LA NATURA GIURIDICA DEI METADATI NEL DIRITTO DEL LAVORO DIGITALE

Avv. Ciro Cafiero

CafieroPezzali
& Associati

Introduzione: L'economia dei dati e la centralità dei Metadati

Nel contesto tecnologico contemporaneo, caratterizzato da un flusso informativo continuo e da una sempre maggiore influenza dei sistemi digitali nella vita quotidiana, la nozione di metadato occupa un ruolo centrale nel dibattito giuridico.

L'economia dei dati ha imposto di prestare attenzione anche verso quelle informazioni che, pur non costituendo contenuto primario di un documento o di una comunicazione, ne descrivono struttura, condizioni di creazione, modalità di trasmissione e caratteristiche essenziali.

Definizione dei Metadati

Definizione

Informazioni come l'autore, la data di creazione o le dimensioni del file, che descrivono un punto dati o un set di dati.

Elementi chiave

I metadati non coincidono con il contenuto, ma ne descrivono il perimetro. Hanno una funzione abilitante per gestire, ricercare e contestualizzare i dati.

Funzioni

Permettono di identificare, categorizzare, localizzare e interpretare un dato principale nei sistemi informatici complessi.

Metadati come "Informazione sull'Informazione"

La Metafora Bibliotecaria

La funzione dei metadati richiama la logica dei sistemi bibliotecari: così come un libro necessita di titolo, autore, editore e classificazione per essere rintracciabile, allo stesso modo un dato digitale necessita di metadati per essere ordinato e reso accessibile.

- Il contenuto è rappresentato dal testo
- I metadati sono il titolo, l'autore, l'indice
- La collocazione e le parole chiave

Senza questi elementi, il libro sarebbe disperso tra milioni di altri volumi. Lo stesso accade ai dati digitali in un ambiente complesso.

Tassonomia dei Metadati

Metadati Descrittivi

Forniscono informazioni sul contenuto: titolo, autore, abstract, parole chiave. Utilizzati in motori di ricerca, banche dati e social network.

Metadati Strutturali

Descrivono l'architettura del dato e come le sue parti si relazionano: struttura XML, relazioni tra tabelle, collegamenti ipertestuali.

Metadati Amministrativi

Riguardano gestione e diritti: proprietario, diritti di accesso, politiche di conservazione, informazioni per cancellazione.

Metadati Tecnici

Riguardano il funzionamento dell'infrastruttura: log di sistema, indirizzi IP, timestamp, parametri di instradamento.

Metadati Semantici

Descrivono il significato e le relazioni concettuali: tassonomie, ontologie, knowledge graphs per intelligenza artificiale.

CAFIEROPEZZALI
& ASSOCIATI

L'Impatto Economico dei Metadati

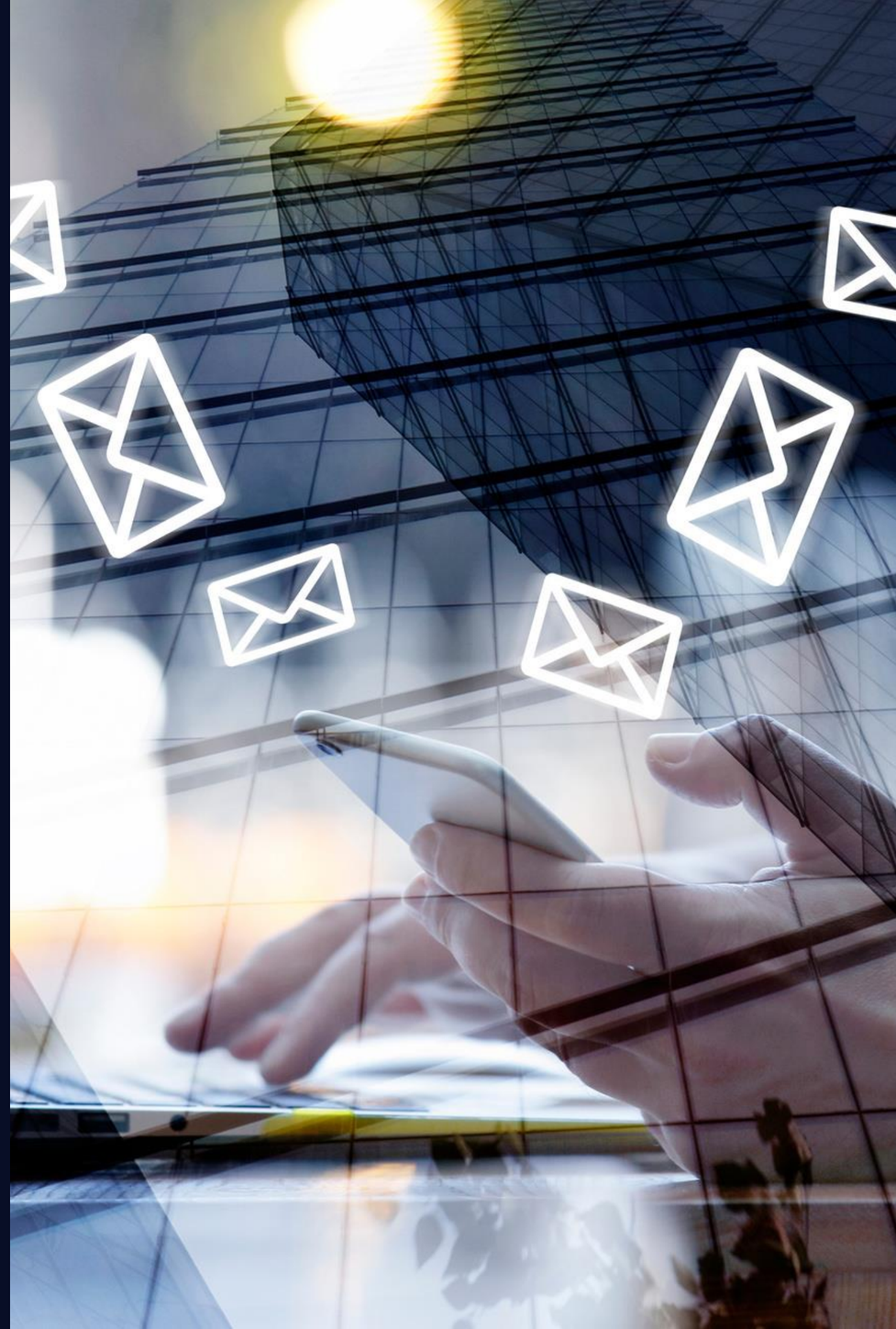
40%

Maggiori Costi

Le organizzazioni senza approccio basato su metadati sostengono fino al 40% in più di costi nella gestione dei dati

Conseguenze

- Difficoltà nella ricerca dei dati
- Inefficienza nei processi aziendali
- Riduzione della qualità delle informazioni
- Maggiori rischi di errori operativi
- Scarsa tracciabilità
- Incoerenze nei flussi informativi
- Aumento dei rischi di non conformità normativa



CAFIERO PEZZALI
& ASSOCIATI

Metadati e Rapporto di Lavoro

La zona di confine tra controllo e tutela

Il tema dei metadati si colloca esattamente nella zona di confine fra esigenze organizzative e produttive del datore, comprese quelle di sicurezza informatica, e tutela dei diritti e delle libertà del lavoratore, primo tra tutti il diritto alla riservatezza delle comunicazioni e quello a non subire controlli occulti o sproporzionati.

Rilevanza Giuridica dei Metadati: Tre Dimensioni Fondamentali

Dati Personali

Molti metadati soddisfano la definizione di dato personale: indirizzo IP, identificativo workstation, timestamp, header email, cronologia navigazione. La loro raccolta deve rispettare artt. 5, 6, 13, 88 GDPR e artt. 113-114 Codice Privacy.

Rivelazione Comportamentale

I metadati possono rivelare abitudini, comportamenti e preferenze: orari di accesso, siti visitati, frequenza comunicazioni, produttività, comportamenti anomali. Informazioni di natura profilante.

Controllo Lavorativo

Nel contesto aziendale permettono monitoraggio tempi, tracciamento flussi informativi, ricostruzione comunicazioni, controllo produttività, individuazione violazioni. Ricadono nell'art. 4 Statuto dei Lavoratori.

Rischi per i Lavoratori: Quattro Dimensioni Critiche

1. Profilazione involontaria

Frequenza di email, orari attività, siti visitati e tempi di risposta possono influire su valutazioni di performance, decisioni disciplinari, progressioni di carriera e licenziamenti senza che il lavoratore ne sia consapevole.

2. Accesso non autorizzato

Amministratori con diritti eccessivi, assenza di logging interno, conservazione eccessiva dei log, mancata informazione ai lavoratori, sistemi cloud che non permettono di ridurre la retention.

3. Violazione della riservatezza

I metadati rivelano con chi comunica il lavoratore, con quale frequenza, su quali argomenti e in quali fasce orarie, impattando direttamente sull'art. 15 Costituzione e sugli artt. 5, 6 e 88 GDPR.

4. Controllo difensivo illegittimo

L'utilizzo retroattivo o massivo di dati informatici raccolti prima dell'insorgere di un sospetto è illecito e rende illegittimo il licenziamento (Cass. 807/2025).

Ricostruzione del Comportamento del Lavoratore

Dimensione Temporale

Orari effettivi di lavoro e pause, ritmo di lavoro e produttività, eventuali ritardi o inattività, pattern comportamentali nel tempo.

Dimensione Relazionale

Interazioni con colleghi, clienti, fornitori, numero di email inviate e ricevute, frequenza e natura delle comunicazioni.

Dimensione Operativa

Siti visitati, ricerche effettuate, applicazioni utilizzate, documenti consultati, modalità di svolgimento delle attività.

Metadati Generati dagli Strumenti di Lavoro

Posta Elettronica

Indirizzo mittente/destinatario, IP server, orari, dimensioni messaggio, allegati, oggetto, identificativo messaggio, header tecnico di instradamento.

Navigazione Web

URL visitati, timestamp accesso, esito richiesta, IP postazione, identificativo dispositivo, redirect, tempo permanenza, alert sicurezza.

Applicativi Cloud

Log accesso/modifica, cronologia documenti, audit trails, interazioni utenti, attività piattaforme collaborative (Microsoft 365, Google Workspace).

Il Quadro Normativo

GDPR, Codice Privacy e Statuto dei Lavoratori

CAFIEROPEZZALI
& ASSOCIATI

Principi GDPR Applicabili ai Metadati

1

Art. 5, par. 1, lett. a) — Liceità, Correttezza, Trasparenza

Il datore deve informare chiaramente i lavoratori dell'esistenza di metadati, delle finalità, dei tempi di conservazione, dell'eventuale accesso da parte di amministratori, del loro possibile uso per esigenze tecniche o di sicurezza.

2

Art. 5, par. 1, lett. b) — Limitazione della Finalità

I metadati possono essere trattati per funzionamento del sistema, sicurezza informatica, risoluzione di malfunzionamenti. Non per monitorare produttività, controllare tempi, finalità disciplinari senza garanzie.

3

Art. 5, par. 1, lett. c) — Minimizzazione

Il datore può trattare solo i metadati strettamente necessari alle finalità tecniche. Trattare metadati eccedenti configura un trattamento sproporzionato e non conforme.

4

Art. 5, par. 1, lett. e) — Limitazione della Conservazione

I metadati devono essere conservati solo per il tempo strettamente necessario. 21 giorni sono un termine orientativo, non una prescrizione rigida.

5

Art. 32 — Sicurezza del Trattamento

I metadati devono essere protetti da accessi non autorizzati, visibili solo agli amministratori autorizzati, tracciati mediante audit, conservati in ambienti sicuri.

Il Codice Privacy

D.lgs. 196/2003 (artt. 113-114)

Gli artt. 113 e 114 del Codice Privacy richiamano, nel contesto lavorativo, l'art. 4 dello Statuto dei Lavoratori e l'art. 8 (divieto di indagini sulle opinioni). Il GDPR non esaurisce la disciplina: i metadati devono rispettare anche i limiti del diritto del lavoro e delle libertà fondamentali.

Principi Integrativi

- Esigenza di informare i lavoratori
- Divieto di controlli occulti
- Necessità di rispettare proporzionalità

CAFIEROPEZZALI & ASSOCIATI

I Metadati come Strumento di Controllo ex Art. 4 Statuto Lavoratori

Comma 1: Controlli a Distanza

Strumenti dai quali può derivare un controllo a distanza richiedono accordo sindacale oppure autorizzazione dell'Ispettorato del Lavoro.

Comma 2: Strumenti di Prestazione

Strumenti utilizzati per rendere la prestazione o registrare accessi/presenze sono esclusi dal comma 1, ma devono rispettare i principi GDPR.

Ambiguità dei Metadati

I metadati appartengono naturalmente alla categoria degli strumenti per rendere la prestazione, ma possono diventare strumenti di controllo a distanza se utilizzati per monitorare il comportamento del lavoratore.

Provvedimento 364/2024: "Possono diventare strumenti di controllo a distanza se i log vengono utilizzati per monitorare il comportamento del lavoratore nelle sue attività quotidiane."

L'Accordo Sindacale come Garanzia Procedurale

Nel contesto della gestione dei metadati, l'accordo aziendale ex art. 4 L. 300/70 assume un ruolo centrale per disciplinare finalità, tempi di conservazione e sicurezza del trattamento, garantendo trasparenza verso i lavoratori ed evitando violazioni normative.

Contenuti dell'Accordo

Definizione limiti chiari all'accesso dei metadati, identificazione delle tipologie trattate, tempi di conservazione, modalità di utilizzo.

Garanzie per i Lavoratori

Trasparenza sui trattamenti, protezione dalla sorveglianza occulta, tutela della dignità e della privacy.

Vantaggi per il Datore

Certezza giuridica, riduzione dei rischi di contenzioso, conformità normativa documentata.

Responsabilità del Titolare del Trattamento

Conoscenza dei Sistemi

Deve conoscere il funzionamento dei sistemi utilizzati, anche quando gestiti da terzi (cloud provider).

Verifica Tecnica

Deve verificare la possibilità di limitare la conservazione dei metadati e adeguare le impostazioni.

Misure di Sicurezza

Deve attuare misure tecniche e organizzative per impedire accessi indebiti ai metadati.

Informativa Chiara

Deve fornire informative chiare e aggiornate ai lavoratori sui trattamenti effettuati.

Principio fondamentale: L'ignoranza tecnica non esonera il titolare da responsabilità. Il datore di lavoro rimane sempre responsabile del trattamento, anche quando i sistemi sono gestiti da fornitori esterni.

Evoluzione dei Provvedimenti del Garante (2023-2025)

2023 — Provv. n. 642

Primo documento di indirizzo che stabiliva un limite rigido di 7 giorni di conservazione dei metadati.

2024 — Provv. n. 127

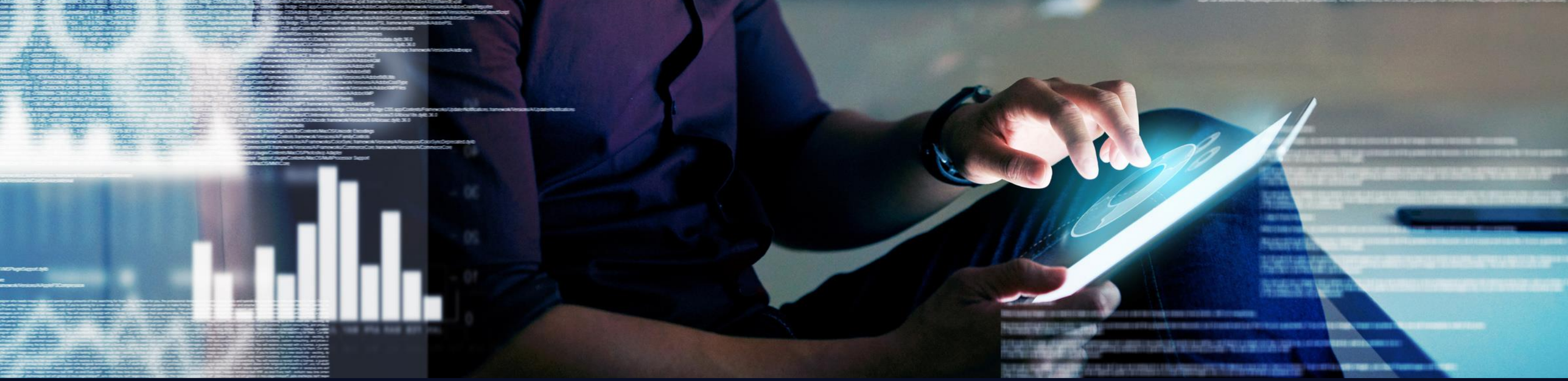
Sospensione dell'efficacia per richieste di chiarimento e avvio di una consultazione pubblica.

2024 — Provv. n. 364

Nuovo documento di indirizzo: definizione tecnica di metadati, responsabilità del titolare, 21 giorni come termine orientativo, linee guida non cogenti.

2025 — Provv. n. 243

Caso Regione Lombardia: analisi di log navigazione (12 mesi), metadati email (90 giorni), sistemi assistenza e sicurezza.



Alcuni casi concreti

Metadati in Pratica

CAFIEROPEZZALI
& ASSOCIATI

CAFIERO PEZZALI
& ASSOCIATI

Metadati nella Posta Elettronica: La Definizione del Garante

Il Garante, nel provvedimento del 6 giugno 2024, identifica i metadati nel contesto della posta elettronica come le informazioni generate dai log dei sistemi di trasporto e smistamento delle email (MTA), che includono elementi tecnici raccolti automaticamente e indipendentemente dalla volontà dell'utente.

Dati Identificativi

Indirizzo email mittente e destinatario, indirizzi IP dei server coinvolti

Dati Temporali

Orari di invio, ritrasmissione e ricezione dei messaggi

Dati Dimensionali

Dimensioni del messaggio, presenza e dimensioni degli allegati

Dati Contenutistici

Oggetto della mail (in alcuni sistemi), parametri di instradamento tecnico

Anatomia Tecnica

Sistemi MTA e MUA

I sistemi Mail Transport Agent e Mail User Agent registrano automaticamente tutti i dati di trasporto, indipendentemente dalla volontà dell'utente.

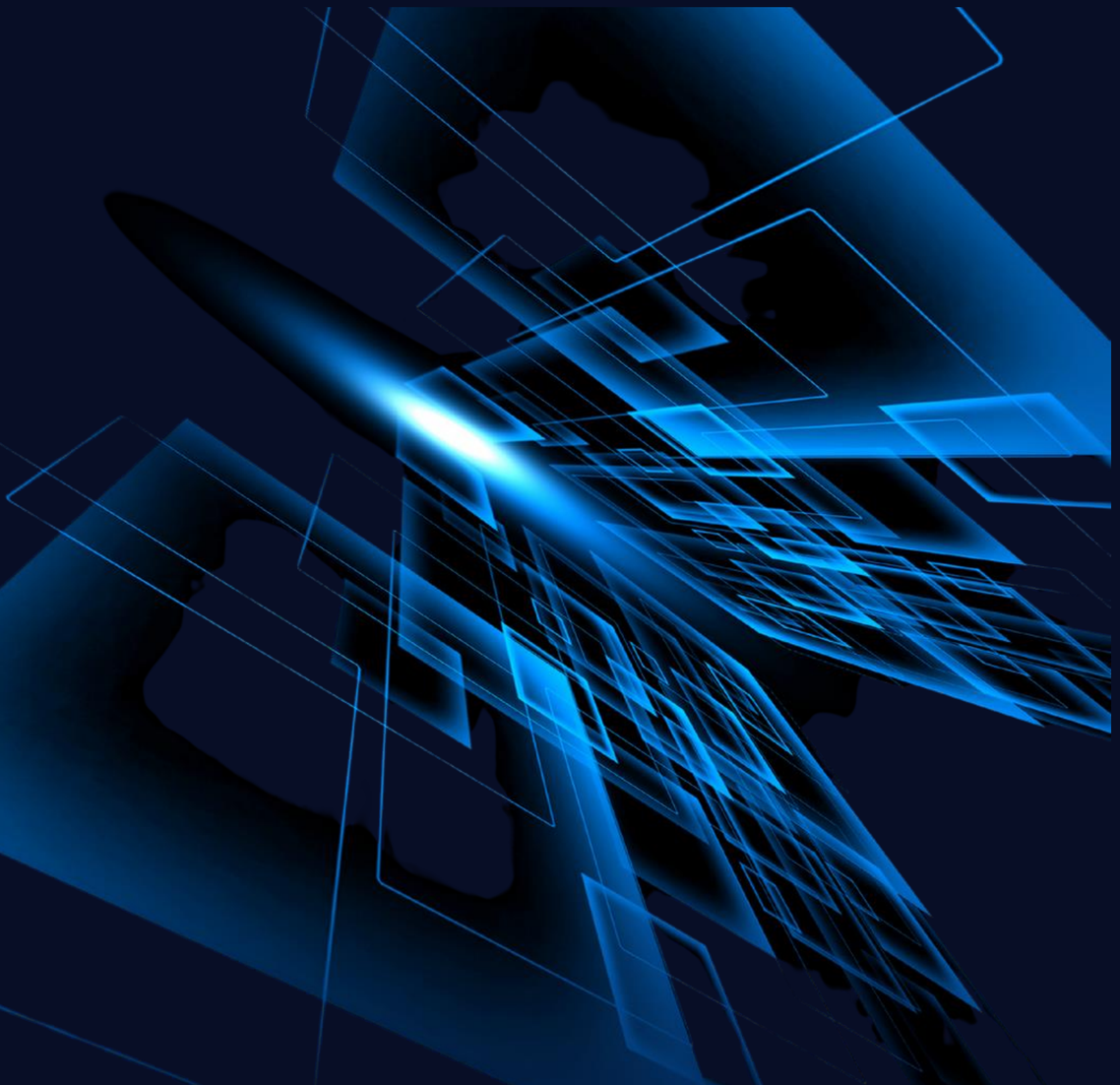
Header Tecnico

Contiene indirizzi IP, percorsi di instradamento, identificativi univoci dei messaggi e timestamp dettagliati di ogni fase di trasmissione.

L'Oggetto come Metadato Ibrido

Pur essendo tecnicamente parte delle intestazioni, può contenere informazioni sensibili (es. "Certificato medico per terapia oncologica").

Cosa Rivelano i Metadati della Navigazione Web



Informazioni Tecniche Raccolte

- URL visitati e timestamp di visita
- Indirizzo IP della macchina
- Codice di risposta HTTP
- Durata della connessione
- Tentativi di accesso a siti bloccati
- Presenza di malware o comportamenti anomali
- Alert di sicurezza generati dai sistemi

Capacità di Ricostruzione

Abitudini di consultazione, fasce orarie di attività, ricerche effettuate, accessi a siti di dubbia natura, preferenze personali, informazioni su sindacati, movimenti politici o religiosi.

Metadati negli Strumenti Cloud: Il Problema della Retention Predefinita

Le piattaforme cloud generano in modo massivo metadati relativi ad accesso documenti, versioni file, timestamp modifiche, attività chat, partecipazione riunioni, durata chiamate, presenza videoconferenza, produzione file e condivisioni. Questi metadati, spesso sottovalutati, rappresentano una vera e propria impronta digitale delle attività degli utenti all'interno dell'ecosistema aziendale e possono rivelare informazioni sensibili quanto i dati contenuti nei documenti stessi.

90
Giorni
Conservazione predefinita log **email** Microsoft 365 (Caso Regione Lombardia)

180
Giorni
Conservazione tipica log di accesso piattaforme **cloud**

12
Mes
Conservazione log **navigazione web** nei sistemi aziendali

21
Giorni
Termine orientativo suggerito dal Garante Privacy

CAFIEROPEZZALI
& ASSOCIATI

Violazioni e Conseguenze Giuridiche

Quando il trattamento è illecito

Inutilizzabilità della Prova e Conseguenze Disciplinari

Prova Inutilizzabile

I metadati raccolti in violazione dell'art. 4 non possono essere utilizzati in giudizio né in procedimenti disciplinari

Contestazione Illegittima

La contestazione disciplinare fondata su metadati illeciti è nulla e priva di effetti giuridici

Sanzione Illegittima

Qualsiasi sanzione disciplinare basata su dati illeciti è annullabile e comporta possibile risarcimento

Licenziamento Nullo

Il licenziamento fondato su metadati illeciti è nullo con reintegrazione del lavoratore e risarcimento integrale

Cassazione 807/2025: L'utilizzo retroattivo o massivo di dati informatici raccolti prima dell'insorgere di un sospetto è illecito e rende illegittimo il licenziamento.

Responsabilità e Sanzioni

Responsabilità Civile

Risarcimento del danno patrimoniale e non patrimoniale (art. 82 GDPR), reintegrazione in caso di licenziamento nullo, pagamento dei contributi omessi.

Responsabilità Amministrativa

Sanzioni GDPR fino a 20 milioni di euro o 4% del fatturato mondiale annuale per violazioni di minimizzazione, conservazione eccessiva, accessi non autorizzati, assenza di informativa o DPIA.

Responsabilità Penale

Art. 38 Statuto Lavoratori punisce l'installazione o utilizzo di strumenti di controllo a distanza in violazione dell'art. 4 con ammenda e arresto fino a un anno.

Responsabilità Amministratori

Gli amministratori di sistema devono essere nominati formalmente, operare su istruzioni, essere tracciati. Possono incorrere in responsabilità personali per accessi non autorizzati.

Linee Guida Operative per la Conformità

01

Informativa Completa

Elenco dettagliato metadati raccolti, finalità del trattamento, tempi di conservazione, destinatari e ruoli, individuazione rischi, diritti dell'interessato

02

Definizione Ruoli

Titolare (datore), Responsabili (fornitori cloud), Amministratori di sistema nominati e tracciati, DPO per vigilanza e conformità

03

Riduzione Conservazione

Verificare impostazioni cloud, adeguare tempi retention, documentare ragioni tecniche, prevedere cancellazioni automatiche

04

DPIA

Valutazione d'impatto per trattamenti sistematici, potenzialmente monitoranti, che coinvolgono lavoratori e grandi volumi di dati sensibili

05

Policy Aziendale

Elenco sistemi, finalità tecniche, limitazioni uso disciplinare, regole di accesso, tracciamento operazioni, divieto uso improprio, formazione obbligatoria

06

Accordi Sindacali

Definire tipologie metadati, limiti conservazione, regolare accessi, prevedere audit, specificare ruoli e responsabilità, distinguere controlli leciti da illeciti

07

Misure Tecniche

Logging con accesso segregato, dashboard aggregate non individuali, pseudonimizzazione dove possibile, cancellazione automatica al termine retention

08

Audit Continuo

Verifiche periodiche, controllo accessi, aggiornamento informative, verifica sistemi cloud, monitoraggio conformità, formazione continua