Smart assistant e dati personali: quali rischi per gli utenti?*

Lavinia Vizzoni

Abstract

Gli *smart assistant* sono programmi di assistenza vocale ormai molto diffusi. Il loro facile utilizzo e soprattutto la loro idoneità a rispondere a semplici richieste inoltrate dall'utente si accompagna però all'estrema pervasività degli stessi, che basano il loro funzionamento sulla raccolta di dati personali dell'utente (spesso di categorie particolari di dati) e si dimostrano idonei a captare pressoché ogni informazione rilasciata nell'ambiente circostante. Numerosi appaiono dunque i profili problematici che gli *assistant* presentano con riguardo alla disciplina del trattamento dei dati personali; i quali fanno emergere la necessità di ricercare una soluzione configurata in termini di "*design*" del programma stesso, all'interno di uno scenario in cui anche le certificazioni sono destinate ad assumere un ruolo sempre più di rilievo.

Smart assistants are now very popular voice assistance programs. Their easy use and above all their suitability to respond to simple requests sent by the user is though accompanied by the extreme pervasiveness of the assistants, which base their functioning on the extensive collection of the user's personal data (often special categories of data), and have proven to be capable of capturing almost any information released into the surrounding environment. Therefore, there are several challenging aspects that assistants show in comparison to the discipline of personal data processing, which reveal a need to seek a solution configured in terms of "design" of the program itself, within a scenario where even certification mechanisms are destined to assume an increasingly crucial role.

Sommario

Keywords

Smart assistant - *internet of Things* - intelligenza artificiale - *privacy by design* - certificazioni

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

1. Assistenti vocali, intelligenza artificiale e *Internet of Things*

Lo sviluppo delle tecnologie digitali applicate alla quotidianità ha condotto, negli ultimi anni, a una massiccia diffusione dei c.d. *smart assistant*. Si tratta di *software* che, grazie al c.d. *machine learning*, ossia a sistemi di apprendimento che utilizzano algoritmi di intelligenza artificiale, sono in grado di riconoscere il linguaggio naturale degli esseri umani e di interagire con gli stessi. Tale interazione può essere rivolta a soddisfare diversi tipi di richieste (ad esempio, fissare appuntamenti, impostare sveglie, *timer* e promemoria, riprodurre musica o notiziari, fornire previsioni meteo e di traffico) o a compiere determinate azioni, come accendere una luce, azionare un elettrodomestico o regolare la temperatura di un'abitazione.

Il loro costo contenuto, la frequente preinstallazione nei *device* e la semplicità di funzionamento ne hanno agevolato la diffusione e l'impiego. Gli assistenti in questione possono infatti essere installati in una pluralità di supporti: dagli *smart speaker* collocati all'interno delle abitazioni domestiche, ma anche di altri ambienti antropizzati, quali i luoghi di lavoro[1], se non anche le automobili, ai *device* che portiamo fisicamente con noi, i c.d. *wearable*, sino ai dispositivi più diffusi come gli *smartphone,* i *personal computer* e i *tablet*. In particolare, gli stessi si prestano anche ad agevolare lo svolgimento di attività quotidiane anche da parte di soggetti con autonomia ridotta.

Per fare questo, gli assistenti vocali raccolgono quasi ininterrottamente dati personali relativi sia all'utente diretto sia, più in generale, a coloro che si trovano nell'ambiente in cui gli stessi operano. Per di più, gli *smart assistant* si possono avvalere anche di soluzioni proprie del c.d. *Internet of Things* (*IoT*)[2], che offre la possibilità di sfruttare i vari oggetti, appunto, le "*things*" che incorporano i programmi di assistenza vocale "intelligente", per la raccolta di informazioni e l'attuazione di interventi finalizzati al miglioramento dei servizi offerti[3]. Gli *smart assistant* sono infatti capaci di "dialogare" con altri dispositivi *IoT*, come *smartwatch*, *smart* TV, sistemi di controllo da remoto o di videosorveglianza; il che amplifica la possibilità di raccolta, incrocio dei dati e diffusione di informazioni personali.

Se in passato l'*Internet of Things* si collocava in una rete di sensori in grado di restituire

[1] Con i conseguenti rilevanti interrogativi che si pongono in ordine alla sorveglianza dei lavoratori. Sulle intersezioni fra *data protection* e diritto del lavoro, v. precipuamente E. Dagnino, *Tecnologie e controlli a distanza*, in *Dir. rel. ind.*, 2015, 988 ss. e A. Stolfa, *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, in *Lav. giur*, 2018, 530 ss.

[2] Sulle applicazioni dell'*Iot*, con particolare riguardo proprio agli assistenti virtuali, cfr. le preoccupazioni espresse già da G. Ramaccioni *La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria*, Napoli, 2017, 16 ss. e 288 ss.

[3] Sulle potenzialità dell'*Iot* cfr. A. Santosuosso, *Intelligenza artificiale e diritto*, Milano, 2020, 180 ss., il quale evidenzia come l'Internet delle cose sia al centro dell'interesse della politica economica dell'Unione Europea. In tale prospettiva, esso diviene punto focale per la digitalizzazione della società, nel contesto dell'implementazione delle tecnologie 5G e nel perseguimento del più ampio obiettivo della realizzazione del *digital single market*. Sugli sviluppi dell'*IoT* e sui relativi impatti in tema di trattamento dei dati personali, cfr. E. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, in Id. (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, Milano, 2019, 36 ss.

informazioni mediante tecnologie di RFID (*Radio Frequency IDentification*)[4], con l'avvento del Web si è passati ad un contesto più evoluto, in grado di catturare quantitativi ben maggiori di informazioni attraverso la connessione dei dispositivi. Le applicazioni dell'*IoT* investono oggi molteplici settori, a partire dall'industria 4.0[5], e si raccordano sempre di più all'uso di piattaforme, che permettono di connettere e controllare esternamente i dispositivi, di memorizzare e analizzare i dati raccolti, di monitorare e comandare gli oggetti connessi[6].

Rispetto ai dati personali raccolti dagli assistenti *smart* connessi diventa inoltre oggi cruciale la nozione non solo di interconnessione, ma anche di interoperabilità fra i sistemi informatici[7]: la tendenza in atto è infatti quella dello sviluppo di multipiattaforme che puntano al controllo di oggetti *smart* di fornitori e marche diverse da un unico punto di contatto. Particolarmente significativo appare l'accordo di recente stretto tra Amazon, Apple e Google, in genere non propensi ad alleanze, per la creazione di un protocollo unitario per la casa connessa, grazie al quale tutti i dispositivi potranno essere controllati con Alexa, Siri e Google Assistant[8].

Lungo tale versante, sono destinate ad imporsi all'attenzione degli studiosi proprio le implicazioni legate alla sicurezza e all'interoperabilità di architetture *IoT*, che assumono sembianze sempre più capillari[9].

---

[4] Cfr. F. Giovanella., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Milano, 2019, 1213.

[5] Nel contesto di quella che è una vera e propria *smart factory*, sono state sviluppate soluzioni che, per quanto futuristiche appaiano, sono già una realtà e vengono attualmente utilizzate in ambienti industriali tecnologicamente progrediti. Rientrano nel novero di siffatte soluzioni i dispositivi di robotica indossabile, quali gli esoscheletri per applicazioni industriali volti ad aumentare le capacità operative dei lavoratori che svolgono attività manuali e di movimentazione; o le *smart suit,* ossia tute realizzate anche tramite scansioni del corpo del lavoratore; così come le postazioni di lavoro auto-adattive, strutturate sulla base delle caratteristiche proprie di chi è chiamato ad utilizzare quelle postazioni, anche in termini di condizioni fisiche e di affaticamento. In proposito, v. l'analisi di L. Greco - A. Mantelero, *Industria 4.0, robotica e* privacy-by-design, in *Dir. informaz. informatica*, 2018, 883 ss.

[6] In generale, sulle piattaforme *online*, v. A. De Franceschi, *La vendita di beni con elementi digitali,* Napoli, 2019, 19 ss. In proposito, cfr. anche C. Busch, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, in A. De Franceschi - R. Schulze (a cura di), *Digital Revolution – New Challenges for Law*, Baden-Baden, 2019, 57 ss.

[7] Sulla interoperabilità v. G.M. Riccio - F. Pezza, *Portabilità dei dati personali e interoperabilità*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 398 ss. Lo scritto (404 s.) si sofferma sulla interoperabilità, in relazione all'effettività del diritto alla portabilità nel settore della telefonia mobile, evidenziando la positività del modello inglese che pone gli obblighi relativi a carico del precedente gestore. Cfr. anche E. Battelli - G. D'Ippolito, *Il diritto alla portabilità dei dati personali*, in E. Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., 202 ss.

[8] La notizia, datata 19 dicembre 2019, è tratta dal sito web www.corriere.it/tecnologia. Oltre ai citati Google, Amazon ed Apple, hanno aderito all'accordo in questione i produttori riuniti nella Zigbee Alliance, fra cui Ikea, Samsung SmartThings e Schneider Electric, a conferma del grande interesse che il mercato della domotica suscita. Il relativo protocollo sarà *open source* e tutti potranno realizzare prodotti compatibili con i tre noti assistenti vocali. Già rilevante era d'altronde apparso l'acquisto, da parte di Google, avvenuto nel 2014, di Nest Labs, azienda che aveva l'obiettivo di creare proprio dispositivi domotici, come i termostati e rilevatori di fumo.

[9] Qualche risultato nella direzione della interoperabilità sembra stia arrivando da ONEM2M (www.onem2m.org), un progetto congiunto di otto enti di standardizzazione mondiali, tra cui ETSI (Europa), ARIB (Giappone), CCIA (Cina), TIA (Nord America) e duecento partner, che si propone di definire

Da altra parte, l'implementazione dei programmi di assistenza vocale si lega strettamente ai progressi ottenuti nel campo dell'intelligenza artificiale. Lanciando ricerche vocali, l'utente inoltra segnali proprio ai sistemi di intelligenza artificiale utilizzati dagli *smart assistant*, che, tramite quegli *input* continuano a implementarsi così riuscendo a comprendere la domanda e a fornire risposte sempre migliori, riducendo progressivamente il margine di errore[10].

Più precisamente, l'intelligenza artificiale utilizza algoritmi sofisticati per ordinare enormi quantità di dati, tracciare schemi e fare previsioni: attività che sarebbero ripetitive e lunghe, se non praticamente impossibili, da eseguire manualmente. Le macchine "intelligenti" contribuiscono fortemente allo svolgimento di tali attività, avvalendosi anche della nota capacità di imparare da sé stesse, attraverso il c.d. *machine learning*, o addirittura di elaborare nuovi percorsi di apprendimento con il c.d. *deep learning*[11]. L'intelligenza artificiale pone però all'attenzione del giurista una serie di interrogativi che mettono alla prova le capacità di risposta dell'ordinamento giuridico e delle relative categorie concettuali[12]. Come osservato, l'idea che una macchina, per quanto "intelligente", possa assumere autonomamente decisioni che riverberano i loro effetti anche su diritti fondamentali della persona, suscita preoccupazione, e impone una riflessione approfondita che, in prospettiva, coinvolge anche le decisioni di politica del diritto da assumere[13].

La vera sfida — che già si profila con una certa chiarezza — dei meccanismi che sfruttano, per il loro funzionamento, algoritmi di intelligenza artificiale, sarà quella di conseguire soluzioni che garantiscano, anche sul versante etico, di soddisfare i criteri di spiegabilità, robustezza, correttezza e tracciabilità[14]. Non a caso, dalla Commissione Europea sono di recente giunte Linee Guida per uno sviluppo etico dell'intelligenza artificiale: si tratta di un documento, dal valore programmatico, che detta indicazioni per uno sviluppo di un'intelligenza artificiale a misura di essere umano[15], da ultimo

---

degli standard di riferimento (*framework* di interlavoro) per la costruzione di piattaforme di servizio interoperanti.

[10] V. G. D'Acquisto - M. Naldi, Big Data *e* Privacy by Design. *Anonimizzazione, Pseudonimizzazione, Sicurezza*, Torino, 2017, 9 ss.

[11] Cfr. F. Crisci, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm*., 2018, 1787 ss.

[12] V. U. Ruffolo - E. Gabrielli, *Introduzione*, in Id (a cura di), *Intelligenza artificiale e diritto,* in *Giur. it*., 2019, 1657 ss. Cfr. inoltre N. Zorzi Galgano, *Introduzione,* in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, 15 ss.

[13] Cfr. A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 63 ss.

[14] Sul bilanciamento, in chiave etica, fra diffusione di soluzioni tecnologiche avanzate e impatto sui diritti e le libertà della persona, cfr. D. Wright, *A framework for the ethical impact assessment of information technology*, in *Ethics Inf. technol*., 2011, 199 ss.

[15] Sono i risultati diffusi dall'*High Level Group on Artificial Intelligence* della Commissione europea, reperibili nel sito web www.ec.europa.eu. La Commissione stessa, nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, ha diffuso la sua visione al riguardo, che sostiene un'AI «etica, sicura e all'avanguardia realizzata in Europa». Le linee guida della Commissione europea per un'intelligenza artificiale affidabile sono peraltro state aggiornate nel settembre 2019 dal centro studi del Parlamento europeo. Sul difficoltoso percorso orientato al pervenir ad un sistema europeo di *governance* dell'intelligenza artificiale, v. inoltre G. Mazzini, *A system of governance for Artificial Intelligence through the lens of emerging intersections between AI and EU law*, in A. De Franceschi R. Schulze (a cura di), *Digital Revolution – New Challenges for*

compendiate nel «Libro bianco sull'intelligenza artificiale — Un approccio europeo all'eccellenza e alla fiducia», datato 19 febbraio 2020.
A livello nazionale, è d'uopo quanto meno ricordare l'elaborazione dalle Proposte per una strategia italiana per l'intelligenza artificiale del Gruppo di esperti MISE[16], che, sulla stessa linea, indicano un percorso verso l'implementazione di un'intelligenza artificiale complementare — piuttosto che sostitutiva — all'intelligenza umana, tale da consentire di garantire il rispetto dei valori e dei principi fondamentali[17].

2. I relativi vantaggi e rischi

Proprio lo sviluppo di algoritmi evoluti di intelligenza artificiale, unitamente all'interconnessione degli oggetti *smart*, ha consentito dunque di creare soluzioni parzialmente o totalmente autonome, le cui capacità di apprendimento e monitoraggio delle abitudini degli utenti crescono esponenzialmente, di pari passo al tentativo, sempre più preciso, di adattare il livello di servizio offerto sulla base delle richieste effettuate dagli individui stessi. E a sua volta, la proficua convergenza fra *IoT* e *AI* dipende dalla disponibilità di dati personali.
In questo contesto, l'attenzione particolare che può essere riservata agli assistenti vocali "intelligenti" deriva da una duplice ragione: lo stretto legame del loro funzionamento con i dati personali, posto che l'operatività del dispositivo abbisogna, anzi, è dichiaratamente funzionale alla raccolta delle informazioni dall'utilizzatore e dal suo ambiente esistenziale, nonché il loro elevato grado di pervasività rispetto alla vita degli utenti.
Soprattutto, considerazioni inerenti all'ingente quantitativo di dati personali raccolti ed elaborati dai *device*, e correlative perplessità, sono state avanzate con riguardo agli *home speaker*, che trovano collocazione proprio nella casa, luogo dell'*habitat* domestico nel quale si svolge la personalità umana, da difendere gelosamente dalle intrusioni esterne, tanto da elevarsi, nella sua accezione di domicilio, ad area inviolabile al pari della stessa libertà personale[18].
Come osservato, gli *home speaker* rappresentano una sorta di *alter ego*[19], se non dei veri e propri «maggiordomi» dei proprietari[20], che raccolgono dati non solo sulle proprie

Law, cit., 245 ss.

[16] La prima versione delle Proposte per una strategia italiana per l'intelligenza artificiale è datata luglio 2019 ed è reperibile nel sito web del Ministero, www.mise.gov.it.

[17] É tuttavia rilevante segnalare che la versione finale di tali Proposte, formulata nel corrente anno dal Gruppo di esperti di alto livello del MISE, esprime apertamente una visuale non del tutto collimante con le indicazioni provenienti dall'Europa. In particolare, nelle Proposte nazionali si fa riferimento alla circostanza per cui l'Unione Europea manifesterebbe una visione del fenomeno eccessivamente orientata in chiave industriale e poco attenta ai profili di sostenibilità dello sviluppo.

[18] In sintesi, sul fondamentale rapporto di derivazione che lega il domicilio alla libertà personale, cfr. P. Scarlatti, *Libertà e inviolabilità del domicilio*, in *Diritto on line-Treccani*, 2016.

[19] Cfr. E. Palmerini, *Dalle* smart cities *allo* scoring *del cittadino*, in *I Confini del Digitale. Nuovi scenari per la protezione dei dati,* Convegno per la Giornata europea della protezione dei dati personali 2019 - 29 gennaio, Roma, 17 ss., spec. 23.

[20] Sono le considerazioni di F. Pizzetti., *Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e*

performance, quali prodotti, ma anche dati personali (scelte, preferenze, abitudini di consumo ...) degli utenti stessi; assistenti personali virtuali, dunque, che imparano a conoscere l'utente che interagisce con loro molto a fondo, e persino ad anticipare le relative richieste, eventualmente stipulando anche i relativi contratti[21].

Inoltre, gli assistenti vocali sono costantemente in attività grazie agli altri dispositivi ai quali sono connessi. Ciò può significare che, anche quando l'*assistant* non è in utilizzo, trasmette in continuazione ogni accadimento o variazione dell'ambiente che è in grado di percepire[22], con la realizzazione di un'operazione continua di monitoraggio dei comportamenti e di profilazione degli individui[23]. In effetti, il rapporto vocale tra le persone e lo *speaker*, così cruciale negli assistenti, appunto, vocali, demandati a rispondere alle richieste dell'utente, è possibile in quanto l'apparecchio è dotato della capacità di ascolto non solo del comando che gli venga di volta in volta impartito, ma di tutto ciò che accade nell'ambiente circostante[24]. D'altronde, i dispositivi in questione hanno dimostrato di registrare indifferentemente tutte le conversazioni che avvengano all'interno dell'ambiente domestico, ivi comprese, dunque, quelle in cui partecipino terzi che potrebbero addirittura ignorare l'esistenza di tali *device* o il relativo funzionamento. Gli utenti, così come i terzi inconsapevoli, potrebbero persino attivare l'*assistant* inavvertitamente, con comandi vocali impartiti involontariamente: studi pratici hanno infatti svelato che molti *speaker* non solo si accendono per effetto della pronunzia delle parole convenzionali, bensì rispondono anche ad una serie di stimoli vocali ulteriori.[25]

Il flusso di dati che i dispositivi generano è dunque costante e consistente: una situazione a cui fa, peraltro, da contraltare un profilo di particolare criticità, ossia la diffusa inconsapevolezza degli utenti[26], a maggior ragione particolarmente problematica pro-

soluzioni per la privacy, reperibileagendadigitale.eu, 4 aprile 2018, secondo il quale gli assistenti digitali intelligenti sono paragonabili a «moderni maggiordomi dell'era digitale, ma, esattamente come i maggiordomi vittoriani, sanno tutto di ciò che accade nella casa e tutto registrano e ritrasmettono».

21 È quanto osservato da E. Palmerini, *Dalle smart cities allo scoring del cittadino,* cit., 24.

22 V. ancora F. Pizzetti, *Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la* privacy, cit.

23 In tema: A. Pierucci, *Elaborazione dei dati e profilazione delle persone*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 413 ss.

24 Nella scheda informativa dell'Autorità Garante per la protezione dei dati personali, su cui v. *infra*, par. 4, si fa espresso riferimento al fatto che «Quando è acceso ma non viene utilizzato, l'assistente digitale è in uno stato detto di *passive listening*, una sorta di "dormiveglia" da cui esce non appena sente la parola di attivazione che abbiamo scelto».

25 Soprattutto gli *home speaker* sembrano rispondere a molti più comandi vocali rispetto a quelle che sono le formule di accensione. Secondo quanto riportato dalla P*olicy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world* dello *European Consumer Consultative Group*, datata 16 maggio 2018, 13: «*In 2017, the Federation of German Consumer Organisations (vzbv) analysed the voice-controlled personal assistant 'Amazon Echo' and found that the device was recording far more conversation than the user intended as it reacted not only to the activating code word 'Alexa' but also to similar words. The same has been found to be true for Google Assistant*». Ancora, nella *Policy* si legge (9): «*Practical testing by the Digital Market Watch project of German consumer association has demonstrated that Google's Home Assistant that is supposed to be activated with the words 'OK Google' also awakens when conversations contain 'OK Kuchen' - meaning "OK cake" in German - and 'OK gut' – meaning 'OK fine'. The unwanted activation of the home assistant system entails that more private conversations are being transmitted and processed by Google than intended. Similar results were obtained for Amazon's Alexa*».

26 A proposito dell'inconsapevolezza dell'utente v. A. Mantelero, *Data protection, e-ticketing, and intelligent*

prio nei soggetti che da quelle soluzioni potrebbero trarre i vantaggi maggiori, ossia i soggetti più vulnerabili[27].

3. Assistenti vocali e trattamento dei dati personali

Già in siffatta esemplificazione si intravedono, a fianco delle molteplici opportunità, altrettanti rischi a carico dell'utente, soprattutto sul versante del trattamento dei dati personali[28]. Non è senza significato che ogni *Big Player* della Rete abbia creato un proprio *smart assistant,* strumento diretto per operare la profilazione dell'utente (i noti Siri di Apple, Alexa di Amazon, Cortana di Microsoft e Google Assistant di Google) e che proprio gli Internet Giants «*are leading the pack ... with no clear competitor in sight*»[29].
È in questa sede possibile soltanto accennare ai singoli profili che, dinanzi alla concreta operatività degli assistenti vocali intelligenti, svelano una particolare problematicità, senza poterli illustrare in dettaglio.
Già alcuni principi declamati dal regolamento si attagliano con difficoltà a scenari tecnologicamente evoluti, come quello in esame, specialmente laddove — e questo può senz'altro accadere — il trattamento dei dati raccolti dagli assistenti vocali si traduca in un'attività di *Big data analytics*, ossia in un procedimento di raccolta e analisi di grandi volumi di dati (*Big Data*)[30]. Fra questi, i tre principi tra loro strettamente connessi della minimizzazione dei dati trattati (art. 5, par. 1, lett. c) GDPR), della limitazione della loro conservazione (art. 5, par. 1, lett. e) GDPR) nonché della limitazione delle finalità del trattamento (art. 5, par. 1, lett. b) GDPR): non è infrequente che spesso si assista a raccolte di dati personali in notevoli quantità, sicuramente eccessive rispetto alle finalità del trattamento[31], con la frequente possibilità che questi vengano, peraltro, conservati oltre il necessario.

---

systems for public transport, in *International Data Privacy Law*, 2015, 309 ss.

[27] Fra questi, i minori. In proposito, cfr. le preoccupazioni espresse da E. Palmerini, *Dalle smart cities allo scoring del cittadino*, cit., 25. Sulla vulnerabilità della posizione dei minori in merito al trattamento dei loro dati personali operato anche da oggetti *smart*, v. inoltre A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019, spec. 5 ss. e 57 ss.

[28] Sulle profonde trasformazioni legislative vissute dal settore, *in primis* legate all'entrata in vigore del Reg. Ue 679/2016, c.d. GDPR, v. in generale G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in Id. (a cura di), L*a protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2017, 5 ss.

[29] Lo riporta lo studio della Commissione europea, datato gennaio 2018, *The rise of Virtual Personal Assistants*, il cui testo è reperibile nel sito webec.europa.eu.

[30] Particolarmente significative, in materia, due relazioni del Garante della privacy inglese (Information Commissioner's Office, ICO), *Big data, artificial intelligence, machine learning and data protection, 2017,* e *Anonymisation: managing data protection risk, code of practice*, 2012, reperibili entrambe sul sito web dell'Autorità.

[31] Sulla problematicità delle situazioni — quali quelle qui in considerazione — in cui le informazioni sono inferite dai dati, tale che la finalità del trattamento non è chiara fin dal principio, ma si va definendo con il trattamento stesso e dunque non può essere comunicata all'interessato, v. G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, in U. Ruffolo - E. Gabrielli (a cura di), *Intelligenza artificiale e diritto*, cit., 1675.

Di fronte a siffatto contesto, neppure l'anonimizzazione[32], anch'essa prevista dal regolamento, e costituente una misura di protezione dei dati personali, a sua volta coerente con il principio di minimizzazione, dimostra particolare efficacia[33]. Premesso che l'anonimato del dato è di per sé un parametro relativo, in quanto correlato alla collegabilità del dato all'interessato, che a sua volta dipende da circostanze specifiche (il soggetto che opera il collegamento, il contesto in cui questi opera, le modalità con le quali il trattamento è eseguito ...)[34], proprio rispetto a grandi volumi di dati raccolti da una pluralità di fonti, le pratiche di anonimizzazione risultano particolarmente inadatte, dal momento che l'incrocio di dati consente un'alta possibilità di re-identificazione dell'interessato[35], vanificando l'anonimato stesso.

Va inoltre tenuta in debita considerazione la circostanza per cui gli *speaker* intelligenti sono idonei a raccogliere e trattare non solo dati che costituiscono caratteristiche personali dell'utilizzatore (sesso, età, ecc.), ma anche informazioni che rientrano fra le categorie particolari *ex* art. 9 GDPR[36], come i dati sanitari (si pensi a uno *smart assistant* istruito per ricordare l'orario di assunzione di farmaci) e soprattutto i dati biometrici[37]. L'attivazione e/o operatività dello *speaker* stesso dipende infatti dal comando vocale; se poi lo *smart assistant* è dotato anche di videocamera lo stesso raccoglierà dati quali la conformazione dell'iride e le espressioni del volto, dalle quali ricavare persino stati emozionali, e sarà in ogni caso capace di geolocalizzare l'utente.

Come noto, i dati biometrici sono una tipologia di dati personali connotata da peculiarità intrinseche, in cui si verifica quella sostanziale coincidenza fra persona e dato che rende il corpo del soggetto strumento per la sua identificazione, con le conseguenti possibili incidenze sull'identità stessa della persona[38]. Inoltre, i dati biometrici sono atti a rivelare caratteristiche uniche del soggetto, tanto da essere i soli dati personali a consentire un'identificazione univoca della persona[39]. Se in generale, le tecnologie bio-

---

[32] Sull'anonimizzazione in generale, e sulle incertezze relative al concetto di identificabilità dell'interessato, cfr. E. Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, 360 ss.

[33] Specificamente sull'anonimizzazione e i rischi di re-identificazione nel contesto dell'*IoT* e dei *Big Data*, v. F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), cit., 1222-23, A. Mantelero, *La* privacy *all'epoca dei* Big Data, ivi, 1190-91. Sulle difficoltà legate all'anonimizzazione nel contesto dei *Big Data* cfr. anche G. De Gregorio, R. Torino, Privacy, *protezione dei dati personali e* Big Data, in E. Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., 474-5.

[34] G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, cit., 1675.

[35] F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., 1219.

[36] G. De Gregorio - R. Torino, Privacy, *protezione dei dati personali e* Big Data, cit., 470-1 evidenziano per vero come perda di significato anche la distinzione fra dati personali e categorie particolari di dati, in merito alla *Big Data Analytics*, laddove quindi vengano raccolti e trattati grandi volumi di dati, e laddove vi sia la possibilità di inferire dati personali da dati rientranti nelle categorie particolari e viceversa.

[37] Sui dati biometrici v. M. Pulice, *Sistemi di rilevazione di dati biometrici e* privacy, in *Lav. giur.*, 2009, 994 ss., e, da ultimo, le riflessioni di R. Ducato, *I dati biometrici*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 1285 ss. (sulla loro definizione e collocazione normativa, prima e dopo l'avvento del GDPR, cfr. in particolare 1294).

[38] Al riguardo, v. le riflessioni di S. Bisi, *Il corpo come* password*: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e dir.*, 2005, 3 ss.

[39] Cfr. L. Greco - A. Mantelero, *Industria 4.0, robotica e* privacy-by-design, cit., 883 ss.

metriche apportano consistenti vantaggi pratici, poiché consentono il riconoscimento automatizzato dei soggetti e incentivano la semplificazione di una pluralità di procedure, anche nell'esercizio delle attività quotidiane[40], dall'altro lato, i rischi che si profilano per l'interessato, connessi ad un utilizzo illegittimo o inappropriato dei dati biometrici, divengono particolarmente consistenti[41]: dai pericoli connessi al furto di identità[42] ai rischi correlati all'idoneità, propria delle tecniche biometriche, di consentire rilevazioni a distanza degli interessati, o di rappresentare la base per trattamenti discriminatori[43]. Ove l'obiettivo prioritario degli *smart assistant* sia la profilazione dell'utente a fini commerciali, per l'invio in particolare di pubblicità comportamentale, il trattamento dei dati sanitari e biometrici apre poi scenari molto più delicati. Il rischio che si prospetta è legato alla presenza di *bias*, per tale intendendo quelle distorsioni che gravano le decisioni assunte da sistemi informatici automatizzati che «discriminano sistematicamente e ingiustamente certi individui o gruppi di individui a favore di altri», negando opportunità o generando risultati indesiderati per motivi irragionevoli o inappropriati[44]. La profilazione è espressamente definita dall'art. 4 (4) e regolata nell'art. 22 del GDPR, mentre il principio di non discriminazione non è sancito esplicitamente dal GDPR. Tuttavia, a parte la sua valenza di principio generale a fondamento delle carte europee[45], come puntualmente osservato, a partire dal considerando n. 71 dello stesso — laddove si stabilisce che è opportuno che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate che tengano conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impediscano tra l'altro effetti discriminatori — si ricava l'esistenza di ulteriore principio fondamentale, definito «latente» nella trama normativa, di «non discriminazione algoritmica», da riferirsi non solo alla profilazione, ma anche a qualsiasi altra forma di algoritmo predittivo[46]. Si tratta di una problematica complessa da risolvere, rispetto alla quale anche le soluzioni avanzate si moltiplicano. Da un lato si propone il ricorso all'intervento normativo atto a regolare i processi decisionali in cui siano coinvolti algoritmi. Questo implicherebbe un'estensione dell'oggetto della disciplina giuridica, che dovrà rivolgersi a entrambi i profili della decisione algoritmica: un profilo definito «interno», concernente il fun-

[40] Per una ricognizione dei settori di operatività delle tecniche biometriche, cfr. R. Ducato, *I dati biometrici*, cit., 1286.

[41] Ivi, 1287.

[42] V. S. Bisi., *Il furto d'identità: panoramica attuale e prospettive giuridiche*, in *Ciberspazio e dir.*, 2004, 303 ss.

[43] Sui rischi di discriminazione derivanti precipuamente dal trattamento di dati biometrici, che possono riguardare anche i lavoratori, v. A. Pierucci, *Videosorveglianza e biometria*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 1627 ss., e M. De Bernart, *Art. 114, Garanzie in materia di controllo a distanza*, in E. Caravà - R. Sciaudone (a cura di), *Il codice della privacy - Commento al d.lgs. 196/2003 e al d.lgs. 101/2018*, Pisa, 2019, 575 ss.

[44] Così B. Friedman - H. Nissenbaum, *Bias in Computer Systems*, in *14 ACM Transactions on Information Systems*, 1996, 332 ss. Cathy O'Neil usa l'efficace espressione «Armi di distruzione matematica», che dà il titolo al suo scritto tradotto da Cavallini e edito nel 2016 da Bompiani.

[45] Ci si può limitare in questa sede a citare il «Manuale di diritto europeo della non discriminazione» edito nel 2011 ad opera della Corte europea dei diritti dell'uomo e dell'Agenzia dell'Unione europea per i diritti fondamentali.

[46] A. Simoncini, *L'algoritmo incostituzionale*, cit., 84 osserva ulteriormente come se anche l'algoritmo sia conoscibile e comprensibile, esso può essere di per sé discriminatorio e dunque incostituzionale.

zionamento dell'intelligenza artificiale, rispetto al quale occorrerà dettare regole volte ad evitare che il sistema possa generare decisioni discriminatorie; e un profilo definito «esterno» al funzionamento dell'intelligenza artificiale, relativo al peso che l'algoritmo esplica sulla decisione finale, e al possibile intervento umano in chiave mitigatrice e di controllo[47].

Dall'altro lato, vi è invece chi, partendo dal presupposto per cui non sia pensabile che gli sviluppatori degli algoritmi possano definire in maniera autoreferenziale e senza rischio di distorsioni i valori codificati negli algoritmi impiegati per governare la società, prospetta non un intervento legislativo, ma piuttosto l'adozione di un approccio partecipativo al processo di analisi del rischio, quale mezzo idoneo anche a consentire la piena attuazione del diritto dei consociati a prendere parte alle decisioni che li riguardano[48]. In tale ottica, si propone pertanto l'ampliamento della valutazione del rischio anche alla partecipazione di comitati di esperti o comitati etici, in grado di rappresentare le istanze sociali insite nelle soluzioni tecnologiche elaborate[49].

Quale che sia la soluzione preferibile, emerge con evidenza che il problema di fondo si traduce sul piano della programmazione e "*design*" dei modelli algoritmici e delle soluzioni tecnologiche che di quei modelli fanno applicazione.

4. Verso una concretizzazione della *privacy by design*: le recenti indicazioni del Garante

Dinanzi alle rilevate difficoltà, una soluzione "a monte" potrebbe essere di tipo "progettuale" e consistere nel compiere opportune scelte appunto di progettazione del programma di assistenza vocale. Così, esso dovrà essere strutturato ad esempio sulla minimizzazione dei dati raccolti, o sull'uso di tecniche di crittografia e/o pseudonimizzazione, per quanto possibile, nella trasmissione degli stessi all'*Internet Service Provider*; e ancora dovrà attivarsi solo quando riconosca l'apposito comando vocale dell'utente primario, escludendo dunque la raccolta e il trattamento di dati riguardanti altri soggetti[50] e dovrà consentire all'utente la possibilità di programmare determinate modalità di funzionamento.

Si tratta di una direzione, quella incentrata sulla progettazione, incoraggiata anche dalla Scheda informativa diffusa dal Garante per la protezione dei dati personali nel

[47] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, 202, e P. Zuddas, *Intelligenza artificiale e discriminazione*, in *Consulta Online*, 16 marzo 2020, 11.

[48] A. Mantelero, *La gestione del rischio nel GDPR, limiti e sfide nel contesto dei* Big Data *e delle applicazioni di* Artificial Intelligence, in A. Mantelero - D. Poletti (a cura di), *Regolare la tecnologia, il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 304.

[49] A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review,* 34(4), 2018, 754 ss.

[50] Con riguardo proprio ai *voice assistants* C. Hoofnagle, *Designing for Consent*, in *EuCML*, 2018, 167, ove si afferma che «[t]echnology may evolve to solve the problem of the secondary user consent. For instance, Amazon already has "voice profiles" that could evolve to the point that Alexa will only "listen" to those it recognizes».

marzo 2020, relativa proprio agli *smart assistant*[51]. Tale documento contiene alcune raccomandazioni, rivolte agli utenti, finalizzate ad un migliore utilizzo degli assistenti vocali. Alcune delle precauzioni formulate appaiono, per vero, assai semplicistiche e manifestano un eccessivo affidamento sulle capacità di discernimento dell'utilizzatore dello *speaker*. Fra queste «Informati sempre su come vengono trattati i tuoi dati» e «Non dire troppe cose allo *smart assistant*»: indicazioni che presumono la possibilità di conseguire un'informazione e una conoscenza di buon livello circa il funzionamento dello *speaker*, per vero raramente verosimili nell'utenza.

Altre raccomandazioni, invece, alludono, ben più significativamente, alle plurime modalità, in termini di operatività, dello *smart assistant* stesso. Fra esse «Decidi quali funzioni dell'assistente digitale mantenere attive[52]», «Disattiva l'assistente digitale quando non lo usi»: simili indicazioni presuppongono, oltre a un livello minimo di conoscenza da parte dell'utente, che l'assistente vocale offra concretamente la possibilità di impostare tali modalità determinando le relative opzioni.

L'adozione di una soluzione di tipo "progettuale", come è stata definita, consentirebbe l'immissione sul mercato di un prodotto o servizio che sia già stato testato non solo come efficiente (ad esempio sul versante energetico) e come sicuro[53], ma anche come conforme alla normativa, dal punto di vista dei trattamenti dei dati.

Verrebbe così a concretizzarsi pienamente la *privacy by design*[54] di cui al GDPR stesso (art. 25); e la *data protection* acquisirebbe un ruolo autonomo appunto nel *design* — inteso come progettazione ma anche come applicazione di opportune *business policies* o strategie organizzative[55] — del programma/dispositivo. Da ciò deriverebbe anche un significativo incoraggiamento, in favore dei produttori, verso l'adozione di criteri di tipo proattivo, anziché reattivo, nell'ottica appunto di prevenire potenziali lesioni ai danni degli interessati[56].

---

[51] La scheda, datata 4 marzo 2020, è reperibile nel sito web dell'Autorità.

[52] La scheda in questione fa espresso riferimento all'opportunità di disattivare funzioni particolarmente "invasive", quali l'invio di messaggi, la pubblicazione sui social o il compimento di acquisti *online*, ovvero, in alternativa, alla possibilità, sempre che sia contemplata dal programma, di inserire una *password* per autorizzare l'attivazione di simili funzioni solo su specifica richiesta dell'utente.

[53] La disciplina della sicurezza generale dei prodotti è contenuta nella direttiva 3 dicembre 2001, n. 95, attuata nel nostro ordinamento giuridico dal d.lgs. 21 maggio 2004, n. 172, poi confluito negli artt. 102 ss. cod. cons. In particolare, secondo il disposto dell'art. 104, c. 1, cod. cons., i produttori possono immettere sul mercato soltanto prodotti sicuri. Con specifico riguardo al tema della sicurezza nel settore della robotica intelligente e degli algoritmi, v. M. Gambini, *Algoritmi e sicurezza*, in *Giur. it.*, 2019, 1726 ss.

[54] Sul rilievo della *privacy by design*, cfr. A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, 211 ss., la quale, sebbene a proposito dei servizi *online*, evidenzia la necessità di adottare soluzioni — riconducibili proprio al paradigma della *privacy by design* — che, adottando un approccio «*user-centric*», rafforzino il potere decisionale dell'interessato, non valorizzato invece dalle soluzioni incentrate sul rilascio del consenso.

[55] Cfr. F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., 1236.

[56] E. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo* Codice Privacy, cit., 40.

5. L'analisi dei rischi e il sistema delle certificazioni

D'altronde, la *privacy by design* è un principio strettamente legato all'analisi del rischio, che a sua volta rappresenta un vero e proprio caposaldo del GDPR. Dal momento che spesso né i titolari né i responsabili del trattamento[57] posseggono però gli strumenti adeguati per operare questa analisi, come è stato proposto, si tratterebbe di traslare l'obbligo di effettuare l'analisi stessa, in modo che i rischi che derivano dai trattamenti operati, nel caso in esame dagli *smart assistant*, siano necessariamente e previamente valutati ad opera di terzi, in maniera sostanzialmente analoga a quanto già avviene in materia di sicurezza dei prodotti[58]. Tali terzi potrebbero essere, come suggerito, le Autorità garanti stesse[59].

In questa prospettiva, si osserva che la valutazione del rischio si sposterebbe, almeno parzialmente e indirettamente, anche a carico del produttore/fornitore del servizio/prodotto *smart*, che verrebbe ad esempio ad essere gravato dell'obbligo di procurarsi idonea certificazione.

È, in effetti, altamente probabile (ed anche auspicabile) che nel contesto in questione un ruolo operativo importante venga assunto dalle certificazioni di cui agli artt. 42 ss. GDPR, ad oggi non ancora operanti nel nostro Paese, ma verso cui si sono ormai mossi i primi passi: la convenzione firmata in data 20 marzo 2019 tra Accredia e l'Autorità Garante, intervenuta subito dopo la pubblicazione del report finale della Commissione europea sui meccanismi di certificazione[60] ha impegnato i due soggetti ad uno scambio di informazioni sulle attività di accreditamento e sulle certificazioni previste dal GDPR. Nello specifico, ad Accredia è affidato il compito di attestare la competenza degli organismi in conformità alla norma UNI CEI EN ISO/IEC 17065, per la certificazione dei prodotti e servizi, e in base ai «requisiti aggiuntivi» che saranno individuati dal Garante a partire dalle Linee guida comuni elaborate dal Comitato europeo per la protezione dei dati personali. Sicuramente, il meccanismo delle certificazioni contribuirà all'identificazione dei rischi, nell'intento di individuare le migliori prassi per attenuare gli stessi e dovrebbe dunque prevenire la verificazione dei relativi danni.

Un'importanza significativa, su un piano distinto ma collaterale, è destinata ad essere assunta dalla normativa in tema di *cybersecurity*, dopo l'approvazione della direttiva 2016/1148 (c.d. direttiva NIS, recante misure per un livello comune elevato di sicurez-

[57] È pur vero che gli stessi soggetti del trattamento sono, in contesti tecnologicamente avanzati, di ardua individuazione, e la scansione operata dal GDPR dagli stessi possa apparire semplicistica. Sul punto, v. A. Mantelero, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.,* 2019, 2779. Pone in luce le relative difficoltà individuando una vera e propria concatenazione di trattamenti, F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 44 ss. e 76-77.

[58] V. A. Mantelero, *Responsabilità e rischio nel Reg. Ue 2016/679*, cit., 149, e F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things*,* cit., 1225, che, nella stessa ottica, valorizza il ruolo del c.d. *Data Protection Impact Assessment* (DPIA).

[59] Cfr. A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer law & security review*, 2014, 643 ss., spec. 661 ss., che si pronuncia a favore della rivitalizzazione del modello autorizzatorio impiegato dalle prime generazioni di normative sui dati personali.

[60] Cfr. il *Final report* della Commissione europea del febbraio 2019 *Data Protection Certification Mechanisms under Articles 42 and 43 of the General Data Protection Regulation* (GDPR) (EU) 2016/679 (*Study on*).

za delle reti e dei sistemi informativi dell'Unione). Anche se questa normativa riguarda un rischio diverso da quello della *Data Protection*, ossia il rischio dell'interruzione o dell'attacco *cyber* al servizio, nel caso del *Cloud computing* il rispetto di essa e l'acquisizione della certificazione europea di *cybersecurity* rafforzerà l'affidabilità del fornitore, specie quando questi si avvalga a sua volta di servizi (ad esempio di stoccaggio delle informazioni) forniti da ulteriori terzi[61]. Non vi è dubbio che gli *smart assistant* rientrino a pieno titolo in questo contesto.

In effetti, il GDPR ha inteso attribuire un ruolo fondamentale proprio agli strumenti di *soft law*[62]: codici di condotta e certificazioni *in primis*. Dall'art 42.1 GDPR risulta infatti evidente come agli Stati membri, alle autorità di controllo, al comitato e alla commissione, sia attribuito il compito di "incoraggiare", a livello di Unione Europea, meccanismi di certificazione della protezione dei dati allo scopo di dimostrare la conformità al regolamento. L'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati rappresenta — o meglio, dovrà rappresentare — un importante strumento di autoregolamentazione privata anche nel settore della *data protection*. Come ulteriormente osservato su un piano più generale, con l'avvento del GDPR, il ruolo delle Autorità di controllo e vigilanza è profondamente mutato in direzione espansiva: esse, nel contesto della società digitale, non si limitano infatti alla mera vigilanza sul rispetto delle norme, bensì devono necessariamente svolgere anche un «ruolo proattivo» nella direzione della protezione concreta dei diritti dei soggetti coinvolti[63]. Tale impianto appare perfettamente in linea proprio con l'esigenza che la protezione dei dati personali venga garantita fin dalla progettazione dei trattamenti, complessivamente intesa nell'accezione di predisposizione, ma anche applicazione di opportune strategie organizzative, conformemente alla tecnica della *privacy by design*.

Nell'assetto del regolamento 2016/679, la centralità degli obblighi che gravano su titolare e responsabile del trattamento assegna alle certificazioni il ruolo non certo di produrre l'effetto di *discharge* di tali obblighi[64], ma piuttosto di agevolare nella dimostra-

---

[61] V. in argomento G. Vaciago, *L'attuazione della Direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi: i punti di contatto con il Regolamento UE 2016/679*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 1147 ss., il quale osserva come in proposito assumerà un'importanza fondamentale l'applicazione del regolamento volto a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali, c.d. Cybersecurity Act, che idealmente si colloca dopo l'approvazione della Direttiva NIS del 2016. Il Cybersecurity Act mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali, oltre che a rafforzare il ruolo dell'ENISA. Esso è entrato in vigore il 27 giugno 2019. Sul tema, più in generale, v. inoltre A. Contaldo - L. Salandri, *La disciplina della cybersecurity nell'Unione Europea*, in A. Contaldo - D. Mula - *Cybersecurity Law*, Pisa, 2020, 1 ss.

[62] La cui non vincolatività non è considerata tale da mettere a rischio quanto meno l'obiettivo dell'armonizzazione da G.M. Riccio, F. Pezza, *Certification Mechanism as a Tool for the Unification of the Data Protection European Law*, in *Medialaws*, 2018, 252.

[63] F. Pizzetti, *Codici di condotta, certificazioni, sigilli, marchi e altri poteri di* soft law *previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in A. Mantelero - D. Poletti (a cura di), *Regolare la tecnologia*, cit., 78.

[64] Come ribadito anche dalla versione definitiva dell'allegato 2 delle Linee guida sulla certificazione del Comitato europeo per la protezione dei dati, aggiornate al 4 giugno 2019.

zione della *compliance* alla normativa europea[65], al punto che le certificazioni vengono definite come veri e propri *accountability tools*[66]. Le certificazioni saranno rilasciate — una volta che il relativo meccanismo diverrà operativo — oltre che da autorità indipendenti, da organismi privati accreditati, chiamati a verificare la conformità del trattamento a criteri approvati alle autorità nazionali o dal Comitato europeo, nell'ottica, in questo secondo caso, di pervenire ad un vero e proprio «sigillo europeo per la protezione dei dati»[67]. Sicuramente, il meccanismo delle certificazioni contribuirà all'identificazione dei rischi, nell'intento di individuare le migliori prassi per attenuare gli stessi[68] e dovrebbe dunque prevenire la verificazione dei relativi danni.

Nella direzione individuata, la nozione di sicurezza del servizio/prodotto da tenere a riferimento non sarebbe più la mera sicurezza informatica[69] o la sicurezza del solo processo di trattamento dei dati, ma, in un'ottica più ampia, la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali della persona, che dall'operatività di quel servizio/prodotto possono essere compromessi[70]. L'analisi del rischio finirebbe in tal modo per "entrare" già dentro il prodotto o il servizio fornito all'utente, il quale non dovrebbe quindi preoccuparsi (sempre che sia in grado di farlo) di comprendere la reale incidenza del funzionamento del programma o dispositivo acquistato — nel caso qui considerato l'assistente vocale — sulla protezione dei propri dati personali.

[65] V. D. Poletti - M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), Privacy *digitale*, cit., 376 ss.

[66] Cfr. ancora ivi, 379 e G.M. Riccio - F. Pezza, *Certification Mechanism as a Tool for the Unification of the Data Protection European Law*, cit., 256 ss.

[67] S. Sileoni, *I codici di condotta e le funzioni di certificazione*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 924 e D. Poletti - M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, cit., 410.

[68] Considerando 77 GDPR.

[69] E. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, cit., 52, propone un approccio integrato che consideri sia le istanze della *privacy* che quelle della *cybersecurity*.

[70] A. Mantelero, *La gestione del rischio nel GDPR*, cit., 305.