NT+ Diritto
Norme & Tributi Plus

Il Sole 24 ORE

Civile

Blockchain e privacy: sfide tecniche e conformità normativa nel trattamento dei dati personali

Le recenti Linee guida, adottate da EDPB lo scorso 8 aprile, affrontano questa complessa intersezione tra innovazione tecnologica e tutela dei diritti fondamentali, delineando un quadro normativo e tecnico dettagliato

*di Vincenzo Candido Renna, Laura Spano**
23 Aprile 2025

Nel panorama tecnologico contemporaneo, la tecnologia blockchain rappresenta un'innovazione disruptiva che promette di rivoluzionare numerosi settori, dalla finanza alla logistica, dalla sanità alla pubblica amministrazione. Tuttavia, la sua **caratteristica fondamentale di immutabilità** - elemento strutturale che garantisce sicurezza e affidabilità - si trova in apparente **contraddizione** con i principi cardine della **normativa europea sulla protezione dei dati personali.**
Le recenti "***Linee guida 02/2025 sul trattamento dei dati personali attraverso le tecnologie blockchain***", adottate l'8 aprile 2025 dal **Comitato europeo per la protezione dei dati (EDPB)**, affrontano questa complessa intersezione tra innovazione tecnologica e tutela dei diritti fondamentali, delineando **un quadro normativo e tecnico** dettagliato.

Il dilemma strutturale: immutabilità vs diritti degli interessati

La **blockchain**, nella sua formulazione tecnica, implementa un **database distribuito** caratterizzato da quattro proprietà fondamentali che vengono esplicitamente identificate nelle linee guida:
1. Distribuzione: "*I dati vengono replicati da più partecipanti peer-to-peer e quindi memorizzati in più posizioni*," come specificato al punto 3 dell'introduzione.
2. Disintermediazione: "*La convalida dei dati aggiunti al database non necessita dell'avallo di una parte fidata o centrale, ma piuttosto dell'accordo dei partecipanti alla blockchain.*"
3. Coerenza e immutabilità: "Qualsiasi aggiornamento o rimozione dei dati convalidati può essere rilevato," creando così un registro a prova di manomissione.
4. Trasparenza: "*L'accesso ai dati e alla loro verifica è disponibile per tutti i partecipanti alla blockchain.*"
Queste caratteristiche, particolarmente **l'immutabilità e la trasparenza**, entrano in tensione diretta con alcuni **principi fondamentali del GDPR**, tra cui:
- **Il principio di limitazione della conservazione** (*articolo 5, paragrafo 1, lettera e*), che prevede che i dati personali debbano essere "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.*"
- **Il diritto alla cancellazione** (*articolo 17*), che garantisce all'interessato **il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.**
- **Il diritto di rettifica** (*articolo 16*), che assicura all'interessato il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano.

Come sottolineato al punto 7 dell'introduzione delle linee guida: *"Ad esempio, una volta che una transazione è registrata sulla catena, non può essere alterata o rimossa individualmente senza che si rilevi un'incongruenza nella catena."*

Architetture blockchain e implicazioni sulla protezione dei dati

Le linee guida forniscono una categorizzazione dettagliata delle diverse **architetture blockchain**, analizzando le rispettive implicazioni in termini di **protezione dei dati**:

Blockchain permissionless vs permissioned

La distinzione primaria nelle architetture blockchain riguarda la **modalità di accesso e partecipazione**:
● **Blockchain permissionless** (*pubbliche*): *"Prevedono partecipanti con pari diritti e capacità: chiunque può leggere, scrivere o creare blocchi. Queste blockchain sono decentralizzate,"* come descritto al punto 22 delle linee guida.
● **Blockchain permissioned** (*autorizzate*): "*Si discostano dai concetti originali e includono un'autorità che deve dare il permesso di partecipare: solo i nodi selezionati possono leggere, scrivere o creare blocchi, a seconda delle regole che si applicano alla blockchain,*" come specificato al punto 23.
L'EDPB esprime una **chiara preferenza per le blockchain permissioned**, affermando al punto 40: "*Questa opzione offre una più chiara attribuzione delle responsabilità, che è un elemento chiave per la protezione degli interessati, e le organizzazioni dovrebbero favorire le blockchain autorizzate.*"

Tipi di dati in una blockchain

Le linee guida operano un'importante distinzione tra diversi tipi di dati presenti in una blockchain:
1. **Metadati delle transazioni:** Comprendono "*sia gli identificatori degli utenti che partecipano alle transazioni sia altri metadati," come specificato al punto 26. In particolare, vengono citati gli "identificativi composti da una serie di caratteri alfanumerici che sembrano casuali e che costituiscono una chiave pubblica derivata da una chiave privata nota all'utente*."
2. **Payload delle transazioni:** Il contenuto effettivo delle transazioni, che "*può trattarsi di una quantità di criptovaluta, di un collegamento a un documento, di un oggetto acquistato, di una chiamata a una procedura di smart contract, ecc*." come descritto al punto 29.
3. **Dati off-chain:** Dati collegati alla blockchain ma memorizzati esternamente, una soluzione che viene fortemente raccomandata dalle linee guida per mitigare i rischi relativi alla protezione dei dati.

Soluzioni tecniche avanzate per la compliance al GDPR

Le linee guida identificano diverse **tecniche crittografiche e architetturali** che possono contribuire a **rendere il trattamento dei dati in ambiente blockchain conforme ai principi del GDPR**:
1. **Crittografia dei dati personali**
"*Utilizzando algoritmi e chiavi di crittografia all'avanguardia, i dati saranno accessibili in chiaro solo a chi conosce la chiave appropriata*" come specificato al punto 51. Tuttavia, le linee guida ribadiscono un principio fondamentale: "*L'EDPB ricorda che i dati personali criptati sono sempre dati personali e la crittografia non elimina la necessità di conformità al GDPR.*"
Viene inoltre evidenziato un rischio temporale: "*Anche potrebbe risultare vulnerabile col passare del tempo se la blockchain viene conservata a tempo indeterminato.*"
2. **Hashing dei dati personali**
L'EDPB descrive dettagliatamente questa tecnica al punto 52: "*Memorizzare sulla blockchain solo un hash salato o codificato dei dati personali. I dati non sottoposti a hash, così come la chiave segreta o il sale casuale lungo utilizzato, vengono memorizzati in modo confidenziale fuori dalla catena*."
Questa tecnica presenta **vantaggi significativi**: "*Un hash ottenuto attraverso una funzione di hash all'avanguardia e una chiave o un sale segreto generato casualmente e di dimensioni sufficienti, sarà in teoria verificabile solo da chi ha accesso ai dati originali e alla chiave o al sale associati.*"
Le linee guida sottolineano anche **i limiti di questa tecnica**: "*L'uso di hash non salati o non cifrati non dovrebbe, in generale, essere considerato sufficiente a garantire il livello necessario di protezione della riservatezza per l'archiviazione di dati personali su una blockchain pubblica*."
3. **Impegni crittografici** (*Cryptographic commitments*)
Una tecnica più avanzata descritta al punto 53: "*Memorizzare invece un impegno crittografico sulla blockchain. Se l'impegno è stato calcolato utilizzando uno schema allo stato dell'arte che nasconde perfettamente i dati, una volta che i dati originali e il loro testimone vengono cancellati, l'impegno che persiste nella blockchain è inutile.*"
4. **Prova di esistenza** (*Proof of existence*)
Al punto 54, le linee guida raccomandano: "*Ogni volta che è necessario memorizzare i dati personali sulla blockchain, è preferibile memorizzare i dati in una forma destinata principalmente a fungere da prova di esistenza (ad esempio mediante l'uso di un puntatore, un impegno crittografico o un hash generato da una funzione hash a*

chiave, ecc.) sulla blockchain, mentre i dati che dovrebbero essere utilizzati per verificare la prova sono conservati al di fuori della blockchain."

Ruoli e responsabilità: titolari e responsabili del trattamento nel contesto blockchain

La **determinazione dei ruoli** ai sensi del **GDPR** rappresenta una **sfida particolare nelle architetture blockchain**, specialmente quelle **pubbliche e permissionless.** Le linee guida affermano al punto 38: "*In alcuni casi di blockchain pubbliche e senza permessi, i nodi non agiscono 'per conto del controllore' e non ricevono istruzioni da alcun controllore; al contrario, in alcuni casi possono decidere in modo significativo di modificare gli scopi e/o i mezzi essenziali per perseguire i propri obiettivi.*"
In questi casi, le linee guida raccomandano fortemente al punto 44 *"la creazione di un consorzio o di qualsiasi altro tipo di entità legale tra i nodi. Questa entità, quando esiste, sarà il controllore di questo trattamento."*

Valutazione d'impatto sulla protezione dei dati (DPIA) per implementazioni blockchain

Le linee guida specificano che, data la natura della tecnologia blockchain e i rischi potenziali per i diritti e le libertà degli interessati, è essenziale condurre una **DPIA approfondita** prima di implementare soluzioni basate su blockchain che trattino dati personali.
Al punto 98, viene delineata una struttura specifica per tale valutazione, che deve includere:
1. Una **descrizione sistematica delle operazioni di trattamento blockchain**, inclusi finalità, infrastruttura, modello di governance e tipologie di dati trattati.
2. Una **valutazione della necessità e proporzionalità delle operazioni di trattamento basate su blockchain**, spiegando perché tale tecnologia è necessaria e "*perché l'obiettivo non può ragionevolmente essere raggiunto in modo altrettanto efficace con modalità meno invasive della privacy*."
3. Una **valutazione dei rischi specifici dell'uso della blockchain**, inclusi quelli relativi alla comunicazione delle transazioni tra diversi soggetti, la gestione dei blocchi, l'archiviazione fuori catena e la gestione delle informazioni crittografiche.

Diritti degli interessati: implementazioni tecniche

Le linee guida affrontano dettagliatamente come garantire l'esercizio dei diritti degli interessati in un ambiente blockchain, fornendo **orientamenti specifici per ciascuno dei diritti sanciti dal GDPR:**

- **Diritto alla cancellazione e all'opposizione**

Al punto 103, le linee guida riconoscono la sfida tecnica: "*L'EDPB osserva che potrebbe essere tecnicamente impraticabile accogliere la richiesta di cancellazione effettiva presentata da un interessato quando i dati personali sono memorizzati direttamente su una blockchain.*"
Tuttavia, suggeriscono un **approccio preventivo:** "*I responsabili del trattamento dovrebbero prendere in considerazione questo requisito sin dalla fase di progettazione e assicurarsi che qualsiasi dato personale memorizzato sulla blockchain possa essere effettivamente reso anonimo in caso richiesta di cancellazione o obiezione*."

- **Diritto di rettifica**

Al punto 106, viene delineata una **soluzione tecnica specifica:** "*In alcuni casi, il diritto alla rettifica può essere soddisfatto da una transazione successiva che annuncia l'annullamento di una transazione precedente, anche se la prima transazione continuerà a comparire nella catena.*"

- **Diritto di opposizione a decisioni automatizzate**

Le linee guida affrontano anche l'applicazione *dell'articolo 22 del GDPR* nel contesto degli **smart contract**, affermando al punto 107: "*L'esecuzione di uno smart contract può, in alcuni casi, costituire una decisione automatizzata. Quando queste decisioni automatizzate rientrano nell'ambito di applicazione dell'articolo 22, il titolare del trattamento deve garantire che siano soddisfatte le garanzie previste da tale disposizione, tra cui la possibilità di un intervento umano e la possibilità per l'interessato di contestare la decisione*."

Raccomandazioni concrete per l'implementazione

L'Allegato A delle linee guida fornisce **16 raccomandazioni specifiche** per organizzazioni che intendono utilizzare la blockchain per il trattamento di dati personali. Tra le più significative:
La Raccomandazione 2 riguarda **l'architettura e lo stoccaggio fuori catena**. L'EDPB raccomanda ai responsabili del trattamento di memorizzare qualsiasi dato personale aggiuntivo fuori dalla catena, oltre agli identificatori già presenti nella catena nei metadati delle transazioni, per ridurre i rischi di protezione dei dati.
La Raccomandazione 9 si concentra sul **consenso**. Se il consenso è alla base giuridica del trattamento, si deve garantire che esso sia dato liberamente e che l'interessato possa rifiutarlo o ritirarlo senza subire danni.
La Raccomandazione 10 afferma che la protezione dei dati deve essere **progettuale e predefinita.** Tutti i principi di protezione dei dati devono essere inclusi per progettazione e per impostazione predefinita in qualsiasi trattamento fin dall'inizio e per tutto il ciclo di vita del trattamento.
La Raccomandazione 11 riguarda la **conservazione dei dati e la loro durata**. Il periodo di conservazione dei metadati, come gli identificativi degli utenti e il payload, deve essere stabilito ai sensi dell'art. 17 in combinato disposto con l'Art. 25(1) GDPR e preso in considerazione al momento di decidere quale tipo di blockchain e quale formato utilizzare per memorizzare tali dati.

Principi di protezione dei dati applicati alla blockchain

Le linee guida analizzano in dettaglio l'applicabilità di ciascuno dei principi fondamentali del GDPR (articolo 5) nel contesto della tecnologia blockchain:

- **Principio di correttezza (fairness)**

Come specificato al punto 58, questo principio "*richiede che i dati personali non siano trattati in modo ingiustificatamente dannoso, illecito, discriminatorio, inatteso o fuorviante per l'interessato*."

- **Principio di trasparenza**

Le linee guida sottolineano al punto 59 che "*il responsabile del trattamento deve essere chiaro e aperto con l'interessato sulle modalità di raccolta, utilizzo e condivisione dei dati personali.*"

- **Principio di limitazione delle finalità**

Al punto 60, si evidenzia una potenziale tensione: "*La tecnologia blockchain, per sua natura, è disintermediata e i rapporti tra i partecipanti non possono sempre essere regolati da contratti o altri atti giuridici*."

- **Principio di minimizzazione dei dati**

Le linee guida evidenziano al punto 61 una particolare sfida: "*La natura di blockchain, che è solo appendice e in continua crescita, mette in discussione il principio di minimizzazione dei dati, esacerbato dal potenziale di persistenza illimitata e di replica multipla.*"

- **Principio di limitazione della conservazione**

Come specificato al punto 63, la cancellazione dei dati in una blockchain presenta sfide specifiche: "*La cancellazione dei dati a livello individuale in una blockchain può essere impegnativa e richiede architetture ingegnerizzate ad hoc. Quando la cancellazione non è stata presa in considerazione dalla progettazione, può essere necessario cancellare l'intera blockchain*."

Conclusione: un approccio bilanciato all'innovazione e alla protezione dei dati

Le linee guida 02/2025 rappresentano un tentativo ambizioso e tecnicamente dettagliato di **riconciliare l'innovazione tecnologica rappresentata dalla blockchain con i principi fondamentali della protezione dei dati personali sanciti dal GDPR.**
Come sottolineato nella sintesi iniziale del documento: "*Alcuni di questi rischi possono essere mitigati attraverso misure tecniche in anticipo, mentre trovare una soluzione per altri rischi di non conformità potrebbe essere più impegnativo in questa fase*."
L'approccio dell'EDPB non è quello di scoraggiare l'uso della tecnologia blockchain, ma piuttosto di **orientare le organizzazioni verso implementazioni conformi al GDPR**, privilegiando architetture che **minimizzino i rischi** (blockchain permissioned), **tecniche crittografiche avanzate**, **archiviazione off-chain dei dati personali e una governance chiara** che definisca inequivocabilmente ruoli e responsabilità.

Il messaggio fondamentale è che **l'impossibilità tecnica non può mai essere invocata come giustificazione per la non conformità ai principi del GDPR.** Come esplicitamente affermato al punto 17 delle linee guida, citando il Report del ChatGPT Taskforce del maggio 2024: "*In particolare, l'impossibilità tecnica non può essere invocata per giustificare l'inosservanza di tali requisiti, soprattutto considerando che il principio della protezione dei dati fin dalla progettazione deve essere preso in considerazione al momento determinazione dei mezzi per il trattamento e al momento del trattamento stesso*."

La sfida per gli sviluppatori, le organizzazioni e i responsabili della protezione dei dati sarà quella di integrare queste linee guida nelle fasi iniziali di progettazione delle soluzioni blockchain, adottando **l'approccio *"privacy by design and by default"*** che rappresenta non solo un requisito normativo ma anche una garanzia di sostenibilità a lungo termine per le tecnologie emergenti in un panorama regolamentare sempre più attento alla tutela dei diritti fondamentali.

_____

**Vincenzo Candido Renna, Partner 24 ORE e Laura Spano, Compliance and Sustainability Specialist*

ISSN 2499-1589 - Norme & Tributi Plus Diritto [https://ntplusdiritto.ilsole24ore.com]