OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Aprile 2025

Aprile 2025

I principali aggiornamenti in materia di TMT & Data Protection del mese.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

EDPB

- Study on the secondary use of personal data in the context of scientific research; [Link]
- Guidelines 02/2025 on processing of personal data through blockchain technologies; [Link]
- Annual Report 2024. [Link]

AGCOM

- Approvate le regole per la verifica della maggiore età degli utenti online (Delibera 96/25/CONS). [Link]

Linee guida sui trattamenti di dati personali effettuati attraverso *blockchain* dell'EDPB in consultazione

La tecnologia *blockchain*, originariamente concepita come registro distribuito e immutabile, ha rapidamente esteso il suo potenziale a una vasta gamma di applicazioni, trasformando settori che spaziano dalla finanza alla logistica, dalla sanità alla gestione dell'identità digitale.

In sostanza, una *blockchain* è una catena di blocchi di dati, ciascuno contenente un certo numero di transazioni, collegati tra loro attraverso la crittografia.

Questa struttura decentralizzata e la natura intrinsecamente immodificabile dei dati registrati conferiscono alla *blockchain* caratteristiche uniche in termini di trasparenza, sicurezza e tracciabilità.

Come funziona la *blockchain*?

In un sistema di *blockchain*, ogni transazione viene immediatamente registrata all'interno di un blocco, dotato di un *header*[1], all'interno del quale è reperibile l'*hash* [2] di tutte le transazioni registrate nel blocco stesso e in quello precedente.

Una nuova transazione si compie solo se è coerente con l'*hash* del blocco nel quale viene conservato.

I blocchi si collegano in sequenza tramite un *hash* parentale: ogni blocco include l'*hash* del blocco che lo precede.

Ogni blocco ha una copia locale dell'intera catena e si aggiorna ad ogni creazione di nuovi blocchi: quando un nodo riceve nuovi blocchi dalla rete, il nodo li valida immediatamente e crea con loro un collegamento alla *blockchain* esistente.

L'aggiunta di nuovi blocchi è eseguita da nodi specifici, denominati *validation nodes*, in base a regole prestabilite dal protocollo informatico e condivise dalla rete.

Le transazioni sono ordinate cronologicamente – attraverso dei server di marcatura temporale, o *timestamps* – mediante la divisione in blocchi, identificati univocamente con una stringa alfanumerica (vale a dire l'*hash*), che include anche l'*hash* del blocco precedente, formando una concatenazione di blocchi: da qui nasce il termine *"blockchain"*.

Tentare di manipolare i dati risulta estremamente difficoltoso: modificare un *hash* spezzerebbe la catena, causando il mutamento degli *hash* susseguenti, e si renderebbe evidente l'alterazione a causa dell'incoerenza con le copie della *blockchain* presenti negli altri nodi della rete.

Ciò conferisce alla *blockchain* una sorta di immutabilità unilaterale. La crittografia asimmetrica risulta fondamentale per l'inserimento dei dati in *blockchain*, poiché

[1] L'*header*, nel gergo informatico, è la componente che contiene informazioni di controllo necessarie al funzionamento del blocco.

[2] L'*hash* è contenuta nell'*header*. La sua funzione è consentire di trasformare una serie di dati di lunghezza arbitraria in una stringa alfanumerica determinata, univocamente riconducibile al contenuto originario.

consente che siano decriptati solo da chi sia in possesso della relativa chiave privata.

Ciò è funzionale al mantenimento della trasparenza propria della *blockchain*, necessaria per un corretto funzionamento, vale a dire la condivisione dei blocchi tra gli utenti, potendo pur mantenere un certo grado, seppur limitato, di riservatezza.

Sulla base dell'architettura informatica si possono, inoltre, individuare 3 macro-insiemi:

- ***blockchain* pubbliche** (c.d. *permissionless*), nelle quali chiunque può compiere transazioni, se valide, e partecipare al meccanismo di formazione del consenso. Queste *blockchain* sono garantite dalla cryptoeconomia. Fungono altresì da database globale per i documenti che hanno la necessità di essere immutabili, salvo meccanismi di consenso complessi. Tuttavia, l'eccessiva simmetria informativa e trasparenza potrebbe sollevare criticità. Infatti, società concorrenti potrebbero venire a conoscenza di informazioni della società che opera nella *blockchain*;
- ***blockchain* private** (c.d. *permissioned*), ove i permessi di scrittura sono accentrati presso un'organizzazione, così come quelli di lettura, che possono essere anche pubblici; e
- **consorzi**, ove il procedimento di formazione del consenso è controllato da un set di nodi preselezionato.

In ogni caso, la peculiare architettura e le complesse implicazioni tecniche della *blockchain* sollevano questioni significative nel contesto della protezione dei dati personali.

La natura distribuita del registro, la potenziale difficoltà nell'identificare i titolari del trattamento e i responsabili del trattamento, l'immutabilità dei dati e le sfide legate all'esercizio dei diritti degli interessati, come il diritto di rettifica e di cancellazione, rappresentano soltanto alcune delle problematiche che emergono dall'applicazione di questa tecnologia.

Proprio in considerazione di tali complessità e del crescente interesse verso l'utilizzo della blockchain in svariati ambiti che implicano il trattamento di dati personali, l'EDPB ha ritenuto necessario fornire un quadro interpretativo e operativo uniforme.

La pubblicazione delle Linee Guida 02/2025 sui trattamenti di dati personali effettuati attraverso *blockchain*, avvenuta lo scorso 8 aprile 2025 e in consultazione pubblica fino al 9 giugno 2025, riveste un'importanza cruciale.

Le Linee Guida e le indicazioni operative

Le Linee Guida mirano a chiarire come i principi e le disposizioni del GDPR si applichino specificamente ai trattamenti che utilizzano la tecnologia *blockchain*, fornendo indicazioni pratiche e raccomandazioni alle aziende che intendono adottare o già utilizzano tali soluzioni.

L'obiettivo primario è quello di garantire un elevato livello di protezione dei diritti e delle libertà fondamentali degli individui in un contesto tecnologico in rapida evoluzione, promuovendo al contempo l'innovazione in modo responsabile e conforme alla normativa in materia di protezione dei dati personali.

Come specificato nelle Linee Guida stesse, le *blockchain* memorizzano i metadati della transazione unitamente a un *payload*[3].

I metadati delle transazioni includono sia gli identificativi degli utenti sia altri metadati.

[3] Nel linguaggio informatico, il *payload* o carico utile indica la parte di dati trasmessi effettiva che è destinata all'utilizzatore.

Ciascun utente che partecipa a una transazione può, ad esempio, essere associato a un identificativo composto da una serie di caratteri alfanumerici che all'apparenza potrebbero risultare casuali, ma che costituiscono una chiave pubblica ottenuta da una chiave privata a disposizione dell'utente.

Se l'utente è una persona fisica e tali chiavi possono essere utilizzate per identificare gli individui con mezzi ragionevolmente utilizzabili, allora tali dati saranno qualificabili come dati personali.

Tra le principali criticità derivanti dall'immutabilità della *blockchain* vi sono, a titolo esemplificativo e non esaustivo, la non conformità a:

- l'art. 5(1)(e) del GDPR e, pertanto, violazione del principio di limitazione della conservazione per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati personali sono trattati;
- l'art. 16 del GDPR, poiché, in caso di modifica, si spezzerebbe la catena della *blockchain*;
- l'art. 17 del GDPR, in quanto l'immutabilità impedirebbe all'interessato di esercitare il proprio diritto alla cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.

Le Linee Guida, oltre a suggerire diverse tecniche da implementare per rendere il trattamento tramite tecnologia *blockchain* conforme al GDPR (ad es. crittografia, *hashing* dei dati personali, *proof of existence* [4]), forniscono ulteriori indicazioni operative:

- effettuare un'analisi e individuare in modo adeguato i ruoli privacy dei soggetti coinvolti, considerando la peculiare architettura della tecnologia *blockchain*;
- effettuare una valutazione d'impatto sulla protezione dei dati personali (DPIA) prima di utilizzare sistemi di *blockchain*, in considerazione della relativa tecnologia e dei potenziali rischi per i diritti e le libertà degli interessati;
- in relazione al diritto di rettifica dell'interessato, valutare l'implementazione della possibilità di inserire in una transazione successiva l'annullamento espresso della transazione precedente;
- rispettare i principi di *privacy by design* e *by default*, implementando sin dalla progettazione misure tecniche che, seppur non possano cancellare i dati personali, possano anonimizzarli.

Come emerge dalle Linee Guida, non tutte le problematiche possono essere mitigate da misure tecniche e organizzative adeguate.

Tuttavia, l'EDPB non ostacola l'utilizzo della tecnologia *blockchain*, ma adotta approccio costruttivo, guidando le aziende verso implementazioni conformi, ma specificando che la difficoltà tecnica non ne giustifica la mancata conformità.

* * *

[4] La *proof of existence* consiste nel registrare l'*hash* stesso sulla *blockchain*.

Controllo a distanza dei dipendenti: il Garante Privacy torna a sanzionare l'uso improprio dei sistemi di geolocalizzazione

L'utilizzo di sistemi di geolocalizzazione è ormai prassi consolidata in molte imprese, soprattutto per la gestione delle flotte aziendali, al fine di soddisfare esigenze organizzative, produttive o di sicurezza sul lavoro.

Tuttavia, l'adozione di tali tecnologie richiede un attento bilanciamento tra le esigenze del datore di lavoro e i diritti fondamentali dei lavoratori, dovendo garantire il rispetto della normativa in materia di protezione dei dati personali e dello Statuto dei Lavoratori.

Un recente provvedimento del Garante per la protezione dei dati personali (provv. 7/2025, doc. web. 10112287) ha riportato l'attenzione su questo tema, disponendo una sanzione pari a 50.000 euro nei confronti di una società di autotrasporti per aver effettuato un monitoraggio illecito su circa 50 dipendenti, tramite un sistema GPS installato sui veicoli aziendali.

Il caso offre l'occasione per riflettere sui presupposti giuridici che legittimano l'impiego di strumenti di localizzazione e sulle misure che ogni impresa dovrebbe adottare per assicurare la conformità normativa ed evitare conseguenze sanzionatorie.

Le violazioni rilevate dal Garante Privacy

Il Garante ha riscontrato diverse violazioni, tra cui:

1. **inadeguatezza dell'informativa privacy fornita ai dipendenti**. In particolare:
    - la diretta identificabilità dei conducenti era possibile grazie all'associazione tra il dispositivo GPS e la targa del veicolo, incrociata con ulteriori informazioni (ad es., documenti relativi ai turni di lavoro)[5];
    - l'informativa fornita non illustrava in modo chiaro e completo le modalità del trattamento effettuato, compromettendone la comprensibilità e la trasparenza nei confronti degli interessati.

2. **Violazione del principio di minimizzazione**:
    - il sistema raccoglieva dati in modalità continuativa, inclusi posizione, stato del veicolo (acceso/spento), telemetria e informazioni indirettamente riferibili all'attività dell'autista, comprese le pause lavorative;
    - sebbene fosse tecnicamente prevista la possibilità di disattivare il tracciamento, la società aveva omesso volontariamente di attivare tale funzione.

3. **Conservazione dei dati per un arco temporale eccessivo**, pari ad oltre cinque mesi, in contrasto con il principio di limitazione della conservazione.

[5] Sul punto si rinvia ai seguenti provvedimenti del Garante Privacy: provv. 396/2018, doc. web. 9023246 e provv. 247/2017 doc. web. 6495708.

4. **Violazione dei limiti stabili dall'autorizzazione rilasciata dall'Ispettorato territoriale del Lavoro** ai sensi dell'art. 4 dello Statuto dei Lavoratori, in quanto:
    - il trattamento, prevedendo un monitoraggio continuo, eccedeva i limiti funzionali e temporali previsti dall'autorizzazione;
    - non erano state adottate misure tecniche per garantire l'anonimizzazione dei dati o per evitare il trattamento di informazioni non pertinenti o eccedenti le finalità perseguite dal titolare (il sistema GPS era infatti stato installato per finalità di tutela dei beni aziendali, di sicurezza sul lavoro e per esigenze di natura organizzativa e produttiva).

Come evitare simili sanzioni?

Sebbene l'importo della sanzione non sia particolarmente elevato, il provvedimento rappresenta un chiaro monito alle imprese sull'importanza di assicurare una gestione conforme dei sistemi di tracciamento dei veicoli aziendali, in particolare quando tale tracciamento può incidere sull'attività dei lavoratori.

In concreto, le aziende che intendano adottare sistemi GPS dovranno:

- redigere e fornire un'**informativa privacy completa e comprensibile**, sia in versione estesa sia nella forma semplificata (c.d. **vetrofania**) mediante cartelli da apporre sui veicoli;
- **limitare il trattamento ai dati strettamente necessari**, evitando la raccolta sistematica o continuativa, salvo nei casi in cui ciò sia giustificato da esigenze legittime e documentate. In particolare, come chiarito dal Garante, il monitoraggio continuativo dei veicoli deve essere considerato eccezionale e non la regola (Garante Privacy, provv. 396/2018, doc. web. 9023246; Garante Privacy provv. 370/2011, doc. web. 1850581);
- **configurare i sistemi in ottica di *privacy by design* e *by default***, adottando soluzioni tecnologiche che, per impostazione predefinita, minimizzino i dati trattati e consentano - ad esempio - la disattivazione del GPS durante le pause lavorative;
- stabilire **tempi di conservazione proporzionati e differenziati**, secondo le specifiche finalità perseguite;
- **rispettare quanto previsto dall'art. 4 dello Statuto dei Lavoratori**, mediante:
    - accordo collettivo con le rappresentanze sindacali, oppure
    - autorizzazione dell'ispettorato del lavoro.

    In ogni caso, il trattamento non dovrà eccedere i limiti previsti in tali atti autorizzativi.
- **formalizzare il rapporto con il fornitore del servizio di localizzazione**, designandolo quale **responsabile del trattamento** ai sensi dell'art. 28 del GDPR, mediante apposito atto scritto conforme ai requisiti normativi.

* * *

L'Unione europea come continente dell'Intelligenza Artificiale: sovranità tecnologica e infrastrutture strategiche

Con la Comunicazione della Commissione europea COM(2025)165 del 9 aprile 2025, la Commissione ha formalmente inaugurato una nuova fase nella strategia digitale dell'Unione europea, ponendo l'obiettivo ambizioso – e al tempo stesso necessario – di rendere l'Europa il primo continente dell'intelligenza artificiale.

In un contesto geopolitico in cui la tecnologia si è affermata come terreno di confronto tra potenze globali, l'Unione europea intende affermare una propria traiettoria autonoma, capace di coniugare leadership tecnologica e rispetto dei valori fondamentali dell'ordinamento europeo.

Il documento della Commissione segna un'evoluzione di paradigma: da regolatore a promotore attivo di un ecosistema europeo dell'intelligenza artificiale.

L'obiettivo dichiarato è duplice: da un lato, favorire l'adozione pervasiva dell'intelligenza artificiale nei settori nevralgici dell'economia; dall'altro, assicurare che tale transizione avvenga nel rispetto della dignità umana, della democrazia e della diversità culturale.

Cinque sono gli assi portanti attorno a cui si articola la strategia europea:

- **sviluppo delle infrastrutture di calcolo**, attraverso il rafforzamento dell'infrastruttura pubblica per l'addestramento e il perfezionamento dei modelli di intelligenza artificiale;
- **accesso sicuro, equo e affidabile ai dati**, mediante una governance dei dati che garantisca apertura e protezione simultaneamente;
- **promozione dell'adozione di sistemi di AI nei settori strategici dell'economia europea**, con l'intento di sostenere la competitività dell'industria e l'autonomia strategica;
- **crescita delle competenze e del capitale umano**, tramite programmi di formazione avanzata, attrazione di talenti e promozione della AI literacy;
- **tutela del mercato unico digitale, attraverso una normativa armonizzata** che eviti la frammentazione giuridica e rafforzi la fiducia nell'innovazione tecnologica.

Al centro di questo disegno si colloca una consapevolezza strutturale: nessuna leadership nell'AI può prescindere da un'infrastruttura computazionale adeguata.

Oggi, infatti, l'Unione europea si trova a fronteggiare una dipendenza sistemica da data center e servizi cloud localizzati in Paesi terzi.

Tale condizione non solo compromette la competitività industriale, ma espone l'Europa a rischi di sicurezza economica e geopolitica.

È in questa prospettiva che la Commissione propone l'adozione del **Cloud and AI Development Act**, un atto legislativo che mira a creare le condizioni necessarie per attrarre investimenti su larga scala nel settore del cloud e dell'edge computing.

L'obiettivo è chiaro: triplicare, entro cinque-sette anni, la capacità europea di calcolo e

archiviazione, così da garantire che - entro il 2035 - imprese e pubbliche amministrazioni possano contare su risorse europee per lo sviluppo e l'uso dell'AI.

Come noto, infatti, l'addestramento e la messa a punto dei modelli di intelligenza artificiale richiedono enormi volumi di dati e potenza computazionale.

L'inferenza, invece, può essere eseguita più agevolmente in ambiente edge. Ne deriva che la centralità dei data center non è soltanto tecnica, ma strategica, in quanto punto di intersezione tra le esigenze computazionali, le istanze di sostenibilità ambientale e la sovranità tecnologica.

La Commissione segnala inoltre che l'attuale capacità computazionale europea non è sufficiente a sostenere lo sviluppo dell'AI, come evidenziato già nel **Rapporto Draghi del 2024**, che riconosce la necessità di rafforzare l'infrastruttura di calcolo come pilastro fondamentale per una piena economia dei dati.

Tuttavia, il percorso non sembra privo di ostacoli. Le difficoltà legate all'accesso a risorse naturali (energia, acqua, suolo), insieme a procedure autorizzative disomogenee e spesso farraginose tra gli Stati membri, rappresentano un freno significativo agli investimenti.

Il tempo medio per l'ottenimento dei permessi per la realizzazione di un **data center** è oggi stimato in circa 48 mesi.

Il Cloud and AI Development Act si propone, quindi, di superare tali criticità, introducendo meccanismi di semplificazione procedurale per i progetti che soddisfino determinati standard in materia di efficienza energetica e idrica, economia circolare e innovazione.

L'obiettivo è duplice: da un lato, accelerare lo sviluppo di nuove infrastrutture; dall'altro, garantire che tali sviluppi avvengano in modo coerente con i principi della transizione ecologica.

In parallelo, inoltre, la Commissione propone una roadmap strategica per la digitalizzazione del settore energetico, che mira a favorire l'integrazione sostenibile dei data center nella rete elettrica, promuovendo al contempo l'efficienza energetica e la flessibilità nella gestione della domanda.

Sul piano ambientale, la futura Water Resiliency Strategy si concentrerà sulla riduzione dell'impatto idrico di queste infrastrutture, attraverso pratiche di raffreddamento a secco, riutilizzo dell'acqua e ottimizzazione dei consumi.

È in questo contesto che si apre, pertanto, la consultazione pubblica sul Cloud and AI Development Act, avviata il 9 aprile 2025 e aperta fino al 4 giugno 2025.

La Commissione invita gli stakeholder a contribuire al processo legislativo, nella consapevolezza che una regolazione efficace dell'infrastruttura digitale non può prescindere da un confronto ampio e informato tra istituzioni, imprese e società civile.

Per maggiori informazioni e approfondimenti

Carlo Impalà

Partner e Responsabile Osservatorio TMT&DP

Carloo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio TMT&DP**

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it