

AXERTA®
INDAGA. DOCUMENTA. ACCERTA.

IL PUNTO

Rassegna Giurisprudenziale
Controlli e indagini nel rapporto di lavoro

Maggio-Giugno 2019

Axerta S.p.A.

Nord-ovest Piazza Duomo 17 - 20121 Milano

Centro-sud Viale Giulio Cesare 71 - 00192 Roma

Nord-est Vicolo Vincenzo Bellini 4 - 35131 Padova

800 800 007

P.IVA 10239431009 | www.axerta.it



L'editoriale del Presidente



Il convegno Axerta che si è tenuto quest'anno a Milano, il 12 aprile scorso, presso l'Aula Magna dell'Università Bocconi, tempio di eccellenza della cultura economica, ha presentato un "Prontuario delle patologie aziendali, dalla A alla Z", con lo scopo di proporre, non senza un pizzico di provocazione ed ironia, strategie difensive tra giurisprudenza e strumenti investigativi idonee a contrastare frodi ed illeciti in azienda.

Il titolo stesso dell'evento, riferendosi alle "patologie", ha voluto richiamare la possibilità che il mondo del lavoro possa essere bersaglio di agenti patogeni, virus o batteri, intendendo per tali le irregolarità e gli illeciti più comuni (assenteismo, false malattie, utilizzazione indebita della legge 104, ecc.) ed imporre conseguentemente la necessità di misure preventive o cure adeguate.

In tal senso si sono espressi, con tesi molto brillanti e ben argomentate, i vari relatori che hanno portato la testimonianza degli HR con Isabella Covili Faggioli, dei security manager con Andrea Chittaro, della magistratura del lavoro con Fabio Massimo Gallo, della dottrina con Nicola Pecchiari, e degli avvocati penalisti e giuslavoristi, con Paola Rubini e Marco Sideri.

Il quadro d'insieme che ne è emerso sembra confermare con forza più esigenze e, prima fra tutte, quella di una tutela della legalità che sfrutti tutti gli strumenti operativi e normativi disponibili, da utilizzare però con particolare attenzione alle forme ed al rispetto delle procedure, per non correre il rischio di vedere vanificati i risultati conseguiti per vizi formali o modalità di controllo approssimative o incomplete.

Particolarmente interessanti sono altresì risultati i contributi offerti quando si è parlato, anche con il concorso preziosissimo del nostro Stefano Martinazzo, di forensic accounting, per mitigare il rischio di frodi aziendali in materia contabile ed amministrativa, nonché ricordando limiti e possibilità nell'applicazione ed utilizzazione del whistleblowing, affinché risulti una risorsa per la tutela della legalità e non un banale elemento di disturbo.

E una conferma dell'attenzione riservata in particolare a questi ultimi due argomenti la si è avuta al momento del question time, animato da domande rivolte al professore di forensic accounting, Nicola Pecchiari, ed al giudice del lavoro Fabio Massimo Gallo, da parte dell'uditorio.

Ma parlando di prevenzione, e non

solo di terapie, sicuramente da sottolineare è il richiamo dei relatori alla necessità di una sempre più forte motivazione al lavoro, da alimentare e sostenere per valorizzare al massimo quello che è il vero capitale di ogni azienda: il capitale umano!

È un obiettivo, questo, da perseguire con forza e convinzione, sempre e comunque, ed uno dei percorsi da seguire è anche quello di non lasciare terreno fertile e di facile percorribilità a chi fa dell'illegalità lo scopo della propria attività lavorativa.

Gen. Michele Franzé
Presidente di Axerta S.p.a.



Whistleblowing

La legge nazionale ed europea tutelano i segnalatori

Whistleblowing più tutele per chi denuncia: approvata la direttiva Ue

Lo scorso 16 aprile il Parlamento europeo ha votato la direttiva sul whistleblowing, con una maggioranza di 591 voti 29 voti contrari e 33 astenuti.

La legge tutela i lavoratori che segnalano le violazioni del diritto comunitario in settori quali appalti pubblici, servizi finanziari, riciclaggio di denaro, sicurezza dei prodotti e dei trasporti, sicurezza nucleare, salute pubblica, protezione dei consumatori e dei dati.

Sono così introdotte delle salvaguardie, per evitare ritorsioni da parte degli enti o aziende datori di lavoro, tutele che si estendono anche a coloro che assistono gli informatori, come i facilitatori, i colleghi e i parenti. Gli Stati membri dovranno garantire agli informatori accesso gratuito a informazioni e consulenze indipendenti, nonché all'assistenza legale durante il procedimento.

I Paesi UE hanno due anni di tempo per adeguare alle nuove disposizioni la normativa nazionale. Attualmente sono solo 10 i Paesi (Francia, Ungheria, Irlanda, Italia, Lituania, Malta, Paesi Bassi, Slovacchia, Svezia e Regno Unito) che offrono tutele complete a tutti settori o categorie di lavoratori. E proprio in questi casi vige la clausola di non regressione: se una legge nazionale prevede maggiori tutele rispetto a quelle della direttiva, le prime non possono essere ridotte in fase di recepimento di quest'ultima.

Vale la pena qui sottolineare alcune importanti novità: le segnalazioni interne ed esterne vengono poste sullo stesso livello (come già accade in Italia) e vige ora l'obbligo di prendere in esame anche le segnalazioni anonime, se ben circostanziate. Infine, in caso di contrasto con la direttiva sul segreto industriale, prevale quella sul whistleblowing (come già nella legge italiana).



Controlli sui dipendenti

L'ordinamento costante della giurisprudenza conferma la legittimità dei controlli fuori dal luogo di lavoro.

Licenziato un “furbetto del cartellino”, grazie agli investigatori privati

Cass. civ. Sez. VI - Lavoro Ord., 01/03/2019, n. 6174

La Suprema Corte ha dichiarato legittimo il licenziamento intimato al dipendente al quale, a seguito di indagine investigativa disposta dal datore di lavoro, veniva contestato di essersi ripetutamente allontanato dal posto di lavoro durante l'orario di servizio, rimanendo assente per diverso tempo senza timbrare il badge in uscita e facendo così risultare la regolare presenza in servizio.

Il lavoratore impugnava il licenziamento, che riteneva illegittimo poiché fondato sulle risultanze di un'attività investigativa svolta in violazione degli artt. 2, 3 e 4 Statuto dei lavoratori.

Gli Ermellini, però, respingono il ricorso, richiamando il principio anche recentemente espresso secondo cui “i controlli del datore di lavoro, anche a mezzo di agenzia investigativa, sono legittimi ove siano finalizzati a verificare comportamenti del lavoratore che possano configurare ipotesi penalmente rilevanti od integrare attività fraudolente, fonti di danno per il datore medesimo, non potendo, invece, avere ad oggetto l'adempimento/inadempimento della prestazione lavorativa”.

La Suprema Corte afferma che il controllo non era diretto a verificare le modalità di adempimento della prestazione lavorativa, bensì la condotta fraudolenta di assenza del dipendente dal luogo di lavoro nonostante la timbratura del badge, e di conseguenza l'attività di indagine non viola il divieto di cui agli artt. 2 e 3 Statuto dei lavoratori.

Il comportamento del lavoratore aveva il fine di indurre in errore il datore di lavoro sulla sua presenza al lavoro, integrando la nozione di giusta causa di licenziamento. I controlli dell'agenzia investigativa, svolti nel rispetto delle prescrizioni di legge, hanno prodotto risultati determinanti per provare la legittimità del licenziamento e risolvere la controversia.

Garante privacy: riaffermata la legalità delle investigazioni private

Garante privacy, provvedimento n. 9086480 del 31 gennaio 2019

Il garante per la protezione dei dati personali ha dichiarato infondato il reclamo di un dipendente che lamentava la trattazione illegittima dei suoi dati e la violazione del diritto di accesso ai dati, raccolti in base ad un mandato investigativo conferito dalla società datrice di lavoro.

Nel caso di specie, Axerta S.p.A. aveva effettuato un'attività di indagine che si è svolta nel periodo in cui il reclamante era assente dal lavoro per malattia. Il garante ha specificato che “tale attività non risulta in sé illecita in relazione alla disciplina vigente in materia di controlli sull'attività del dipendente, né pertanto risultano allo stato sussistenti gli estremi per poter dichiarare inutilizzabili i dati personali trattati in occasione della predetta attività. Infatti, come costantemente affermato dalla giurisprudenza di legittimità, il datore di lavoro può effettuare controlli - anche attraverso un'agenzia investigativa - purché tale attività non riguardi l'adempimento della prestazione lavorativa, essendo effettuata al di fuori dell'orario di lavoro”.

Per quanto riguarda il diritto di accesso il Garante ha ritenuto di accogliere le istanze di limitazione dell'esercizio del diritto di accesso “limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per l'esercizio del diritto in sede giudiziaria”.

Chiarita la legittimità delle indagini svolte al di fuori del luogo di lavoro, preme eviscerare la questione dell'accesso ai dati. Nel processo giuslavoristico l'onere della prova ricade sul datore di lavoro, si può allora facilmente constatare quale pregiudizio deriverebbe per quest'ultimo dall'esposizione delle risultanze dell'attività investigativa (dossier riservato, in questo caso prodotto da Axerta S.p.A.).



Cybersecurity e GDPR

Interazioni, strategie ed equilibri

Regolamento Ue sulla cybersecurity: una riflessione sul nuovo principio di accountability

Giuseppe D'Acquisto – funzionario direttivo del Garante Privacy

Per garantire un vero salto di qualità nel livello di sicurezza continentale, Parlamento Europeo, Consiglio dell'Unione Europea e Commissione Europea stanno spingendo su un nuovo Regolamento Europeo in materia di cybersecurity.

Infatti, risolta la “questione adempimenti” (nomina dei DPO, approntamento di procedure per la notifica dei data breach ecc.), si avverte la necessità di ragionare sul nuovo principio di accountability e sulla sua capacità di innescare nuove dinamiche di mercato tali da consentire ai titolari di ottenere vantaggi competitivi dalla compliance.

Il GDPR non si occupa del complesso meccanismo di incentivi (prevalentemente economici) che condurranno i titolari a realizzare l'accountability. Non è una dimenticanza: il GDPR offre uno scenario di lungo termine per il mantenimento della centralità della persona nella futura economia digitale, attraverso il rispetto del diritto fondamentale alla protezione dei dati personali.

Sulle motivazioni contingenti che spingeranno i titolari a scegliere l'una o l'altra modalità di attuazione dei principi, molto conteranno le tecnologie disponibili, la loro efficacia e il loro costo, ma anche, forse soprattutto, una visione strategica che accompagni le scelte in modo da non farle percepire come un adempimento formale, guidato prevalentemente dalla forza deterrente delle sanzioni, ma piuttosto come un passaggio necessario, benefico a livello individuale e collettivo, verso una compiuta digitalizzazione della società.

Il GDPR ha elevato la sicurezza a principio del trattamento, rendendola una necessità e non più un'opzione. Non è una novità di poco conto: ciò equivale a dire che tutti i titolari dovranno sempre pensare alla sicurezza dei dati prima di procedere ai trattamenti. Tuttavia, la spesa per cybersecurity, ancora spaventosamente bassa, denota una percezione della sicurezza come ancora opzionale e, al limite, come scelta obbligata.