**Come proteggersi dalle truffe nel metaverso**

**Marco Tullio Giordano**

(<https://www.shutterstock.com/it/image-vector/data-protection-vector-illustration-cartoon-flat-1808414635>)

Come ogni territorio di frontiera, anche il metaverso presta il fianco ad alcuni rischi - sempre presenti quando si parla di innovazione e nuove tecnologie - più che per l’incolumità dei suoi frequentatori, per l’integrità dei loro fondi e dei digital asset coinvolti. Del resto, se anche un giorno, quando la polvere si sarà finalmente posata su questo novello Far West, si potranno sicuramente scorgere le fondamenta di una nuova e laboriosa San Francisco, attualmente siamo nel bel mezzo della corsa all’oro e - si sa - in questa fase non è possibile evitare l’accorrere di banditi, razziatori di bestiame, imbonitori ed altri soggetti che preferiscono, alla onesta collaborazione, comportamenti atti ad approfittarsi della confusione e della scarsa dimestichezza del prossimo.

Questo, tuttavia, non è un buon motivo per desistere dall’esplorazione del metaverso, ed anzi, deve essere un monito a non abbassare mai la guardia ma, al contempo, ad appropriarsi di spazi comuni che, seppur virtuali, sono dedicati alla socialità, al confronto ed alla collaborazione tra gli individui.

**Uno, nessuno, centomila: la verifica dell’identità dei creators e dell’originalità dei digital asset**

Il rischio principale, nel metaverso così come del resto nell’internet tradizionale, rimane quello di non poter effettivamente conoscere la reale identità delle controparti con cui si interagisce. Fin dagli albori della rete, i navigatori più incauti non hanno mai tenuto in considerazione il fatto che, dall’altra parte dello schermo, ci possa essere un individuo che mente sulla propria reale identità e sulle caratteristiche riferite nei rapporti online. Nei mondi virtuali, questa situazione è ulteriormente accentuata dal fatto che ciascun utente può creare un **avatar** - una rappresentazione grafica e virtuale di sè - completamente diverso dalla propria reale identità.

Ora, se questo fenomeno è indice del grado di libertà ed autodeterminazione degli utenti del metaverso - che vuole, dichiaratamente, essere un mondo parallelo dove ognuno sia libero di interpretare la propria essenza nel modo che meglio ritiene, è pur vero che il fenomeno può indurre ad errori di valutazione e, nel peggiore dei casi, allo sfruttamento della fiducia altrui per porre in essere raggiri o, peggio, condotte illecite.

L’ordinamento prevede, a tutela di queste situazioni, la contestabilità del reato di **sostituzione di persona** (art. 494 c.p.): il furto d’identità consiste nel sostituirsi illegittimamente ad un’altra persona e di nascosto, con il fine di indurre gli altri in errore e quindi ricavarne un vantaggio personale, non necessariamente economico, o procurare un danno alla persona sostituita. E tale condotta non esclude che si possano contestare anche la truffa (art. 640 c.p.) o il trattamento illecito di dati (art. 167 del Codice Privacy), ove rinvenibili.

Oltre al camuffamento della propria identità, tuttavia, coloro i quali volessero illecitamente approfittarsi della buona fede delle loro controparti nel metaverso, potrebbero fittiziamente dichiararsi titolari di **digital asset contraffatti** o privi dei diritti di paternità o di sfruttamento patrimoniale ad essi connessi. Nessuno impedisce, infatti, di creare un NFT contraffatto, o in violazione dei diritti di privativa, raffigurante un’opera d’arte, un brano musicale, un oggetto di design, un prodotto coperto da marchio o brevetto e - di conseguenza - di metterlo in vendita in un marketplace online o scambiarlo direttamente con altri frequentatori del metaverso.

Se da un lato, i grandi marchi si stanno già attrezzando per attuare campagne di monitoraggio degli store online, come del resto fanno da anni con i market legali, e sono alle cronache le prime diffide alla rimozione di prodotti coperti da marchi e diritti di privativa, anche gli utenti hanno a disposizione alcuni strumenti per verificare l’identità delle loro controparti e la genuinità dei digital asset che vengono offerti nel metaverso. Trattandosi di scambi di token crittografici, che avvengono sulla blockchain, infatti, vi è modo di sfruttare la trasparenza e l’immutabilità del registro distribuito al fine di indagare l’origine dell’asset stesso e le interazioni che il suo proprietario o il suo creatore ha posto in essere prima di arrivare sino a noi. Strumenti di **blockchain analysis** come quelli messi a disposizione da [Chainanalysis](https://www.chainalysis.com/) o da [Cyphertrace](https://ciphertrace.com/) permettono, infatti, di indagare le precedenti transazioni riferibili ad un wallet, ad un indirizzo o ad uno smart contract e verificare, ad esempio, la provenienza di un NFT, la sua origine, i precedenti proprietari, ma anche le ulteriori interazioni che il suo possessore ha posto in essere sulla rete. Certo, questo non mette al riparo da truffe articolate e studiate ad arte, ma permette almeno una prima scrematura: se le tracce indelebili sulla blockchain portano ad interazioni con il deep web, con marketplace illegali, con indirizzi inseriti in blacklist per via di precedenti illeciti che li hanno visti coinvolti, è il caso di desistere da qualsivoglia interazione. Ugualmente, se i wallet coinvolti non risultano essere quelli pubblicamente dichiarati - o facilmente reperibili grazie a tecniche di **OSINT, acronimo di Open Source Intelligence** - con buona probabilità il nostro interlocutore potrebbe essere un impostore e sarà meglio approfondire la verifica di quanto sta dichiarando nell’interazione con noi.

**Pagamenti in valute virtuali e rischio di double-spending nel metaverso**

Sotto un altro punto di vista, se è vero che le valute virtuali e, più in generale, i crypto-asset sono strumenti di libertà ed indipendenza finanziaria e garantiscono agli individui una proprietà disintermediata dei propri digital asset, è il caso di tenere a mente che **l’assenza di un intermediario centralizzato** - sia esso una banca, una piattaforma di vendita, un marketplace tradizionale - impedisce di fare affidamento sulla concreta possibilità di intervento *ex post* nel caso qualcosa vada storto.

Ogni transazione economica effettuata sulla blockchain, infatti, è per sua stessa natura irripetibile ed immutabile. Se si sbaglia indirizzo di destinazione, ad esempio, non vi è modo di chiedere la restituzione di quanto inviato. Non c’è un ufficio reclami, né tantomeno un intermediario che possa intervenire per sistemare le cose in caso di errore. Il rischio è quello di perdere i propri fondi, o i propri beni digitali, irrimediabilmente.

A prescindere dai potenziali errori degli utenti, tuttavia, il funzionamento dell’algoritmo di consenso, che permette ai nodi di una blockchain di validare le transazioni ed iscriverle sulla catena di blocchi, viene sfruttato da agenti malevoli per mettere a punto la truffa del c.d. **double spending**: la “doppia spendita” è un potenziale problema che può emergere in un sistema di moneta digitale in cui gli stessi fondi vengono inviati, o spesi, a due destinatari contemporaneamente. Se qualcuno vi paga in criptovaluta per cedergli un vostro NFT nel metaverso, ad esempio, è sempre meglio attendere che il pagamento abbia ricevuto un certo numero di conferme sulla blockchain. Finchè non sarà stato validato, infatti, il suo autore potrà sempre replicare la stessa spesa, dirottando i fondi su un suo indirizzo di favore e facendo leva su una pool di validazione più potente e veloce: così facendo, voi avrete inviato il vostro bene digitale e lui tornerà anche in possesso della somma pagata per averlo.

**Gli smart contract e la funzione di escrow a tutela dei consumatori: attenzione al codice sorgente.**

Per evitare inconvenienti come quello sopra descritto, nel mondo delle valute virtuali - e quindi anche nel metaverso - si utilizzano spesso gli escrow. Tecnicamente un **escrow** è un **deposito fiduciario**, ossia un accordo in cui una terza parte (estranea alla transazione) detiene e regola il pagamento di una somma tra due parti (acquirente e venditore) coinvolte in una determinata operazione. In questo modo, le transazioni saranno sempre sicure, in quanto il pagamento verrà mantenuto in un conto di deposito fiduciario e verrà liberato solo quando tutti i termini dell’accordo saranno rispettati.

Sulla blockchain, la funzione di escrow è generalmente affidata ad uno **smart contract**: un software che esegue in maniera automatizzata ed immodificabile le clausole di un contratto tra le parti. In questo modo, non c’è intervento umano e - nel momento stesso in cui il venditore ha consegnato il bene digitale - la somma pagata dall’acquirente e vincolata nello smart contract che fa da escrow viene sbloccata e recapitata al suo destinatario.

L’argomento è utile per ricordare che gli smart contract eseguono esclusivamente le operazioni codificate nel loro codice sorgente, secondo il principio “**code is law**”: se il programmatore ha predisposto delle clausole errate, o dolosamente differenti da quanto dichiarato, una volta che le parti avranno interagito con lo smart contract, non vi è modo per lamentarsi dell’errore o del codice malevolo. Questa condizione, in alcuni casi, ha portato all’utilizzo doloso di smart contract scritti appositamente in maniera difforme da quanto dichiarato: programmi che prevedono il dirottamento dei fondi verso indirizzi terzi, wallet in cui è possibile soltanto depositare fondi, ma non prelevarli (le c.d. “**honeypot**”), indirizzi in cui i fondi non sono lockati e vengono svuotati dai loro proprietari non appena un numero elevato di utenti ha depositato le proprie criptovalute (tecnicamente si dice “**rug pull**”, tirare il tappeto da sotto i piedi degli incauti utenti).

A tutela di tutti questi rischi, è sempre bene verificare - anche tramite tools automatizzati come [www.honeypot.is](http://www.honeypot.is) o [www.rugdoc.io](http://www.rugdoc.io) - la bontà del codice di uno smart contract con cui si intende interagire: lo strumento analizzerà il codice del contratto a caccia di eventuali comandi fraudolenti ed assegnerà un punteggio di affidabilità al contratto con cui intendete interagire.