Blockchain e Data Protection: prospettive future nelle policy UE



I precedenti articoli dedicati al rapporto fra tecnologie DLT e tutela dei dati personali hanno rispettivamente esposto il contesto giuridico-terminologico di riferimento e i punti di contatto, nonché di potenziale contrasto, fra tali strumenti e la cornice comunitaria. Quest'ultima, rappresentata in primo luogo dal GDPR, oggi risulta peraltro ampliata dal **Regolamento 2022/858** che istituisce un regime pilota per le infrastrutture di mercato basate su tecnologie a registro distribuito (la maggior parte delle previsioni acquisterà vigore a partire dal 2023).

Qui – a chiusura di una sintetica disamina ispirata dalla ricerca UE *"Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?"* – si guarderà alle possibili soluzioni che negli anni a venire dovranno armonizzare l'impiego, presumibilmente sempre più massiccio, delle *Distributed Ledger Technologies* con i principi della *Data Protection* facenti parte del patrimonio normativo europeo.

DLT e GDPR: le proposte dell'EPRS

Come già emerso nel secondo contenuto, il principale elemento critico nella relazione fra tecnologie distribuite e tutela dei dati personali risiede nella difficoltà – stante la **natura decentralizzata** delle prime – di identificare i responsabili del trattamento dei secondi garantendone l'*accountability*, particolarmente nelle blockchain *permissionless.* Ma anche l'immodificabilità delle transazioni condotte su un registro distribuito suscita non pochi problemi, rendendo difficile

(quando non impossibile) l'esercizio dei diritti alla rettifica o alla cancellazione dei propri dati attribuiti al titolare dagli articoli 16 e 17 GDPR.

Assunte tali difficoltà la citata ricerca UE ipotizza comunque che queste tecnologie, in quanto strumenti di *Data Governance*, possano contribuire agli obiettivi del Regolamento; indicando a tal fine **tre distinte opzioni**, che intendono rappresentare altrettante proposte rivolte al legislatore comunitario.

1. La prima opzione di policy apre alla possibilità di individuare delle linee guida interpretative del GDPR (senza che ne siano necessarie modifiche, in quanto cornice neutrale applicabile a ogni tipo di tecnologia) per facilitarne un'attuazione uniforme nei vari Stati membri, nel contesto di una *data-economy* in rapida evoluzione;
2. la seconda ipotesi prevede il sostegno all'adozione di codici di condotta e meccanismi di certificazione da parte del settore privato, che meglio saprebbe individuare possibili casi d'uso e identificare le diverse tipologie di informazioni trattate;
3. l'ultima azione riguarda il supporto alla ricerca, per integrare le conoscenze attualmente disponibili con indagini interdisciplinari (es. sugli algoritmi di consenso) ed esperimenti volti a individuare nuovi protocolli blockchain che possano dimostrarsi *"compliant by design".*

Ma non c'è solo l'Europa

Il citato Regolamento UE n. 858, adottato lo scorso 30 maggio, parte proprio dalla "tokenizzazione" degli strumenti finanziari in atto per sottolineare la necessità che tale tendenza venga contemperata con l'economia "reale": a tale scopo designa l'ESMA – *European Securities and Markets Authority* come soggetto centrale incaricato di rilasciare eventuali autorizzazioni e monitorare le relative attività,

prevedendo taluni standard essenziali a difesa degli investitori e della stabilità dei mercati per evitare vuoti di disciplina (*"regulatory loopholes"*) che lascino spazio a incertezze o ad abusi.

Anche la **Banca d'Italia**, con la recente "Comunicazione in materia di tecnologie decentralizzate nella finanza e cripto-attività" (datata 2 giugno 2022), evidenzia la scarsità di regole condivise per questi "ecosistemi decentralizzati", rammentando che *"la forte connessione esistente tra tali fenomeni e le istanze di mantenimento della stabilità finanziaria e monetaria costituisce la ragione per cui le banche centrali osservano e monitorano con grande attenzione l'operatività di tali soggetti"*.
Tra le caratteristiche che le tecnologie DLT impiegate in ambito finanziario devono necessariamente garantire, il documento menziona continuità del servizio, resilienza agli attacchi informatici, scalabilità ed efficienza (sia economica sia ambientale) e una *governance* "robusta e identificabile": tutte senz'altro necessarie a fini di stabilità dei mercati finanziari ma, in effetti, anche per garantire la salvaguardia dei dati personali a vario titolo coinvolti.

Ma le tecnologie distribuite esistono e prosperano **anche al di fuori dei confini europei**, senza tenere in alcun conto i confini geografici o i vari "paletti" imposti dalle normative locali; qualunque previsione, per quanto stringente, rischia allora di risultare evanescente e poco risolutiva rispetto a transazioni i cui effetti si propagano in un mercato globale sempre più smaterializzato.

Nell'impossibilità di concepire – e di far rispettare – una disciplina della materia organicamente internazionale, per l'Europa l'alternativa percorribile sembra allora seguire nel solco di una disciplina "minima" che si limiti a mantenere gli standard a protezione dei dati personali aggiornati al mutevole contesto tecnologico: approccio sicuramente rispettoso delle cornici nazionali e maggiormente flessibile

rispetto alle novità di mercato, purché si sia consapevoli dei *“regulatory loopholes”* paventati dall’EPRS e si rimanga pronti a gestire le inevitabili criticità o controversie con un’accorta valutazione *case by case*.

Articolo a cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/blockchain-e-data-protection-prospettive-future-nelle-policy-ue/