**Come gestire i dati personali nel metaverso?**

**Giuseppe Vaciago e Stefano Ricci**

**(**[**https://www.shutterstock.com/it/image-vector/most-promising-business-future-metaverse-2031697775**](https://www.shutterstock.com/it/image-vector/most-promising-business-future-metaverse-2031697775)**)**

Se la protezione dei dati personali è un problema nell'attuale mondo dominato dai social media, **il metaverso aggiunge una dimensione di notevole complessità al quale si aggiunge un diverso livello di raccolta e utilizzo dei dati** soprattutto quando gli utenti sfrutteranno tutte le nuove tecnologie offerte dalla realtà virtuale. Dai “Power Glove” della mitica Nitendo “8 bit” ai guanti aptici abilitati all'elettromiografia il passaggio non è banale se si considera che tali guanti saranno in grado di raccogliere dati estremamente precisi sulla funzionalità dei muscoli della mano e del sistema nervoso dell’utente. Tutto questo in un contesto dove gli avatar codec sviluppati da Meta permetteranno, con estrema facilità, ai bambini di apparire come adulti.

In poche parole, **il metaverso confonde le linee tra il reale e il virtuale su una scala mai vista** prima raccogliendo una grande quantità di informazioni personali che non riguarderanno solo le abitudini di consumo o le opinioni politiche, religiose e sessuali, ma anche i movimenti, il battito cardiaco, le onde cerebrali e, da ultimo, le emozioni vissute nelle varie esperienze di vita virtuale. Gli utenti, attraverso molteplici canali, come i dispositivi indossabili, i microfoni, le videocamere e i monitor cardiaci vorranno sempre di più offrire al metaverso questi dati per poter soddisfare la naturale curiosità umana verso le novità che la tecnologia ci sta fornendo con una rapidità che sfida la stessa legge di Moore.

Alla luce di questo scenario, quali sono gli aspetti legali sui quali l’imprenditore del metaverso dovrà concentrarsi?

**Consenso e informativa**

Nel metaverso il consenso dovrebbe essere ripensato specialmente quando i grandi marchi entreranno in pista con i loro prodotti e la pubblicità. In un contesto di questo tipo, **i meccanismi di consenso devono essere pensati in ottica “legal design”** dando la possibilità all’utente di comprendere il trattamento effettuato e l’eventuale profilazione condotta dal titolare del trattamento sui dati dell’utente. Inoltre, deve essere garantito un meccanismo, presente oramai in quasi tutte le piattaforme social, che consenta in tempo reale all’utente di aggiornare i suoi consensi e le sue preferenze di utilizzo.

**Trasparenza e intelligenza artificiale**

Gli utenti **devono essere informati quando stanno interagendo con l'intelligenza artificiale** nel rispetto dell’articolo 22 del GDPR che prescrive regole molto rigide qualora l’interessato sia sottoposto ad un trattamento automatizzato. In un recente sondaggio fatto a più di 6.000 utenti in 6 diversi Paesi, è stato chiesto se avessero mai interagito con una intelligenza artificiale. Solo un terzo (34%) ha risposto di sì, ma in realtà più di due terzi (84%) aveva incontrato un’interfaccia di intelligenza artificiale. Questo significa che il 50% degli utenti intervistati non sono stati in grado di comprendere se stavano interagendo con un’intelligenza artificiale o con un umano. Per una completa trasparenza, i bot dovrebbero essere dotati di etichette in modo che gli utenti sappiano sempre con chi stanno condividendo i loro dati.

**Data Protection Impact Assessment e Legitimate Interest Assessment**

Le aziende che intendono operare nel metaverso dovranno imporsi, nell’ottica del principio dell’accountability, una **rigida autoregolamentazione** attraverso delle attente valutazioni che consentano di identificare eventuali rischi per i diritti e le libertà degli interessati (Data Protection Impact Assessment). Tali valutazioni dovranno essere condotte da team in grado di avere sia una competenza legale che tecnologica in modo da comprendere il tipo di tecnologia utilizzata nel metaverso.

Inoltre, in molte situazioni, sarà necessario valutare il legittimo interesse del titolare ad effettuare un **trattamento senza il consenso** (Legitimate Interest Assessment). Anche in questo caso, la documentazione prodotta al termine dell’analisi deve essere accuratamente conservata dal titolare del trattamento qualora venga richiesta dall’Autorità Garante per la Protezione dei Dati Personali.

**Monetizzazione trasparente**

Il 2020 ha visto “scoppiare” la bolla della pubblicità online, come racconta molto bene il Correspondent in un articolo intitolato “The new dot com bubble is here: it’s called online advertising”. **La “personalizzazione” venduta dai grandi network**, “spacciata” per precisa e puntuale, **semplicemente non funziona** e il mercato se ne sta accorgendo: sempre più realtà si affidano al RTB (Real Time Bidding) andando a comprare e vendere "cookies" di profilazione sempre più precisi per dare un senso agli investimenti pubblicitari che non possono più essere "gettati nel mucchio".

Se quindi il futuro va verso la **monetizzazione del dato personale del singolo utente**, tale processo di trasformazione deve avvenire in modo trasparente per contrastare le preoccupazioni sull'uso improprio dei dati. Sotto questo profilo, il metaverso può diventare un terreno estremamente fertile per la monetizzazione del dato attraverso il gaming, ma proprio perché ci sono grandi opportunità, ci deve essere massima attenzione nel rispetto di una comunicazione chiara e trasparente nei confronti dell’interessato.

**Sicurezza e Data Breach**

Il metaverso, proprio in considerazione dell’enorme volume di dati degli utenti che il metaverso ospiterà, dovrebbe essere **sicuro “by design”**. Gli sviluppatori, in un mondo perfetto, dovrebbero azzerare ogni rischio di vulnerabilità adottando principi di secure coding.

Sappiamo bene, tuttavia, che queste raccomandazioni potranno essere difficilmente messe in atto, in quanto la crescita del cybercrime e degli attacchi informatici non potrà non riguardare anche il metaverso. Per questa ragione, è importante che chi intenda fare business in questa nuova realtà si tuteli attraverso una **policy data breach** che non sia solo formalizzata a livello documentale, ma che costituisca un meccanismo perfettamente oliato all’interno del quale tre figure professionali gestiranno l’eventuale crisi: il data protection officer e/o il consulente legale, il CISO e un esperto di comunicazione.

Un’errata gestione di un data breach potrebbe rivelarsi costosa per le aziende e creare un danno reputazionale dal quale una società potrebbe riprendersi molto lentamente.

**Gestione dei diritti degli interessati**

Uno degli aspetti cruciali nella gestione della protezione dei dati personali sarà sicuramente la **gestione dei diritti degli interessati all’interno del metaverso**. Tali diritti sono: l’accesso (art. 15 GDPR) finalizzato a chiedere conferma che sia o meno in essere un trattamento di dati personali; rettifica (art. 16 GDPR) per chiedere di rettificare o integrare i dati forniti, qualora inesatti; cancellazione (art. 17 GDPR) per chiedere che i dati trattati vengano cancellati; limitazione di trattamento (art. 18 GDPR) affinché i dati trattati vengano contrassegnati in modo da limitarne il loro trattamento in futuro; portabilità dei dati (art. 20 GDPR) al fine di ottenere la ricezione di dati personali, o la trasmissione dei dati ad altro titolare, in un formato strutturato; opposizione (art. 21 GDPR): per opporsi in qualunque momento al trattamento dei dati, salvo che vi siano motivi legittimi per procedere al trattamento.

La gestione di queste richieste deve avvenire in modo oculato in quanto tutte le richieste devono ricevere un’adeguata e motivata risposta nel termine di 30 giorni estendibile fino ad un massimo di 90 giorni. Immaginiamo, ad esempio, una richiesta di cancellazione dei dati di un utente che ha navigato per anni nel metaverso. Non è banale garantire una completa e definitiva cancellazione del dato.

Inoltre, nell’ultimo anno sono nate una serie di iniziative volte ad **assistere gli utenti nell’esercizio dei loro diritti** che potrebbero far crescere il numero delle richieste anche nel contesto del metaverso. Si pensi, ad esempio, all’italiana Weople o all’israeliana Mine che stanno diventando dei punti di riferimento nel settore.

**Conclusioni**

Nel metaverso, il motto “nothing to hide” con il quale si demonizzava l’eccessiva attenzione al rispetto della privacy degli utenti, potrebbe essere sostituito da “something to protect”. Chi vorrà fare business nel metaverso non potrà sottovalutare questo cambio di paradigma e investire in una privacy by design che parta da un presupposto fondamentale per il prossimo futuro: implementare procedure di verifica dell'età per garantire interazioni adeguate all'età nelle sue piattaforme.