Blockchain e Data Protection: (in)compatibilità fra GDPR e tecnologie DLT



In un precedente contenuto in tema di *Distributed Ledger Technologies* (DLT) e protezione dati sono state analizzate le principali fonti normative e le definizioni maggiormente condivise dalla comunità internazionale, al fine di ricostruire l'esatto contesto giuridico e terminologico di riferimento per la materia trattata.

La trasversalità delle tecnologie DLT – in particolare della blockchain – a numerosi e rilevanti settori di attività economica, finanziaria, commerciale ne impongono infatti il contemperamento con la disciplina nazionale e 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).

La prospettiva europea

A riprova dell'attenzione degli organi UE sul tema, già nel 2019 lo European Parliamentary Research Service (EPRS) pubblicava la ricerca condotta dal Panel for the Future of Science and Technology (STOA) *"Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?"*, frutto di un approfondito esame del quadro normativo e tecnologico esistente al fine di rispondere alla domanda posta nel titolo.

Ma questa ricerca, pur dettagliata, non risolve certo ogni questione che solleva: resta ad esempio da chiedersi se

chiunque conduca transazioni capaci di produrre effetti nel territorio UE sia tenuto all'osservanza del GDPR, con gli annessi oneri di *compliance* (ad esempio svolgere la DPIA) e soprattutto se, laddove siano riscontrate violazioni o inottemperanze della relativa disciplina, vada soggetto ad alcun tipo di sanzioni.

Domande tuttora aperte, come anche la scelta delle possibili soluzioni; specie considerando che a breve il quadro sarà significativamente impattato dalla citata proposta di **Regolamento MiCA**, volta a disciplinare il mercato dei *cryptoasset* – dove l'impiego di database distribuiti è la regola, non l'eccezione – in chiave antiriciclaggio e di prevenzione delle frodi.

Aspetti problematici: tipologie di dati e principi del trattamento

Il Regolamento del 2018, fra le sue numerose statuizioni, dedica ampio spazio ai **principi di correttezza e trasparenza** che devono permeare ogni processo di gestione dei dati personali: principi in apparenza coerenti con il pianeta blockchain, che della trasparenza ha sempre fatto una delle sue bandiere (come riconosciuto anche nel documento UE) ma spesso difficili da applicare sul piano concreto.

Va ancora una volta ricordato che, ai sensi dell'art. 4 del GDPR, si definisce dato personale *"qualsiasi informazione riguardante una persona fisica identificata o identificabile… [come] il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".*

Al di là delle opzioni di anonimizzazione ammesse dall'impiego di tecnologie DLT, infatti, l'abbinamento di una **chiave pubblica** a tutte le transazioni condotte facendone uso potrebbe ben consentire l'identificazione della persona fisica

che utilizza quella specifica chiave, così da riportare queste informazioni entro il concetto di “dato personale” previsto dal Regolamento.

E il diritto all’oblio?

Le cose si complicano se ricordiamo che il GDPR, come d’altronde il Codice in materia di protezione dei dati personali italiano, esige sia sempre possibile identificare titolare e responsabile del trattamento dei dati, verso cui ogni interessato potrà far valere eventuali richieste di rettifica o rimozione degli stessi.

Rispetto alle piattaforme *permissioned* il problema dell’identificazione si attenua grazie alla necessaria registrazione/autorizzazione a cui va soggetto chiunque intenda farsi nodo della rete; la persona o ente incaricato di rilasciare tali autorizzazioni sarà, tendenzialmente, titolare del trattamento ai sensi del GDPR. Meno intuitiva è la soluzione per le *permissionless*, dove l’ingresso di nuovi soggetti non è subordinato ad alcuna forma di controllo “centrale”.

Inoltre le caratteristiche di **immodificabilità** di quanto immesso in una blockchain o altra piattaforma DLT – previste a garanzia della certezza e stabilità delle transazioni – appaiono in evidente conflitto con la pretesa legale di veder modificati, se non cancellati, i propri dati; aspetto che tuttavia la ricerca UE, richamando l’art. 17 del GDPR, solennemente definisce “strumento di autodeterminazione” nella gestione delle informazioni personali (*“an important tool towards more informational self-determination*”).

Anche su questo fronte, che include il delicato tema del diritto all’oblio, le questioni poste dallo STOA restano per lo più irrisolte: nel prossimo articolo, conclusivo di questa breve panoramica sul rapporto fra *Distributed Ledger Technologies* e tutela dei dati personali, saranno esaminate le

differenti soluzioni regolatorie ipotizzabili per il futuro.

Articolo a cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/blockchain-e-data-protection-incompatibilita-fra-gdpr-e-tecnologie-dlt/