IPSOA Quotidiano

L'EDITORIALE DI LUCA FAILLA 08 MAGGIO 2026

Controlli difensivi aziendali e gestione dei (meta)dati nel mondo del lavoro. Attenzione alle sanzioni

Luca Failla - Professore a contratto di Diritto del Lavoro presso l'Università degli Studi LUM

Si sta ormai assistendo ad una sempre più precisa e penetrante azione di attrazione della legittimità o meno dei controlli difensivi aziendali nell'ambito del GDPR. Il rischio per il datore di lavoro non è più soltanto quello di vedersi contestare le modalità del controllo, ma anche il merito, con il rischio di incorrere in sanzioni amministrative di rilevante portata, in aggiunta all'inutilizzabilità del dato acquisito nell'eventuale procedimento disciplinare a carico del proprio dipendente. Per il Garante della privacy, oggi più che mai, sbagliare costa molto caro.

Da alcuni anni assistiamo ormai ad un progressivo inasprimento da parte del **Garante della privacy** delle **sanzioni** collegate all'uso non corretto delle informazioni e dei dati collegati agli **strumenti di lavoro**. Ci eravamo abituati a considerare ormai ben definita dal nuovo testo dell'art. 4 L. n. 300/1970 la fondamentale **distinzione** tra **strumenti e apparecchi** dai quali possono derivare **forme di controllo a distanza** (come ad esempio le videocamere), per i quali è richiesta apposita autorizzazione amministrativa e gli **strumenti** di lavoro in senso stretto per i quali - dopo la novella del Jobs Act del 2015 - l'uso, anche a fini disciplinari, delle informazioni raccolte non integra una forma di controllo occulto dell'attività lavorativa, ma costituisce da sempre **presupposto** per garantire la **legittimità** dei **controlli difensivi**, legati ad esigenze organizzative, produttive o dalla sicurezza del lavoro e finalizzati anche alla protezione dei beni e del know how aziendali.

Il vigente testo dell'art. 4 L. n. 300/1970 ha, infatti, cercato di costruire un **efficace bilanciamento** tra la necessità di regolare l'**uso** degli **strumenti (tecnologici)** di lavoro, la potenziale **raccolta** di **dati** da parte delle aziende - utilizzabili eventualmente anche a fini disciplinari - e la fondamentale esigenza di tutelare la dignità morale, la riservatezza ed i **dati personali** dei **lavoratori**, nel rispetto dei principi già da tempo sanciti dagli artt. 1 e 8 dello Statuto dei lavoratori e dalla disciplina sulla protezione dei dati personali di cui al Reg. UE n. 679/2016 (GDPR). Disciplina che oggi si intreccia anche con la disciplina specifica in materia di uso dell'**intelligenza artificiale** nei **luoghi di lavoro** (si pensi al divieto di uso dei dati biometrici) nel quadro del Regolamento (UE) 2024/1689 (AI Act) e della legge n. 132/2025.

Negli ultimi anni, tuttavia, abbiamo assistito ad un **progressivo inasprimento** della posizione del **Garante della privacy** in questa delicata materia. Se, infatti, la **giurisprudenza** dopo l'entrata in vigore del nuovo testo dell'art. 4 L. n. 300/1970 è rimasta in via generale **conforme** al proprio **consolidato orientamento** (cfr. l'Editoriale dell'11 aprile 2025 Controlli difensivi sul luogo di lavoro. Cosa dice la giurisprudenza) - seppure in parte rivisto proprio alla luce della estensione e pervasività della tecnologia altrettanto non può dirsi per quanto riguarda la posizione del **Garante della privacy**, il quale ha non solo progressivamente **ridefinito** in senso restrittivo i **confini operativi** dei **controlli difensivi**, ma si è anche spinto a **dettare regole** che in molti casi, lungi dall'essere mera linea di indirizzo, sono divenuti veri e propri **strumenti sanzionatori** a carico delle **aziende**.

Sul punto, la **giurisprudenza** della **Cassazione** ha in questi anni delineato un assetto relativamente stabile: i dati raccolti tramite strumenti utilizzati dal lavoratore per rendere la prestazione possono essere impiegati "per tutti i fini connessi al rapporto di lavoro" (inclusi quelli disciplinari come recita oggi l'art. 4 L. 300/70) purché il trattamento avvenga nel rispetto del GDPR e sia preceduto da adeguata informativa al diretto interessato. Questa impostazione

risulta oggi consolidata in giurisprudenza, seppure attenuata dalle pronunce più recenti che hanno iniziato a porre **limiti temporali** e **funzionali** a tali **controll**i, circoscrivendone l'ammissibilità ai soli dati **successivi** (e, quindi, a posteriori rispetto) all'**insorgenza** di un **fondato sospetto** di un **illecito** (cfr. Cass. n. 807/2025; Cass. n. 24204/2025).

Ed è proprio qui che ha iniziato a farsi strada un'azione sempre più incisiva e radicale da parte del **Garante** della **privacy**, con il risultato oggi evidente di comprimere ulteriormente gli spazi di manovra dei controlli difensivi a **tutela** delle **aziende** e del patrimonio aziendale. L'Autorità ha, infatti, progressivamente **spostato** il **baricentro** delle **indagini** dalla **legittimità** del **controllo** in senso stretto sugli strumenti di lavoro (giustificato come è noto da esigenze organizzative, produttive o dalla sicurezza del lavoro) alla **illiceità tout court** del **trattamento** dei **dati personali** del **lavoratore** attraverso i quali le aziende accertano gli avvenuti illeciti (molto spesso dati di log) con **conseguenze**, in alcuni casi, anche **pesantemente sanzionatorie**.

Un esempio è il **Documento** di **indirizzo** sui **metadati della posta elettronica** n. 364 del 2024.

Riformulato - nella versione appunto corretta a giugno 2024 - come semplice documento di indirizzo senza carattere precettivo, esso ha di fatto introdotto una serie di **prescrizioni puntuali** e pressoché **obbligatorie** sulla **gestione dei metadati** della **posta elettronica**, sui tempi di conservazione degli stessi e sulla trasparenza dei sistemi informatici utilizzati nei contesti lavorativi, che risulta oggi un vero e proprio **spartiacque** tra ciò che **si può fare** e ciò che **non è più consigliabile fare**, pur in presenza di adeguata ed aggiornata informativa ex art. 13 GDPR.

In particolare, l'Autorità ha enfatizzato il principio di minimizzazione del dato ed ha **imposto** alle **aziende** una verifica stringente della **proporzionalità dei trattamenti**, rendendo evidente che la mera disponibilità tecnica dei log o dei metadati non equivale (mai o quasi mai) alla loro legittima utilizzabilità, specialmente nelle indagini a carico dei propri dipendenti.

Lo stringente punto di **passaggio da "indirizzo"** a **"prassi sanzionatoria"** è stato poi molto rapido.

Ne è, infatti, un chiaro esempio il provvedimento n. 243 del 29 aprile 2025 nei confronti della Regione Lombardia. In questo caso, l'**utilizzo combinato** dei **log di navigazione** Internet e dei **metadati delle e-mail** per **finalità disciplinari** è stato ritenuto **illecito** non solo in ragione di carenza di adeguata informativa, ma soprattutto sul piano della eccessiva durata dei tempi di conservazione dei dati, nonché in merito alla scarsa chiarezza sulle modalità di accesso agli stessi. Non si trattava, dunque, di controlli occulti in senso tradizionale, né di strumenti installati in violazione delle garanzie statutarie; ciò che ha determinato la sanzione è stato piuttosto lo scollamento tra quanto dichiarato nelle policy aziendali e quanto effettivamente realizzato dai sistemi informatici.

Questo approccio conferma una linea interpretativa già emersa in altri provvedimenti di questi anni (nel 2022 con l'ordinanza ingiunzione del 1° dicembre 2022 emessa nei confronti della Regione Lazio), con i quali il Garante censura quasi sempre le modalità di trattamento dei dati connessi all'utilizzo di strumenti digitali.

Si sta ormai assistendo ad una sempre più precisa e penetrante azione di attrazione della **legittimità o meno** dei **controlli difensivi aziendali** nell'ambito del GDPR vero e proprio. Il **rischio** per il **datore di lavoro** non è più soltanto quello di vedersi contestare le modalità del controllo, ma anche il merito, quando trattasi di controlli difensivi, con il rischio di incorrere in **sanzioni amministrative** di rilevante portata in aggiunta alla inutilizzabilità del dato acquisito nell'eventuale procedimento disciplinare a carico del proprio dipendente.

In altri termini, la **legittimità del controllo** non è più valutata soltanto ex ante in relazione alla sua finalità difensiva (l'esistenza o meno di un valido e fondato sospetto circa la commissione di un illecito), ma anche ex post alla luce delle concrete modalità di gestione dei dati raccolti (una vera e propria trappola dal punto di vista tecnico, con buona pace degli strumenti di IT Compliance).

L'automazione dei processi, la diffusione di piattaforme digitali e l'impiego crescente di strumenti di tracciamento - dalla logistica alla gestione dello smart working - rendono oggi possibili **forme di sorveglianza** sempre **più capillari**.

Proprio per questo il Garante della privacy tende a **interpretare in modo rigoroso** i **principi** del **GDPR**, temendo che la facilità tecnica di raccolta e analisi dei dati possa tradursi in una compressione sistematica della sfera privata dei lavoratori. Non a caso, l'Autorità richiama spesso il rischio di controllo indiretto, continuativo, occulto, anche quando l'obiettivo dichiarato (e reale) è unicamente quello della tutela del patrimonio aziendale oppure la prevenzione di illeciti o di forme di concorrenza sleale.

In questo scenario, la tradizionale distinzione tra controlli difensivi "in senso stretto" e controlli sugli strumenti di lavoro perde parte della sua rilevanza operativa. Ciò che **conta**, sempre più, è la **qualità** del **trattamento** dei **dati**: la chiarezza dell'**informativa**, la coerenza delle **policy** con il funzionamento reale dei sistemi, la limitazione dei **tempi di conservazione** e la tracciabilità degli **accessi**.

La sanzione della Regione Lombardia ha reso evidente che un provvedimento concepito come **atto di indirizzo** può trasformarsi, nella pratica, in uno **standard vincolante** di comportamento, con effetti immediati sull'**operato** dell'**azienda**, anche quando questo sia già legittimo e coerente con la disciplina di riferimento. Il che implica l'adozione di livelli di attenzione e di progettazione dei **sistemi di controllo** sempre più **sofisticati e strutturati** e non solo secondo i meccanismi della privacy by design (art. 25 GDPR), ma sul piano di più ampie e capillari procedure di analisi e di compliance.

Oggi più che mai occorre tenere gli occhi - e gli orecchi - ben aperti. **Sbagliare costa molto caro**.