Vittoria Diotallevi

LA BLOCKCHAIN ED IL RAPPORTO CON IL GDPR

Con l'avvento e la diffusione della tecnologia blockchain e, in generale, delle DLT (*Distributed ledger technologies*) la materia della protezione dei dati personali, disciplinata a livello europeo dal Regolamento UE 679/2016 (GDPR), ha dovuto interfacciarsi con nuovi aspetti e sfide nella sua applicazione.
Soffermandoci, in particolare, sulla blockchain, per apprezzarne l'impatto in questo contesto, è necessario partire proprio dalla sua definizione.
Tralasciando lo stretto dettame normativo[1], la si deve considerare un registro digitale in cui vengono raccolti **dati** sotto forma di unità (blocchi o nodi), contenenti informazioni complete e cristallizzate nel tempo, identificate attraverso un codice univoco (*hash*).
L'aspetto innovativo di un tale tipo di tecnologia risiede principalmente nella decentralizzazione e nella immutabilità dei dati raccolti.
Assieme ai summenzionati aspetti di decentralizzazione e di immutabilità, non vanno tralasciati i diversi meccanismi di *governance* (registri distribuiti con autorizzazione -*permissioned*- e senza autorizzazione -*permissionless*- in combinazione *private* o *public*) e di algoritmi di consenso (PoW e PoS) attraverso cui questo tipo di tecnologia funziona e può essere strutturata.
In che modo, quindi, il GDPR potrebbe entrare in gioco? Se i dati conservati sulla blockchain rientrano nella definizione dell'art. 4, co. I[2], allora siamo in presenza di dati personali e di conseguenza si dovrà applicare tale normativa (con le dovute deroghe previste dallo stesso GDPR, applicate caso per caso).
Abbiamo appena parlato di "raccolta di dati", di "decentralizzazione", di "immutabilità", di "*governance*" e di "algoritmi di consenso"; ebbene, tali caratteristiche della blockchain rivelano una prima possibile *impasse* nel confronto con una normativa di principi, come quella del GDPR, 1) che disciplina il trattamento di dati di carattere personale in modo centralizzato, 2) per cui il consenso non è più focale nella sua architettura[3], 3) che prevede per l'interessato tutta una serie di diritti da poter esercitare, tra cui il diritto di accesso (art. 15) e di cancellazione (art. 17).
Uno dei punti di maggior attrito tra la normativa a tutela della *data protection* e la sua applicazione alla blockchain risiede proprio nel tipo di *governance* con cui essa è stata strutturata.
Si pensi, ad esempio, al caso di una blockchain *permissionless* e *public*, che maggiormente esprime la rivoluzione che ha voluto apportare questo tipo di tecnologia: in una situazione di decentralizzazione massima è certamente difficile individuare i contorni esatti dei ruoli e delle responsabilità in capo ad essi, così come previsti da una normativa che richiede l'esatta identificazione dei soggetti e delle attività che questi devono andare a svolgere nella raccolta, nel trattamento e nella conservazione dei dati personali[4] [5].
L'espressione massima di tale problematica è presente, ad esempio, nel settore della DeFi.

Il Regolamento 679/2016 - è utile ricordarlo - disciplina a livello sovrannazionale e in modo direttamente esecutivo ed applicabile nei Paesi membri UE la materia della *data protection*: il cambio di prospettiva rispetto alla precedente Direttiva 95/46/CE è rinvenibile, in prima analisi, nell'attore

[1] A livello nazionale la ritroviamo nella legge di conversione del D.L. 135/2018 ("*Decreto semplificazioni*"), art. 8 ter, co.I ricompresa nella categoria delle DLT.
[2] *"«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.
[3] L'art. 6 "*Liceità del trattamento*" del GDPR ha inserito nuove basi giuridiche, diverse dal consenso, con cui il titolare può trattare i dati: consenso, esecuzione del contratto, obbligo di legge, salvaguardia degli interessi vitali dell'interessato o di una persona fisica, interesse legittimo.
[4] Principi di minimizzazione e trasparenza, soggetti titolari e responsabili del trattamento, attuazione di misure di sicurezza, tempi chiari di data retention ecc.
[5] "*Blockchain and data protection regulation- Can distributed ledgers be squared with European data protection data protection law*", studio del 2019 dell'EPRS presso il Parlamento europeo, scritto dal Dr Michèle Finck.

a cui è rivolto (il titolare del trattamento[6]) e nel principio attorno a cui tale normativa ruota: l'*accountability*, ossia la responsabilizzazione del titolare nell'applicazione delle regole *de qua*; l'approfondimento di tali aspetti lascia intravedere quanto possa essere difficile applicare la normativa ai soggetti coinvolti nell'erogazione dei servizi su blockchain, che spesso possono non avere alcun potere effettivo sulla sua architettura, ma anche ai validatori stessi, che *in primis* "creano" la blockchain;

Provando, però, a considerare non solo i punti di frizione, è possibile cogliere alcuni elementi di convergenza tra i due temi in parola: l'intento comune è quello di favorire lo sviluppo del mercato digitale e delle tecnologie, attraverso una normativa che rispetti il principio di neutralità della tecnologia, da un lato, e l'applicazione delle DLT ad un numero sempre maggiore di settori, dall'altro[7]; la *cybersicurezza* assume un ruolo centrale, come attività obbligatoria e necessaria di salvaguardia dei dati raccolti, che i soggetti del GDPR devono prevedere, al fine di scongiurare la possibilità del *data breach*, e ciò ha un evidente risvolto sulla efficacia e credibilità in colui che intende utilizzare la blockchain; la possibilità di sviluppare blockchain seguendo i principi di privacy *by design* e *by default*.
Ancora. In relazione alle tecniche di pseudonimizzazione (C26,29,75 art.4, co. V GDPR) e anonimizzazione applicate dal titolare, potrà risultare più o meno agevole l'individuazione di quest'ultimo, in base alla dotazione di mezzi idonei a re-identificare gli interessati a cui sono riconducibili le chiavi pubbliche registrate sulla blockchain (ad es. ciò che accade agli *exchange*)[8].

---

[6] *Art. 24 GDPR "Responsabilità del titolare del trattamento": 1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

[7] **Risoluzione del Parlamento europeo del 3 ottobre 2018**: *"**Ecosistema della DLT. Auto-sovranità, identità e fiducia***
*28. evidenzia che la DLT consente agli utenti di identificarsi e al contempo **offre loro la facoltà di controllare quali dati personali intendono condividere**; osserva che un'ampia gamma di applicazioni può consentire diversi **livelli di trasparenza**, il che aumenta la necessità che le applicazioni siano **conformi al diritto dell'UE**; sottolinea anche che i dati in un registro pubblico sono **pseudonimi e non anonimi**;*
*29. sottolinea che la DLT sostiene la creazione di nuovi modelli al fine di cambiare l'attuale concetto e l'odierna architettura delle **identità digitali**; rileva che, di conseguenza, l'identità digitale **si estende** alle persone, alle organizzazioni e agli oggetti e semplifica ulteriormente i processi identitari quali "Conosci il tuo cliente", consentendo al contempo il controllo personale sui dati;*
30. sottolinea che la gestione dei dati personali implica che gli utenti abbiano la capacità e le conoscenze e competenze tecniche per gestire i propri dati; è preoccupato per i rischi di un uso scorretto dei propri dati e per la vulnerabilità dinanzi a sistemi fraudolenti a causa della mancanza di conoscenza;
*31. sottolinea che **le identità digitali sono indispensabili per il futuro di questa tecnologia**; ritiene che gli Stati membri dovrebbero scambiarsi le migliori pratiche su come garantire la sicurezza di tali dati;*
*32. sottolinea che, **sebbene la DLT promuova l'identità auto-sovrana, il "diritto all'oblio" non è facilmente applicabile in questa tecnologia**;*
33. sottolinea che è della massima importanza che gli usi della DLT siano conformi alla legislazione dell'UE sulla protezione dei dati, in particolare al regolamento generale sulla protezione dei dati (GDPR); invita la Commissione e il Garante europeo della protezione dei dati (GEPD) a fornire ulteriori orientamenti su questo punto;
*34. sottolinea che la fiducia nella DLT è garantita da **algoritmi crittografici** che sostituiscono l'intermediario terzo attraverso un meccanismo che esegue la convalida, la salvaguardia e la conservazione delle transazioni;*
*35. sottolinea che la fiducia nelle blockchain pubbliche (**permissionless**) si fonda su algoritmi crittografici, sui partecipanti, sulla configurazione della rete e sulla struttura e che gli intermediari terzi possono essere sostituiti attraverso un meccanismo che effettua la convalida, la salvaguardia e la conservazione delle transazioni e accelera la compensazione e il regolamento di alcune operazioni in titoli; rileva che l'efficacia delle salvaguardie dipende dalla **corretta applicazione della tecnologia** e pertanto richiede sviluppi tecnologici che garantiscano la sicurezza reale, rafforzando così la fiducia".*

[8] *"La rivelazione della disciplina in materia di protezione e valorizzazione dei dati personali nel FinTech"*, *"2.2.2 Un tentativo di ricostruzione della disciplina del trattamento dei dati personali su blockchain permissionaless nel Fintech ed in particolare nei servizi DeFi"*, M. Nicotra, in "*Privacy e libero mercato digitale*" a cura di L. Bolognini, Giuffrè, 2021.

La realtà allo stato dell'arte è la mancanza di una normativa sulla *data protection* attagliata perfettamente sulla blockchain e sulle DLT.
Gli sforzi del legislatore europeo, però, sin dalle prime fasi di elaborazione del GDPR, son stati nel senso di rispettare il c.d. **principio di neutralità della tecnologia (C15)**: a parere della scrivente, non è, pertanto, auspicabile un nuovo ed ulteriore intervento normativo, quanto quello delle Autorità di controllo, come i Garanti della privacy a livello nazionale o di concerto tra loro in ambito europeo (EDPB), al fine di semplificare l'applicazione di ciò che già esiste e di indirizzare l'interprete, attraverso *best practice* e Linee Guida.
In tale direzione, qualche indicazione va rinvenuta nei report dell'EU Blockchain Observatory and Forum o del Garante francese CNIL; il Parlamento europeo, inoltre, ha provato a fornire tre policy che permetterebbero di non andare a modificare la normativa esistente: interpretazione del regolamento, creazione di codici di condotta (già previsti all'art. 40 GDPR) e sistemi di certificazione di settore (art.42 GDPR) e la promozione di ricerca multidisciplinare.

Alla luce di quanto sopra esposto, la vera domanda è: come e, soprattutto, è davvero possibile normare e attribuire ruoli e responsabilità a qualcosa che nasce con la finalità di rendere davvero operante il meccanismo *peer to peer* tra gli utenti e, perciò, di attuare la decentralizzazione dei prodotti, dei servizi e della loro fruizione?