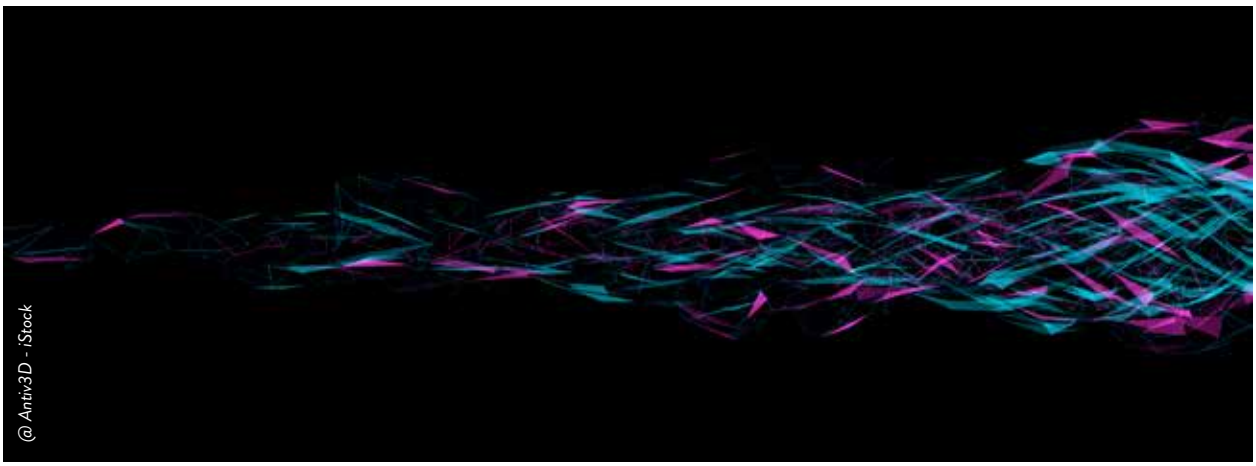
SMART CONTRACT, LA SFIDA DEL GDPR

di GIACOMO CORVI

LA DIFFUSIONE DELLA BLOCKCHAIN OFFRE LA SUGGESTIONE DI CONTRATTI IN GRADO DI ESEGUIRE AUTONOMAMENTE LA VOLONTÀ DELLE PARTI. LA TUTELA DEI DATI PERSONALI, SANCITA DAL REGOLAMENTO EUROPEO, PONE TUTTAVIA CRITICITÀ CHE RISCHIANO DI MINARNE LO SVILUPPO



@ Antiv3D - iStock

Il 31 ottobre 2008, con la pubblicazione del cosiddetto *white paper*, il fantomatico **Satoshi Nakamoto** gettava le fondamenta della *blockchain*. Sono passati più di dieci anni da quella data. E tante sono le aspettative che questo registro elettronico e distribuito, alla base del *bitcoin* e di altre monete virtuali, ha saputo alimentare nei settori più disparati: entro il 2025, secondo le stime del **World Economic Forum**, il 10% del Pil mondiale sarà prodotto da attività e servizi che saranno erogati e distribuiti attraverso la tecnologia blockchain.

Le possibili applicazioni, come accennato, sono tante: dalla sicurezza informatica al trasferimento di denaro, passando persino per la validazione dei risultati elettorali. L'ultimo passo, secondo molti, saranno probabilmente gli *smart contract*, ossia protocolli informatici che sfruttano le potenzialità della blockchain per eseguire i termini di un contratto al verificarsi di determinate condizioni. Il tutto senza la necessità di terze parti o, più in generale, di un qualsiasi intervento umano che vada oltre la semplice programmazione. Sul tema è intervenuto recentemente anche il legislatore italiano che, con il cosiddetto ddl *Semplificazioni*, ha ammesso la validità giuridica della "memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti".

I punti critici però non mancano. A cominciare da una tutela dei dati personali che, come emerso nel corso

del convegno *Persone in rete – I dati tra poteri e diritti*, promosso dallo studio legale **Nctm** lo scorso 15 gennaio, rischia di venir sacrificata sull'altare del progresso tecnologico.

LA PRIVACY AI TEMPI DEL WEB

"Dobbiamo comprendere che il valore del dato personale equivale a libertà, e nessuno metterebbe a rischio la proprio libertà", ha esordito **Antonello Soro**, presidente dell'autorità garante per la protezione dei dati personali, nelle battute iniziali della mattinata. E dobbiamo comprenderlo soprattutto oggi, ai tempi del web, quando "la persona stessa diventa dato e viene esposta in un'arena, quella digitale, che non è presidiata come l'ambiente fisico in cui siamo abituati a muoverci". Anche perché, ha aggiunto, "la rete non conosce confini e ha pesanti ripercussioni anche sulla nostra vita di tutti i giorni". Il recente caso che ha coinvolto **Facebook** e **Cambridge Analytica** sta lì a ricordarcelo.
Per Soro, l'unica soluzione è mantenere la bussola puntata sulla tutela della dignità della persona. Solo così, ha osservato, "sarà possibile superare le sfide sempre più complesse che il progresso tecnologico ci pone davanti". Magari attraverso l'individuazione di standard etici a livello sovranazionale che sappiano garantire il rispetto della dignità personale.

LA MINACCIA DELL'ALGOCRAZIA

La tutela della privacy e della dignità personale deve declinarsi nello svolgimento di qualsiasi attività. Ne è ben consapevole **Armando Spataro**, magistrato ed ex procuratore di Torino, il quale ha evidenziato come la giustizia sia "il settore in cui si manifesta in maniera più rilevante il contrasto fra protezione dei dati personali, esigenze di sicurezza e tutela del diritto". Il dibattito sulla diffusione delle intercettazioni giudiziarie, tornato recentemente celebre con il proposito governativo di smantellare il cosiddetto *decreto Orlando*, ne è forse il sintomo più evidente. E la tecnologia rischia di esacerbare una discussione già logorata.
In particolare, Spataro punta il dito su quella che definisce *algocrazia*, ossia il rilievo sempre maggiore che sta assumendo la capacità di elaborare grandi moli di dati attraverso algoritmi. "In alcune giurisdizioni come Cina e Stati Uniti – ha osservato, portando l'esempio delle indagini sul terrorismo – gli algoritmi non vengono utilizzati soltanto in fase di investigazione, ma anche per definire la sentenza". La chiave, ha concluso, non sta tanto nella bontà o meno di certi strumenti, quanto piuttosto nella "professionalità di chi è chiamato a utilizzarli".

BLOCKCHAIN, PROFILO GIURIDICO CERCASI

La blockchain, nella visione di Spataro, diventa così un nuovo strumento a disposizione delle istituzioni. E prima ancora di capire se possa essere uno strumento utile o meno, bisogna forse interrogarsi su cosa sia davvero la blockchain. La domanda non è scontata, visto che, come ha osservato **Paolo Gallarati**, partner di Ntcm, "in Italia, e forse anche nel mondo, definizioni giuridiche della blockchain ancora non esistono". E che l'assenza di riferimenti ben definiti crea zone grigie su cui è necessario fare chiarezza, soprattutto quando si parla di tutela dei dati personali.
Il nodo principale riguarda l'assegnazione delle responsabilità. "In quanto registro condiviso – ha osservato Gallarati – la titolarità del dato risulta diffusa e tutti partecipano al funzionamento della piattaforma". Identificare i responsabili di eventuali danni o perdite (improbabili, ma sempre possibili) può risultare difficile, forse anche impossibile, nel caso in cui la struttura risulti decentralizzata e distribuita. Si rischia, ha aggiunto, di arrivare a una sorta di "*tecnocrazia* in cui i dati vengono inseriti in una piattaforma che nessuno di fatto controlla".

IL BALUARDO DEL GDPR

La definizione delle responsabilità, unita alla più generale tutela dei dati personali, costituisce uno degli elementi principali del *Gdpr*. Dopo aver rivoluzionato il settore della privacy, il regolamento europeo rischia oggi di avere pesanti ripercussioni sullo sviluppo della blockchain e, in particolare, degli smart contract. E ciò, quasi paradossalmente, proprio in ragione della sicurezza offerta dal registro elettronico e distribuito.
Come ha osservato **Carlo Grignani**, partner di Nctm, "un smart contract basato sulla blockchain risulta sostanzialmente irreversibile: è alla macchina che si rimette l'esecuzione della volontà delle parti". Nelle blockchain non si può infatti tornare indietro e, ha spiegato, "qualsiasi vizio di forma è destinato a restare nella catena". In questo contesto, la tutela del diritto all'oblio o alla revisione dei propri dati personali, dunque, non può essere garantita. Gli smart contract, ha concluso Grignani, "presentano una rigidità tale che pare limitarne l'utilizzo a contenuti molto standardizzati". Almeno per il momento.