UNIVERSITÀ CATTOLICA del Sacro Cuore

E-MAIL AZIENDALE: MODALITÀ DI UTILIZZO E POTERI DI CONTROLLO

Prof. Avv. Marco Marazza

Avvocato e Professore Ordinario di Diritto del Lavoro

Università Cattolica del Sacro Cuore

INDICE

1. FONTI DI RIFERIMENTO

I PRINCIPI DI RIFERIMENTO NELLE CARTE FONDAMENTALI

Art. 2 Costituzione: «*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*»

Art. 15 Costituzione: «*La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.*
La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria [Cost. 111] con le garanzie stabilite dalla legge.».

Art. 7 Carta dei Diritti Fondamentali dell'Unione Europea – Rispetto della vita privata e della vita familiare: «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

Art. 8 Carta dei Diritti Fondamentali dell'Unione Europea – Protezione dei dati di carattere personale: «*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Art. 8 Convenzione Europea dei Diritti dell'Uomo – Diritto al rispetto della vita privata e familiare: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

IL GDPR

Art. 88 GDPR – TRATTAMENTO DEI DATI NELL'AMBITO DEL RAPPORTO DI LAVORO

*«1. **Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro**.*

2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro il 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.»

IL BILANCIAMENTO DEL DIRITTO ALLA SEGRETEZZA

Art. 16 Carta dei Diritti Fondamentali dell'Unione Europea – Libertà d'impresa: «È riconosciuta la libertà d'impresa, conformemente al diritto dell'Unione e alle legislazioni e prassi nazionali».

Art. 41 Costituzione: «L'iniziativa economica privata è libera. Non può svolgersi in contrasto con la utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali e ambientali».

Art. 2094 – PRESTATORE DI LAVORO SUBORDINATO: «È prestatore di lavoro subordinato chi si obbliga mediante retribuzione a collaborare nell'impresa, prestando il proprio lavoro intellettuale o manuale alle dipendenze e sotto la direzione dell'imprenditore»

…SEGUE…

IPOTESI IN CUI IL LAVORATORE ABBIA LA CONSAPEVOLEZZA CHE LO STRUMENTO DI COMUNICAZIONE UTILIZZATO NON SIA FUNZIONALE A GARANTIRE LA SEGRETEZZA

↓

Giurisprudenza in tema di *chat* / gruppi *Facebook*

Cass. civ., Sez. lavoro, Ord. 10.09.2018, n. 21965: La vicenda ha ad oggetto il licenziamento intimato al dipendente in ragione di un commento offensivo rivolto da quest'ultimo nei confronti dell'A.D. reso nell'ambito di una conversazione avvenuta sul gruppo Facebook del Sindacato di appartenenza del lavoratore. La Corte ha espresso il seguente principio: «*i messaggi che circolano attraverso le nuove "forme di comunicazione", ove inoltrati non ad una moltitudine indistinta di persone ma unicamente agli iscritti ad un determinato gruppo, come appunto nelle chat private o chiuse, devono essere considerati alla stregua della corrispondenza privata, chiusa e inviolabile*»

Cass. civ., Sez. lavoro, Ord. 06.05.2024, n. 12142: La Corte si è espressa sulla legittimità del licenziamento per giusta causa intimato al dipendente per avere il medesimo diffuso tramite un *post* su *Facebook* affermazioni diffamatorie nei confronti del datore di lavoro e dei vertici aziendali. Nell'ambito di tale vicenda la Corte ha statuito che «*la portata diffamatoria del contenuto del «post» sarebbe rimasta intatta anche ove la diffusione dello stesso fosse stata limitata al comunque amplissimo elenco di amicizie documentate dallo stesso ricorrente*» → **il diritto alla segretezza dei contenuti scambiati non è indifferente al numero dei partecipanti alla chat / gruppo Facebook perché la popolosità dello strumento deve far sorgere nel lavoratore il dubbio che il mezzo non garantisca la riservatezza.**

Cass. civ., Sez. lavoro, Sent. 13.10.2021, n. 27939: Nel decidere sulla legittimità del licenziamento intimato al dipendente in ragione dei commenti denigratori rivolti alla datrice di lavoro tramite *post* sul proprio profilo *Facebook*, la Corte ha rimarcato «*l'esigenza di tutela della libertà e segretezza dei messaggi scambiati in una chat privata, in quanto diretti unicamente agli iscritti ad un determinato gruppo e non ad una moltitudine indistinta di persone, pertanto da considerare come la corrispondenza privata, chiusa e inviolabile*». In quel caso, tuttavia, il mezzo utilizzato per la pubblicazione del commento offensivo – vale a dire, **il profilo Facebook del lavoratore – era stato considerato idoneo "a determinare la circolazione del messaggio tra un gruppo indeterminato di persone", con conseguente legittimità del licenziamento**. In particolare, secondo la Corte d'Appello di Roma, pronunciatasi nella fase di merito, «*nel momento in cui si pubblicano informazioni e foto sulla pagina dedicata al proprio profilo personale, si accetta il rischio che le stesse possano essere portate a conoscenza anche di terze persone non rientranti nell'ambito delle c.d. "amicizie" accettate dall'utente, il che le rende, per il solo fatto della loro pubblicazione, conoscibili da terzi ed utilizzabili anche in sede giudiziaria*» (Corte d'Appello di Roma, 27.11.2018, n. 4530). Dunque, in quella particolare vicenda, non era stata riconosciuta, in capo al lavoratore, una aspettativa di riservatezza.

Corte d'Appello di Genova, Sez. Lavoro, 18.03.2019, n. 150: il Collegio, respingendo le argomentazioni del lavoratore circa la realizzazione della condotta offensiva nell'ambito di una *chat* chiusa, confermava la legittimità del licenziamento, evidenziando che la *chat* in questione non rappresentava un «*gruppo costituito da un dipendente o comunque da un soggetto che operava nell'interesse dei dipendenti, con evidente scopo di consentire uno sfogo a seguito delle provocazioni del datore di lavoro*» e che tale circostanza, «*nonché* ***il fatto che la chat era aperta ad un numero elevato di persone, non tutti dipendenti, e soprattutto il fatto che vi partecipavano soggetti legati a società concorrenti che avevano tutto l'interesse a divulgarne il contenuto***» **rivelavano, secondo la Corte, la mancanza della «*volontà dei partecipanti alla chat di non voler diffondere all'esterno il suo contenuto*».**

...SEGUE...

E- mail aziendale: diversamente da un indirizzo e-mail privato, **l'indirizzo e-mail aziendale deve essere utilizzato nel rispetto di *policy* ed informative che definiscono le modalità di utilizzo dello strumento e del relativo controllo da parte del datore di lavoro.**

CENTRALITÀ DELL'INFORMATIVA

Corte d'Appello di Milano, sent. 504/2020: Il caso ha riguardato alcuni dipendenti contestati dalla datrice di lavoro per violazione dell'obbligo di fedeltà sulla base di corrispondenza inviata dagli *account* di posta elettronica personale dei dipendenti rinvenuta, tramite perizia informatica, sul PC aziendale. La Corte ha ritenuto illegittimo l'utilizzo di detta corrispondenza da parte della datrice di lavoro posto che: a) la circostanza che i dipendenti avessero effettuato l'accesso al proprio account di posta elettronica privato dal PC aziendale non poteva dirsi sufficiente a renderla legittimamente accessibile al datore di lavoro; b) anche a volere equiparare la corrispondenza privata rinvenuta sul PC aziendale a quella proveniente da *account* aziendale, difettavano, nel caso di specie, specifiche disposizioni finalizzate a regolamentare ed indicare al dipendente le modalità di controllo e/o duplicazione della corrispondenza. Conseguentemente la Corte enunciava il principio *«dell'assoluta inacessibilità all'e-mail personale del dipendente, pena la commissione di un reato* [n.d.r. art. 616 c.p. – Violazione, sottrazione e soppressione di corrispondenza] *e la violazione delle regole costituzionali sul segreto della corrispondenza,* ***mentre per l'e-mail aziendale l'accesso è subordinato a determinate condizioni quali l'informativa del lavoratore tramite contratto di lavoro e/o policy aziendale; controlli sull'account di posta aziendale rispettosi e non eccedenti rispetto alle finalità perseguite e tracciabili; controlli consentiti solo per finalità di sicurezza nei limiti individuati dal Garante Privacy o qualora sussistano fondati sospetti nei confronti del dipendente infedele e sempre che il lavoratore sia al corrente della potenziale conservazione dei dati e della loro duplicazione***.»

2. E-MAIL AZIENDALE E STATUTO DEI LAVORATORI

E-MAIL E STATUTO DEI LAVORATORI

Art. 4 L.n. 300/1970 – IMPIANTI AUDIOVISIVI

«1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per ***esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*** *e possono essere installati previo* ***accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali****. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa* ***autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro*** *o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali,* ***della sede centrale dell'Ispettorato nazionale del lavor****o. I provvedimenti di cui al terzo periodo sono definitivi.*

2. La disposizione di cui al comma 1 non si applica agli ***strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*** *e agli strumenti di registrazione degli accessi e delle presenze.*

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196».

DEFINIZIONE DI STRUMENTI DI LAVORO *EX* ART. 4, COMMA 2, STATUO DEI LAVORATORI: TRA PRASSI AMMINISTRATIVA E INTERPRETAZIONE GIURISPRUDENZIALE

Circolare Ispettorato del Lavoro n. 2/2016: «*Apparecchi, dispositivi, apparati e congegni che costituiscono il* ***mezzo indispensabile al lavoratore*** *per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano stati posti in uso e messi a sua disposizione*».

Provvedimento GPDP del 13 luglio 2016 n. 303: «*servizi, software o applicativi* ***strettamente funzionali alla prestazione lavorativa****, anche sotto il profilo della sicurezza*».

Cass. civ., Sez. lavoro, Ord., del 03 giugno 2024, n. 15391: «*Il telepass, se installato su auto aziendali destinate allo svolgimento di specifici servizi,* ***si deve considerare uno strumento direttamente funzionale all'efficienza della singola prestazione****, oltre che ormai fortemente compenetrato con essa nell'odierna pratica lavorativa, sicché il telepass così contestualizzato rientra nell'ambito applicativo del comma 2 dell'art. 4 L. n. 300/1970*».

Tribunale di Milano 24 ottobre 2017: «*Ove vengano in rilievo apparati per l'informatica e le telecomunicazioni, occorre allora distinguere tra componenti hardware e componenti software e verificare in relazione a ciascuna di esse (da considerarsi quale distinto «strumento» ai sensi della norma in esame [n.d.r. art. 4 L.n. 300/1970]), se sia ravvisabile il nesso di funzionalizzazione allo svolgimento della prestazione lavorativa. […] Lo smartphone, infatti, non può essere considerato ai fini che qui interessano, come strumento unitario e inscindibile;* ***esso è formato da una pluralità di componenti hardware (apparato telefonico, GPS, CPU etc.) e software (sistema operativo, programmi e applicazioni, tra cui WhatsApp). Ognuna di tali componenti va considerata come autonomo strumento di lavoro e di potenziale controllo***».

3. E-MAIL AZIENDALE E TRATTAMENTO DEI METADATI

INDIRIZZI DEL GARANTE SUI METADATI DELLE E-MAIL TRATTATI DAL SERVER

Il GPDP si è espresso sul trattamento dei metadati relativi alla *e-mail* aziendale e registrati nei *server* aziendali con due recenti documenti:

- **Documento di indirizzo del 21 dicembre 2023** «*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*»;

- **Documento di indirizzo del 6 giugno 2024** «*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*» che ha aggiornato e sostituito il documento del precedente 21 dicembre.

***RATIO* DEI DOCUMENTI:**

Nell'ambito di accertamenti condotti dal Garante con riguardo ai trattamenti di dati personali effettuati nel contesto lavorativo è emerso **il rischio che programmi e servizi informatici per la gestione della posta elettronica, anche qualora commercializzati da fornitori in modalità cloud, possano raccogliere per impostazione predefinita, in modo preventivo e generalizzato, I METADATI RELATIVI ALL'UTILIZZO DEGLI ACCOUNT DI POSTA ELETTRONICA in uso ai dipendenti, conservando gli stessi per un esteso arco temporale**.

DEFINIZIONE DI METADATO

I METADATI secondo il Documento di Indirizzo del 6 giugno 2024: «*informazioni registrate nei log generati dai sistemi di server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client (le postazioni terminali che effettuano l'invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali MUA – Mail User Agent)*».

I **METADATI** cui fa riferimento il **Documento di Indirizzo del 6 giugno 2024** possono:

- avere **origine prettamente tecnica**;
- oppure, **essere determinati dagli utenti** (es. il campo "Oggetto")

Esempi METADATI: gli indirizzi e-mail del mittente e del destinatario, gli indirizzi IP dei server o dei *client* coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, in relazione al sistema di gestione del servizio di posta elettronica utilizzato, **anche l'oggetto del messaggio spedito o ricevuto**.

DIFFERENZA TRA METADATI, CORPO DEL TESTO DELLA E-MAIL ED ENVELOPE

Il GPDP, nel Documento di Indirizzo del 6 giugno 2024 specifica che i **METADATI,** così come ivi definiti, non vanno confusi con le informazioni contenute nel **CORPO DEL MESSAGGIO** e nell'**ENVELOPE**.

ENVELOPE: «*l'insieme delle intestazioni tecniche strutturate che documentano l'instradamento del messaggio, la sua provenienza e altri parametri tecnici*. ***Le informazioni contenute nell'envelope, ancorché corrispondenti a metadati registrati automaticamente nei log dei servizi di posta, sono inscindibili dal messaggio di cui fanno parte integrante e che rimane sotto l'esclusivo controllo dell'utente (sia esso il mittente o il destinatario dei messaggi***».

LA CONSERVAZIONE DEI METADATI SECONDO IL GARANTE PRIVACY

DOCUMENTO DI INDIRIZZO DEL 21 DICEMBRE 2023

Discrimine per ricondurre il metadato al comma 1 o al comma 2 dell'art. 4 Stat. Lav.

=

TERMINE DI CONSERVAZIONE DEL METADATO

< 7 giorni – RICONDUCIBILITÀ AL COMMA 2

↓

affinché sia ritenuto applicabile il comma 2 dell'art. 4 della L. n. 300/1970, l'attività di raccolta e conservazione dei metadati «**non può essere superiore di norma a poche ore o ad alcuni giorni, in ogni caso non oltre sette giorni, estensibili, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento, di ulteriori 48 ore».**

> 7 giorni – RICONDUCIBILITÀ AL COMMA 1

«la generalizzata raccolta e la conservazione di tali metadati, per un lasso di tempo più esteso [...]*, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori,* ***richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta L. n. 300/1970****».*

↓

«Resta fermo che anche tale conservazione dovrà avvenire nel rispetto del principio di limitazione della conservazione» (art. 5, par. 1, lett. e), del Regolamento)

LA CONSERVAZIONE DEI METADATI SECONDO IL GARANTE PRIVACY: AGGIORNAMENTO

DOCUMENTO DI INDIRIZZO DEL 6 GIUGNO 2024

Discrimine per ricondurre il metadato al comma 1 o al comma 2 dell'art. 4 Stat. Lav.

=

TERMINE DI CONSERVAZIONE DEL METADATO

< 21 giorni – RICONDUCIBILITÀ AL COMMA 2

«**affinché sia ritenuto applicabile il comma 2 dell'art. 4 della L. n. 300/1970, l'attività di raccolta e conservazione** dei soli metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione, **si ritiene che possa essere effettuata, di norma, per un periodo limitato a pochi giorni; a titolo orientativo, tale conservazione non dovrebbe comunque superare i 21 giorni**».

> 21 giorni – RICONDUCIBILITÀ AL COMMA 1

«*la generalizzata raccolta e la conservazione dei log di posta elettronica, per un lasso di tempo più esteso, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori,* ***richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta L. n. 300/1970***».

↓

«*Resta fermo che anche tale conservazione dovrà avvenire nel rispetto del principio di limitazione della conservazione*» (art. 5, par. 1, lett. e), del Regolamento).

ECCEZIONE

ECCEZIONE AL TERMINE DEI 21 GIORNI PER L'APPLICAZIONE DELL'ART. 4 COMMA 2

DOCUMENTO DI INDIRIZZO DEL 6 GIUGNO 2024

ECCEZIONE:

Sempre nell'ambito della predetta finalità (assicurare il funzionamento delle infrastrutture del sistema della posta elettronica), il comma 2 dell'art. 4 della L. n. 300/1970 è applicabile anche nell'ipotesi di **conservazione per un termine più ampio rispetto a 21 giorni:**

↓

«***IN PRESENZA DI PARTICOLARI CONDIZIONI CHE NE RENDANO NECESSARIA L'ESTENSIONE, COMPROVANDO ADEGUATAMENTE, IN APPLICAZIONE DEL PRINCIPIO DI ACCOUNTABILITY PREVISTO DALL'ART. 5, PAR. 2, DEL REGOLAMENTO, LE SPECIFICITÀ DELLA REALTÀ TECNICA E ORGANIZZATIVA DEL TITOLARE***».

Art. 5 – PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. **Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).**

...SEGUE...

Nell'ambito della **GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA**, di seguiti alcuni **esempi di circostanze** che potrebbero giustificare l'applicazione del comma 2 dell'art. 4 L. n. 300/1970 anche nell'ipotesi di **conservazione dei metadati per un termine più ampio rispetto a 21 giorni:**

- **INVESTIGAZIONE INCIDENTI**: alcune minacce/attacchi possono svilupparsi nel corso di diversi mesi, di talché una cronologia più ampia consente di identificare con precisione gli impatti di possibili compromissioni in termini CIA (Confidentiality, Integrity e Availability), permettendo di stabilire in dettaglio le comunicazioni effettuate e quindi la dinamica e la causa e di un incidente di sicurezza. In assenza dei metadati, eventuali verifiche possono essere svolte soltanto direttamente sulla casella di posta dell'utente, che potrebbe subire modifiche nel tempo (cancellazioni della posta, che tipicamente vengono svolte dai *threat actor* in fase di attacco) e non fornire evidenze attendibili o probatorie.

- **ANALISI DEI TREND**: Un periodo più lungo di 21 giorni potrebbe essere necessario per analizzare i *trend* degli attacchi informatici e rivelare possibili cambiamenti nei modelli di attacco, aiutando a implementare misure preventive più efficaci.

- **AUDIT**: Per scopi di *audit* interni o esterni, spesso viene richiesto accesso ad cronologia degli eventi alquanto ampia, al fine di garantire la disponibilità di dati storici per scopi di verifica e *audit*, anche su casi di eventuali attività illecite effettuate attraverso l'utilizzo della posta elettronica o richieste da parte delle autorità.

- **TENANT MULTI-COUNTRY**: potrebbe non essere possibile discriminare la *retention* per casella/paese nel caso di tenant di posta di organizzazioni internazionali.

- **CONFORMITÀ NORMATIVA**: alcune regolamentazioni e normative che richiedono un periodo specifico di *retention* dei log. Ad esempio lo *standard* PCI-DSS (Payment Card Industry Data Security Standard: standard di sicurezza che stabilisce un insieme di regole che garantiscono che tutte le aziende che si occupano dell'accettazione, dell'elaborazione, dell'archiviazione o del trasferimento dei dati delle carte di credito mantengano un ambiente sicuro) richiede almeno 12 mesi.

...SEGUE...

Anche il **FORNITORE DEL SERVIZIO** può avere necessità di un **periodo di conservazione dei dati dei *log* della *e-mail* aziendale superiore a 21 giorni**, ad esempio al fine di:

a) **mantenere un sistema di servizio di posta ben funzionante** (ad esempio, nel caso in cui le e-mail non vengano recapitate o siano in ritardo per qualsiasi motivo, i registri di tracciamento dei messaggi vengono utilizzati per identificare le cause principali che potrebbero aver causato un errore e/o configurazioni errate);

b) **garantire un adeguato livello di cyber sicurezza essenziale** (ad esempio, per rilevare gli eventi di sicurezza, tenuto conto che un incidente di sicurezza non è immediatamente rilevabile; identificazione, blocco e messa in quarantena di e-mail sospette; verifica dell'autenticità delle email; indagine sugli incidenti, in quanto i metadati aiutano a tracciare l'origine e il percorso delle e-mail dannose);

a) **fornire indicazioni per verificare l'invio di e-mail** (ad esempio, per verificare quando e dove è stata inviata un'e-mail).

UTILIZZABILITÀ DELLE E-MAIL AZIENDALI E DEI METADATI RACCOLTI

Art. 4, comma 3, L. n. 300/1970: «*Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196*».

L'art. 4, comma 1, l. n. 300/1970 individua tassativamente le **finalità** (vale a dire quelle organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale) per le quali gli strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati nel contesto lavorativo, stabilendo precise **garanzie procedurali** (accordo sindacale o autorizzazione pubblica).

Ai sensi **dell'art. 4, comma 2, L.n. 300/1970**, le predette garanzie non trovano invece applicazione «agli strumenti di registrazione degli accessi e delle presenze» e «**agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa**».

I METADATI secondo il Documento di Indirizzo del 6 giugno 2024: «*informazioni registrate nei log generati dai sistemi di server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client (le postazioni terminali che effettuano l'invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali MUA – Mail User Agent)*».

LA RILEVANZA PENALE DELLA VIOLAZIONE DELLE NORME SUI CONTROLLI A DISTANZA

Art. 38 L.n. 300/1970 – DISPOSIZIONI PENALI

*«Le violazioni degli articoli 2, 5,6, e 15, primo comma, lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con **l'ammenda** da euro 154 (lire 300.000) 93 a euro 1.549 (lire 3.000.000) o con **l'arresto** da 15 giorni ad un anno. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente.*

Quando, per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.

Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del Codice penale».

Art. 171 D.Lgs. 196/2003 – VIOLAZIONI DELLE DISPOSIZIONI IN MATERIA DI CONTROLLO A DISTANZA E INDAGINI SULLE OPINIONI DEI LAVORATORI

«1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.».

L'INTERPRETAZIONE DEL GARANTE PRIVACY

Interpretazione del Garante dell'art. 4, comma 2, L.n. 300/1970:
«*Tale disposizione introduce un'eccezione, rispetto al più restrittivo regime previsto dal comma 1, e deve, pertanto, essere oggetto di stretta interpretazione, considerate le responsabilità anche sul piano penale che possono derivare dalla violazione del predetto quadro normativo* (**Documento di indirizzo GPDP 21 dicembre 2023 e Documento di indirizzo GPDP 6 giugno 2024**)

↓

Secondo il Garante «*solo gli strumenti **preordinati**, anche in ragione delle caratteristiche tecniche di configurazione* [...] *allo "svolgimento della prestazione" non soggiacciono quindi ai limiti e alle garanzie di cui al primo comma* (n.d.r. dell'art. 4 L.n. 300/1970), *in quanto **funzionali** a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro*» (Documento di indirizzo GPDP 21 dicembre 2023 e Documento di indirizzo GPDP 6 giugno 2024)

↓

INCOMPATIBILITA' CON IL PRINCIPIO DI STRETTA LEGALITÀ DEL DIRITTO PENALE

PRINCIPIO DI STRETTA LEGALITÀ DEL DIRITTO PENALE

INCOMPATIBILITA' CON IL PRINCIPIO DI STRETTA LEGALITÀ DEL DIRITTO PENALE

Art. 14 Preleggi – APPLICAZIONE DELLE LEGGI PENALI ED ECCEZIONALI
«*Le leggi penali e quelle che fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati*».

Art. 1 Codice Penale – REATI E PENE: DISPOSIZIONE ESPRESSA DI LEGGE
«Nessuno può essere punito per un fatto che non sia espressamente preveduto come reato dalla legge, né con pene che non siano da essa stabilite»

**Cass. pen., Sent. 03.03.2023, n. 9187: «*Il divieto di analogia non consente di riferire la norma incriminatrice a situazioni non ascrivibili ad alcuno dei suoi possibili significati letterali, e costituisce così un limite insuperabile rispetto alle opzioni interpretative a disposizione del giudice di fronte al testo legislativo*....*sicchè non è tollerabile che la sanzione possa colpirlo (il consociato) per fatti che il linguaggio comune non consente di ricondurre al significato letterale delle espressioni utilizzate dal legislatore*»

LA COMPETENZA DELL'INL SULL'INTERPRETAZIONE DELL'ART. 4

Art. 4 L.n. 628/1961 – MODIFICHE ALL'ORDINAMENTO DEL MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE:
«L'Ispettorato del lavoro ha il compito:
a) di vigilare sull'esecuzione di tutte le leggi in materia di lavoro e di previdenza sociale nelle aziende industriali, commerciali, negli uffici, nell'agricoltura, ed in genere ovunque è prestato un lavoro salariato o stipendiato, con le eccezioni stabilite dalle leggi;
b) di vigilare sull'esecuzione dei contratti collettivi di lavoro;
*c) **di fornire tutti i chiarimenti che vengano richiesti intorno alle leggi sulla cui applicazione esso deve vigilare**;*
[...]»

Interpretazione art. 4 Statuto dei Lavoratori

=

prerogativa dell'Ispettorato Nazionale del Lavoro

↓

Non sentito per la redazione dei Documenti di indirizzo sui metadati

4. GLI OBBLIGHI INFORMATIVI DEL DATORE DI LAVORO

OBBLIGHI INFORMATIVI DEL DATORE DI LAVORO

ART. 13 GDPR: «*in caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:* [...] *c)* ***le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento***».

ART. 4, COMMA 3, L. N. 300/1970: «*Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che* ***sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*** *e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196*».

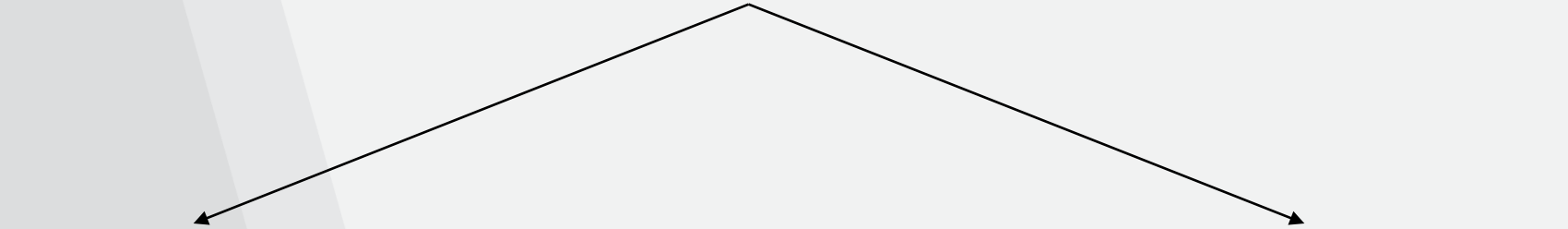
LINEE GUIDA GPDP N. 13 DEL 1° MARZO 2007: «*Grava sul datore di lavoro* ***l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli***».

Ordinanza ingiunzione GPDP 1 dicembre 2022 – REGIONE LAZIO: «*Nel rispetto del principio di "liceità, correttezza e trasparenza",* ***il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro*** *(art. 12 del Regolamento)* [...] ***l'adempimento degli obblighi informativi*** *nei confronti dei dipendenti (****consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli"****) costituisce una* ***specifica precondizione per il lecito utilizzo dei raccolti attraverso strumenti tecnologici, da parte del datore di lavoro, anche a tutti i fini connessi al rapporto di lavoro*** *(art. 4, co. 3, della l. n. 300/1970)*».

L'INFORMATIVA PRIVACY E LE POLICY AZIENDALI

DOVE FORNIRE QUESTE INFORMAZIONI?

LINEE GUIDA GPDP N. 13 DEL 1° MARZO 2007:



***POLICY* AZIENDALI**
(Es. *Policy* ICT)

INFORMATIVA PRIVACY *ex*
art. 13 GDPR

LE INFORMAZIONI OGGETTO DI COMUNICAZIONE

QUALI INFORMAZIONI COMUNICARE?

LINEE GUIDA GPDP N. 13 DEL 1° MARZO 2007:

MODALITÀ DI UTILIZZO DELLO STRUMENTO

a) **Se ed in quale misura è consentito utilizzare anche per ragioni personali i servizi di posta elettronica aziendale**

MODALITÀ DI EFFETTUAZIONE DEI CONTROLLI DA PARTE DEL DATORE DI LAVORO

a) **Base giuridica del trattamento;**

b) **Tempi di conservazione dei dati;**

c) **Modalità di conservazione delle e-mail;**

d) **Procedura del controllo**;

e) **Quali conseguenze, anche di tipo disciplinare**, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica sia utilizzata indebitamente.

5. L'OBBLIGO DI SPECIFICARE LE MODALITÀ DI UTILIZZO DELLO STRUMENTO E-MAIL

E-MAIL AZIENDALE E LIMITI AL DIVIETO DI COMUNICAZIONI PRIVATE

Nonostante il datore possa limitare, nella propria *policy aziendale*, l'utilizzo dell'account di posta elettronica aziendale ai soli fini lavorativi, **secondo il Garante Privacy NON PUÒ ESSERE PRECLUSA LA POSSIBILITÀ DI COMUNICAZIONI ANCHE STRETTAMENTE PRIVATE**.

⬇

LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET DEL 1 MARZO 2007: «*il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui* ratio *risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali*».

…SEGUE…

<u>Ordinanza ingiunzione GPDP 1 dicembre 2022 – REGIONE LAZIO</u>: La Regione, in presenza del sospetto in merito a possibili rivelazione a terzi di notizie d'ufficio, effettuava un controllo sui metadati relativi all'utilizzo degli *account* di posta elettronica istituzionale da parte dei lavoratori. In particolare, nell'ambito del procedimento svolto innanzi al Garante la Società ha specificato di aver richiesto ai propri dipendenti di limitare l'utilizzo della posta elettronica ai soli fini istituzionali o connessi al rapporto di lavoro. Tuttavia, il Garante rilevava che ciò non fosse sufficiente in quanto «***anche nel contesto lavorativo, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza*** *[…] Ciò in quanto, considerato che la linea di confine tra ambito lavorativo e professionale e quello strettamente privato non può sempre essere tracciata in modo netto,* ***non può essere prefigurato il completo annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, anche nei casi in cui il dipendente sia connesso ai servizi di rete messi a disposizione del datore di lavoro o utilizzi una risorsa aziendale****, ragione per la quale la Corte europea dei diritti dell'uomo ha nel tempo confermato che la protezione della vita privata si estende anche all'ambito lavorativo, ove si svolgono le relazioni della persona che lavora».*

...SEGUE...

Corte EDU, Copland v. UK, 03.04.2007: la Corte si è pronunciata circa la legittimità del controllo effettuato dal datore di lavoro sulla e-mail aziendale della dipendente, sul telefono e sul traffico internet e **finalizzato a determinare se la lavoratrice facesse un utilizzo eccessivo e personale di dette risorse**. Nell'esaminare la vicenda la Corte ha sancito l'applicabilità dell'art. 8 CEDU anche alle e-mail aziendali, statuendo che: «*la protezione della vita privata si estende anche all'ambito lavorativo, considerato che proprio in occasione dello svolgimento di attività lavorative e/o professionali si sviluppano relazioni dove si esplica la personalità del lavoratore. Tenuto anche conto che la linea di confine tra ambito lavorativo/professionale e ambito strettamente privato non sempre può essere tracciata con chiarezza, la Corte ha ritenuto applicabile l'art. 8 della Convenzione europea dei diritti dell'uomo, posto a tutela della vita privata, senza distinguere tra sfera privata e sfera professionale*» (nello stesso senso **Corte EDU, Barbulescu c. Romania, 05.09.20217**).

6. L'OBBLIGO DI SPECIFICARE LE MODALITÀ DI EFFETTUAZIONE DEI CONTROLLI

L'INFORMAZIONE SUL MONITORAGGIO

Corte EDU, Barbulescu c. Romania, sentenza della Grande Camera del 5 settembre 2017, richiamata anche da Cass. civ., Sez. Lav., n. 25732/2021: Nel caso **Barbulescu c. Romania**, la Corte Europea dei diritti dell'uomo, chiamata a pronunciarsi - in relazione all'art. 8 CEDU - con riguardo ad una vicenda in cui un datore di lavoro aveva sottoposto a controllo il *software* aziendale *Yahoo Messenger* in uso al lavoratore, al fine di verificarne un indebito utilizzo, ha fornito una **interpretazione estensiva del concetto di «*vita privata*», tanto da includervi la «*vita professionale*»**.

In particolare, la Corte ha ritenuto che la Romania avesse tenuto un comportamento non conforme alle garanzie accordate dalla norma della Convenzione, per avere le Corti nazionali omesso di accertare se il ricorrente fosse stato preliminarmente informato dal datore di lavoro:

- «*della possibilità che le comunicazioni che effettuava mediante Yahoo Messenger avrebbero potuto essere **monitorate***»;
- «*del **carattere** o della **portata del monitoraggio** o del **livello di invasività** nella sua vita privata e nella sua corrispondenza*»;

A ciò si aggiunga che le Corti nazionali non avevano indagato:

- «*i **motivi specifici che giustificavano l'introduzione delle misure di monitoraggio***»;
- «*se il datore di lavoro avrebbe potuto utilizzare **misure che comportavano una minore invasione** nella vita e nella corrispondenza del ricorrente»;*
- «*se sarebbe stato possibile **accedere alle comunicazioni a sua insaputa***» (n.d.r. del dipendente/ ricorrente).

LA BASE GIURIDICA DEL TRATTAMENTO

Art. 6 GDPR – LICEITÀ DEL TRATTAMENTO

«1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) ***il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;***

c) ***il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;***

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) ***il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento****;*

f) ***il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento*** *o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore* **[…].**

→Esempio lett. b): NECESSITÀ DEL DATORE DI LAVORO DI ACCERTARE UN ILLECITO.

→Esempio lett. c): ADEMPIMENTO AD UNA RICHIESTA DELL'AUTORITÀ GIUDIZIARIA.

→Esempio lett. f): NECESSITÀ DI UN ACCESSO FUNZIONALE AD ACCERTARE ELEMENTI DI TUTELA DELLA SICUREZZA AZIENDALE E DEL PATRIMONIO AVIENDALE O ESERCIZIO DEL DIRITTO DI DIFESA.

Sul diritto di difesa:

Ordinanza ingiunzione GPDP 21 luglio 2022 – STAY OVER S.R.L.: La società dichiarava di **conservare le e-mail aziendali per 10 anni, soprattutto per fini probatori**. In proposito il Garante specificava che**:** «*Il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a* ***contenziosi in atto o a situazioni precontenziose****, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti*».

Ordinanza ingiunzione GPDP 7 aprile 2022 – PALUMBO SUPERYACHT S.R.L.: La società provvedeva ad impedire l'accesso alla casella di posta elettronica della collaboratrice in ragione di un'indebita rivelazione di informazioni aziendali riservate, imputata alla medesima. Tale condotta era stata oggetto di due contestazioni formali rivolte alla collaboratrice propedeutiche alla risoluzione del contratto per giusta causa, poi formalizzata dalla Società che, tuttavia, manteneva attiva la casella di posta in ragione del contenzioso in essere con la lavoratrice e per eventuali "indagini difensive". In proposito il Garante specificava che: «*Il trattamento di dati personali effettuato per la finalità di tutela dei propri diritti - come invocata dalla Società - è riferito a un* ***contenzioso (pur ancora stragiudiziale, per quanto emergente dall'istruttoria condotta) in atto*** *e non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione […] risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (v. artt. 6, par. 1, lett. b), c) e f) e 9, par. 2, lett. b) del Regolamento*».

…SEGUE…

IMPORTANZA DI ESPLICITARE LA BASE GIURIDICA

Ordinanza ingiunzione GPDP 1 dicembre 2022 – REGIONE LAZIO:

La Regione, in presenza del sospetto in merito a possibili rivelazione a terzi di notizie d'ufficio, effettuava un controllo sui metadati relativi all'utilizzo degli *account* di posta elettronica istituzionale da parte dei lavoratori.

- La Regione, nel fornire ai propri dipendenti **l'informativa sul trattamento** dei dati personali comunicava «*esclusivamente la circostanza che* ***essa "si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia)"***»**;**

- Nel corso del procedimento è poi emerso che la Regione aveva adottato anche un **disciplinare per l'utilizzo delle dotazioni ICT** «***riservandosi "per motivi organizzativi o di sicurezza […] la facoltà di effettuare, attraverso LAZIOcrea, controlli saltuari e occasionali", e in particolare di "monitorare le reti e le Dotazioni [in caso di] […] constatazione di utilizzo indebito della posta elettronica", anche in merito al "volume dei messaggi scambiati, formato e dimensione dei file allegati***».

↓

Ciò posto, secondo il Garante: «***né l'originaria informativa resa ai dipendenti né tale documento*** [n.d.r. il disciplinare di utilizzo delle dotazioni ICT] ***contengono tutti gli elementi espressamente richiesti dalla normativa in materia di protezione dei dati – segnatamente la "base giuridica del trattamento" e il "periodo di conservazione dei dati personali"*** *(art. 13, par. 1, lett. c) e par. 2, lett. a), del Regolamento) - e forniscono agli stessi una chiara e trasparente rappresentazione del complessivo trattamento effettuato*»

IMPOSTAZIONE MOLTO FORMALISTICA:

per il Garante dire genericamente che il datore di lavoro si riserva il controllo in caso di illeciti non necessariamente equivale a indicare la base giuridica del controllo.

TEMPI DI CONSERVAZIONE DELLE E-MAIL

Art. 5 GDPR – PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) **conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati**; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

ART. 13 GDPR – INFORMATIVA PRIVACY: «[...] *2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:* ***a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo***».

Provvedimento GPDP 1° febbraio 2018 – SICILY BY CAR: La Società provvedeva al licenziamento del lavoratore sulla base di alcune *e-mail* inviate da quest'ultimo ad un altro collega e rinvenuta in forza un controllo sul server aziendale esteso fino al gennaio 2016. Emergeva che la conservazione della e-mail riguardava tutte le e-mail dei dipendenti ed era effettuata per tutta la durata del rapporto di lavoro e sino a un mese dopo la cessazione per gli impiegati e sino a dodici mesi dopo per i dirigenti e gli apicali. Su siffatta tempistica di conservazione il Garante evidenziava che: «***La conservazione sistematica dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli account aziendali****, allo scopo di poter ricostruire gli scambi di comunicazioni tra gli uffici interni nonché tutti i rapporti intrattenuti con gli interlocutori esterni (clienti, fornitori, enti assicurativi, tour operator), anche in vista di possibili contenziosi, effettuata da soggetti diversi dal titolare della specifica casella di posta elettronica per l'intera durata del rapporto di lavoro e successivamente all'interruzione dello stesso,* ***non risulta altresì conforme ai principi di liceità, necessità e proporzionalità del trattamento***».

MODALITÀ DI CONSERVAZIONE DELLE E-MAIL

Provvedimento GPDP 22 giugno 2023 – MAVIGLIA ASSICURAZIONI; Ordinanza ingiunzione GPDP 7 aprile 2022 – PALUMBO SUPERYACHT ANCONA S.R.L. e Provvedimento GPDP 1° febbraio 2018 – SICILY BY CAR:
In tutti e tre i provvedimenti, i datori di lavoro, a seguito della cessazione del rapporto del lavoratore, al fine di provvedere alla gestione dei flussi documentali aziendali in transito sulle caselle del lavoratore cessato, provvedevano ad accedere direttamente al contenuto delle comunicazioni pervenute sugli *account* dell'ex dipendente/collaboratore. Il Garante ha giudicato tale attività di accesso come **non necessaria e proporzionata allo scopo**, posto che: «*la legittima necessità di assicurare la conservazione di documentazione necessaria per l´ordinario svolgimento e la continuità dell'attività aziendale, anche in relazione ai rapporti intrattenuti con soggetti privati e pubblici, nonché in base a specifiche disposizioni dell'ordinamento, è assicurata, in primo luogo, dalla* ***predisposizione di sistemi di gestione documentale con i quali – attraverso l'adozione di appropriate misure organizzative e tecnologiche – individuare i documenti che nel corso dello svolgimento dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche***».

DIFFERENZA CON I «CONTROLLI DIFENSIVI»

IL PRESUPPOSTO DEL CONTROLLO

Tribunale di Genova n. 239/2021 del 14.12.2021, avente ad oggetto la legittimità del licenziamento irrogato alla dipendente in ragione dell'inoltro a terzi - e alla ricezione da questi ultimi - di alcune *e-mail* contenenti notizie riservate della società. In particolare, il Tribunale, nel dichiarare l'illegittimità del licenziamento, ricordava la distinzione tra:

- **Controllo *ex* art. 4 Statuto dei Lavoratori: *fumus* che realizza uno dei presupposti di controllo indicati e tipizzati nell'informativa + controllo sul passato rispetto all'insorgenza del sospetto.**

- **Controllo «difensivo»: *fumus* di un illecito + controllo sul futuro rispetto all'insorgenza del sospetto.**

L'informativa resa al lavoratore deve comprendere entrambe le tipologie di controllo

DAI DATI AGGREGATI AL DETTAGLIO

LINEE GUIDA GPDP N. 13 DEL 1° MARZO 2007:

- Deve essere per quanto possibile preferito un **controllo preliminare su dati aggregati**, riferiti all'intera struttura lavorativa o a sue aree;
- In assenza di successive anomalie non è di regola giustificato effettuare **controlli su base individuale;**
- Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

LE PROCEDURE DI *DIGITAL FORENSICS*

ATTIVITÀ DI INVESTIGAZIONE DIGITALE

↓

Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 – Provvedimento GPDP del 19 dicembre 2018.

Nella lettera di incarico per chi svolge le indagini è necessario:

- menzionare il diritto che si intende esercitare in sede giudiziaria ovvero il procedimento penale al quale l'investigazione è collegata;
- esplicitare l'elemento di fatto che giustifica l'investigazione;
- indicare il termine ragionevole entro cui questa deve essere conclusa.

IL CODICE DELLA PROPRIETÀ INDUSTRIALE (D.LGS. 30/2005)

Art. 1. – DIRITTI DI PROPRIETÀ INDUSTRIALE: «*1. Ai fini del presente codice, l'espressione proprietà industriale comprende marchi ed altri segni distintivi, indicazioni geografiche, denominazioni di origine, disegni e modelli, invenzioni, modelli di utilità, topografie dei prodotti a semiconduttori,* ***segreti commerciali*** *e nuove varietà vegetali*».

Art. 2. – COSTITUZIONE ED ACQUISTO DEI DIRITTI: «*1. I diritti di proprietà industriale si acquistano mediante brevettazione, mediante registrazione o negli altri modi previsti dal presente codice. La brevettazione e la registrazione danno luogo ai titoli di proprietà industriale.*
2. Sono oggetto di brevettazione le invenzioni, i modelli di utilità, le nuove varietà vegetali.
3. Sono oggetto di registrazione i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori.
4. Sono protetti, ricorrendone i presupposti di legge, i segni distintivi diversi dal marchio registrato, i segreti commerciali, le indicazioni geografiche e le denominazioni di origine.
5. L'attività amministrativa di brevettazione e di registrazione ha natura di accertamento costitutivo e dà luogo a titoli soggetti ad un regime speciale di nullità e decadenza sulla base delle norme contenute nel presente codice».

Art. 98 – SEGRETI COMMERCIALI: «*1. Costituiscono oggetto di tutela i segreti commerciali. Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*
a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;
b) abbiano valore economico in quanto segrete;
c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete*.*
2. Costituiscono altresì oggetto di protezione i dati relativi a prove o altri dati segreti, la cui elaborazione comporti un considerevole impegno ed alla cui presentazione sia subordinata l'autorizzazione dell'immissione in commercio di prodotti chimici, farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche»

...SEGUE...

Art. 129. Descrizione e sequestro: «*1. **Il titolare di un diritto di proprietà industriale può chiedere la descrizione o il sequestro, ed anche il sequestro subordinatamente alla descrizione, di alcuni o di tutti gli oggetti costituenti violazione di tale diritto, nonché dei mezzi adibiti alla produzione dei medesimi e degli elementi di prova concernenti la denunciata violazione e la sua entità**. Sono adottate le misure idonee a garantire la tutela delle informazioni riservate.*
2 . Il giudice, sentite le parti e assunte, quando occorre, sommarie informazioni, provvede con ordinanza e, se dispone la descrizione, autorizza l'eventuale prelevamento di campioni degli oggetti di cui al comma 1. In casi di speciale urgenza, e in particolare quando eventuali ritardi potrebbero causare un danno irreparabile al titolare dei diritti o quando la convocazione della controparte potrebbe pregiudicare l'attuazione del provvedimento di descrizione o di sequestro, provvede sull'istanza con decreto motivato.
[3. Salve le esigenze della giustizia penale non possono essere sequestrati, ma soltanto descritti, gli oggetti nei quali si ravvisi la violazione di un diritto di proprietà industriale, finché figurino nel recinto di un'esposizione, ufficiale o ufficialmente riconosciuta, tenuta nel territorio dello Stato, o siano in transito da o per la medesima]
4. I procedimenti di descrizione e di sequestro sono disciplinati dalle norme del codice di procedura civile concernenti i procedimenti cautelari, in quanto compatibili e non derogate dal presente codice. Ai fini della conferma, modifica o revoca della descrizione e dell'eventuale concessione delle misure cautelari chieste unitamente o subordinatamente alla descrizione, il giudice fissa l'udienza di discussione tenendo conto della descrizione allo scopo di valutarne il risultato».

Art. 130. Esecuzione di descrizione e sequestro: «*1. **La descrizione e il sequestro vengono eseguiti a mezzo di ufficiale giudiziario, con l'assistenza, ove occorra, di uno o più periti ed anche con l'impiego di mezzi tecnici di accertamento, fotografici o di altra natura**.*
2 . Gli interessati possono essere autorizzati ad assistere alle operazioni anche a mezzo di loro rappresentanti e ad essere assistiti da tecnici di loro fiducia.
3 . Decorso il termine dell'articolo 675 del codice di procedura civile, possono essere completate le operazioni di descrizione e di sequestro già iniziate, ma non possono esserne iniziate altre fondate sullo stesso provvedimento. Resta salva la facoltà di chiedere al giudice di disporre ulteriori provvedimenti di descrizione o sequestro nel corso del procedimento di merito.
4 . La descrizione e il sequestro possono concernere oggetti appartenenti a soggetti anche non identificati nel ricorso, purché si tratti di oggetti prodotti, offerti, importati, esportati o messi in commercio dalla parte nei cui confronti siano stati emessi i suddetti provvedimenti e purché tali oggetti non siano adibiti ad uso personale.
5 . Il verbale delle operazioni di sequestro e di descrizione, con il ricorso ed il provvedimento, deve essere notificato al terzo cui appartengono gli oggetti sui quali descrizione o sequestro sono stati eseguiti, entro quindici giorni dalla data di conclusione delle operazioni stesse a pena di inefficacia».

7. E-MAIL E RAPPORTO DI LAVORO

E-MAIL E CESSAZIONE DEL RAPPORTO DI LAVORO

Provvedimento GPDP del 24 gennaio 2024 – MP1: Dopo la cessazione del rapporto di collaborazione la Società acconsentiva affinché l'ex collaboratore utilizzasse per 6 mesi l'account di posta elettronica assegnatogli. Successivamente la società reindirizzava il predetto account su un altro indirizzo e-mail aziendale, accessibile al rappresentante legale e al personale amministrativo per un periodo che non è stato possibile quantificare (certi almeno 6 mesi). Non venivano avvisati i terzi che scrivevano all'account del collaboratore della cessazione del suo rapporto con la società. Sul tema il Garante argomentava come segue: «*In termini generali, lo scambio di corrispondenza elettronica estranea o meno all'attività lavorativa su un account aziendale di tipo individualizzato configura un'operazione che consente di conoscere alcune informazioni personali relative all'interessato (v. "Linee guida del Garante per posta elettronica e Internet", 1.3.2007, in G. U. n. 58 del 10.3.2007, spec. punto 5.2, lett. b), il Garante ha già ritenuto conforme ai principi di necessità e minimizzazione che dopo la cessazione del rapporto di lavoro il titolare provveda alla rimozione dell'account previa disattivazione dello stesso e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti alla sua attività professionale* [...] **Ciò anche a tutela dei terzi mittenti delle comunicazioni**, la cui aspettativa di riservatezza non risulta essere stata tutelata nel caso concreto posto che gli stessi sono stati resi edotti della cessazione del rapporto professionale del reclamante con la Società dopo che il contenuto delle comunicazioni indirizzate all'account riferito a quest'ultimo era stata appresa dalla Società».

Provvedimento GPDP 1° febbraio 2018 – SICILY BY CAR: A seguito della cessazione del rapporto del lavoratore, al fine di provvedere alla gestione dei flussi documentali aziendali in transito sulle caselle del lavoratore cessato, il datore di lavoro provvedeva ad accedere direttamente al contenuto delle comunicazioni pervenute sull'account del collaboratore cessato. Sul tema, il garante ha rilevato che: «*Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, **gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all´attività professionale del titolare del trattamento**. L'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività, pertanto, deve essere contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi [...] Si rammenta infine che, come precisato dal Garante, la disattivazione deve essere realizzata "secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi su server aziendali"*».

APPLICABILITA' DEI PRINCIPI IN MATERIA DI PRIVACY ANCHE A FORME DI LAVORO PARASUBORDINATO

Provvedimento GPDP del 22 giugno 2023 – MAVIGLIA ASSICURAZIONI: «I principi e le disposizioni in materia di dati personali «*risultano pienamente applicabili* ***anche con riferimento a relazioni professionali e di collaborazione*** *che, pur non essendo caratterizzati da una relazione di dipendenza, attribuiscono comunque al titolare del trattamento un ampio potere organizzativo, sia interno che esterno*».

Ordinanza ingiunzione GPDP 7 aprile 2022 – PALUMBO SUPERYACHT ANCONA S.R.L.: «Pertanto – pur tenuto conto della strutturale diversità fra un rapporto di lavoro subordinato e un rapporto di agenzia - evidentemente incidente in particolare sulla richiamabilità delle disposizioni dello Statuto dei lavoratori (e quindi anche degli art. 113 e 114 del Codice), nonché del carattere decisivo del piano fattuale, **a dispetto del mero *nomen iuris*, ai fini della corretta qualificazione del rapporto in essere (v. Cass, sent. n. 4884 del 1.03.2018) - il trattamento dei dati effettuato mediante tecnologie informatiche nell'ambito di un qualsivoglia rapporto di lavoro deve conformarsi al rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, a tutela di lavoratori e di terzi**».