e deve interagire all'interno di esso grazie all'uso di Internet che facilita questa comunicazione.

Come direbbe Antonio Spadaro: "***Il concetto chiave non è più la 'presenza' in rete, ma la 'connessione': se si è presenti ma non connessi, si è soli***". Il tutto ricorda il famoso dilemma

Shakespeariano “essere o non essere”, risolvibile cercando di analizzare con maggiore esattezza l’espressione “*Internet Of Things*”. Questo è tutto ciò che dà valore all’espressione “essere connessi”, che si distacca completamente da quella più semplice di “apparire connessi”. Un qualcosa che appare non è sempre così come si mostra. Un individuo può aprire un profilo social, un proprio blog, una propria pagina professionale ma la scelta dello stile del blog, dell’impostazione di una pagina non è sinonimo di connessione con gli altri, perché il tutto richiede continui aggiornamenti di dati e informazioni. Bisogna quindi saper utilizzare la rete, bisogna saper sviluppare al meglio gli aspetti vantaggiosi *dell’Internet Of Things*, come la digitalizzazione e l’automazione dei processi. È stato però uno sviluppo che ha reso inadeguata la normativa europea dinanzi a tutte le violazioni ed i rischi derivanti da trattamento illecito o da profilazione non consentita di dati personali. Ma gli aspetti negativi di questo sviluppo non si limitano ad una semplice, anche se in maniera molto relativa, inadeguatezza della disciplina, estendendosi anche alla violazione di Privacy e Security.
Proprio per i rischi che potrebbero derivare dall’uso improprio di dispositivi smart è giusto saper riconoscere un dispositivo *trusted* da uno *untrusted*. Un device può dirsi “fidato” quando svolge attività per uno specifico scopo per il quale viene progettato. Attualmente però appare davvero complicato ritenere “fidato” un dispositivo, in primo luogo perché usufruisce di una rete Internet e perché può essere facilmente violato ad esempio dall’inoculazione del virus **Trojan**. Possiamo dichiarare questo perché siccome tutto è potenzialmente incentrato sul mondo dei dati, si è sentito il bisogno di creare una rete sicura. Per tale ragione è stato progettato il modello **Zero Trust Network** di Kindervarg, che considera ogni dispositivo “non fidato”, compreso il servizio di rete. È un modello che va a sostituire l’architettura tradizionale di sicurezza di tipo perimetrale, considerata più debole.
Per le situazioni critiche presentate, bisogna effettuare un controllo di qualsiasi dispositivo che si connette prima di consentirgli effettivamente l’accesso, cui segue un’attenta analisi e registrazione di dati, garantendo così una **protezione completa di dati e risorse**. Questo modello è applicabile specialmente in presenza di sistemi iOS e Android che non sono forniti di Firewall[2], il cui concetto rinvia al *single packet authentication* per ridurre la superficie di attacco dell’host.

Ritornando ai protagonisti, gli Smart Assistant sono dei dispositivi programmati per soddisfare le richieste vocali di un utente. Pertanto sono in grado di ascoltare il comando vocale, di interpretare la richiesta e di rispondere, adattandosi agli impulsi vocali che gli stessi ricevono dagli utenti. La capacità di tali assistenti vocali nell’interagire con gli individui in maniera sempre più naturale è sicuramente frutto di sistemi basati sul Machine Learning e sull’Intelligenza Artificiale.
Quando parliamo di **Machine Learning** o apprendimento automatico, facciamo riferimento a una branca dell’informatica legata all’Intelligenza Artificiale. Per definirlo in maniera davvero semplice possiamo provare ad intendere per Machine Learning un insieme di meccanismi che favoriscono un continuo apprendimento, grazie all’attività di algoritmi che aiutano il dispositivo a prendere una decisione piuttosto che un’altra, sulla base di quanto la macchina ha appreso nel tempo. A seconda del tipo di algoritmo utilizzato, è possibile riconoscere tre modalità di apprendimento: quello **supervisionato** che fornisce al sistema delle nozioni per creare un database di informazioni ed esperienze già codificate, con dei modelli/esempi confezionati. In altri termini la macchina impara da questi modelli dove sono indicati degli input e dei risultati corretti. Questo aiuta la macchina ad attingere dal suo stesso database le informazioni utili per rispondere a determinati comandi in maniera appropriata; l’apprendimento **senza supervisione**, invece, rilascia maggiore libertà alla macchina nella scelta della risposta migliore ad un problema, di cui però non conosce l’utilizzo. Questo accade

[2]Funge da filtro, infatti va a posizionarsi tra la rete interna e quella esterna, consentendo o bloccando il traffico indesiderato, potenzialmente rischioso per quel sistema. È una misura di sicurezza per i sistemi informatici.

perché le informazioni non sono codificate, quindi appaiono nuove alla macchina, che si troverà a dover lei stessa catalogare in maniera intelligente tutte le informazioni apprese e i risultati migliori ottenuti. Legato all'apprendimento non supervisionato vi è l'esperienza Netflix, nata come Machine Learning via posta. L'azienda Netflix nasce nel 1997 come attività di noleggio di DVD e videogiochi. Ogni utente poteva prenotare via internet il DVD e questo veniva poi successivamente spedito a casa. Dopo poco tempo ritornava al mittente con la relativa recensione del contenuto con un giudizio su di una scala da uno a cinque. Tutti i risultati ottenuti furono in grado di rendere l'azienda più prestante circa i suggerimenti dei migliori film agli utenti. La capacità di apprendimento è data dall'analisi delle informazioni in possesso, che ha permesso a Netflix di costruire un business intorno ai risultati ottenuti.

Sono proprio le capacità di suggerimento che rendono una macchina più intelligente di un'altra, perché questo è sintomo di aver appreso le abitudini, le abituali ricerche e gli interessi dell'utente.[3]

Infine vi è l'apprendimento **per rinforzo**, quello più complesso, poiché le macchine vengono dotate di sistemi che permettono l'apprendimento anche in base alle circostanze ambientali. Basti pensare alle automobili, dotate di sensori o di localizzatori GPS che intendono fornire al dispositivo degli input circa l'ambiente circostante, in modo da rendere la macchina in grado di rispondere a quelle specifiche condizioni.

Nella vita di tutti i giorni ogni individuo, in possesso di uno smartphone, è legato ad un dispositivo che apprende dalle azioni quotidiane. Ma non solo gli smartphone sono capaci all'apprendimento automatico, anche una semplice ricerca web consente di raccogliere e archiviare grandi quantità di dati (*Big Data*) relative alle nostre abitudini e di proporre delle inserzioni pubblicitarie ad hoc, per soddisfare le esigenze degli utenti.

La raccolta di questi dati è comunque disciplinata dal Regolamento Europeo del 2018.

L'apprendimento automatico mira quindi al miglioramento sempre più profondo del dispositivo, sia sulla base di nuove conoscenze da inserire nel database e sia delle conoscenze già codificate, che se migliorate possono contribuire a rendere utilizzabile la macchina per scopi nettamente più specifici. Il Machine Learning rappresenta l'aspetto teorico dell'apprendimento automatico, ma nella realtà le aziende che archiviano dati utilizzano il Data Mining[4]. Quest'ultimo è l'applicazione pratica (Hardware e Software) dell'Intelligenza Artificiale (Machine Learning e Deep Learning) che consiste nell'elaborazione ed analisi di dati di grandi dimensioni. Questo forte sviluppo potrebbe rendere tali macchine troppo intelligenti, sottraendo all'uomo la libertà e la facoltà di scegliere. A tal proposito si sta diffondendo rapidamente questo timore, così come dichiarato anche dal professore Pedro Domingos, esperto di Machine Learning e Data Mining: "***La gente ha paura che i computer diventino troppo intelligenti e dominino il mondo, ma il vero problema è che pur essendo ancora troppo stupidi l'hanno già conquistato***".[5]

Un timore che va a toccare ambiti sociali e personali come il lavoro, in quanto tutte le aziende potrebbero essere automatizzate, eliminando la presenza dell'uomo e della sua forza. In effetti già oggi si parla di automazione parziale che può comportare notevoli vantaggi nelle vendite e nello sviluppo interno aziendale.

Quando invece viene usato il termine Intelligenza Artificiale, ci si riferisce all'abilità, simile a quella della mente umana (grazie alla presenza del Deep Learning), del sistema di problem solving e di

---

[3] N. POLSON, J. SCOTT, "*Numeri intelligenti. La matematica che fa funzionare l'intelligenza artificiale di Google, Facebook, Apple & Co*", Milano, DeA Planeta Libri, 2019.

[4] È l'insieme di tecniche, automatizzate o semi-automatizzate, che consentono l'estrazione di informazioni da grandi quantità di dati. Si parte da informazioni criptiche e senza ordine e si arriva ad una conoscenza impiegabile in qualsiasi ambito.

[5] http://www.intelligenzaartificiale.it/machine-learning/ .

svolgimento di tutte le attività. In maniera più tecnica, si definisce l'AI come un insieme di algoritmi. Ogni algoritmo è costituito da semplici istruzioni, quindi è noto che preso singolarmente un algoritmo non può rendere un dispositivo intelligente. E' proprio l'insieme che permette il lavoro tipico degli assistenti vocali. Basti pensare che quando l'utente esprime un comando vocale vi è un algoritmo che converte il segnale vocale in segnale digitale, vi è poi un algoritmo che lo traduce, un altro ancora che raggruppa i fonemi in parole, altri si occuperanno di tradurre la domanda per offrire la risposta elaborata in maniera logica da altri algoritmi e si termina il ciclo con un ultimo algoritmo che invece riproduce in suono quello che è stato elaborato. È quindi proprio vero che l'unione fa la forza.
Appare ovvio che la mente umana non potrà mai essere clonata da un dispositivo super tecnologico, perché il nostro cervello è capace di trasformare ciò che è un'idea in tante parole. Si vedano le difficoltà che spesso incontriamo quando non riusciamo a chiamare per nome un determinato oggetto e quindi lo indichiamo oppure ne diamo un'identificazione diversa. È il nostro cervello che riesce poi a creare una correlazione nome - oggetto diversa, perché comprende o semplicemente perché vede, e associa poi correttamente. La stessa cosa non può dirsi per gli assistenti vocali che invece hanno un funzionamento simile a quello umano ma davvero molto limitato. In altri termini quello che ci differenzia dagli Smart Assistant è la flessibilità.

Prendiamo in analisi uno dei più grandi assistenti vocali prodotto da **Amazon** con nome e voce femminile: ***Alexa***. Viene lanciata nel 2014 insieme ad Amazon Echo, ma solamente nel 2018 è stata rilasciata in lingua italiana. Alexa è nata sotto l'ispirazione del sistema di comunicazione presente all'interno della navicella spaziale di "*Star Trek*". La progettazione di Amazon Alexa è frutto del forte desiderio di servire l'utente in ogni attività giornaliera, per cercare di migliorare la vita, di offrire momenti di relax e gestire ogni cosa con dei semplici comandi vocali. Dopo Alexa non ci sarà più timore di doversi alzare dal divano per recuperare il telecomando troppo lontano, basterà un semplice comando vocale e il relax assume tutto un altro sapore. Alexa è il nome che identifica gli algoritmi che si trovano all'interno dell'Hardware. Gli smart speaker di Alexa si presentano come degli altoparlanti, quindi dotati di casse e microfoni, sono indipendenti in quanto contengono al loro interno un proprio processore. Visualizzando un Amazon Echo Dot Hardware, è possibile individuare al suo interno: un Processore 64-bit quad-core, 4GB di storage dove si visualizzano i dati utente, i dati dell'account e i File Log[6], Chip Wi-Fi/Bluetooth per la connessione alla rete Internet, Chip di gestione dell'alimentazione, Memoria per il caching dei dati e per l'aggiornamento del software[7].
Una volta acquistato il dispositivo si procede con la configurazione dello stesso, tramite delle applicazioni scaricabili sia sui sistemi Android sia su quelli iOS, a differenza di quanto accade per Siri, invece progettata per il solo funzionamento sui sistemi iOS. È altrettanto necessario munirsi di un relativo account con il quale identificarsi tramite app. Successivamente si procede con l'accensione di tale dispositivo, che si illuminerà nella parte superiore e una voce interagirà con l'utente in tante lingue. Terminato il download dell'applicazione, ci si trova dinanzi ad un'interfaccia con cinque icone tra cui il tasto Alexa, che consente di interagire con il dispositivo, attendendo i comandi vocali. Ora tutto ciò che l'utente chiede ad Alexa, viene registrato e inviato al cloud di Amazon dove avviene l'elaborazione della richiesta. Il cloud di Amazon può procedete autonomamente all'elaborazione della risposta, o può interfacciarsi con cloud esterni per quella che noi definiamo una ricerca più specifica. Tutte le registrazioni contenute all'interno del cloud sono utili per i miglioramenti, e per lo sviluppo

[6] Sono file che contengono informazioni circa tutte le attività che sono state svolte, le varie modifiche, i vari accessi.
[7] Intervento intitolato "*Da Google Home ad Amazon Alexa: indagini informatiche sui personal assistant*" all'IISFA Forum (17-18 Maggio 2019) del Dott. Stefano Fratepietro, CEO Tesla Consulting srl, Director Industrial Leader Be Consulting S.p.A., Consulente di Informatica Forense, Docente UniBO, UniMoRE, STELMILIT, CINEAS, FAV, Project Leader – DEFT Linux, Since 2005.

delle capacità di riconoscimento degli accenti, dei dialetti e dei vocaboli utilizzati così da diventare sempre più prestante. È utile precisare che quello che viene inviato è tutto ciò che segue la parola di attivazione "Alexa", perché è in quel momento che il dispositivo si mette in ascolto. La parola di attivazione può anche essere modificata, ad esempio perché si usano più dispositivi intelligenti Alexa e quindi si cerca di differenziare i comandi. La scelta della modifica può avvenire solo tra: "Echo", "Computer" oppure "Amazon".[8]
Appare quindi lecito chiedere a cosa possa servire l'app scaricata, dato che il dispositivo si attiva anche senza premere il tasto presente tra le cinque icone dell'applicazione. È semplice rispondere a tale curiosità, poiché l'applicazione ci permette di rivedere ogni richiesta/registrazione effettuata accedendo alla cronologia di Alexa. Infatti vi sono due registri, uno che raccoglie le sole richieste elaborate e l'altro con la cronologia delle intere azioni richieste. La cronologia consente all'utente di valutare anche il range temporale della richiesta.[9] D'altro canto Alexa con l'applicazione ci permette di cancellare anche quelle registrazioni indesiderate. Per quest'ultima funzione è possibile procedere anche con un comando vocale e Alexa eseguirà la cancellazione autonomamente. L'azione di cancellazione effettuata verrà comunque visualizzata, poiché non risulta possibile non lasciare traccia di quanto si compie. Si badi che la cancellazione delle registrazione potrebbe peggiorare l'esperienza con Alexa e questo perché, tutto ciò che il dispositivo apprende viene utilizzato per il suo miglioramento. I dispositivi Amazon Alexa sono governabili o da centraline completamente online oppure da hub che necessitano di installazione in loco, perché non tutti i dispositivi possono collegarsi alla rete internet per funzionare.

Come già precedentemente dichiarato, questa tecnologia del riconoscimento vocale, applicata ai dispositivi smart comporta numerosi vantaggi, ma altrettante conseguenze come quella di esporre l'utente a rischi quali violazione della Privacy e della Security. Lo sviluppo e la diffusione della smart home e di questo continuo aggiornamento di dispositivi, che tentano in maniera sempre così insistente di clonare gli esseri umani, di pensare come loro, di comprendere gli stati d'animo e di interagire con gli utenti in maniera sempre più naturale, sta comportando una sempre più semplice sostituzione dell'uomo con le macchine. Tutto questo è stato confermato dalle statistiche registrate, che vede l'impiego di tali dispostivi nell'85% delle aziende, per il servizio clienti. Si nota che sono tecnologie utilizzate oltre che in ambito privatistico anche sul fronte delle aziende e di tutti servizi aperti al pubblico, per minimizzare risorse e aumentare i vantaggi. La **minaccia alla Privacy e alla Security** nasce dalla circostanza che acquistare uno Smart Assistant comporta la presenza di un dispositivo in continuo ascolto, in quanto per recepire la parola di attivazione deve essere sempre sull'attenti. È meglio precisare che le registrazioni senza aver ufficialmente consentito l'ascolto non sono inviate al cloud, ma potrebbero presentarsi delle situazioni in cui l'ascolto può essere attivato dalla pronuncia di una parola simile a quella di attivazione, consentendo al dispositivo l'esecuzione di determinate attività. Infatti nella cronologia è possibile visualizzare le richieste non comprese, spesso causate perché Alexa ha erroneamente captato la *Key –Word* e si è messa in ascolto. Per far fronte a questi problemi si potrebbe disattivare il microfono quando non si utilizza il dispositivo, ma ciò comporta un successivo approccio fisico con lo stesso, per abilitarlo nuovamente, il che è poco pratico.
Per tale ragione è stato segnalato un **progetto** Open Source [10] chiamato "***Alias***" che viene

[8] https://www.punto-informatico.it/speciali/amazon-alexa/ .
[9] Intervento intitolato "*Da Google Home ad Amazon Alexa: indagini informatiche sui personal assistant*" all'IISFA Forum (17-18 Maggio 2019) del Dott. Stefano Fratepietro, CEO Tesla Consulting srl, Director Industrial Leader Be Consulting S.p.A., Consulente di Informatica Forense, Docente UniBO, UniMoRE, STELMILIT, CINEAS, FAV, Project Leader - DEFT Linux, Since 2005.
[10] In italiano "*sorgente aperta*" che quindi lo rende modificabile o migliorabile da parte di chiunque, in riferimento ad un tipo di software o al suo modello di sviluppo o distribuzione. Un esempio potrebbe essere

configurato mediante una connessione ad Internet e continua a funzionare in modalità offline. Alias va a generare un rumore che non consente all'assistente vocale di percepire la conversazione tra gli utenti e può essere disattivato con la pronuncia della parola di attivazione "*Alias*", permettendo così la comune interazione con lo Smart Assistant.

Questi dispositivi possono essere violati nella loro Security, danneggiando in maniera rilevante l'utente. Basti pensare ai bug di malfunzionamento che potrebbero causare ad esempio l'attivazione del microfono in maniera inconsapevole all'utente, la violazione di altri dispositivi connessi a Internet, utilizzando da tramite l'assistente vocale e infine avere accesso ai comandi della casa smart, configurando una vera e propria violazione di sicurezza. In merito a quest'ultimo rischio che potrebbe verificarsi, si ricordi la famosa scena della serie "*Mr. Robot*", nella quale viene hackerata la casa completamente tecnologica dell'avvocato Susan Jacobs.[11] Per quanto enfatizzata come scena, rappresenta uno dei tanti rischi che si potrebbero verificare in futuro con il continuo sviluppo di tali tecnologie. Questa visione futuristica va a sostituirsi completamente alle antiche tecniche di effrazione e di violazione di domicilio. I ladri di domani potranno semplicemente accedere a dei computer che gestiscono i comandi della casa e violeranno la nostra Privacy e Security. Sicuramente quello che riuscirebbe a tenere lontani i rischi è un'efficiente configurazione, infatti basterebbe separare i dispositivi smart della casa dal resto, in quanto un attacco al singolo dispositivo, se la rete non è segmentata, può causare una violazione di tutto ciò che è a essa collegata. Sarebbe buona pratica evitare di memorizzare dati di carte di credito, per effettuare pagamenti mediante comando vocale, evitare di memorizzare password, evitare di codificare comandi come "apri la porta di casa" o "attiva le telecamere" poiché ci si espone a un maggior rischio di violazioni, in quanto chiunque potrebbe dettare questo comando all'assistente. Inoltre risulta consigliabile la creazione di un account nuovo per la configurazione del dispositivo, cancellare le registrazioni contenenti dati sensibili[12], utilizzare reti coperte da password e impostare come unica voce di riconoscimento quella dell'utente, proprio per evitare interferenze di terzi. [13]

In conclusione per quanto vantaggiosi nello svolgimento di attività quotidiane, la tecnologia degli Smart Assistant ha trascinato con sé numerosi aspetti critici.

Tra i tantissimi casi di violazioni, possiamo ricordare il **caso** di una coppia americana di **Portland**, che ha subito una vera e propria violazione della privacy, mentre si stava intrattenendo in una conversazione privata. L'audio di questa conversazione è stato inviato a un contatto scelto tra quelli presenti in rubrica. La coppia, a seguito della segnalazione ricevuta proprio dalla persona che aveva ricevuto quel file audio, si è interessata di contattare Amazon per investigare sull'accaduto. Amazon ha replicato dichiarando che la progettazione Alexa mostra davvero tanta sensibilità nell'ambito della privacy e che molto probabilmente tale conversazione risulta registrata, perché è stata pronunciata una parola con lo stesso suono di quella di attivazione e questo ha consentito l'ascolto del dispositivo, che ha poi inviato questa a un contatto in rubrica poiché aveva appreso questo comando dalla stessa conversazione, con la relativa conferma. La coppia ha affermato di non aver sentito Alexa annunciare l'inoltro del file e questo rappresenta un grave problema, che potrebbe comportare una sanzione.[14]

Non sono pochi i casi denominati "***Creepy Alexa Stories***", ovvero post pubblicati da utenti su anomalie del dispositivo Alexa. Infatti numerosi utenti hanno segnalato risate provenienti dall'assistente vocale, in maniera autonoma quindi senza alcun comando. Episodi davvero da brividi.

GNU/LINUX, MOZZILLA FIREFOX.

[11] https://www.youtube.com/watch?v=aAj8zHOEfiI.

[12] I dati sensibili sono dati che comunicano informazioni circa l'orientamento sessuale, le convinzioni politiche e religiose, sono inclusi anche i dati biometrici e genetici, vedi Articolo 9 GDPR.

[13] https://www.agendadigitale.eu/cultura-digitale/assistenti-vocali-tutelare-privacy-e-security-quali-soluzioni/.

[14] https://www.kiro7.com/www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974 .

La spiegazione? Semplice. Secondo il colosso Amazon, Alexa fraintende l'ordine "*off*" di spegnimento delle luci con la parola "*laugh*" ovvero la risata e questo genera una risposta in base a ciò che il dispositivo ha appreso. Non per forza questi episodi scaturiscono da fraintendimenti del linguaggio, poiché essendo sempre in ascolto tali dispositivi sono sensibili anche ai rumori ambientali e quindi percepire come comandi semplici suoni, simili alla pronuncia di parole.[15]
Le violazioni di Alexa stanno interessando anche la legge sulla protezione della privacy e la tutela dei minori, la **legge COPPA**[16]. La legge prevede infatti il consenso dei genitori circa il trattamento e il divieto di trattare dati non idonei allo scopo del trattamento stesso.
Ovviamente Amazon ha respinto tale accusa perché ha affermato che i dispositivi non raccolgono dati illegalmente e che quindi possono dirsi conformi alla normativa della legge COPPA, molto spesso abbreviata in COPA. Un gruppo di utenti ha coinvolto la FTC chiedendo l'apertura di un'inchiesta a riguardo.
Ulteriore violazione che vede protagonista Alexa è il **caso** di **Berlino** in cui si è configurata la diffusione di circa 1700 conversazioni registrate con il dispositivo, all'utente sbagliato. L'utente aveva chiesto ad Amazon le conversazioni effettuate con l'assistente vocale e fin qui appare tutto conforme con la normativa del GDPR, quello che non è incluso è la violazione commessa. Amazon, infatti, ha inviato all'utente, in risposta alla sua richiesta, le conversazioni di un altro utente, violando così la privacy di quest'ultimo. Ha cercato di tamponare la violazione, disattivando il link che permetteva il download delle registrazioni, ma questo apparve essere inutile, in quanto il soggetto, a seguito di un reclamo al servizio clienti, aveva già scaricato il file. In questo caso la prima violazione del GDPR colpisce la privacy. Ma è importante soffermare l'attenzione anche su altre violazioni commesse da Amazon, ovvero quella relativa alla mancata notifica della violazione sia all'autorità competente entro le 72 h e sia all'interessato, che è rimasto inconsapevole che tutti i suoi dati, tutte le informazioni e i comandi codificati erano nelle mani di un altro soggetto. Ci si è chiesti, in ragione di tale violazione, se fosse legittimo conservare le registrazioni e quindi esporsi al rischio di diffusione illegittima di conversazioni, violando così la privacy. Amazon a sua discolpa ha dichiarato che le conversazioni vengono conservate perché sono di aiuto ad Alexa nel processo di evoluzione e sviluppo.
Sicuramente il timore di altre violazioni è molto alto e questo classifica questo caso come uno dei tanti che potrebbero verificarsi, il tutto in contrasto con quanto dichiarato da Amazon, che ha definito questa violazione come il frutto di un errore umano, un caso in altre parole isolato e che sono state adottate tutte le misure di sicurezza idonee a rendere tale dispositivo più sicuro per gli utenti.
Sicuramente in risposta a tale violazioni, Amazon non potrà tirarsi indietro.

Sorge al quanto spontanea la curiosità di sapere chi gestisce le registrazioni, dove queste vengono conservate, per cosa vengono utilizzate e la relativa gestione della profilazione di dati contenuti all'interno delle stesse. Secondo Martorana, DPO certificato, infatti: "***Lo strumento principale previsto dal* GDPR *in questo senso è l'informativa, il documento che prevede esplicitamente che siano indicati al soggetto interessato del trattamento alcuni elementi chiave: chi raccoglie, tratta e decide le finalità di utilizzo dei suoi dati, con quale scopo e modalità, quali siano effettivamente i soggetti che potrebbero conoscere tali dati (diversi dal Titolare del trattamento), quale sia il tempo di conservazione di tali dati prima della loro cancellazione (prevista dal regolamento), quali i sistemi di sicurezza apprestati e i diritti esercitabili (dove e***

[15] https://www.vice.com/it/article/neqg9q/bug-amazon-alexa-riproduce-risata-random.
[16] Legge federale approvata nel 1998 con l'obiettivo di proteggere i minori dal materiale di natura sessuale, o qualsiasi materiale ritenuto dannoso che proveniva dal web. Fu bloccata fino al 1999 nei tribunali perché considerata troppo vaga o addirittura incostituzionale. In seguito nel 2006 sono stati chiesti i database di ricerca Google (rifiuta di rispondere a tale richiesta) per dimostrare l'importanza di rendere applicabile tale legge.

come), fra cui il diritto all'oblio".[17] Un intervento in linea con quanto stabilito nell'articolo 5 del GDPR, secondo il quale ogni trattamento deve avere una corretta base giuridica quale adempimento degli obblighi contrattuali, interessi legittimi del titolare e il consenso dell'interessato, espresso liberamente e a seguito dell'informativa che mette a conoscenza l'interessato di eventuali trasferimenti dati, dell'identità del titolare e del responsabile che si occuperanno del trattamento, del periodo di conservazione dei dati. Quest'informativa deve essere scritta o elettronica e soprattutto deve essere semplice, evitando molti tecnicismi. Ogni trattamento deve avere ad oggetto dati pertinenti e adeguati allo scopo (*minimizzazione dei dati*) e proprio per mantenere questa adeguatezza, devono essere costantemente aggiornati (*esattezza dei dati*), il ché implica la cancellazioni di quelli che non risultano più utili per lo scopo del trattamento. Per concludere occorre ritenere che la conservazione dei dati può estendersi solo entro i limiti previsti per quel trattamento (*limitazione della conservazione*). Questi appena evidenziati solo i principi applicabili al trattamento.

Prima di analizzare le norme del Regolamento Europeo, occorre capire come si è arrivati a questo GDPR.
Quando la riservatezza e la sicurezza dei dati personali vennero identificate come diritti fondamentali, più vicini ai diritti della persona, si è sentita l'esigenza di una legislazione che fosse in grado di tutelarle. Tra le **fonti in materia di protezione dati** è bene sapere che la Dichiarazione Universale dei Diritti dell'Uomo del 1948, con il suo articolo 12 ha ispirato sia l'articolo 8 della CEDU del 1953 dove è sancito il principio secondo cui ogni uomo ha diritto al rispetto della sfera privata e quindi qualsiasi intervento o interferenza deve essere motivata per uno scopo legittimo e sia l'articolo 17 del Patto Internazionale sui Diritti Civili e Politici del 1976. Ma oltre a fonti comunitarie ricordiamo la Costituzione Italiana del 1948 che disciplina con la lettura degli artt. 14 e 15 sia l'inviolabilità del domicilio e sia l'inviolabilità della corrispondenza, senza però alcun accenno ai sistemi elettronici, in quanto al tempo della stesura non esistevano problemi legati alla protezione dati contenuti all'interno di dispositivi informatici. Per concludere alla base di tale disciplina vi è anche la Carta di Nizza del 2000 che con gli artt. 7 e 8, regola rispettivamente il rispetto alla vita privata, familiare e la corrispondenza e la protezione dei dati che dovranno essere trattati con assoluta lealtà. Si iniziò però a parlare realmente di protezione di dati con la Convenzione 108 emanata dal Consiglio d'Europa nel 1981,vincolante sia per gli stati membri del Consiglio e sia per quelli non appartenenti, in quanto la Convenzione era aperta alla firma su invito. Proprio per il carattere della vincolabilità doveva contenere un lessico molto semplice e chiaro per permettere a chiunque di comprenderne il significato. Questa però presentava un limite, ovvero quello di non prevedere né l'istituzione dell'autorità di protezione (DPA), né prevedeva la limitazione del flusso di dati a paesi terzi e per colmare queste lacune è stato affiancato a questa Convenzione il Protocollo Addizionale del 2001 che regolava la previsione dell'autorità di protezione e la limitazione del trasferimento dati a paesi terzi solo se questi erano in grado di garantire un'adeguata tutela dei dati. Inizialmente si è sempre pensato che tale disciplina della Convenzione fosse da sola sufficiente a regolare in maniera omogenea la materia, ma così non fu e proprio per questo il Parlamento e il Consiglio Europeo hanno emanato la direttiva 95/46/CE[18] che diede vita in Italia alla legge 675/1996 [19], che ha diffuso la consapevolezza dell'esistenza di una sfera degna di tutela dell'individuo. La sua scarsa forza applicativa ha favorito la nascita del "Codice Privacy", ovvero la legge 196/2003. Questo codice si è interessato di interrompere l'atteggiamento indifferente di tutti coloro che rifiutavano di adeguarsi alla normativa in materia Privacy. Anche la direttiva presentava il

[17] https://www.01net.it/assistenti-vocali-privacy-parere-legale/.
[18]Era il principale strumento giuridico dell'Unione Europea in materia di protezione dei dati in,https://protezionedatipersonali.it/direttive-europee.
[19] Legge sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

carattere vincolante con la sola differenza di essere applicabile ai soli stati membri del Consiglio. Oltre a tale direttiva, considerata *lex generalis*, vi è anche una direttiva in materia di protezione dei dati in ambito di telecomunicazioni, la 97/66/CE sostituita dalla direttiva e-Privacy 2002/58/CE. Questa direttiva è individuata come *lex specialis* e quindi complementare alla direttiva madre 95/46/CE. Sorge però il dubbio circa la complementarietà della direttiva e-privacy con il Regolamento Europeo che ha sostituito la direttiva madre. È stata proposta nel 2017 la sostituzione della direttiva 2002/58/CE con un Regolamento e-Privacy, per poter camminare in maniera conforme al passo del GDPR. La proposta è ancora oggetto di dibattiti, ma possiamo anticipare che tra i tanti obbiettivi vi è quello di aumentare la privacy nell'ambito delle comunicazioni elettroniche di whatsapp, per garantire una maggiore sicurezza come quella già raggiunta dai tradizionali operatori di telefonia; e ancora una disciplina per la protezione antispam, per bloccare e vietare le comunicazioni elettroniche indesiderate. Comune alle direttive è la materia che regolano che deve essere limitata a quelle di competenza dell'UE, inoltre per poter essere vincolanti, necessitano di essere recepite all'interno degli ordinamenti e questa manovra rilascia maggiore discrezionalità agli stati, con conseguente disomogeneità nella disciplina. Proprio per armonizzare la disciplina a livello europeo è stato studiato e creato il nuovo Regolamento Europeo GDPR, che è entrato in vigore il 25 Maggio del 2018. Proprio per introdurre l'argomento, all'articolo 1 del GDPR viene visualizzata la sua duplice finalità. Da un lato si muove per tutelare l'autonomia individuale con la protezione dei dati personali, dall'altra invece si muove per garantire un libertà economica e favorire la libera circolazione dei dati che potrebbe portare ad una patrimonializzazione del dato inteso come informazione del soggetto. È ovvio che questi due orientamenti devono essere mantenuti in perfetto equilibrio grazie ad un bilanciamento di interessi.

Perché è importante il nuovo Regolamento Europeo?

Il Regolamento ha introdotto un **maggiore controllo sui dati**, passando da una visione proprietaristica del dato a una visione di controllo che favorisce la libera circolazione dei dati con il diritto dell'interessato di conoscere come e per cosa viene utilizzato quel dato. Questo controllo sui dati ha sviluppato negli utenti una maggiore fiducia nel sistema digitale.

Altra novità del GDPR è il Data Protection Officer, cosiddetto **DPO** che viene designato così come stabilito dall'articolo 37 del GDPR, come figura di controllo affinché il Regolamento venga messo in pratica e funzione di garanzia del trattamento dati, in quanto può fungere da punto di contatto tra titolare e Garante e titolare e interessato (che ha quindi maggiore controllo sul trattamento). Proprio con la designazione di tale figura si è innalzato davvero di tanto il livello di sicurezza.

Altra novità è la **valutazione d'impatto**. Il titolare del trattamento ex dell'articolo 35 del GDPR deve effettuare tale valutazione quando vi è elevato rischio di Data Breach. Ma cosa intendiamo per elevato rischio? C'è chi lo lega all'elevata possibilità che possa verificarsi il danno, chi lo intende come elevato danno che ne conseguirebbe e altri che invece si riferiscono all'elevata forza penetrante della violazione. Quello che si consiglia è di valutare l'elevato rischio sulla base della natura, del contesto e delle finalità del trattamento. Questa DPIA è obbligatoria per quei trattamenti automatizzati con effetti giuridici che possono riflettersi ed incidere sulle persone fisiche, per quei trattamenti su larga scala di dati relativi a condanne penali, e ancora per situazioni di sorveglianza sistematica all'interno di luoghi pubblici. Mentre non è obbligatoria quando non vi è elevato rischio, quando il trattamento ha le medesime finalità di un altro trattamento già oggetto di valutazione e quando è stato già sottoposto alla valutazione dell'autorità di controllo prima dell'entrata in vigore del Regolamento, salvo modifiche di finalità dello stesso. Prima di svolgere un qualsiasi trattamento, il titolare per individuare in maniera anticipata la presenza di taluni rischi procede con una valutazione non formale. Se vi è esistenza di questo rischio si procede con una valutazione formale che se conforma il rischio obbliga il titolare a

consultare il Garante che procederà con dei propri poteri d'indagine ex dell'articolo 58 del GDPR. Questo aspetto sottolinea la differenza tra codice privacy e regolamento. Nel codice privacy si parlava di verifica preliminare, mentre nel Regolamento parliamo di consultazione preventiva che può comportare una sottostimazione del rischio, in quanto il titolare muovendosi autonomamente nell'individuazione del rischio, potrebbe non efficacemente individuarlo, lasciando al caso la risoluzione, senza poter ricevere un parere del Garante (che dovrà rispondere entro le 8 settimane, prorogabili per altre 6 settimane. Se non vi è risposta si procede per silenzio-assenso).
La vera grande novità del GDPR è la sensibilizzazione al concetto di **responsabilità e accountability**. Il primo è legato al "dover agire", ovvero obbligo di fare qualcosa, il secondo è legato al "rendersi conto di quanto fatto e rispondere di quanto prodotto". Entrambi concetti fondamentali per una buona governance e per un buon modo di far fronte ai problemi circa il trattamento dati. Questo principio di accountability va a confermare l'orientamento del Regolamento alla mitigazione del rischio, a dimostrazione anche di aver aderito al **RISK - BASED APPROACH** che impone quindi al titolare di assumere un atteggiamento proattivo, di assorbire questa capacità di valutazione anticipata di situazioni critiche prevedibili e possibili. Deve per tanto dimostrare formalmente di avere il consenso di trattare taluni dati, ma deve anche sostanzialmente agire nell'interesse del soggetto, tutelandolo dalle violazioni, proteggendo quindi i suoi diritti e le sue libertà.
Il soggetto secondo la normativa del GDPR ha la possibilità di esercitare propri diritti, così come disciplinato nel Capo del Regolamento, quali ad esempio: Diritto di accesso dell'interessato ex dell'articolo 15, Diritto di rettifica ex dell'articolo 16, Diritto all'oblio o alla cancellazione come disciplinato dall'articolo 17, Diritto di opposizione sancito dall'articolo 21 del regolamento UE.

Si fa fronte, pertanto, al problema delle violazioni causate da un uso non corretto di tali assistenti vocali, leggendo attentamente l'informativa privacy dell'azienda produttrice, proteggendo la rete che ridurrebbe l'attacco informatico. È meglio precisare che nella normativa GDPR non ci sono norme che menzionano esplicitamente assistenti vocali intelligenti però implicitamente è possibile ricondurre l'Intelligenza Artificiale all'articolo 22 del GDPR[20] che sancisce l'esigenza, per ragioni legali, di richiedere al consumatore un consenso esplicito all'adesione di termini e condizioni. Dalla lettura di questo articolo è possibile evincere il diritto di NON essere sottoposto a decisioni automatizzate, compresa la profilazione, che possano incidere sulla sfera personale del soggetto. Però più che diritto, è consigliabile intenderlo come divieto del titolare di procedere, perché se fosse stato un vero e proprio diritto, l'interessato poteva pretendere l'intervento umano nella decisione, eliminando l'automazione della stessa e quindi la formula della disposizione avrebbe assunto un carattere meno negativo. Dopo aver analizzato il quadro completo, inclusa tutta la normativa inerente alla disciplina, è necessario aprire una parentesi circa l'estensione dell'applicabilità dell'Intelligenza Artificiale alla fase decisionale. L'Unione Europea sembra essersi fatta carico del "problema" e ha emanato la "***Carta Europea per l'uso dell'Intelligenza Artificiale nei sistemi giudiziari***" [21]. Questa Carta contiene tutti i principi fondamentali che devono essere alla base di un corretto utilizzo, quali ad esempio il rispetto dei diritti e delle libertà fondamentali, il principio di non discriminazione, quello di trasparenza e infine il

[20] Articolo 22 GDPR, "*Processo decisionale individuale automatizzato, compresa la profilazione*", che recita: "L'interessato ha diritto di non essere soggetto a decisione basata esclusivamente sul trattamento automatizzato, compresa la profilazione, che produce effetti legali che lo riguardano o che influiscono in modo significativo anche su di lui (a meno che non sia fornito il consenso esplicito)".
[21] La commissione Europea per l'efficacia della giustizia (CEPEJ) del consiglio d'Europa ha adottato questa Carta per fornire principi guida per i giuristi e i professionisti circa la gestione dello sviluppo dell'Intelligenza Artificiale nei processi giudiziari. L'applicazione per tanto dovrà essere rispettosa della CEDU in, https://www.coe.int/it/web/portal/-/council-of-europe-adopts-first-european-ethical-charter-on-the-use-of-artificial-intelligence-in-judicial-systems .

principio di controllo dell'utente.[22] Se viene rispettato il principio "***Under User Control***", può dirsi certa l'applicazione dell'AI nella giustizia penale e/o civile in quanto deve essere un utilizzo dominato e controllato dall'intervento umano, escludendo qualsiasi tipo di automatismo nelle decisioni.

Quanto dichiarato alla fine è in linea anche agli ordinari principi del processo, dove il giudice in sede penale dovrà raggiungere una decisione "*oltre ogni ragionevole dubbio*", mentre in sede civile deve fare affidamento ad una tesi che possa risultare più probabile rispetto a tutte le alternative. Infatti proprio sulla base di questi principi è possibile affermare che non potrà mai verificarsi una piena sostituzione dell'uomo con l'attività digitale dei dispositivi basati su questa tecnologia, in primo luogo perché deve essere rispettato il principio del controllo dell'utente, in secondo luogo perché la macchina non potrà mai raggiungere un giudizio completo, quindi basato su tutti gli elementi presentati sia a favore sia a sfavore dell'imputato, non potrà elaborare un risultato oggettivo, pertinente e affidabile, poiché non tiene conto del contraddittorio e dei tentativi di smentita ai quali sono sottoposte le ipotesi per ricavare quella migliore, capace di ricostruire in maniera quanto meno veritiera l'accaduto. Appare, pertanto, improbabile questa sostituzione uomo-macchina, grazie al fatto che la mente umana è ricca di esperienza e con le continue decisioni penali porta avanti l'orientamento giurisprudenziale. Stessa cosa non può dirsi per gli assistenti vocali. L'AI è stata raffigurata come un collaboratore degli operatori giuridici, poiché aiuta questi nell'analisi dei documenti, nell'interpretazione delle norme e la relativa applicazione delle stesse a sostegno di svariate tesi, nella previsione dell'esito della causa, grazie all'azione degli algoritmi, nella formulazione di un giudizio finale e ancora più attuale l'impiego risulta utile per l'attività di prevenzione della criminalità, con la possibilità di prevedere luoghi e orari di atti delittuosi. Questa attività predittiva degli smart speaker è stata sperimentata sotto l'ordinamento statunitense sulla base di accertamento sulla possibilità di recidiva del soggetto imputato, sulla determinazione della pena detentiva o delle misure alternative alla detenzione da applicare. L'Estonia si presenta con "***The Digital Republic***", in quanto ha ufficialmente esteso l'applicabilità dell'AI ai sistemi giudiziari, con funzionalità di confronto dei dati e delle informazioni per giungere al giudizio, nel rispetto del principio del controllo dell'utente e con la possibilità per le parti del processo di opporsi al giudizio del dispositivo e di procedere nelle modalità ordinarie. Sicuramente questo è stato un passo che potrà portare alla digitalizzazione della giustizia.

Per tornare all'oggetto della nostra analisi legati alla raccolta delle informazioni digitali da parte di Amazon Alexa, possiamo dire che non è un caso isolato. Nel 2016 l'Apple si è rifiutata di fornire i codici di cifratura dello smartphone, imposto da un Giudice della California, di un utente indagato dall'FBI in quanto il dispositivo poteva contenere dati utili alle indagini[23].
Detto questo, **che ruolo, le conversazioni registrate con Alexa, possono assumere in un tribunale di giustizia?**
Al momento dell'acquisto, gli utenti danno il loro consenso affinchè il dispositivo possa registrare quello che con un comando si chiede all'assistente vocale, quindi tutto ciò che risulterà nella cronologia può essere utilizzato nei tribunali penali, a differenza di quanto accade per le registrazioni acquisite illegalmente, per finalità ad esempio di spionaggio, che essendo documenti illegali non possono proprio entrare all'interno del processo penale, come stabilito anche dalle regole di esclusione tipiche del procedimento penale. Si faccia riferimento ad un caso nel quale il giudice ha ordinato ad Amazon la consegna di talune registrazioni che presumibilmente potevano contenere indizi circa un omicidio di due donne avvenuto in un'abitazione. Nel processo è stato accusato di omicidio di primo grado Timothy Verrill che ha sempre difeso la sua innocenza. La pubblica accusa è

[22] https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808fed10
[23] https://www.tomshw.it/smartphone/iphone-cifrati-apple-dice-no-alla-backdoor-chiesta-dallfbi/

fortemente convinta del fatto che Alexa possa aver registrato il momento dell'omicidio e tutto quello che è accaduto prima e dopo.[24] Un altro caso simile ha riportato lo stesso tipo di dinamica, la polizia è riuscita ad ottenere il mandato dal giudice per farsi consegnare da Amazon queste registrazioni. Il colosso si è opposto a tale richiesta d'ufficio generica, appellandosi alla libertà di parola di ogni individuo, non fornendo pertanto le informazioni rivendicando richiesta legale, valida, vincolante e adeguatamente presentata.[25]

Le segreterie del ministero degli interni tedesco hanno affermato che per entrare in possesso delle registrazioni di Alexa non è necessario un mandato del giudice per le operazioni di *intercettazione ambientale*, ma solo di un mandato di *perquisizione e sequestro*, dato che le registrazioni sono già presenti all'interno del dispositivo e non sono state effettuate per scopo investigativo. La raccolta dei dati può avvenire con le tecniche di ***Digital Forensics***. Si procede all'individuazione dei dati, all'acquisizione tenendo conto della scarsa materialità dei dati informatici, più facilmente modificabili andando ad alterare la genuinità degli stessi. Per l'acquisizione è necessaria la "*bit stream image*" con il relativo blocco di accesso in scrittura che impedisce alternazioni quando si collega lo strumento, per procedere alla clonazione dell'hard disk, al supporto informatico. Una volta acquisito bisogna garantire la genuinità del dato e quindi è necessario creare un'impronta digitale, detta hash, che tecnicamente è un algoritmo a base simmetrica di classe MD5 che trasforma un testo di lunghezza arbitraria in una stringa a lunghezza fissa. Vi è genuinità del dato quando, dopo aver effettuato più copie, l'impronta dà lo stesso risultato. Le informazioni digitali vanno accuratamente conservate e successivamente il file, contenente i dati, deve essere presentato su *CD-ROM* non riscrivibile, seguendo il formato *"html"* per la navigazione.

Se le digital evidence sono coperte da misure di sicurezza, gli operatori dovranno liberare i file da password e dovranno presentare un file contente i dati coperti da password, un file contenente i dati decodificati e un file contenente solo le password. Ovviamente i dati/parti di registrazione da selezionare sono solo quelli in relazione all'accaduto. Il tutto sembra seguire la disciplina relativa alle intercettazioni.

Sono tanti gli aspetti che dovrebbero essere risolti in materia di Smart Assistant, perché con il progresso tecnologico, forse si rischia di subire ancor più violazioni ed è quindi opportuno anticiparle con le giuste cautele. Nonostante il grande sviluppo tecnologico, si anela sempre ad ottenere un'adeguata tutela della Privacy, cosi come anche dichiarato dall'ex procuratore Cunningham. Nell'era della tecnologia e delle informazioni digitali, quest'evoluzione della vita di tutti i giorni, non potrà che toccare tutti gli ambiti sociali. Si apre quindi un nuovo paradigma nelle investigazioni, che potrà mettere al servizio della giustizia penale, elementi utili alle indagini: gli ***Smart Assistant***.

Dottoressa Francesca Giordano

20 dicembre 2019

[24] https://it.dailystormer.name/amazon-alexa-sta-registrando-tutto-cio-che-accade-nella-vostra-casa-caricandolo-su-un-cloud-e-le-registrazioni-possono-essere-utilizzate-nei-casi-penali/.
[25] https://www.google.it/amps/s/www.tomshw.it/altro/amazon-alexa-chiamata-a-testimoniare-in-tribunale/%3famp.