LA TECNOLOGIA *BLOCKCHAIN* ALLA PROVA DEL GDPR

Le nuove linee guida EDPB e le prospettive di dialogo con l'AI Office

28 aprile 2025

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Giovanni Lombardi
Associate

Alessandro Carlini
Associate

La tecnologia *blockchain*, sin dal suo avvento nel panorama dell'innovazione digitale, ha rappresentato uno dei fenomeni più affascinanti e, al contempo, controversi: distribuita, disintermediata, immutabile, essa si è proposta quale presidio di trasparenza e integrità. Tuttavia, allorquando tale tecnologia intersechi il trattamento di dati personali – e, conseguentemente, il complesso sistema di tutele delineato dal Regolamento (UE) 2016/679 ("**GDPR**") – emergono criticità di notevole rilievo e, per molti versi, ancora irrisolte.

In tale contesto si collocano le recenti "*Guidelines 02/2025 on processing of personal data through blockchain technologies*", adottate l'8 aprile dal Comitato Europeo per la Protezione dei Dati ("**EDPB**") e sottoposte a consultazione pubblica sino al 9 giugno 2025 (le "**Linee Guida**"). Trattasi di un'iniziativa di particolare significatività in uno scenario tecnologico in cui le applicazioni fondate su *blockchain* stanno registrando una rapida diffusione: dalla finanza decentralizzata (DeFi) agli NFT, dalle piattaforme di *supply chain management* alle soluzioni di *digital identity*.

Parallelamente, l'EDPB ha comunicato l'avvio di una collaborazione organica con l'AI Office, l'autorità preposta alla vigilanza sull'attuazione dell'AI Act, finalizzata all'elaborazione di linee guida congiunte in materia di interazione tra intelligenza artificiale, AI Act e disciplina europea sulla protezione dei dati personali.

▼ ▼ ▼

1. IL CONTESTO NORMATIVO E LE FRIZIONI STRUTTURALI

L'impianto del GDPR è edificato su principi cardine che prescindono dalla tecnologia impiegata ma che, inevitabilmente, con essa devono confrontarsi. La liceità, correttezza e trasparenza dei trattamenti; la limitazione delle finalità perseguite; la minimizzazione dei dati raccolti; l'esattezza e l'aggiornamento delle informazioni; la limitazione temporale della conservazione: tutti questi principi si scontrano con la natura stessa della *blockchain*, fondata sull'immutabilità e sulla persistenza delle registrazioni.

Quest'antinomia strutturale raggiunge il suo apice nel confronto con i diritti riconosciuti agli interessati: se la *blockchain* si fonda sulla permanenza inalterabile delle informazioni inserite nella catena, come coniugare tale caratteristica con il diritto alla rettifica, alla cancellazione o all'opposizione al trattamento?

IL PARADOSSO DELL'IMMUTABILITÀ E LA SFIDA PER I DIRITTI DEGLI INTERESSATI

Il conflitto assume dimensioni particolarmente critiche nelle *blockchain* pubbliche (*permissionless*), dove:

- ciascun nodo conserva l'intera catena di transazioni;
- il modello "*append-only*" costituisce un elemento imprescindibile dell'architettura;
- le transazioni, una volta validate e inserite nei blocchi, divengono parte integrante e immodificabile della catena.

Il paradosso dell'immutabilità e la tensione con i diritti GDPR

In simili contesti, la possibilità per l'interessato di ottenere la rettifica di dati inesatti, la cancellazione di informazioni non più necessarie o l'opposizione a trattamenti fondati sul legittimo interesse del titolare risulta fortemente compromessa sul piano pratico.

Anche nelle *blockchain* private o *permissioned*, caratterizzate da una *governance* più definita e da limitazioni nell'accesso ai nodi, l'immutabilità delle registrazioni richiede soluzioni tecniche e organizzative sofisticate che consentano, se non la rimozione fisica del dato, quantomeno l'impossibilità del suo ulteriore utilizzo mediante tecniche quali la de-referenziazione, la revoca delle chiavi crittografiche o la segregazione delle informazioni identificative in ambienti *off-chain*.

LA QUESTIONE DELL'AUTOMAZIONE DECISIONALE: GLI *SMART CONTRACT* ALLA PROVA DELL'ART. 22 GDPR

Un profilo di criticità ulteriore, spesso sottovalutato nella progettazione di soluzioni basate su *blockchain*, attiene all'automazione decisionale. Il GDPR, all'art. 22, tutela l'interessato rispetto a decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici o incidano significativamente sulla sua sfera personale.

Numerose implementazioni *blockchain* incorporano *smart contract*, ossia protocolli autoesecutivi che attivano determinate azioni al verificarsi di condizioni predefinite: si pensi, a titolo esemplificativo, a contratti che, verificato un inadempimento, blocchino automaticamente l'accesso a risorse digitali o trasferiscano asset senza intervento umano. In tali scenari, diviene essenziale verificare se l'automazione integri una "decisione" ai sensi dell'art. 22 GDPR e, in caso affermativo, se siano rispettate le garanzie prescritte dalla norma: il diritto dell'interessato all'intervento umano; la possibilità di esprimere il proprio punto di vista; il diritto di contestare la decisione.

L'assenza di meccanismi efficaci che consentano l'intervento umano o la revisione delle decisioni automatizzate espone i sistemi *blockchain* a significativi rischi di non conformità normativa, rendendo indispensabile un ripensamento dell'architettura tecnica in funzione delle esigenze di tutela dei diritti fondamentali.

2. SCELTA CONSAPEVOLE DELL'ARCHITETTURA *BLOCKCHAIN*

Uno dei punti cardine delle Guidelines 02/2025 dell'EDPB è la raccomandazione che l'adozione di tecnologie *blockchain* sia il risultato di una valutazione consapevole, basata su un'analisi di necessità, proporzionalità e adeguatezza rispetto alle finalità del trattamento.

Il principio di protezione dei dati fin dalla progettazione e per impostazione predefinita (*data protection by design and by default*, art. 25 GDPR) impone infatti di adottare fin dalla fase di ideazione della soluzione tecnologica tutte le misure – sia tecniche che organizzative – che possano minimizzare l'esposizione dei dati personali, limitandone la diffusione e garantendo il rispetto dei principi di minimizzazione e limitazione della finalità.

LA SCELTA DELL'ARCHITETTURA: *PUBLIC, PRIVATE, PERMISSIONED*

La corretta selezione dell'architettura della *blockchain* rappresenta una delle decisioni più rilevanti ai fini della compliance. Le linee guida sottolineano la necessità di valutare attentamente la tipologia di *blockchain* da utilizzare in funzione:

- delle caratteristiche del trattamento previsto;
- della natura e della sensibilità dei dati coinvolti;
- dei diritti e delle libertà degli interessati potenzialmente impattati.

In particolare, è utile distinguere tra:

A) *Blockchain* pubbliche (*permissionless*):

Consentono a chiunque di partecipare alla rete come nodo validatore e di consultare il contenuto della *blockchain*. È il modello tipico delle criptovalute come Bitcoin ed Ethereum, degli NFT e di molte applicazioni DeFi. In questo contesto, il controllo sull'accesso ai dati è limitato, e la trasparenza si traduce spesso in una potenziale esposizione illimitata delle informazioni. Di conseguenza, il ricorso a *blockchain* pubbliche per il trattamento di dati personali comporta criticità significative in termini di rispetto del principio di minimizzazione e di tutela dei diritti degli interessati.

B) *Blockchain* private o *permissioned*:

Prevedono meccanismi di controllo sull'ammissione e sulle modalità di partecipazione dei nodi. L'accesso può essere riservato a una cerchia di soggetti selezionati o subordinato al rispetto di specifiche regole di governance. Questa tipologia è spesso utilizzata per registri immobiliari, tracciabilità delle filiere agroalimentari, sistemi di supply chain, gestione di credenziali accademiche o sanitarie. L'adozione di *blockchain* permissioned facilita l'identificazione delle responsabilità dei partecipanti e consente una maggiore flessibilità nell'applicazione delle misure di sicurezza e protezione dei dati.

È opportuno sottolineare che, anche all'interno delle *blockchain permissioned*, il grado di decentralizzazione può variare considerevolmente; la *governance* — ossia le modalità con cui vengono adottate le decisioni nella rete, incluse le scelte relative a validatori, aggiornamenti del protocollo e gestione delle chiavi — assume dunque un ruolo centrale anche per la *compliance privacy*.

Blockchain pubbliche vs. private: implicazioni per la protezione dei dati

TECNOLOGIE PRIVACY-ENHANCING E ALTERNATIVE DI DESIGN

Oltre alla scelta del tipo di *blockchain*, le Linee Guida incoraggiano l'adozione di Privacy-Enhancing Technologies (PETs) che consentano di limitare la diffusione delle informazioni personali senza compromettere la funzionalità del sistema. Tra le soluzioni più rilevanti:

- Zero-Knowledge Proofs (ZKPs): tecniche crittografiche che permettono di dimostrare la veridicità di un'informazione senza rivelarne il contenuto. Utilizzabili, ad esempio, per dimostrare l'idoneità di un soggetto a effettuare una transazione senza esporre l'identità o altre informazioni sensibili.
- *Salted Hashing* o con chiavi segrete, *commitment schemes* e tecniche di pseudonimizzazione avanzata: modalità che permettono di memorizzare in *blockchain* solo impronte digitali (*hash*) o riferimenti ai dati, mantenendo i dati identificativi veri e propri *off-chain* e riducendo il rischio di esposizione.
- *Decentralized Identifiers* (DID) e Verifiable Credentials: approcci emergenti nel campo della *digital identity*, che possono contribuire a conciliare le esigenze di verifica con il rispetto dei principi di minimizzazione e controllo da parte dell'interessato.

LA NECESSITÀ DI DOCUMENTARE LE SCELTE

L'EDPB raccomanda di documentare accuratamente le motivazioni che hanno condotto a selezionare una determinata architettura o soluzione tecnica, nel quadro della più ampia *accountability* richiesta dal GDPR (art. 5, par. 2 e art. 24); in particolare, si suggerisce di esplicitare: le ragioni per cui la *blockchain* sia considerata la tecnologia più adeguata per lo specifico caso d'uso; le alternative valutate e le motivazioni per cui siano state scartate; le misure di mitigazione dei rischi previste.

Questa documentazione sarà essenziale sia in caso di controlli da parte delle autorità, sia per assicurare la trasparenza nei confronti degli interessati.

3. L'AGGIORNAMENTO DELLA DOCUMENTAZIONE *PRIVACY* AZIENDALE

Alla luce delle indicazioni fornite dall'EDPB nelle nuove Linee Guida, le organizzazioni che impiegano o intendono implementare soluzioni *blockchain* si trovano dinanzi alla necessità di procedere a un aggiornamento significativo della propria documentazione in materia di protezione dei dati personali. Tale revisione, lungi dall'essere un mero adempimento formale, rappresenta un imperativo strategico per garantire la compliance al GDPR e mitigare i rischi connessi all'utilizzo di tecnologie emergenti: la documentazione *privacy* aziendale costituisce, infatti, l'ossatura dell'accountability richiesta dal Regolamento, configurandosi come lo strumento attraverso cui il titolare può dimostrare di aver adottato misure tecniche e organizzative adeguate a garantire, ed essere in grado di comprovare, che il trattamento è effettuato conformemente alla normativa (art. 5, par. 2, GDPR).

Nel contesto specifico della *blockchain*, l'aggiornamento documentale dovrebbe interessare diversi livelli, ciascuno dei quali richiede un approccio distintivo e specialistico.

IL REGISTRO DEI TRATTAMENTI

Il Registro dei trattamenti (art. 30 GDPR) costituisce il punto di partenza per una ricognizione sistemica dei flussi di dati all'interno dell'organizzazione; e nel caso di implementazioni *blockchain*, esso dovrebbe essere integrato con sezioni specifiche che descrivano in modo granulare: la tipologia di *blockchain* adottata (pubblica/privata, permissioned/permissionless), con indicazione delle motivazioni alla base della scelta e delle relative implicazioni in termini di accessibilità dei dati; le categorie di dati personali trattati *on-chain* e *off-chain*, specificando per ciascuna categoria la base giuridica del trattamento, le finalità perseguite e il periodo di conservazione previsto; i nodi della rete e il loro ruolo nel trattamento, con

indicazione di eventuali trasferimenti verso paesi terzi e delle relative garanzie adottate ai sensi degli artt. 44-50 GDPR; le misure tecniche e organizzative implementate per garantire la sicurezza dei dati e l'esercizio effettivo dei diritti degli interessati, con particolare attenzione alle soluzioni adottate per conciliare l'immutabilità della *blockchain* con il diritto alla rettifica e alla cancellazione.

La revisione del Registro non costituisce una mera formalità, bensì un'opportunità per ripensare l'architettura complessiva dei trattamenti alla luce delle specificità della tecnologia *blockchain*, identificando preventivamente potenziali criticità e predisponendo misure di mitigazione adeguate.

LA VALUTAZIONE D'IMPATTO: ANTICIPARE E GESTIRE I RISCHI

La DPIA per la blockchain: adempimento imprescindibile

La DPIA assume carattere imprescindibile nei contesti *blockchain*, configurandosi come strumento privilegiato per l'analisi preventiva dei rischi e l'individuazione delle misure più appropriate per mitigarli. L'aggiornamento di tale documento dovrebbe includere: un'analisi approfondita della necessità e proporzionalità dell'utilizzo della *blockchain* rispetto alle finalità perseguite, evidenziando i benefici attesi in termini di trasparenza, integrità e disintermediazione delle transazioni, nonché le ragioni per cui soluzioni alternative non risulterebbero ugualmente efficaci; una mappatura dettagliata dei rischi specifici derivanti dall'architettura *blockchain*, con particolare attenzione ai profili di immutabilità, trasparenza e decentralizzazione che possono incidere sui diritti e le libertà degli interessati; una descrizione delle misure tecniche e organizzative adottate per mitigare tali rischi, includendo soluzioni quali il *salted hashing*, gli *zero-knowledge proofs*, i commitment schemes o la segregazione dei dati in ambienti *off-chain*; una valutazione del rischio residuo e, ove necessario, la documentazione della consultazione preventiva con l'autorità di controllo ai sensi dell'art. 36 GDPR.

La DPIA non deve essere concepita come un documento statico, bensì come un processo dinamico che accompagna l'evoluzione della soluzione *blockchain*, richiedendo revisioni periodiche in funzione di cambiamenti nel contesto tecnologico, normativo o organizzativo.

È opportuno evidenziare che le indicazioni contenute nelle Linee Guida su *blockchain* si pongono in linea di continuità con i criteri generali per la DPIA già fissati dal WP29, ma introducono elementi di specificità legati alla natura decentralizzata delle DLT:

Criterio WP29/EDPB per DPIA	Specificità nel contesto *blockchain*
Nuove tecnologie	*Blockchain* è, per definizione, una tecnologia innovativa
Difficoltà nell'esercizio dei diritti	Immutabilità "*on-chain*" può impedire rettifica o cancellazione diretta
Trasferimenti internazionali	Dislocazione globale dei nodi può comportare flussi non controllabili di dati
Trattamento su larga scala	Le DLT possono comportare trattamenti estesi su ampie popolazioni di utenti o transazioni

Questo raffronto conferma che, nel contesto *blockchain*, la DPIA non è solo raccomandata, ma nella maggior parte dei casi **necessaria per garantire una corretta gestione dei rischi legati alla protezione dei dati personali**.

L'INFORMATIVA AGLI INTERESSATI: TRASPARENZA E COMPRENSIBILITÀ

L'informativa agli interessati (artt. 13-14 GDPR) rappresenta lo strumento principale attraverso cui il titolare comunica le caratteristiche essenziali del trattamento, consentendo agli individui di esercitare un controllo effettivo sui propri dati personali.

Nel contesto *blockchain*, tale documento dovrebbe essere aggiornato per includere: una descrizione chiara e comprensibile delle specificità del trattamento mediante *blockchain*, evitando tecnicismi eccessivi ma fornendo informazioni sufficienti a comprendere le implicazioni di tale tecnologia per la protezione dei dati; l'indicazione dei dati trattati *on-chain* e *off-chain*, con specificazione delle relative finalità e basi giuridiche, nonché dei periodi di conservazione previsti; le modalità concrete di esercizio dei diritti in un contesto tecnologicamente complesso, illustrando come l'interessato possa richiedere la rettifica, la cancellazione o la limitazione del trattamento dei propri dati in un ambiente caratterizzato dall'immutabilità delle registrazioni; i destinatari o le categorie di destinatari dei dati, con particolare attenzione ai nodi della rete e alla loro dislocazione geografica, nonché alle eventuali garanzie adottate per i trasferimenti verso Paesi terzi.

4. DETERMINAZIONE DELLE RESPONSABILITÀ

Uno dei profili più complessi e discussi nell'ambito dell'applicazione del GDPR alle tecnologie *blockchain* riguarda l'**allocazione delle responsabilità** tra i diversi soggetti che partecipano alla rete. La decentralizzazione, caratteristica distintiva di molte architetture DLT, non può e non deve essere interpretata come un'esenzione dagli obblighi previsti dal Regolamento: al contrario, il GDPR si fonda sul principio di ***accountability***, imponendo di identificare con chiarezza chi, tra i soggetti coinvolti, determini finalità e mezzi del trattamento dei dati personali.

Le Linee Guida richiamano le precedenti **linee guida EDPB sui concetti di titolare, contitolare e responsabile del trattamento** (WP29, Versione 2.0, 2021), ribadendo che la natura distribuita di una tecnologia non esonera dall'obbligo di individuare ruoli e responsabilità giuridiche. La complessità tecnica di una *blockchain* non può tradursi in una deresponsabilizzazione di fatto.

LA SFIDA DELL'IDENTIFICAZIONE DEI RUOLI: TITOLARE, CONTITOLARE, RESPONSABILE

Nel contesto di una *blockchain*, il soggetto che determina le finalità e i mezzi essenziali del trattamento (ad esempio, il tipo di dati memorizzati sulla catena, le modalità di accesso, le regole di partecipazione alla rete) deve essere qualificato come **titolare del trattamento**.

Tuttavia, in molte applicazioni *blockchain*, queste scelte sono frutto di una decisione condivisa tra più soggetti (es. consorzi, gruppi di validatori), rendendo frequente la configurazione della **contitolarità** ai sensi dell'art. 26 GDPR. Tale contitolarità comporta la necessità di definire in modo trasparente, tramite accordi tra le parti, le rispettive responsabilità e modalità di cooperazione, nonché di informare adeguatamente gli interessati sui principali elementi di tale accordo.

Dove invece un partecipante opera per conto del titolare e secondo istruzioni vincolanti, si configura il ruolo di **responsabile del trattamento** (art. 28 GDPR), con conseguente obbligo di predisporre un contratto conforme ai requisiti di legge.

PERMISSIONED VS. PERMISSIONLESS: LA GOVERNANCE COME STRUMENTO DI COMPLIANCE

La **definizione della *governance*** gioca un ruolo centrale nella possibilità di identificare correttamente i ruoli dei diversi attori. Nelle *blockchain* ***permissioned*** o private, l'esistenza di un'autorità di coordinamento (ad esempio un consorzio o un ente promotore) facilita la distribuzione delle responsabilità e la stipula degli accordi tra i partecipanti. In questo contesto, è spesso possibile:

- definire in modo puntuale chi decide le finalità e i mezzi del trattamento;
- determinare quali nodi abbiano accesso ai dati personali e a quali condizioni;
- regolare le procedure di esercizio dei diritti degli interessati e gestione delle richieste.

Al contrario, nelle *blockchain* **pubbliche (*permissionless*)**, la mancanza di una *governance* formale e di un'organizzazione centrale rende più difficile individuare chi detenga il controllo effettivo sul trattamento dei dati. In questi casi, l'EDPB suggerisce di valutare la possibilità di costituire **consorzi o entità giuridiche *ad hoc*** che possano svolgere il ruolo di coordinamento e rappresentanza, anche al fine di assicurare un canale efficace per l'esercizio dei diritti degli interessati.

IL NODO DEI TRASFERIMENTI INTERNAZIONALI

Trasferimenti internazionali di dati: criticità nelle blockchain globali

Un ulteriore profilo di criticità, strettamente connesso all'allocazione delle responsabilità, riguarda i **trasferimenti internazionali di dati**. In molte

implementazioni *blockchain*, i nodi possono essere dislocati in paesi extra-UE, inclusi quelli che non offrono un livello di protezione dei dati considerato adeguato dalla Commissione Europea ai sensi dell'art. 45 GDPR.

In tali scenari, l'adozione di una *blockchain* comporta potenzialmente un trasferimento di dati personali verso tali paesi, con tutte le conseguenze che ne derivano:

- necessità di implementare **garanzie adeguate** (es. clausole contrattuali standard, *binding corporate rules*, deroghe ex art. 49);
- obbligo di condurre una ***transfer impact assessment*** **(TIA)** per valutare il livello di rischio connesso ai trasferimenti;
- obbligo di informare adeguatamente gli interessati circa i possibili trasferimenti e le misure di tutela adottate.

5. COOPERAZIONE EDPB E AI OFFICE: VERSO LINEE GUIDA CONGIUNTE SU AI ACT E GDPR

La decisione dell'EDPB di collaborare con l'AI Office, l'autorità chiamata a supervisionare l'attuazione del nuovo AI Act, rappresenta un passo significativo verso una **armonizzazione interpretativa tra i due principali pilastri della regolamentazione europea sul digitale**: il quadro per l'intelligenza artificiale e quello per la protezione dei dati personali.

Le implicazioni del trattamento di dati personali nei sistemi di AI – soprattutto per quanto riguarda i **sistemi classificati come ad alto rischio** dal Regolamento sull'intelligenza artificiale – rendono cruciale il coordinamento tra questi due ambiti normativi. In particolare, il rischio di approcci disallineati potrebbe compromettere l'efficacia delle tutele previste dal GDPR, specie in relazione a:

- ***accountability*** **dei fornitori e degli utilizzatori di sistemi di AI**;
- **garanzia dei diritti degli interessati**, inclusi il diritto all'informazione, il diritto alla spiegazione e il diritto alla contestazione delle decisioni automatizzate;
- **valutazione del rischio e DPIA**, con particolare attenzione ai profili etici e di protezione dei dati.

L'EDPB e l'AI Office si sono impegnati a elaborare linee guida congiunte che chiariscano come applicare il GDPR in relazione ai sistemi di intelligenza artificiale regolamentati dall'AI Act, fornendo alle imprese uno strumento di orientamento per la progettazione di soluzioni ***compliant by design***, sia dal punto di vista della protezione dei dati, sia da quello della sicurezza e dell'etica dell'AI.

In questo quadro, la cooperazione tra EDPB e AI Office si pone come un tassello fondamentale per evitare la frammentazione interpretativa tra discipline che, per quanto distinte, condividono un obiettivo comune: la tutela effettiva dei diritti delle persone nell'economia digitale.

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Giovanni Lombardi

Associate

Alessandro Carlini

Associate