LA PROTEZIONE DEI DATI PERSONALI DEL MINORE

WEBINAR DEL 19 GENNAIO 2021

SMART TOYS E INTERNET OF THING

INTERVENTO A CURA DEL DOTT. DANIELE ONORI, MEMBRO DEL DIRETTIVO DEL CENTRO STUDI ROSARIO LIVATINO

1. IOT E TUTELA DEI DATI PERSONALI

IoT e GDPR rappresentano un binomio indissolubile, considerando che la Internet of Things abbraccia i più disparati ambiti applicativi coinvolgendo cose e persone.

Le smart technologies, infatti, sempre più giocano un ruolo da protagoniste della comunicazione e delle relazioni, generando e incrociando sempre nuovi flussi di dati in cui rientrano quelli personali.

Con Internet of Things, lo ricordiamo, si intende l'insieme di connessioni internet operate da oggetti e da luoghi, senza l'intervento di operatori umani. In questo contesto gli oggetti possono collegarsi alla rete, comunicare il proprio status e dati sul proprio operato, come statistiche e altro, e accedere a informazioni utili per il proprio funzionamento, in modo del tutto automatico.

Le applicazioni nel campo dell'Internet of Things sono molteplici: oggetti che si connettono a Internet in modo indipendente possono essere sfruttati per sviluppare i settori della domotica, dei trasporti, della logistica, della medicina e moltissimi altri ambiti.

Sensori di fitness intelligenti e tracker possono trasformare l'assistenza sanitaria e migliorare la forma fisica e la salute personale. Sensori integrati possono misurare autonomamente umidità, aria e acqua livelli di inquinamento consentendo un monitoraggio più stretto di problemi ambientali.

Tali proprietà dovrebbero tradursi in opportunità, ma anche in rischi che implicano la sicurezza.

La "connessione perenne" tra oggetti e il trattamento massivo di dati connesso all'IoT genera interrogativi sul trattamento dei dati personali e sulla tutela dei diritti e delle libertà delle persone fisiche coinvolte nel trattamento.

Nel corso degli anni 2016-2017 si sono svolti diversi studi sui profili dell'IoT in grado di avere impatti sul trattamento dei dati personali.

Nel maggio del 2017 il network delle autorità per la protezione dei dati personali appartenenti al Global Privacy Enforcement Network (GpEN), ha svolto un'indagine su base internazionale, a cui ha aderito anche il Garante italiano, per verificare il rispetto della privacy nella Internet delle cose.

Su oltre trecento dispositivi elettronici connessi a Internet, **più del 60% non ha superato l'esame dei Garanti della privacy di 26 paesi**, facendo emergere, a livello globale, gravi carenze nella tutela della privacy degli utenti.

È emerso in particolare che:

- il 59% degli apparecchi non offre informazioni adeguate su come i dati personali degli interessati sono raccolti, utilizzati e comunicati a terzi;
- il 68% non fornisce appropriate informazioni sulle modalità di conservazione dei dati;
- il 72% non spiega agli utenti come cancellare i dati dal dispositivo;

- il 38% non garantisce semplici modalità di contatto ai clienti che desiderano chiarimenti in merito al rispetto della propria privacy.

Per far fronte ai rischi della sicurezza informatica in Europa, il 27 giugno 2019 è entrato in vigore il **Cybersecurity Act**, ossia il regolamento che assegna all'Agenzia comunitaria per la sicurezza informatica (ENISA) nuovi compiti e risorse per proteggere gli utenti dagli attacchi hacker, anche grazie ad una certificazione per gli oggetti connessi.

Inoltre, il comitato tecnico per la cyber security (ETSI) ha rilasciato lo standard per la sicurezza informatica da applicare al mercato IoT, con 13 regole per garantire la sicurezza nei dispositivi connessi, renderli conformi al GDPR e fornire linee guida per certificazioni future nel settore.

L'altro aspetto chiave, dicevamo, è quello della privacy. Se fino a tre anni fa solo il 27% dei consumatori era restio a condividere i propri dati personali, negli ultimi anni tale percentuale è aumentata in modo considerevole, raggiungendo il 44% nel 2017 e il 51% a inizio 2018.

Per poter comprendere la portata dei cambiamenti introdotti dalla normativa è necessario sottolineare il cambio di filosofia, con il passaggio a un approccio di "responsabilizzazione" del titolare (principio di accountability). Potremo chiaramente affermare che la "security by design" applicata all'IoT rispetta il principio enunciato all'art. 25 del GDPR.

Il GDPR, infatti, prevede che il titolare del trattamento, già dalle fasi preliminari del trattamento, assuma un ruolo proattivo nella scelta e nell'adozione delle misure tecniche e organizzative e nella definizione delle modalità di adeguamento; inoltre, egli deve essere sempre in grado di dimostrare il principio e il fondamento che sta alla base delle scelte effettuate e la propria compliance al GDPR.

I dati trattati devono essere, inoltre, adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità perseguite, realizzandosi, così, il principio della minimizzazione dei dati (considerando 39 – art. 5, lett. c).

Le vulnerabilità dei dispositivi IoT e dei servizi associati possono essere sfruttate per accedere, danneggiare e distruggere hardware e dati o causare altri danni materiali o immateriali.

I dispositivi IoT con un basso livello di sicurezza presentano dei rischi che rientrano in due grandi gruppi:

- diventare una minaccia per la sicurezza informatica e la privacy degli utenti;
- diventare oggetto di attacchi su larga scala.

I rischi dei dispositivi IoT per la sicurezza e la privacy appartengono a tre classi di mitigazione:

1. **proteggere la sicurezza del dispositivo**: significa impedire che i dispositivi siano utilizzati per condurre attacchi (intercettazione in rete, compromissione di altri dispositivi sullo stesso segmento di rete);
2. **proteggere la sicurezza delle informazioni**: significa proteggere la confidenzialità, integrità e disponibilità delle informazioni, incluse quelle personali, acquisite, memorizzate, elaborate o trasmesse dai dispositivi IoT;
3. **proteggere i dati personali dei soggetti interessati**: significa proteggere i diritti e le libertà degli individui i cui dati personali sono trattati, al di là dei rischi legati al dispositivo e ai dati in generale.

Il GDPR prevede l'incorporazione delle misure di protezione dati negli stessi sistemi e dispositivi, in modo che essi siano progettati e configurati in maniera da minimizzare l'uso di dati personali e proteggerli adeguatamente. Queste misure compensano quel deficit di consapevolezza nell'utilizzo di dispositivi intelligenti di uso quotidiano, la cui apparente innocuità ci induce a sottovalutarne la potenziale esposizione ad attacchi informatici o comunque la capacità di rivelare, tramite i dati

raccolti, stili e tenore di vita, persino patologie o dipendenze. Inoltre, rispetto alla profilazione e al microtargeting che questi dispositivi possono incentivare, risultano determinanti il diritto di opposizione e quello di contestare la decisione automatizzata, nonché di ottenere l'intervento umano nel processo decisionale.

Dall'analisi delle disposizioni che si occupano specificamente dei minori si coglie che il legislatore europeo ha inteso operare una scelta dettata dalla necessità di adeguare la disciplina giuridica alla realtà fattuale, con l'intento di trovare un equilibrio tra l'esigenza di protezione e quella di accordare ai minori una capacità di autodeterminazione sufficiente a consentire lo sviluppo della loro personalità, prendendo atto che essa si forma anche nella dimensione digitale.

Il Gdpr innova rispetto al passato, prevedendo disposizioni che sono espressione di tale approccio come:

- L'art.6 par.1 lett. f: a mente del quale, laddove la base giuridica del trattamento sia costituita dal legittimo interesse del titolare, egli deve operare con particolare prudenza il bilanciamento tra i propri interessi ed i diritti e le libertà fondamentali;
- L'art.12 che richiede una particolare attenzione nel linguaggio e nella forma con cui devono essere assolti gli obblighi informativi che gravano in capo al titolare, al cospetto di un interessato minorenne;
- L'art.8 che consente ai soggetti maggiori degli anni 16 di esprimere un valido consenso al trattamento dei propri dati personali, tutte le volte in cui il consenso assurga a base giuridica per il trattamento di dati comuni (art.6 lett. a), ma solo con riferimento all'offerta diretta di servizi della società dell'informazione. Tale disposizione lascia un margine di discrezionalità agli Stati nell'individuazione di una soglia di età inferiore agli anni 16, purchè superiore agli anni 13, per ritenere valido il consenso prestato ai fini sopra descritti. Il legislatore italiano, con il d.lgs 101/2018, di adeguamento della legislazione italiana al Gdpr, ha stabilito detta soglia negli anni 14, come prescritto ad oggi dall'art.2-quinquies del d.lgs 196/2003.
- L'art.17 par.1, lett. f) in tema di diritto all'oblio, che conferisce all'interessato il diritto di ottenere dal titolare la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, se essi sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art.8, paragrafo 1.

Accanto a questo quadro normativo che si compone di due poli, da un lato, del riconoscimento di un favor per il minore, promuovendo la sua capacità di autodeterminazione, dall'altro, della previsione di una serie di cautele quali obblighi informativi più forti e diritto di ripensamento, si affiancano azioni di politica educativa a livello europeo, quali ad esempio il Better Internet for Kids, volte a costruire una cultura dell'uso del mezzo digitale, tanto più necessaria considerando che non solo gli adolescenti ma anche i bambini, già in età prescolare, navigano in rete e lo fanno spesso senza la vigilanza dei genitori.

2. SMART TOYS E TUTELA DEI DATI PERSONALI

Contrariamente a quanto si possa pensare, infatti, la cessione di dati personali non avviene solo mediante l'utilizzo di uno smartphone, di un tablet o di un computer: sono tanti i prodotti connessi sviluppati nell'ambito di infrastrutture riconducibili al concetto di Internet of things.

Tra questi è possibile annoverare i cosiddetti wearables – dispositivi elettronici indossabili – gli smart toys – bambole o pupazzi smart sempre e continuamente connessi – o gli assistenti virtuali che sempre più popolano le abitazioni private. Si tratta di prodotti commerciali di sempre maggior diffusione, dotati di una serie di sensori in grado di captare, registrare ed immagazzinare dati in modo continuo ed indistinto.

Questi giocattoli sono in grado di “trattare” (anche) dati personali interagendo con le persone e con l’ambiente circostante tramite microfoni, fotocamere, sistemi di localizzazione e sensori, nonché di connettersi alla rete per navigare online e comunicare con smartphone, tablet, PC e altri smart toys. Come scrive il Garante della privacy, è bene leggere con attenzione l´informativa sul trattamento dei dati personali raccolti, che dovrebbe sempre essere disponibile nella confezione e/o pubblicata sul sito dell´azienda produttrice.

Qualcuno si ricorderà – anzi non si ricorderà – del caso della bambola interattiva Cayla. Biondina, giacca di jeans e gonna rosa. È oggi considerata in Germana uno strumento di spionaggio. L’Autorità garante delle telecomunicazioni l’ha messa al bando l’estate scorsa. Non solo non è più possibile venderla ma non si può neppure detenerla. Chi l’ha acquistata dovrà distruggerla.

È importante comprendere anche quali e quante informazioni saranno acquisite direttamente dal giocattolo (ad esempio, tramite fotocamera o microfono) e come potrebbero eventualmente essere utilizzate (solo per far funzionare lo smart toy o anche per altre finalità). La nostra legislazione già chiede che i sistemi elettronici siano prodotti e configurati per ridurre al minimo la raccolta e il trattamento di dati personali (privacy by design e privacy by default).

Ma al netto della progettazione, ai genitori viene chiesto di studiare questi dispositivi, non solo sotto il profilo della normativa ma soprattutto su quello delle conseguenze che l’interazione con questi dispositivi avrà sulla psicologia dei bambini. Un dato su tutti? Il 57% dei genitori che usano una smart speaker come Alexa o Google Home lo usa per raccontare favole. Anche qui, non c’è giudizio ma solo ricerca degli strumenti per la comprensione degli effetti.

I dati così ottenuti, relativi a comportamenti, abitudini, preferenze, stati di salute possono costituire risorse preziose per comprendere a pieno il funzionamento del corpo umano, tenere traccia delle abitudini di vita degli utenti e, dunque, delle loro preferenze. La disponibilità di una così grande quantità di dati può essere utile per realizzare applicazioni in campo medico-scientifico o per fornire servizi e prodotti sempre più personalizzati.

E’, però, altrettanto evidente che l’intrusività di detti dispositivi nella sfera privata dell’utilizzatore faccia aumentare esponenzialmente il rischio di violazioni della libertà individuale.

Ancora ad oggi l’utente digitale ha scarsa consapevolezza del potere della rete: non si comprende facilmente che ogni informazione, ogni dato personale, che viene messo in rete oggi, resterà nella disponibilità della rete per sempre. Ogni volta che vengono ceduti dati personali, contestualmente viene operata una cessione di parti della propria libertà personale.

Il tema è ben noto al Garante Privacy italiano che nella scheda del 15 ottobre 2018 (disponibile al seguente link: https://www.garanteprivacy.it/iot/smarttoys), più che mai attuale, ha fornito utili suggerimenti ed alcune semplici regole “per giochi a prova di privacy”.
I suggerimenti del Garante si inseriscono in un contesto di buone prassi che dovrebbero essere acquisite prima di relazionarsi con uno smart toys, quali:

- fare attenzione alla descrizione del prodotto per capire come e quando si connette ad internet e come interagirà con le persone. In pratica occorre scoprire cosa fa effettivamente il giocattolo e come interagisce in concreto con i minorenni;
- analizzare se e quali dati vengono raccolti durante il funzionamento;
- leggere e comprendere la privacy policy del produttore facendo particolare attenzione all’uso dei dati, se e come questi vengono condivisi con terze parti;
- consultare il manuale di istruzioni (generalmente reperibile online) per ben comprendere quali siano i controlli e le impostazioni sul gioco offerti ai genitori (es. password, controllo dei dati raccolti tramite account, ecc.);
- informarsi su eventuali aggiornamenti e relativa frequenza del gioco (automatici e/o manuali)

- informarsi online per vedere se in precedenza sono stati sollevati problemi di sicurezza relativi al giocattolo, come una perdita di dati personali.
- tenere d'occhio il minore quando gioca con lo smart toys, in particolare se può inviare o ricevere messaggi. Non è mai consigliabile lasciarli incustoditi.
- spegnere completamente lo smart toys quando non viene utilizzato in modo che non sia vulnerabile allo sfruttamento.

Alcuni trastulli elettronici di ultima generazione, per funzionare a dovere, hanno bisogno di processare i dati personali rilasciati dal bimbo durante il gioco: ascoltano, registrano ed elaborano informazioni in modo continuativo per migliorare e customizzare il livello di interazione e per alimentare un'intelligenza artificiale che deve crescere nel tempo.

I genitori devono essere consapevoli che, con tutta probabilità, qualcuno (il produttore e i suoi partner commerciali) utilizzerà queste stesse informazioni per profilare l'utente e per eseguire su di esso attività di *targeted advertising*. Un intento, questo, che in linea generale è normale, oltre che legittimo: oggi i dati personali derivanti da un acquisto rappresentano un patrimonio su cui architettare strategie per generare una seconda ondata di profitti nella fase *after-sale*.

L'importante è che il produttore sia chiaro e trasparente nel veicolare agli acquirenti i propri intenti di marketing, esplicitando che il profilo sarà alimentato non solo grazie ai dati iniziali – dati di acquisto ed eventuali di *setup* del giocattolo (preferenze, impostazioni via app, etc.) – ma anche con dati derivanti dall'utilizzo in itinere del *device*.

Noi genitori dobbiamo essere consci di tutto questo e, nel caso, chiederci se la cosa sia opportuna: è proprio necessario che parole, pensieri, voci, immagini e abitudini dei nostri bambini finiscano in server remoti per essere costantemente analizzati a fini di profilazione? Siamo consapevoli che talora, se non leggiamo bene le condizioni contrattuali, i profili *consumer* dei nostri piccoli possono essere **venduti ad aziende terze di modo che queste possano veicolare** (magari anche attraverso la vocina o lo schermo dello stesso fidato *smart toy* che giace nelle mani dell'infante) **messaggi pubblicitari mirati** anche di natura subliminale?

È per tale ragione che le parole chiave di una riflessione sul tema dell'uso del mezzo digitale e dei rischi che questo può provocare, tanto nei minori quanto negli adulti, non possano che essere: consapevolezza, educazione e prevenzione.

È, quindi, necessario che venga implementata una cultura della prevenzione e dell'educazione del cittadino digitale all'utilizzo di Internet e dei servizi da esso derivati. Ciò al fine di comprendere e conoscere le implicazioni di comportamenti impropri del mezzo digitale, capaci di condizionare l'esistenza in modo irrimediabile.

È fondamentale, dunque, portare avanti un'opera di sensibilizzazione poiché nessuno strumento normativo, tanto più se di carattere repressivo, per sua natura, sarà mai in grado di stare al passo con lo sviluppo tecnologico.

DANIELE ONORI