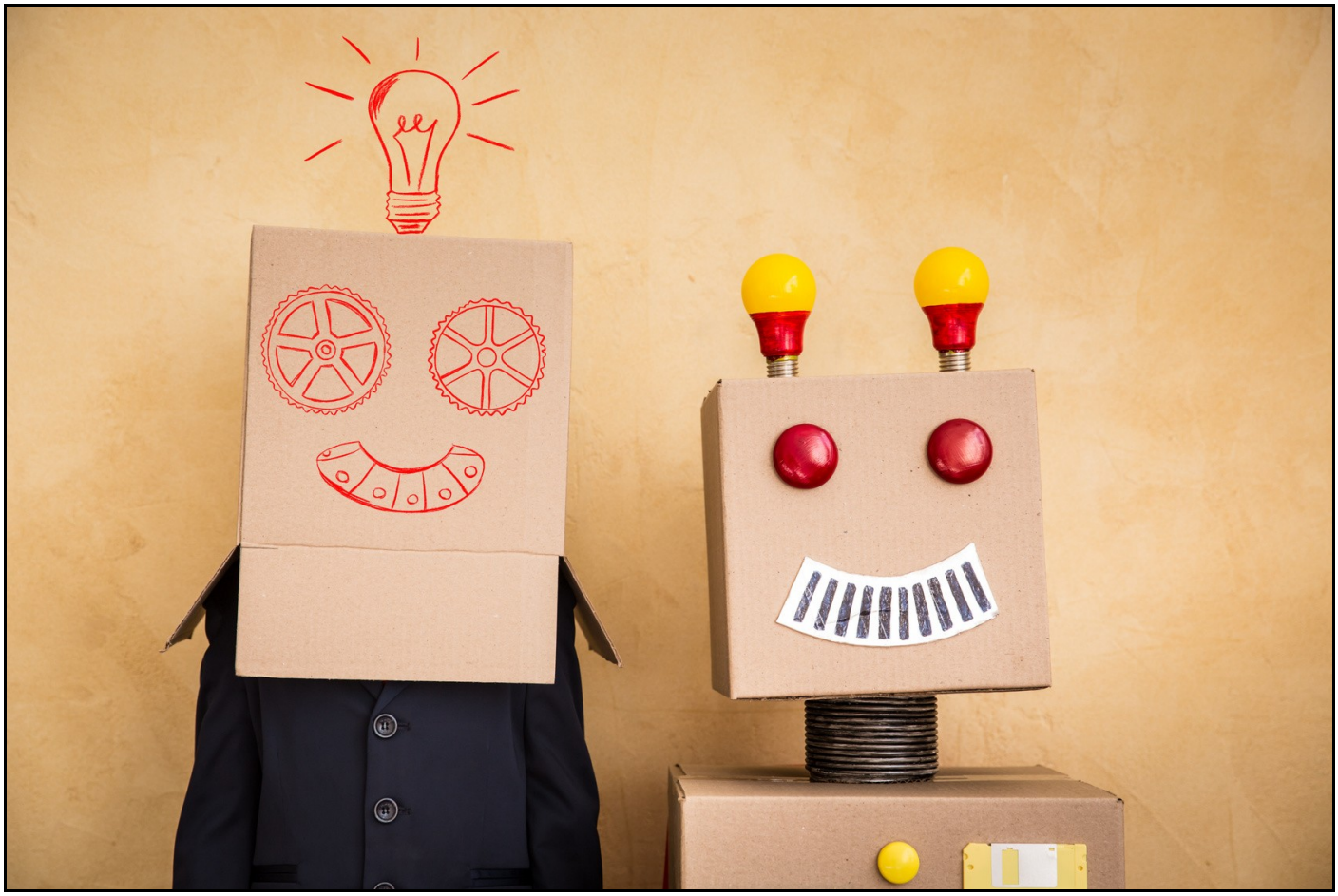


Smart toys: i suggerimenti del Garante per giochi a prova di privacy

La scheda ha mere finalità divulgative e sarà aggiornata in base alle evoluzioni tecnologiche e normative

Cosa sono gli smart toys

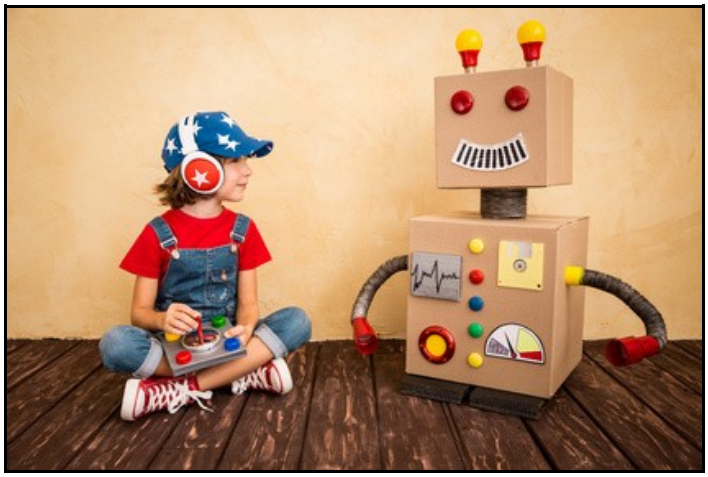
Gli **smart toys** sono giocattoli capaci di **interagire** (tramite microfoni, fotocamere, sistemi di localizzazione e sensori) con le persone e con l'ambiente circostante e di **connettersi** alla rete per navigare online e comunicare con smartphone, tablet, pc, altri smart toys.

Parliamo quindi di bambole, peluche, robot e giochi educativi - ma anche di altri dispositivi per bambini, come i baby monitor - progettati per rapportarsi attivamente con gli esseri umani e, in molti casi, in grado di compiere automaticamente varie operazioni, come registrare suoni, scattare foto, girare video e collegarsi con web e social network.

Occorre quindi ricordare che - per quanto giochi divertenti e a volte anche con funzioni educative - gli smart toys sono pur sempre strumenti che raccolgono, elaborano e comunicano dati e informazioni, con possibili rischi per la privacy, soprattutto quella dei **minori**.

È allora utile conoscere e seguire alcune semplici regole.

Cerca di essere "smart" anche tu: informati su quali e quanti dati tratterà il giocattolo



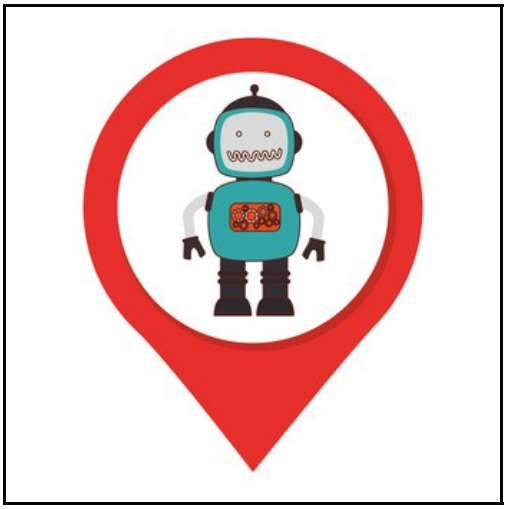
Se per attivare un giocattolo intelligente è necessario registrarsi fornendo dati personali, oppure vengono richieste alcune informazioni (come il nome del bambino o la sua età), è bene leggere con attenzione l'**informativa sul trattamento dei dati personali raccolti**, che dovrebbe sempre essere disponibile nella confezione e/o pubblicata sul sito dell'azienda produttrice.

E' 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).

Non "dire" troppe cose allo smart toy

Nel momento in cui viene attivata la connessione a Internet dello smart toy o della app che lo gestisce, occorre fare attenzione a fornire **solo** le informazioni specificamente necessarie per la registrazione ed eventualmente utilizzare **pseudonimi** per gli account, soprattutto se sono riferiti a minori.

E' opportuno limitare la possibilità di raccolta e memorizzazione di **dati** da parte del giocattolo. Ad esempio, si possono disattivare **strumenti di rilevazione** che possono risultare non indispensabili per il funzionamento, come la geolocalizzazione.



Alcune app utilizzate per gestire smart toys possono richiedere l'accesso alla memoria, al microfono, al WiFi o alla connessione Bluetooth dello smartphone o del tablet su cui vengono installate. Meglio evitare di concedere queste **autorizzazioni** se non sono strettamente necessarie per il funzionamento del giocattolo. In ogni caso, è importante informarsi sempre su **chi** e **come** potrebbe utilizzare i dati raccolti.

Il giocattolo "intelligente" impara interagendo con chi lo usa. Se è in grado di parlare, può allora ripetere le parole che gli vengono dette, comprese eventuali "parolacce", espressioni violente o frasi offensive. E' allora opportuno ricordare che, se si vuole uno smart toy "educato", il punto di partenza è interagire con lui in modo educato.

È bene tenere presente inoltre che gli smart toys, come tutti i dispositivi che sono parte dell'Internet delle cose (IoT), non si limitano ad essere in connessione soltanto con la rete, ma sono anche in grado di "dialogare" tra loro. Questa capacità amplifica la possibilità di incrocio dei dati e di diffusione delle nostre informazioni personali. E' allora importante ricordarsi di utilizzare in modo responsabile **tutti gli oggetti "intelligenti"** eventualmente presenti nell'ambiente domestico in cui viviamo.

Password, impostazioni privacy e sistemi antivirus per un gioco sicuro

Eventuali malintenzionati potrebbero tentare di entrare negli smart toys attraverso la rete, ad esempio per accedere ai dati che contengono, oppure ai microfoni, alle fotocamere e ai sensori di cui sono dotati.

Come per tutti i dispositivi elettronici, una buona regola di base è impostare **password di accesso complesse sicure** per la connessione a Internet dello smart toy, oltre che eventualmente per l'accesso al giocattolo o alla app che lo gestisce.

Se il sistema operativo del giocattolo o della app di gestione prevedono delle **impostazioni privacy,** è opportuno controllarle e regolarle su livelli ottimali di protezione.

Nel caso in cui il software del dispositivo o della app di gestione sia dotato di **sistemi di protezione anti-virus**, è importante verificare che questi siano attivi e tenerli costantemente aggiornati.

Se non lo usi, spegnilo

Per limitare l'acquisizione e la trasmissione di dati, è bene **spegnere** lo smart toy e **disconnetterlo dalla rete** quando non viene utilizzato.

Basti pensare che un giocattolo capace di ascoltare e riconoscere le voci lasciato acceso in un ambiente domestico potrebbe essere in grado di raccogliere e trasmettere informazioni sui gusti, le scelte e le abitudini non solo del bambino, ma dell'intera famiglia.

Social, ma non troppo

In alcuni casi, l'app di gestione dello smart toy consente di condividere online foto e video.

E' buona abitudine **non lasciare che i più piccoli utilizzino questa funzione da soli** e, in ogni caso, è utile passare del tempo in loro compagnia quando giocano con dispositivi connessi alla rete, spiegando **quali rischi possono correre** e **cosa è meglio evitare di fare**.

Se l'app di gestione lo consente, si possono poi impostare password e limitazioni d'uso, per evitare che i minori la possano utilizzare quando non c'è un adulto presente.

Se dai via il giocattolo, non dare via i tuoi dati

Nel caso in cui il giocattolo sia **venduto, regalato o gettato nei rifiuti**, è bene disattivare gli eventuali account personali creati per connetterlo online e provvedere alla **cancellazione di tutti i dati** eventualmente registrati al suo interno o sulla app di gestione.

I dati raccolti potrebbero comunque essere stati trasmessi e conservati nei database dell'azienda produttrice o di altri soggetti: è allora opportuno valutare di chiederne la cancellazione.

Giocattoli a prova di privacy

Il **Codice privacy** (in particolare l'art. 3) e il **nuovo Regolamento UE/2016/679** in materia di protezione dati (che sarà definitivamente applicabile il 25 maggio 2018) prevedono 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)*.

Tali regole debbono essere conosciute e rispettate anche dai produttori di smart toys ed eventualmente certificate.

Nei casi in cui ci siano dubbi sull'effettivo rispetto delle norme o sul corretto uso dei propri dati personali, ci si può rivolgere al Garante per la protezione dei dati personali, scrivendo a urp@gpdp.it.