Il trattamento dei dati personali nelle attività di internal investigation

Privacy Day Forum 2023

CNR Area della Ricerca di Pisa, 25 maggio 2023

Avv. Alessandro Colella (*Socio* – KPMG Studio Associato Consulenza legale e tributaria)

01

Il trattamento dei dati dei lavoratori nella normativa sulla protezione dei dati personali

Lavoratori e Normativa sulla Personal Data Protection

Sviluppi tecnologici e nuove esigenze

Lo sviluppo tecnologico degli ultimi decenni ha portato a riconsiderare gli equilibri tra le esigenze di organizzazione e supervisione delle attività lavorative del datore di lavoro e la legittima aspettativa dei lavoratori di non essere oggetto di controlli effettuati mediante modalità lesive della propria dignità e riservatezza. Le disposizioni giuslavoristiche si sono così trovate a "convivere" con quelle in materia di protezione di dati personali.

L. 300/70 – Statuto dei lavoratori

Introduce nell'ordinamento italiano un generale diritto del lavoratore a non essere sottoposto ai cosiddetti "controlli a distanza", a garanzia della riservatezza e della dignità del lavoratore.

Reg. EU 2016/679 – GDPR

Disciplina in generale il trattamento dei dati personali sancendo principî ed oneri normativi a garanzia dei diritti e delle libertà degli Interessati. Con riferimento al contesto lavorativo, l'art. 88 del GDPR delega ai singoli Stati Membri l'emanazione di disposizioni specifiche in ambito lavoristico.

D.Lgs. 196/2003 – Codice Privacy

Con la modifica del D.Lgs 101/2018, costituisce la normativa di raccordo del GDPR con l'ordinamento giuridico italiano. Non contiene alcuna regolamentazione *ad hoc* per adeguare la normativa eurounitaria al contesto giuslavoristico italiano.

Provvedimenti del Garante Privacy

Stante l'assenza di alcuna normativa di dettaglio in ambito lavorativo nell'ordinamento italiano, i provvedimenti emanati nel corso degli anni dal Garante per la Protezione dei Dati Personali rappresentano un importante punto di riferimento di carattere tanto interpretativo quanto operativo.

I soggetti coinvolti nel trattamento dei dati in amb lavorativo

Implicazioni nelle attività di *internal investigation*

La corretta individuazione dei ruoli e delle figure coinvolte nel trattamento dei dati personali è fondamentale per poter correttamente attribuire **oneri** e **responsabilità** ai vari soggetti coinvolti.

Titolare del trattamento

«*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e I mezzi del trattamento di dati personali*» (art. 4 GDPR).

In ambito lavorativo è normalmente il **datore di lavoro** ad assumere il ruolo di Titolare

Responsabile del trattamento

«La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento» (art 4 GDPR).

È il soggetto incaricato di svolgere un'attività che comporti il trattamento di dati personali per conto del Titolare. Deve essere designato tramite una **nomina** che ha **natura contrattuale**.

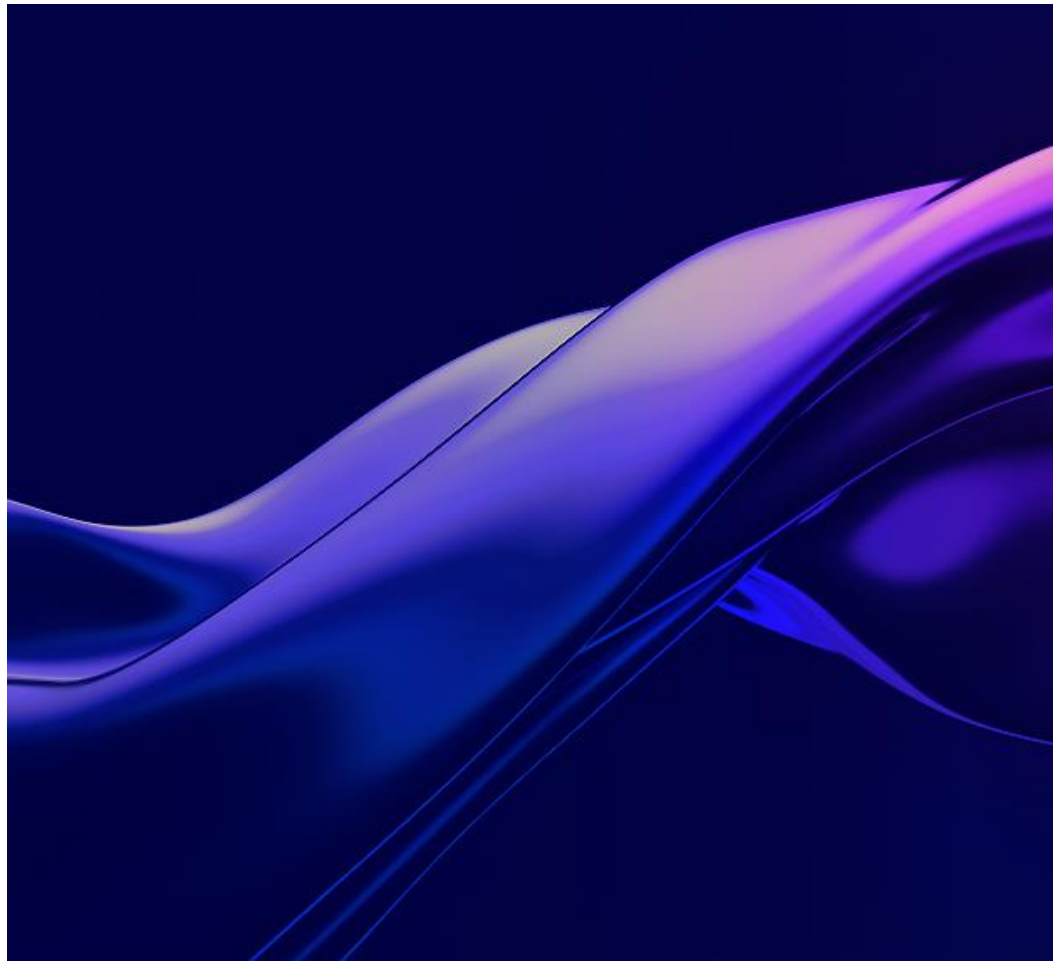
Interessato del trattamento

La persona fisica identificata o identificabile a cui si riferiscono i dati personali trattati.

Nel caso delle *internal investigation* tale figura è normalmente ricoperta dal **lavoratore**, indipendentemente dal tipo di rapporto contrattuale intercorrente con il datore di lavoro.

Gruppi di imprese e privacy

- Le società controllate o collegate possono **delegare** alle società capogruppo lo svolgimento delle attività (ad esempio, in materia di **lavoro**, **previdenza** e **assistenza**, *ivi* incluse le attività di *internal audit)*. In questi casi la capogruppo riveste normalmente il ruolo di **Responsabile del trattamento**.
- È possibile che, per determinate finalità di trattamento, Capogruppo e controllata siano **contitolari del trattamento** e che determinino **congiuntamente** le finalità e i mezzi del trattamento.
- Nell'ambito di un incarico ad un professionista per l'esecuzione di un incarico di *internal* investigation, è possibile che non vi sia **coincidenza** fra **conferente** dell'incarico e **Titolare** del trattamento (es. conferimento di incarico da parte della controllante per investigazioni su una società controllata).



Tipologia di dati personali

Dati Comuni

- Dati identificativi
- Video e immagini
- Dati finanziari *etc*.

Categorie Particolari di dati personali

- Dati sull'origina etnica o razziale;
- Dati su opinioni politiche, filosofiche o religiose;
- Dati sull'appartenenza sindacale;
- Dati biometrici, sanitari *etc.*

Dati Giudiziari

- Dati sulle condanne penali;
- Dati sulle misure di sicurezza.

I dati personali generati dal lavoratore nello svolgimento delle proprie mansioni vengono sovente trattati nell'ambito delle *internal investigations* al fine di **ricostruire comportamenti, fatti o eventi anomali e/o Illeciti**:

- Contenuto *e-mail;*
- *Log* dei sistemi informativi;
- *File* di lavoro;
- *etc*.

Principî applicabili

Liceità, correttezza e trasparenza

Il trattamento deve avvenire nel rispetto della legge, in buona fede e rendendo possibile in ogni momento all'Interessato di venire a **conoscenza** del tipo di **trattamento** effettuato sui propri dati personali.

Limitazione della finalità

Le finalità del trattamento devono: (*i*) essere **determinate** *ex ante* dal Titolare*; (ii)* essere **esplicitate** nell'informative all'Interessato; (*iii*) essere coperte da una **base giuridica** del trattamento di cui all'art. 6 GDPR (legittimità della finalità).

Esattezza dei dati personali

Il Titolare deve garantire **l'accuratezza** dei dati oggetto di trattamento, operando gli **aggiornamenti** e le **rettifiche** a tal fine necessarie.

Limitazione della conservazione dei dati personali

Il Titolare deve conservare I dati personali per un arco di tempo non superiore a quello **necessario** per il raggiungimento della **finalità** predeterminata, salvo l'archiviazione per fini di pubblico interesse, di ricerca scientifica e storica o per finalità statistiche.

Minimizzazione dei dati personali

Il Titolare deve trattare unicamente I dati personali **adeguati**, **pertinenti** e **limitati** al raggiungimento della finalità predeterminata, effettuando una raccolta secondo una logica di necessità e di sufficienza.

Integrità e riservatezza dei dati personali

Il Titolare deve garantire che il trattamento avvenga in un contesto di **misure** tecniche e organizzative **adeguate** che riducano il rischio di trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

02

Le attività di internal investigation

Principali riferimenti normativi e pareri delle Autorità

Art. 4 St. Lavoratori

Dopo la riforma c.d. Jobs Act, tale articolo subordina **l'utilizzabilità** dei dati generati dal lavoratore con gli strumenti di lavoro al rispetto della normativa sulla protezione dei dati personali.

Parere 8/01 WP29

Ogni attività di monitoraggio deve costituire una risposta **proporzionata** a rischi precedentemente individuati, tenendo conto del legittimo interesse dei lavoratori alla privacy e di altri diritti e libertà. I dati devono essere **adeguati**, **pertinenti** e **non eccedenti** alle finalità di individuate ed i controlli devono essere effettuati con la minor invasività possibile.

Linee guida 2007 GPDP

Il Datore di lavoro deve predisporre **policy** ed **informative** che indichino le modalità di utilizzo e di controllo relative agli strumenti di lavoro. I controlli non possono essere prolungati, costanti ed indiscriminati.

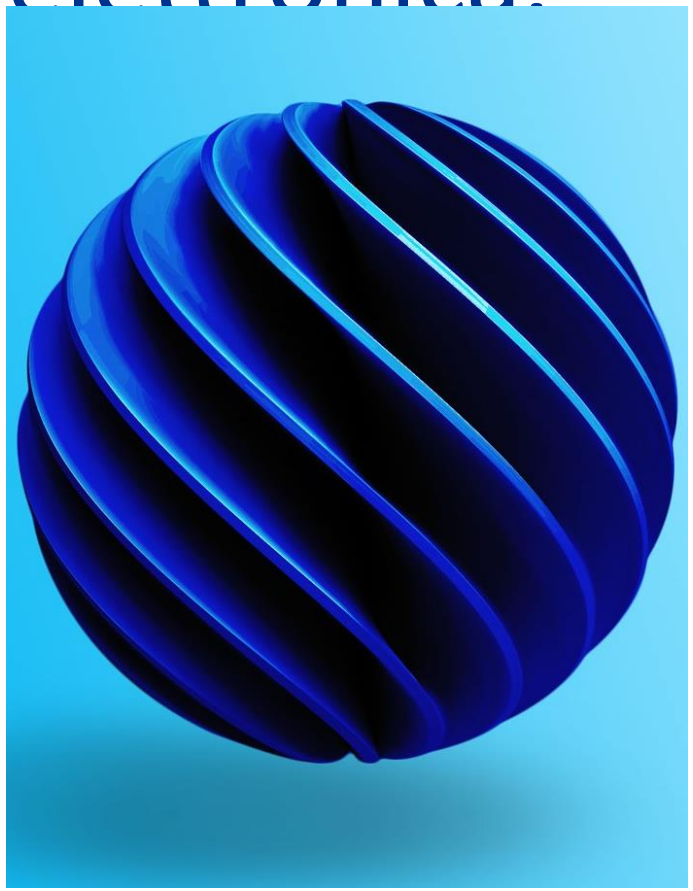
Parere 5/02 WP29

L'interesse legittimo del datore di lavoro a condurre e organizzare la propria attività può costituire la base giuridica per il trattamento di dati personali strumentali ad alcune forme sorveglianza, ma unicamente in via **eccezionale** e nel **rispetto dei principî** della protezione dei dati personali.

Parere 2/17 WP29

È necessario tenere conto degli **sviluppi tecnologici** che consentono nuove modalità di monitoraggio potenzialmente maggiormente invasive.

Le attività di *investigation* condotte sugli strumenti di lavoro. Un focus sulla posta elettronica.



Il controllo datoriale sugli strumenti di lavoro ed in particolare sugli *account* di posta elettronica aziendale è stato spesso oggetto di pronunce da parte del GPDP.

La casistica tipica afferisce a controlli condotti dal datore di lavoro in seguito a comportamenti anomali o sospetti da parte del lavoratore ed alla conseguente attivazione di controlli sulle risorse informatiche a quest'ultimo date in uso (Tipicamente le *e-mail*).

Il Garante ha spesso evidenziato come l'accesso alla messaggistica del lavoratore vada effettuata nel rispetto dei principî di liceità, correttezza e trasparenza.

In quest'ambito, il Garante ha frequentemente censurato casi di controlli effettuati in assenza di una corretta informazione del lavoratore, asserendo l'insufficienza a soddisfare i requisiti di **correttezza** e **trasparenza** di policy che si limitino a statuire la natura "aziendale" degli strumenti affidati ai dipendenti in violazione dei.

Vengono inoltre censurati i controlli consistenti in registrazioni sistematiche delle connessioni di rete effettuate dal lavoratore e la conservazione per lunghi periodi di tempo dei dati medesimi. Tali sistemi di monitoraggio rappresentano forme di controllo massivo, prolungato, costante ed indiscriminato contrastanti con I principî di **necessità**, **pertinenza** e **non eccedenza**.

L’evoluzione giurisprudenziale in materia di controlli difensivi (1/2)

Vigente l’art. 4 della L. 300/70 (Statuto dei Lavoratori) nella formulazione precedente alla riforma del cd. Jobs Act, la giurisprudenza aveva elaborato la categoria dei cd “controlli difensivi”.

Tale tipologia di controllo, diretta alla tutela del patrimonio e dell’immagine aziendale, non soggiaceva agli adempimenti previsti dall’art. 4 della L. 300/70 vigente.

L’evoluzione giurisprudenziale in materia di controlli difensivi

L’attuale **formulazione dell’art. 4 dello Statuto dei Lavoratori** annovera la tutela del patrimonio aziendale tra le esigenze che legittimano l’installazione di strumenti atti a determinare un controllo a distanza dei lavoratori.

Ci si è quindi domandati se i “controlli difensivi” fossero stati attratti nell’area di operatività dell’art. 4 L. 300/70.

Per rispondere a tale quesito si è distinto tra “controlli difensivi in **senso stretto**” e “controlli difensivi in **senso lato**”.

Sarebbero “controlli difensivi in senso lato” quei controlli a difesa del **patrimonio aziendale** che riguardano **tutti i dipendenti** (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio e che dovranno essere realizzati nel rispetto delle previsioni dell’art. 4.

Per “controlli difensivi in senso stretto” si intenderebbero invece quei controlli diretti ad accertare **specificamente** condotte illecite ascrivibili - in base a **concreti indizi** - a **singoli dipendenti**, anche se questo si verifica durante la prestazione di lavoro. Questi ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situerebbero all’esterno del perimetro applicativo dell’art. 4 (nella formulazione oggi vigente).

Il controllo difensivo rappresenta pertanto la reazione, caratterizzata da un bilanciamento tra le esigenze di protezione dei beni aziendali e la tutela della dignità e riservatezza del lavoratore, al fondato sospetto circa la commissione di un illecito, sempre che il controllo riguardi dati acquisiti successivamente all’insorgere del sospetto.

Considerazioni operative

Assetto privacy adeguato

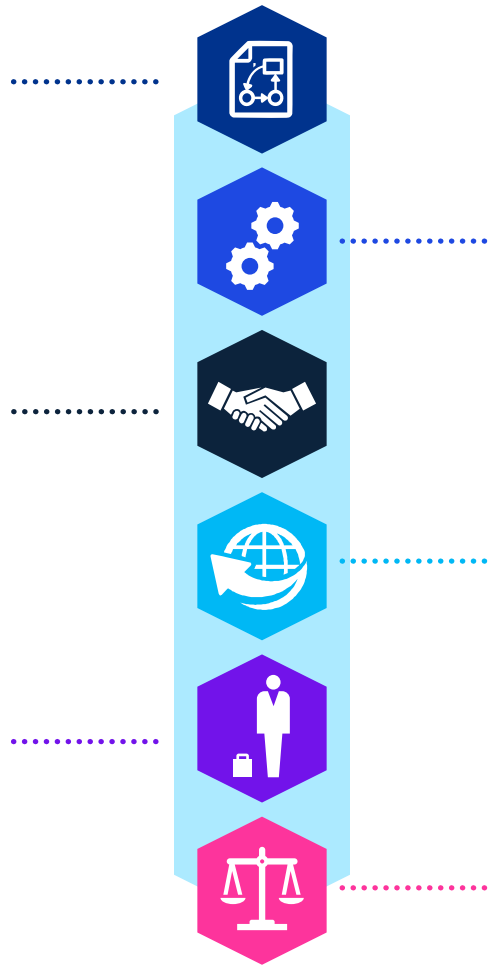
L'avvio di qualsivoglia attività di investigazione non può prescindere da una verifica di una corretta implementazione di un assetto privacy. In particolare sono fondamentali la corretta preparazione delle **informative**, la regolare tenuta del **Registro dei trattamenti** e, ove necessario, l'effettuazione di **DPIA**.

Ottenimento del consenso

L'ottenimento del consenso da parte del lavoratore all'effettuazione di controlli, stante il limite della sua generale validità in contesti lavorativi, può tuttavia essere preso in considerazione in caso di fattispecie che si prestino ad **interpretazioni non univoche** circa la sussistenza di basi giuridiche alternative, soprattutto con riferimento a controlli sugli ex dipendenti.

Coinvolgimento del DPO

Il coinvolgimento del DPO nell'ambito della sua funzione di **consulenza specialistica** può essere strategico per l'individuazione delle corrette modalità esecutive e delle più idonee misure di sicurezza circa la conservazione ed utilizzo dei dati generati dall'*investigation*.



Modalità esecutive *investigation*

Le attività di controllo dovrebbero essere effettuate con modalità tese a **minimizzare l'accesso** e la **visione dei dati** a quanto pertinente all'oggetto dell'*investigation*. A tal fine sono utili le ricerche effettuate mediante parole chiave e la limitazione del controllo a comunicazioni intercorse fra soggetti determinati.

Circolazione dei dati acquisiti

Una volta effettuate le attività di controllo è necessaria l'implementazione di misure idonee a garantire la **limitazione** della loro **circolazione** e **trattamento** all'interno del contesto e della finalità della *investigation.*

Legittimo interesse e proporzionalità

Il legittimo interesse del Titolare invocato come base giuridica del trattamento dei dati per finalità di controllo deve essere **bilanciato** e **proporzionato** ai diritti ed alle libertà dei lavoratori sacrificate con il controllo medesimo.

Grazie per l’attenzione

kpmg.com/socialmedia

kpmg.com/it

Tutte le informazioni qui fornite sono di carattere generale e non intendono prendere in considerazione fatti riguardanti persone o entità specifiche. Nonostante tutti i nostri sforzi, non siamo in grado di garantire che le informazioni qui fornite siano precise ed accurate al momento in cui vengono ricevute o che continueranno ad esserlo anche in futuro. Non è consigliabile agire sulla base delle informazioni qui fornite senza prima aver ottenuto un parere professionale ed aver accuratamente controllato tutti i fatti relativi ad una particolare situazione.

Document Classification: KPMG Public