BonelliErede
with LOMBARDI

**Focus Team Corporate Compliance & Investigations**
3 ottobre 2022

# *Internal investigations* e normativa *privacy*: un equilibrio da presidiare


**Focus Team Corporate Compliance & Investigations**

***Focus Team Leader***
Alessandro Musella
alessandro.musella@belex.com
Tel. +39-02-771131

***Autori***

Alessandro Musella
alessandro.musella@belex.com
Tel. +39-02-771131

Vittorio Pomarici
vittorio.pomarici@belex.com
Tel. +39-02-771131

Valentina Frignati
valentina.frignati@belex.com
Tel. +39-02-771131


## 1. Introduzione

Quando gli organi di governo e di controllo di una società si trovano a dover avviare una *internal investigation*, le prime problematiche legali da affrontare riguardano sempre l'**acquisizione dei dati** e le correlate **implicazioni in tema di *data privacy* e *data protection***.

Le *internal investigations* comportano ormai sempre l'acquisizione della casella di posta elettronica dei soggetti interessati dall'indagine, di copia dei dati dei loro computer e, il più delle volte, anche di copia di *smartphone*, *tablet* e altri *device* aziendali da loro utilizzati, per l'esame ad esempio delle *chat* di *WhatsApp*, *Teams* e altri *provider* di messaggistica. Tutto ciò comporta inevitabilmente il trattamento di dati personali[1], i quali sono oggetto di tutela da parte del Regolamento UE 2016/679[2] (GDPR) e della normativa italiana di cui al Codice Privacy[3]. **Il rispetto di tali norme è senza dubbio un requisito legale di cui si deve tenere conto già nella fase di avvio e organizzazione delle investigazioni interne**.

In particolare, il GDPR sancisce una serie di principi fondamentali sulla base dei quali deve essere improntato il trattamento dei dati personali, quali il principio di **liceità** (avere una valida base giuridica per procedere con la raccolta e il trattamento), di **trasparenza** (informare il lavoratore fra l'altro delle ragioni per cui i suoi dati vengono trattati, da chi e dove), di **minimizzazione** (raccogliere solo i dati strettamente necessari all'oggetto dell'indagine), di **affidabilità/sicurezza** (garantire che il processa-

[1] Definiti dall'art. 4, n.1 GDPR come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*". Così, ad es., i dati anagrafici, le immagini del lavoratore, gli account aziendali di posta elettronica, i file di log, la cronologia di navigazione in internet, oltre chiaramente ai dati sensibili o ai dati relativi alle condanne penali.

[2] Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016 n. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati – c.d. "**GDPR**").

[3] D. lgs. 30 giugno 2003, n. 196 (c.d. "**Codice Privacy**"), così come modificato dal d. lgs. 10 agosto 2018, n. 101, recante le disposizioni di adeguamento della normativa nazionale alle disposizioni del GDPR, in vigore dal 19 settembre 2018.

mento e il trattamento dei dati nel contesto dell'indagine interna avvenga in modo corretto e nel rispetto della normativa privacy).

## 2. Le condizioni per poter procedere

Da questi principi deriva che una società potrà procedere legittimamente alla raccolta ed esame dei dati personali dei destinatari dell'indagine interna a condizione che:

a. esista una valida **base giuridica** per il trattamento dei dati;
b. i destinatari abbiano ricevuto un'**adeguata informativa**;
c. il trattamento avvenga nel **rispetto della normativa privacy**.

### *2.1. Base giuridica*

Quanto al primo requisito, nel caso di indagini interne svolte a seguito della notizia di possibili violazioni di legge o di policy aziendali non manifestamente infondate, l'**interesse legittimo** è dato dall'esigenza della società di accertare situazioni che la espongono a responsabilità legale e/o a un danno patrimoniale e reputazionale. Questo interesse legittimo costituisce la base giuridica del trattamento, alternativa al consenso degli interessati, e **rende non necessaria l'acquisizione del consenso degli interessati**. Anzi il consenso difficilmente potrà costituire una idonea base giuridica del trattamento, stante il probabile squilibrio dei rapporti che si verifica soprattutto nel caso di indagini interne che riguardano lavoratori dipendenti.

### *2.2. Adeguata informativa*

Il secondo requisito (l'informativa agli interessati) deve essere assolto attraverso un'**informativa preventiva** sull'uso dell'*email* e dei dispositivi aziendali e sulla possibilità che essi siano soggetti ad attività di controllo e indagine da parte della società. Di regola questa informativa preventiva viene fornita mediante una **policy interna aziendale**, che deve essere stata adottata e adeguatamente diffusa prima dell'indagine interna. Questo aspetto è molto importante, e spesso trascurato in diverse realtà. È essenziale, per poter svolgere efficacemente una *internal investigation*, che le società adottino policy interne adeguate, con cui informino in modo chiaro e particolareggiato dipendenti, amministratori e altri collaboratori che la *email* aziendale e ogni altra comunicazione scambiata sui *device* e/o sistemi aziendali (*Teams chat*, SMS, W*hatsApp*) è di proprietà della società e che quest'ultima si riserva il diritto di effettuare controlli anche senza il consenso degli interessati, qualora via sia un suo legittimo interesse, costituito dall'esigenza di svolgere indagini interne per finalità di difesa e/o di protezione del patrimonio aziendale. Una policy incompleta o troppo generica rischia di non costituire una valida informativa preventiva e quindi di far mancare uno dei requisiti di legittimità dell'attività di indagine interna.

Oltre all'informativa preventiva, è poi necessaria una **informativa specifica** verso i soggetti direttamente interessati dall'indagine, circa le modalità

e le finalità del trattamento dei dati. Tale informativa va fornita al momento dell'accesso ai dati (quando questi sono raccolti presso l'interessato – si pensi all'accesso ai dispositivi aziendali del dipendente quali laptop e cellulari) o, in determinate condizioni, dopo l'avvenuto accesso ai dati (ciò solo nell'ipotesi in cui i dati non siano raccolti presso l'interessato – si pensi ad es. all'acquisizione delle caselle *email* e di altri dati direttamente tramite i *server* aziendali). L'informativa specifica **può essere rinviata** se vi è il pericolo che comunicare tale informazione al lavoratore possa "*rendere impossibile o … pregiudicare gravemente il conseguimento delle finalità di tale trattamento*", ovvero andare a pregiudicare/compromettere l'*investigation*[4].

### *2.3. Rispetto dei principi della normativa privacy*

Infine, quanto al terzo requisito (rispetto delle prescrizioni della normativa privacy), al fine di rispettare i principi di proporzionalità e minimizzazione nel trattamento dei dati personali previsti dal GDPR, l'analisi dei dati raccolti deve essere svolta mediante l'applicazione di **parole chiave** e con adeguata **limitazione del periodo rilevante** al fine di identificare solo i dati strettamente necessari all'*investigation* e pertinenti all'attività lavorativa, minimizzando la possibilità di rivedere documenti dell'interessato strettamente personali.

Per rispettare i medesimi principi, si ritiene che l'*internal investigation* debba svolgersi **per gradi**, partendo dalle *email* aziendali recuperabili sul *server* e spostandosi solo in via gradata al contenuto dei dispositivi aziendali (*laptop* e cellulari) – solo se necessario alla luce degli esiti dell'esame delle *email* o se la società ha una ragionevole aspettativa che le informazioni rilevanti non si trovino sulle *email* conservate nei *server* – e addirittura alle *chat* di messaggistica e/o alle caselle *email* personali scambiate su dispositivo aziendale se necessario alla luce degli esiti delle analisi precedenti (cioè se dalle analisi precedenti si scopre che certe conversazioni si svolgevano su *account* personali o su chat).

## 3. *Internal investigation* e Statuto dei Lavoratori

Come noto, la possibilità per il datore di lavoro di svolgere **controlli mirati** sui propri lavoratori in caso di fondato sospetto circa la commissione di un illecito o di una violazione (c.d. "**controlli difensivi**"[5]) è pacificamente ammessa dalla giurisprudenza, la quale colloca questo tipo di controlli al di fuori del perimetro applicativo dell'art. 4 dello Statuto dei Lavoratori, relativo invece ai **controlli generalizzati** sulla prestazione lavorativa.

---

[4] In proposito si veda l'art. 14, par. 5, lett. b) GDPR.

[5] Categoria di creazione giurisprudenziale, prospettata esplicitamente per la prima volta nella sentenza della Cass. civ., sez. lav., n. 4746 del 3 aprile 2002, nella quale rientravano i controlli aventi ad oggetto non l'esatto adempimento delle obbligazioni discendenti dal contratto, ma comportamenti illeciti dei lavoratori e lesivi del patrimonio e dell'immagine aziendale.

Secondo la giurisprudenza – sia nella vigenza della precedente versione dell'art. 4, sia a seguito delle modifiche introdotte con il c.d. "*Jobs Act*"[6] – i controlli difensivi non sono dunque soggetti al limite del previo accordo sindacale e/o autorizzazione amministrativa da parte dell'Ispettorato nazionale del lavoro, perché non hanno ad oggetto la normale attività del lavoratore, ma condotte specifiche ascrivibili – in base a concreti indizi – a singoli dipendenti.
Ciò nondimeno, la giurisprudenza ritiene che il controllo difensivo non sia esente da limitazioni, essendo consentito solo a condizione che lo stesso muova da un fondato sospetto e che sia rispettato il trattamento dei dati riservati[7].

Anche l'art. 4 dello Statuto dei Lavoratori come da ultimo novellato – applicabile ai controlli a distanza generalizzati sulla prestazione lavorativa per esigenze organizzative e produttive, per la sicurezza del lavoro e per la **tutela del patrimonio aziendale** – fa ora riferimento al rispetto della normativa privacy prevedendo espressamente che "*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***" (v. art. 4, c. 3).

In altri termini, è sicuramente consentito a un datore di lavoro svolgere controlli sui propri lavoratori finalizzati alla tutela del patrimonio aziendale, come quelli volti ad accertare la commissione di fatti illeciti, così come è consentito utilizzare le prove raccolte durante questi controlli anche a fini disciplinari, **a condizione** però che il trattamento dei dati si sia svolto **nel rispetto della normativa *privacy*** e giuslavoristica.

## 4. Conseguenze del trattamento illegittimo in base alla normativa privacy

Un trattamento illegittimo dei dati può esporre il datore di lavoro ad un procedimento davanti all'Autorità Garante della Privacy, con conseguente rischio di **sanzioni amministrative pecuniarie** fino a 20.000.000 EUR o

---

[6] D. Lgs n. 151/2015 emanato in attuazione della legge delega n. 183/2014, che all'art. 4, c. 1 ha inserito espressamente la finalità di "***tutela del patrimonio aziendale***" tra quelle contemplate per poter effettuare i controlli a distanza sui propri lavoratori (i.e. controlli mediante strumenti tecnologici come le telecamere, gli "*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa* [quali la casella di posta elettronica o altri dispositivi aziendali, ndr]" o gli "*strumenti di registrazione degli accessi e delle presenze*", questi ultimi due peraltro controllabili senza la necessità del previo accordo sindacale e/o autorizzazione amministrativa da parte dell'Ispettorato del lavoro in base al novellato art. 4, c. 2).

[7] Per completezza si segnala che una recente pronuncia della Cassazione (Cass. n. 34092/2021) pare aggiungere come ulteriore requisito per svolgere un controllo difensivo che lo stesso attenga a dati raccolti **dopo** l'insorgenza del sospetto. Questo requisito pone forti dubbi interpretativi, posto che l'esigenza di svolgere una *internal investigation* nasce quando la società viene a conoscenza di una condotta ormai consumata, sicché il non poter svolgere un controllo su dati passati vanificherebbe lo scopo stesso del controllo.

fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[8].

Inoltre, l'art. 2-decies del Codice Privacy dispone che: "*I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali* ***non possono essere utilizzati, salvo quanto previsto dall'articolo 160-bis***". A sua volta, l'art. 160-bis del Codice Privacy prevede che: "La *validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento* ***restano disciplinate dalle pertinenti disposizioni processuali***."

Rinviando ad un prossimo numero di questa newsletter per approfondimenti specifici relativi al tema, si sottolinea come la conduzione di *internal investigations* nel pieno rispetto della normativa *privacy* pone al riparo da contestazioni e assicura la piena utilizzabilità delle prove raccolte nei procedimenti giudiziari.

In ogni caso, vale la pena di ricordare che **in molti casi lo scopo delle *internal investigations* è semplicemente quello di verificare il funzionamento e l'adeguatezza del sistema di controllo interno rispetto a casi di probabili violazioni e/o quello di rispondere a richieste di Autorità di controllo**.

## 5. Conclusioni

Concludendo, al fine di dotare la società della capacità di svolgere *internal investigations*, è fondamentale:

- adottare la ***policy* interna** nei termini sopra indicati;
- fornire ai soggetti interessati dall'indagine una **informativa *privacy* specifica** sull'attività di trattamento dei dati connessa all'*internal investigation* (differibile qualora vi sia il rischio di pregiudicare l'indagine); e
- svolgere le attività di analisi dei dati con l'applicazione di **parole chiave**, con adeguata **limitazione del periodo rilevante** e **per gradi**, nel rispetto dei principi di proporzionalità e minimizzazione nel trattamento dei dati personali previsti dal GDPR.

Pur in assenza di una adeguata *policy* interna preventiva è possibile agire nel rispetto degli altri due requisiti sopra menzionati e quindi procedere ugualmente con una *internal investigation*, bilanciando l'interesse alla tutela delle prerogative *privacy* dei soggetti interessati con l'interesse legittimo alla difesa della società coinvolta.

[8] In proposito si veda l'art. 83, par. 5 del GDPR.

## Focus Team Corporate Compliance & Investigations

Il Focus Team è una costellazione di competenze in ambito penale, societario, *compliance*, lavoro e privacy a cui si aggiungono le risorse dedicate e la tecnologia di *e-discovery* del nostro team di beLab.

Alessandro Musella
*Societario, Compliance*

Angelino Alfano
*Internazionale, Public Affairs*

Giuseppe Manzo
*Societario*

Vittorio Pomarici
*Lavoro*

Francesco Sbisà
*Penale*

Vincenzo Dell'Osso
*Societario, Investigations*

Valentina Frignati
*Societario, Investigations*

Michela Maccarini
*beLab*