Il metaverso: rischi e potenziali minacce alla sicurezza

Il metaverso

Il metaverso[1] può essere definito come un'evoluzione di Internet, attualmente in fase di progettazione, basata su una realtà virtuale immersiva nella quale gli utenti potranno interagire con rappresentazioni digitali di se stessi e di altre persone e con oggetti digitali. Utilizzando dei singoli *avatar* virtuali, gli utenti, in numero illimitato, potranno muoversi, interagire con altre persone, lavorare, apprendere, giocare o svolgere altre attività in spazi virtuali tridimensionali permanenti e condivisi (tra gli altri, si veda Vonorio 2021).

Secondo alcune stime recenti, lo sviluppo di queste nuove tecnologie potrebbe produrre un impulso all'economia globale quantificabile in 1.400 miliardi di dollari entro il 2030 e il 25% delle persone potrebbe trascorrere almeno un'ora al giorno nel metaverso entro il 2026 (dati citati in Europol 2022, 5). Queste stime segnalano la portata delle conseguenze che il metaverso potrebbe comportare.

Non sorprende quindi che grandi aziende tecnologiche abbiano già deciso di dedicare ingenti energie a questo settore. Nell'autunno del 2021, Facebook ha annunciato investimenti massicci. Il 28 ottobre 2021 il Presidente e amministratore delegato nonché fondatore dell'azienda, Mark Zuckerberg, ha persino annunciato la decisione di cambiare il nome della società madre da Facebook in Meta (ufficialmente Meta Platforms, Inc.), ribadendo esplicitamente l'interesse per questo ambizioso progetto. Nell'ottobre del 2022 sono tuttavia emerse alcune indicazioni secondo le quali Meta starebbe affrontando ritardi e difficoltà nello sviluppo di un proprio metaverso (Heath 2022). In aggiunta a Meta, anche altre aziende tecnologiche, con sede in Paesi occidentali, come Microsoft, o in altre regioni (specialmente in Cina), si sono impegnate in questo settore (tra gli altri, Consiglio dell'Unione Europea 2022).

A questo proposito, vale la pena di osservare che, se grandi imprese private occupano oggi un ruolo centrale nello sviluppo del metaverso, molte delle tecnologie che ne sono alla base derivano da iniziative di ricerca pubblica a lungo termine, anche di natura militare (Vonorio 2021).

I rischi del metaverso

Come la maggior parte delle tecnologie, il metaverso potrebbe offrire notevoli opportunità, ma potrebbe anche comportare vulnerabilità e pericoli, comprese potenziali minacce alla sicurezza (in particolare, Europol 2022; Interpol 2022).

In aggiunta a diverse attività di criminalità comune (tra gli altri, Europol 2022), il metaverso potrebbe essere utilizzato per promuovere forme di estremismo violento e attività terroristiche (tra gli altri, Elson et al. 2022).

In primo luogo, questa nuova tecnologia potrebbe facilitare attività di indottrinamento e di reclutamento a favore di gruppi estremisti violenti. Com'è noto, internet si è già rivelato uno strumento assai utile per questi processi (tra gli altri, Marone 2019). Lo sviluppo del metaverso potrebbe determinare un ulteriore incremento dei rischi, fornendo ambienti virtuali in cui messaggi estremistici possono essere efficacemente discussi e diffusi.

Analogamente, il metaverso potrebbe costituire un terreno fertile per attività di misinformazione e di disinformazione (cf. Marone 2022), ancor più insidiose perché ritagliate su misura in base alle caratteristiche dei destinatari (in particolare, Europol 2022, 20).

[1] Il concetto di "metaverso" (*metaverse* in inglese) deriva dal romanzo di fantascienza *Snow Crash*, scritto nel 1992 dall'autore statunitense Neal Stephenson.

Estremisti violenti potrebbero altresì costruire interi spazi virtuali in cui le loro credenze e norme sociali vengono poste in atto e propagandate, in una sorta di mondo parallelo estremistico (formato, per esempio, da "califfati" jihadisti o comunità fondate sui principii del suprematismo bianco) (Europol 2022, 19).

In secondo luogo, il metaverso rischia di offrire nuove opportunità per il coordinamento tra estremisti violenti e persino per la pianificazione di atti di violenza. Per esempio, sulla base di preliminari attività di raccolta delle informazioni e di ricognizione, estremisti violenti potrebbero creare ambienti virtuali che riproducano l'effettiva disposizione di edifici, strade e altri oggetti fisici del mondo reale al fine di selezionare con precisione gli obiettivi da colpire, preparare il compimento di attacchi, individuare vie di fuga e studiare piani alternativi in caso di inconvenienti o imprevisti (Elson et al. 2022).[2]

Il metaverso potrebbe infine offrire nuovi bersagli per azioni ostili direttamente nel metaverso. Estremisti violenti e altri attori malintenzionati potrebbero, per esempio, interrompere le attività e i servizi di soggetti economici e autorità pubbliche. Potrebbero inoltre recare danno o oltraggiare eventi o luoghi virtuali (a titolo di esempio, siti virtuali di carattere politico o religioso o con funzioni commemorative). A questo proposito, può essere tuttavia utile ricordare che molti studi hanno mostrato come, nel complesso, i terroristi tendano a essere poco inclini alle innovazioni tattiche e operative (tra gli altri, Dolnik 2007; Gill et al 2013; cf. Marone 2021).

Questo genere di azioni ostili potrebbe provocare seri danni materiali nel mondo reale (perdite finanziarie, danni reputazionali, ecc.). Potrebbe altresì produrre rilevanti conseguenze simboliche (Elson et al. 2022); le indicazioni attualmente disponibili suggeriscono, infatti, che le reazioni psicologiche a fatti che avvengono nella realtà virtuale tendono a non si differenziarsi sensibilmente da quelle che hanno luogo nel mondo reale (Jurecic e Rozenshtein 2021).

La risposta alle minacce potenziali

I rischi associati al metaverso richiedono risposte adeguate. Innanzitutto, le imprese private impegnate nella costruzione di questi spazi virtuali potranno essere chiamate a individuare e bandire attività e individui che promuovano l'odio e la violenza. Nondimeno, è opportuno notare che, anche qualora vi sia un'effettiva volontà di impegnarsi in tale direzione (anche a costo di ridurre eventualmente margini di profitto), il contenimento dell'odio e della violenza si sta già rivelando un compito non agevole nella sfera di internet (si veda Jurecic e Rozenshtein 2021).

Le autorità pubbliche saranno quindi chiamate a intervenire per contenere questi rischi e vulnerabilità del metaverso. A questo scopo, esse potrebbero fin da ora rafforzare la loro presenza *online*, anche negli spazi virtuali più sofisticati, formare il proprio personale in vista di questo tipo di sfide e promuovere il confronto con le principali aziende tecnologiche (si veda Europol 2022).

Altri soggetti rilevanti, come ricercatori e attivisti, potrebbero giocare un ruolo rilevante nella risposta alle minacce poste dalle tecnologie più avanzate del mondo virtuale (Elson et al. 2022).

Conclusioni

Sebbene ad oggi il metaverso costituisca ancora un progetto in costruzione, appare evidente che sia opportuno dedicare la dovuta attenzione alle minacce potenziali che potrebbe presentare. Il metaverso potrebbe infatti ingigantire rischi e vulnerabilità già presenti nel Web. Analogamente, è utile riflettere sin da ora sulle risposte che potrebbe essere necessario mettere in campo.

[2] A titolo di esempio, si può segnalare che nel febbraio 2022 un adolescente siberiano è stato condannato a cinque anni di carcere per terrorismo con l'accusa di essersi impegnato nel progettare un attacco contro un edificio virtuale dell'FSB (la principale agenzia di sicurezza della Federazione Russa), creato appositamente su Minecraft (il popolare videogioco in 3D che contiene già alcuni elementi preliminari di metaverso) (Euronews 2022; cf. Lakhani et al. 2021).

Bibliografia

- Dolnik, A. (2007). *Understanding Terrorist Innovation: Technology, Tactics and Global Trends.* Abingdon: Routledge.
- Consiglio dell'Unione Europea (2022). Metaverse – Virtual World, Real Challenges. Council of the European Union – General Secretariat, 9 marzo, testo disponibile al sito: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf (consultato il 3 novembre 2022).
- Elson, J. S. Austin, C. D., Hunter, S. (2022). The Metaverse Offers a Future Full of Potential – for Terrorists and Extremists, Too. VOX-Pol, 2 febbraio, testo disponibile al sito: https://www.voxpol.eu/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too/ (consultato il 3 novembre 2022).
- Euronews (2022). Russian teen jailed for 5 years over 'terrorism' plot to blow up virtual spy HQ on Minecraft. Euronews, 10 febbraio, testo disponibile al sito: https://www.euronews.com/next/2022/02/10/russian-teen-jailed-for-5-years-over-terrorism-plot-to-blow-up-virtual-spy-hq-on-minecraft (consultato il 3 novembre 2022).
- Europol (2022). *Policing in the Metaverse: What Law Enforcement Needs to Know*. Observatory Report, Europol Innovation Lab.
- Gill, P. Horgan, J., Hunter, S. T., Cushenbery, L. D. (2013). Malevolent creativity in terrorist organizations. *The Journal of Creative Behavior* 47: 125-151.
- Heath, A. (2022). Meta's flagship metaverse app is too buggy and employees are barely using it, says exec in charge. *The Verge*, 7 ottobre, testo disponibile al sito: https://www.theverge.com/2022/10/6/23391895/meta-facebook-horizon-worlds-vr-social-network-too-buggy-leaked-memo (consultato il 3 novembre 2022).
- Interpol (2022). *Interpol Technology Assessment Report on Metaverse*. Interopol, ottobre, testo disponibile al sito: https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse (consultato il 3 novembre 2022).
- Jurecic, Q., Rozenshtein, A. Z. (2021). Mark Zuckerberg's Metaverse Unlocks a New World of Content Moderation Chaos. *Lawfare*, 3 novembre, testo disponibile al sito: https://www.lawfareblog.com/mark-zuckerbergs-metaverse-unlocks-new-world-content-moderation-chaos (consultato il 3 novembre 2022).
- Lakhani, S., White, J., Wallner, C. (2021). *The Gamification of (Violent) Extremism: An Exploration of Emerging Trends, Future Threat Scenarios and Potential P/CVE Solutions*. RAN Policy Support – European Commission.
- Marone F., a cura di (2019). *Digital Jihad: Online Communication and Violent Extremism*. Report, ISPI.
- Marone, F. (2021) A Farewell to Firearms? The logic of weapon selection in terrorism: the case of jihadist attacks in Europe. *Global Change, Peace & Security* 33: 221-240.
- Marone, F. (2022). L'evoluzione della disinformazione come minaccia ibrida. Osservatorio Strategico 03-2022, Prima parte, IRAD – CASD, Ministero della Difesa.
- Vonorio, F. (2021). *Metaverso e Sicurezza Nazionale. Internet 3.0 e Nuovo Ordine Mondiale Digitale*. Istituto Italiano di Studi Strategici.