Blockchain vs GDPR: contatti e contrasti

Author : Leonardo Scalera

Date : 15 Febbraio 2019

Nell'attuale panorama economico globale, **l'importanza che i dati rivestono è un dato di fatto**. I dati vengono ormai definiti dai più come "il nuovo petrolio", una nuova ricchezza che, almeno per il momento, giorno dopo giorno cresce in maniera esponenziale invece di ridursi.

Non è un mistero per nessuno come diversi Stati o unioni di Stati abbiano lavorato, in questi anni, per creare norme che potessero dare ai singoli individui una serie di garanzie, certezze, diritti proprio in merito al grande valore che i loro dati - e le operazioni effettuate su di essi - hanno via via acquisito.

Il Regolamento europeo **Reg. UE 2016/679 (GDPR)** è un lampante esempio di questo impegno, con il quale conviviamo e che quotidianamente ci sforziamo, come tutti gli operatori coinvolti (P.A., aziende, professionisti ecc.), di applicare a tutte le operazioni, anche di vita quotidiana, che comportano interventi sui dati personali.

Sebbene il GDPR veda fra i suoi **principi basilari** proprio quello di aggiornare una **normativa preesistente oramai fuori luogo** (la Direttiva 95/46/CE, definita "la direttiva madre" in materia), visti gli anni trascorsi dalla sua emanazione e in rapporto ai cambiamenti epocali delle nuove tecnologie nel medesimo periodo, per alcuni versi **potrebbe esso stesso considerarsi "in ritardo"**.

Ebbene sì, in ritardo lo si potrebbe considerare proprio facendo un confronto con alcune "tecnologie" che prepotentemente si stanno affermando nel panorama globale: le tecnologie **blockchain**.

Queste, sviluppate principalmente in relazione alla creazione, circolazione e utilizzo di cripto valute (motivo per il quale sono da sempre apprezzate nel dark web) rappresentano, in realtà, una grossa opportunità proprio sulla base delle loro caratteristiche tecniche e di funzionamento.

Procediamo con ordine. La Protezione dei Dati (o più precisamente "delle persone fisiche") oggetto del GDPR è stata fortemente voluta dal legislatore europeo proprio per arginare e regolamentare **l'utilizzo indiscriminato dei dati degli utenti su web, app e social media da**

parte delle web e media company che, sulla profilazione degli utenti, stanno cercando di costruire il proprio vantaggio competitivo.

Questo ci introduce ad alcuni articoli del GDPR che recitano:

Art. 12: *le persone hanno il diritto di chiedere e avere risposte sull'uso che un'azienda farà dei propri dati e a chiedere un risarcimento qualora queste domande non abbiano risposte chiare, concise e tempestive*;

Artt. 13 e 14: *gli utenti hanno il diritto di sapere come verranno utilizzati i dati personali al momento della loro raccolta/richiesta e di sapere per quanto tempo saranno conservati*;

Art. 15: *gli utenti hanno il diritto di sapere e accedere ai dati personali che vengono elaborati/processati da chi ne ha chiesto il consenso*;

Art. 16: *le persone possono rettificare e modificare i propri dati personali* (nonché, *ex* **art. 19**: *chi raccoglie i dati deve informare anche le "terze parti" ammesse ad utilizzarli per interrompere l'uso dei dati rettificati o cancellati)*;

Art. 17: *gli utenti hanno il diritto di chiedere (e ottenere) la cancellazione dei propri dati personali quando non sono più necessari agli scopi per i quali erano stati raccolti*;

Art. 18: *le persone possono limitare il trattamento dei propri dati (quando risultano inesatti, quando sono stati raccolti illegalmente o non seguendo le procedure giuridiche…)*;

Art. 20: *gli utenti hanno diritto a ricevere i propri dati personali in un formato strutturato e comunemente usato in modo che possano essere letti facilmente da una qualsiasi macchina (Pc, smartphone, app, ecc.)*;

Art. 21: *le persone hanno il diritto di opporsi all'utilizzo dei propri dati per profilazione o commercializzazione e devono essere messe nelle condizioni di poter dire di no.*

E ancora ci sarebbe da ricordare quanto prescritto in materia di ***privacy by design*** (art. 25), sicurezza del trattamento (art. 32) ecc., dato che, anche per questi articoli, è possibile trovare dei collegamenti parlando di tecnologia blockchain.

Chiariamo ora alcuni punti fondamentali che caratterizzano questa tecnologia:

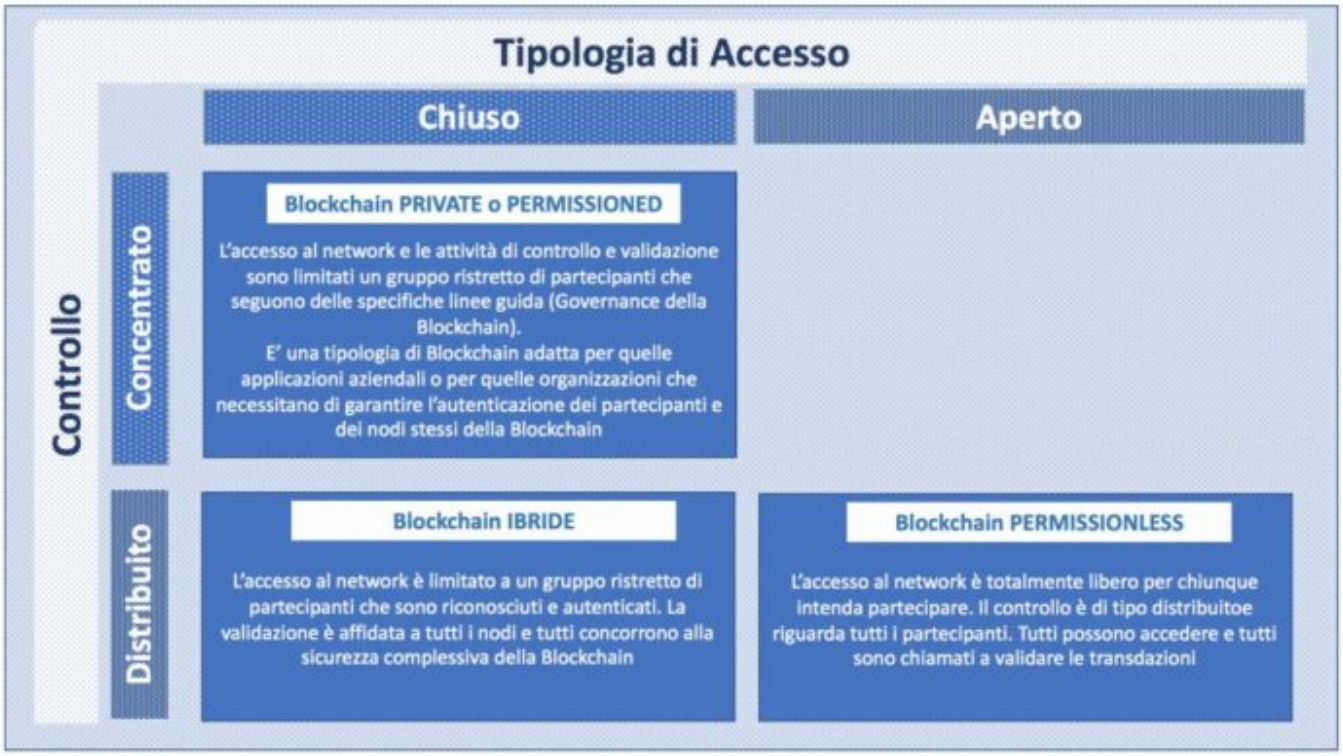
- **Affidabilità**: la blockchain è affidabile. Non essendo governata dal centro, ma dando a tutti i partecipanti diretti una parte di controllo dell'intera catena, diventa un sistema meno centralizzato, meno governabile e, allo stesso tempo, molto più sicuro e affidabile, ad esempio rispetto agli attacchi esterni. Se infatti soltanto uno dei nodi della catena subisce un attacco e si danneggia, tutti gli altri nodi del database distribuito continueranno comunque a essere attivi e operativi, saldando la catena e prevenendo, in questo modo, la perdita di informazioni importanti.
- **Trasparenza**: le transazioni effettuate attraverso la blockchain sono visibili a tutti i

partecipanti, garantendo così trasparenza nelle operazioni.

- **Convenienza**: effettuare transazioni attraverso questa tecnologia è conveniente per tutti i partecipanti, in quanto vengono meno interlocutori di terze parti, necessari in tutte le transazioni convenzionali che avvengono tra due o più parti (ovvero, banche e altri enti simili).
- **Solidità**: le informazioni già inserite non possono essere modificate in alcun modo. Le informazioni contenute nella blockchain sono più solide e attendibili proprio per il fatto che non si possono alterare e, quindi, restano così come sono state inserite all'origine.
- **Irrevocabilità**: con la blockchain è possibile effettuare transazioni irrevocabili e, allo stesso tempo, più facilmente tracciabili: si ha così garanzia che le transazioni siano definitive, senza alcuna possibilità di essere modificate o annullate.
- **Digitalità**: con la blockchain tutto diventa virtuale. Grazie alla digitalizzazione, gli ambiti applicativi di questa nuova tecnologia diventano tantissimi.

In merito agli ambiti di applicazione, un'ulteriore distinzione risulta doverosa collegandoci, più precisamente, alle **modalità di accesso e controllo:**

1. Blockchain Permissioned ? necessitano di una governance specifica e la validazione delle operazioni avviene solo in capo ad un gruppo "ristretto";
2. Blockchain Permissionless ? accesso libero al network, tutti sono chiamati a partecipare e a validare le operazioni (Fig. 1).



Osservando la figura e calandola nella realtà quotidiana, alcuni esempi di applicazione potrebbero risultare abbastanza chiari: commercio, sanità, vendita, logistica, istruzione, vendite immobiliari e, perché no, servizi della Pubblica Amministrazione.

Ovviamente “ad ognuno il suo”. Proprio c**onsiderando le caratteristiche e le normative di settore, risulterà, di volta in volta, più corretto utilizzare una blockchain permissioned invece di una permissionless**.

Tornando al rapporto fra la tecnologia blockchain e il GDPR è possibile individuare, quindi, alcuni ***punti di convergenza***, come ad esempio: l’utilizzo della crittografia completa dei blocchi, l’utilizzo di tecniche di pseudonimizzazione (uso di hash), la minimizzazione del dato, il controllo da parte dell’utente dei propri dati (mediante la corrispondenza alla propria chiave pubblica), la resistenza ad attacchi o eventi legati al cyber crime (data la presenza e la ridondanza dei dati – identici – sui nodi, l’eventuale compromissione di uno di essi non comporterebbe la perdita del dato, comunque criptato, né il crollo della catena) e non solo.

Nel contempo, ragionando sull’attuale testo del GDPR, risulta facile trovare anche ***punti di contrasto*** con l’uso di queste tecnologie. Vediamone alcuni: problematiche nell’individuare chiaramente il responsabile del trattamento (la definizione presente nell’art. 28 del GDPR mal si presta ad essere abbinata alla tecnologia blockchain), legislazione da applicare in caso di controversie (i dati sicuramente potrebbero trovarsi in “N” nodi della catena che, a loro volta, possono essere distribuiti in “N” Stati), individuazione chiara di cosa, all’interno della catena, possa essere considerato “dato personale” (dato che nella catena risultano visibili chiavi pubbliche e non dati “in chiaro”, secondo la definizione del GDPR dovremmo allora considerare la *chiave* come *dato personale*?, in caso di blockchain pubblica il concetto di minimizzazione del dato risulterebbe, quantomeno, di difficile applicazione), esercizio dei diritti (ad esempio del diritto all’oblio, in considerazione della presenza dei dati identici su tutti i nodi della catena, del diritto di limitazione al trattamento o alla correzione di dati errati, ecc.)

Sicuramente molti di questi punti di “contrasto” fra il GDPR e la tecnologia blockchain sono **già all’attenzione degli “addetti ai lavori”**, data l’impossibilità di imporre uno stop alla tecnologia e, al tempo stesso, le sempre maggiori richieste di protezione da parte dei soggetti finali; ma, in questa sede, potremmo spingerci a lanciare qualche **spunto di riflessione** che si spera possa tornare utile:

- considerando che, secondo il Gruppo di Lavoro art. 29 – Opinion 5/2014, l’*hashing* rientra fra le tecniche di pseudonimizzazione (in quanto esisterebbe la possibilità di collegare l’hash a dati esterni personali) e per questo sarebbe da considerarsi all’interno della blockchain al pari di un dato personale, si potrebbe pensare di inserire l’hash all’interno della procedura di crittografia;

- si potrebbero memorizzare i dati personali all’esterno della catena inserendo in questa solo un riferimento codificato ad essi in maniera che, cancellando il riferimento (codice) la catena resti intatta, ma si perda definitivamente il collegamento con i dati personali;

- prevedere la possibilità di distruzione definitiva delle chiavi crittografate.

Ovvio che, al momento, diverse soluzioni sono sicuramente allo studio dei tecnici ma, oggettivamente, anche i legislatori non potranno per molto tempo non affrontare direttamente le nuove “sfide legislative” che l’aumento della diffusione di queste tecnologie richiede e per le quali, sicuramente, sarà prodotta una normativa specifica.

Nel frattempo e nel caso in cui non si possa fare a meno di inserire, all'interno di una blockchain, anche dei dati personali, la **massima attenzione va sicuramente posta su alcuni punti:**

a) Utilizzo (quanto più possibile) di tecniche di crittografia per aumentare il livello di privacy;

b) Limitazione al minimo dei "nodi" della catena autorizzati alla visione delle informazioni (es. blockchain permissioned o ibrida);

c) Procedure in merito ai comportamenti da tenersi trascorsi i tempi di *data retention*;

d) Procedure di intervento/*disaster recovery*/continuità operativa in caso di interruzione della catena di crittografia.

Articolo a cura di **Leonardo Scalera**