Lavoro nell'era digitale

**Social media, WhatsApp, IA, telecamere, licenziamenti:
la guida per gestire i nuovi rischi nel rapporto di lavoro**

Mario Cassaro

Sistema RATIO
Centro Studi Castelli Srl

INDICE

Premessa 6

Parte prima - Fondamenti normativi e prova digitale 7

Capitolo 1 - Il quadro normativo: controlli tecnologici e privacy 8
1.1 L'art. 4 dello Statuto dei Lavoratori dopo il Jobs Act 9
1.2 GDPR e Codice Privacy: il bilanciamento secondo la giurisprudenza 10
1.3 Controlli difensivi e investigativi 12
1.4 Potere disciplinare e proporzionalità della sanzione 14

Capitolo 2 - Prova digitale nel procedimento disciplinare 17
2.1 Ammissibilità e valore probatorio (screenshot, messaggi, post) 18
2.2 Prova illecita per violazione della privacy 19
2.3 Acquisizione di dati e garanzie costituzionali 20
2.4 Inutilizzabilità della prova 21
2.5 Prove acquisite da terzi e colleghi 22

Parte seconda - Messaggistica e social media 25

Capitolo 3 - WhatsApp, chat aziendali e contenuti illeciti 26
3.1 Messaggistica istantanea come fonte di prova 27
3.2 Contenuti legittimanti il licenziamento 27
3.3 Chat private del lavoratore: limiti all'acquisizione 29
3.4 Ammissibilità dei messaggi WhatsApp 30
3.5 Gruppi WhatsApp: uso improprio e violazioni disciplinari 32
3.6 E-mail aziendale: accesso del datore e tutela privacy 33
3.7 Informazione sindacale tramite WhatsApp 36

Capitolo 4 - Social media: uso illecito e licenziamento 39
4.1 Profilo pubblico vs. privato 40
4.2 Casi di licenziamento per condotte sui social 41
4.3 Manifestazione del pensiero fuori dall'orario di lavoro 44
4.4 Algoritmo come prova nel licenziamento disciplinare 45
4.5 Social media policy: elaborazione ed efficacia 47
4.6 *Social screening* nella selezione del personale: limiti e discriminazioni 47
4.6.1 Principali pronunce giurisprudenziali suddivise per aree tematiche 49

Parte terza - Comunicazioni digitali e controlli tecnologici 59

Capitolo 5 - Licenziamento e contestazione via strumenti digitali 60
5.1 Forma scritta e comunicazioni digitali 61
5.2 Licenziamento via SMS, WhatsApp, e-mail: validità e termini 61
5.3 PEC vs. e-mail ordinaria: conseguenze processuali 64

5.4 Contestazione disciplinare digitale 65

Capitolo 6 - Sistemi di controllo tecnologico sul luogo di lavoro 67
6.1 Geolocalizzazione (GPS) e app di tracciamento: finalità legittime 68
6.2 Videosorveglianza: presupposti e utilizzo disciplinare 69
6.3 Videosorveglianza: violazioni diffuse e inefficacia del consenso individuale 70
6.4 Software di monitoraggio della produttività e sistemi biometrici 72
6.5 *Smart working*: controlli a distanza e diritto alla disconnessione 73
6.6 *Keystroke logging* e screenshot automatici 74
6.7 Controlli occulti 74

Parte quarta - Fattispecie emergenti 77

Capitolo 7 - Intelligenza artificiale, cybersecurity e nuove tecnologie 78
7.1 L'intelligenza artificiale nel rapporto di lavoro: profili giuridici tra innovazione e tutela dei diritti fondamentali 79
7.2 Sistemi automatizzati di valutazione e principali settori di applicazione 83
7.2.1 Profili critici sul piano giuslavoristico 83
7.2.2 I principi applicabili 84
7.3 Il licenziamento nell'era dell'intelligenza artificiale 84
7.4 *Data breach* per negligenza e sottrazione di dati aziendali 88
7.4.1 Premessa: la responsabilità del lavoratore nella tutela dei dati 88
7.4.2 Il *data breach* per negligenza del lavoratore 88
7.4.2.1 Configurazione della negligenza 88
7.4.2.2 Conseguenze disciplinari 89
7.4.3 La sottrazione dolosa di dati aziendali 89
7.4.3.1 Tipologie di sottrazione 89
7.4.3.2 Profili penali: l'accesso abusivo a sistema informatico 90
7.4.3.3 Altri profili penali: appropriazione indebita e furto 90
7.4.3.4 Il concorso di reati 91
7.4.3.5 Conseguenze disciplinari della sottrazione dolosa 91
7.4.3.6 La responsabilità del nuovo datore di lavoro 92
7.4.4 Misure di prevenzione e protezione 92
7.4.4.1 Formazione e informazione 93
7.4.4.2 Il ruolo delle clausole contrattuali 93
7.4.5 L'onere probatorio nei giudizi disciplinari 93
7.4.6 Differenze tra settore pubblico e privato (cenni) 94
7.5 *Cloud* aziendale e conservazione dati dopo la cessazione del rapportox 94
7.5.1 *Cloud computing* nel rapporto di lavoro 94
7.5.2 Titolarità dei dati conservati nel *cloud* aziendale 95
7.5.3 Accesso del datore ai dati del dipendente nel *cloud* 95
7.5.4 La cessazione del rapporto e l'accesso ai dati 96
7.5.4.1 Recupero dei dati personali 96
7.5.4.2 Restituzione e cancellazione dei dati aziendali 96
7.5.5 La conservazione dei dati del lavoratore da parte del datore 97
7.5.6 *Best practices* per la gestione del *cloud* aziendale 97
7.6 *Cyber-mobbing* e molestie digitali: responsabilità del datore 98
7.6.1 Le nuove forme di violenza nel contesto digitale 98

7.6.2 Caratteristiche distintive e condotte costitutive del *cyber-mobbing* 98
7.6.3 Il quadro normativo e gli obblighi del datore di lavoro 99
7.6.4 Conseguenze per il lavoratore autore di *cyber-mobbing* 100
7.6.5 Tutela della vittima e obblighi del datore di adottare misure di contrasto 100
7.7 *Whistleblowing* digitale 101
7.7.1 Il quadro normativo e le procedure 102
7.7.2 *Whistleblowing* e rapporto di lavoro: i confini della tutela 104
7.8 Il rischio informatico nel rapporto di lavoro: *phishing*, negligenza e responsabilità disciplinare 104
7.8.1 La frode informatica nel contesto aziendale: il fenomeno del *Business E-mail Compromise* (BEC) 105
7.8.2 Le misure di prevenzione: doveri organizzativi dell'impresa e obblighi normativi 106
7.8.3 La responsabilità disciplinare del lavoratore: il caso del bonifico eseguito per *phishing* 107
7.8.4 *Smart working*, controllo a distanza e rischio informatico 107
7.8.5 Considerazioni conclusive: la diligenza digitale come componente della prestazione lavorativa 108

Appendice 110
Tavola n. 1 - Check-list gestione data breach con profili disciplinari del lavoratore 111
Tavola n. 2 - Check-list per il procedimento disciplinare fondato su prove digitali 113
Tavola n. 3 - Fac-simile di lettera di contestazione disciplinare fondata su prove digitali 115
Tavola n. 4 - Modello Social Media Policy aziendale (fac-simile) 117
Tavola n. 5 - Lettera al dipendente: restituzione dati aziendali e gestione accessi digitali alla cessazione del rapporto 119

Premessa

C'è un momento preciso in cui un professionista del lavoro si rende conto che qualcosa è cambiato in modo irreversibile, quando ad esempio si trova a dover valutare il valore probatorio di uno screenshot, oppure quando un datore di lavoro gli chiede se può licenziare un dipendente per un post pubblicato su un social network o su WhatsApp. Ciò che fino a ieri era un'eccezione è diventato, rapidamente, la norma.

Strumenti pensati per comunicare, condividere o semplificare sono diventati, nel tempo, fonti di prova, strumenti di controllo, terreno di conflitto, mentre il confine tra sfera privata e sfera professionale si è fatto labile e incerto. Le norme esistenti sono state interpretate, adattate dalla giurisprudenza caso per caso, finché il legislatore - europeo e nazionale - ha cominciato a intervenire con strumenti più mirati.

Questo volume intende offrire al consulente del lavoro, all'avvocato, al responsabile delle risorse umane un riferimento concreto e aggiornato su tutto ciò che il digitale ha introdotto - o modificato - nella disciplina e nella gestione dei rapporti di lavoro. I temi affrontati non nascono dalla teoria, ma dall'analisi di situazioni concrete che ormai rappresentano la quotidianità. Dalle chat private prodotte in giudizio alle decisioni prese da un algoritmo, passando per il monitoraggio delle e-mail del dipendente e dalla videosorveglianza, il testo accompagna il lettore attraverso le situazioni più critiche e controverse, con un'attenzione costante al dato normativo e alla giurisprudenza in materia.

Particolare rilievo è riservato alle condotte illecite che il digitale ha reso più facili da realizzare e, al tempo stesso, più difficili da gestire sul piano disciplinare: il *cyber-mobbing* e le molestie perpetrate attraverso strumenti informatici o piattaforme social, le frodi informatiche e il *phishing* a danno dell'azienda o di terzi e l'uso distorto dei sistemi aziendali per finalità illecite. Si tratta di fattispecie emergenti in cui la dimensione tecnologica incide direttamente sulla qualificazione giuridica della condotta, sulla raccolta delle prove e sulla proporzionalità della sanzione irrogabile.

Ampio spazio è dedicato all'intelligenza artificiale applicata al rapporto di lavoro, il fronte più aperto e, per certi versi, più imprevedibile della trasformazione in atto, le cui implicazioni concrete in termini di trasparenza, diritti del lavoratore e tutele di fronte alle decisioni automatizzate, sono ancora in larga parte da definire. Il volume ne offre una ricognizione aggiornata, individuando le linee di tendenza più probabili alla luce del quadro regolatorio europeo in via di consolidamento.

In un contesto in rapida evoluzione, sapere non basta ma occorre saper agire. Questo E-book è pensato per affrontare con competenza temi destinati a diventare sempre più centrali nella gestione del rapporto di lavoro. Tabelle di sintesi, schemi riepilogativi, fac-simile, check-list e riferimenti giurisprudenziali, anche distinti per tema, completano la trattazione e ne facilitano la consultazione.

Parte prima

Fondamenti normativi e prova digitale

Capitolo 1

Il quadro normativo: controlli tecnologici e privacy

1.1 L'art. 4 dello Statuto dei Lavoratori dopo il Jobs Act

L'evoluzione tecnologica ha profondamente modificato le modalità di svolgimento della prestazione lavorativa, rendendo necessario un aggiornamento della disciplina dei controlli sul lavoro. L'art. 4 L. 20.05.1970, n. 300 (Statuto dei Lavoratori) rappresenta da sempre il cardine della regolamentazione dei controlli a distanza sull'attività dei lavoratori, costituendo un punto di equilibrio tra le esigenze organizzative e produttive del datore di lavoro e la tutela della dignità e della riservatezza dei prestatori di lavoro.

La riforma operata dal D.Lgs. 14.09.2015, n. 151 (c.d. Jobs Act), attraverso l'art. 23, ha profondamente innovato l'impianto originario della norma, superando il modello previgente fondato sul divieto generale di utilizzo di impianti audiovisivi e altri strumenti di controllo a distanza dell'attività lavorativa.

Nella sua formulazione originaria, l'art. 4 contemplava un divieto assoluto di installazione di apparecchiature finalizzate al controllo a distanza dei lavoratori, ammettendo deroghe solo in presenza di esigenze organizzative, produttive o di sicurezza sul lavoro, e subordinando comunque l'installazione di tali strumenti all'accordo con le rappresentanze sindacali aziendali o, in mancanza, all'autorizzazione dell'Ispettorato del lavoro. Tale regime configurava il controllo a distanza come eccezione al divieto generale, richiedendo che esso fosse meramente incidentale e preterintenzionale rispetto alle finalità legittimanti l'installazione degli strumenti.

Il nuovo assetto normativo ha invece abbandonato la logica del divieto assoluto, introducendo un sistema articolato che distingue tra diverse tipologie di strumenti e modalità di controllo. Il c. 1, art. 4 conferma il divieto di utilizzo di impianti audiovisivi e altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, ma consente l'installazione di tali apparecchiature, previo accordo collettivo con le rappresentanze sindacali aziendali o, in mancanza, autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro, esclusivamente per 3 categorie di esigenze: esigenze organizzative e produttive, sicurezza del lavoro, e tutela del patrimonio aziendale.

L'inserimento esplicito della tutela del patrimonio aziendale tra le finalità legittimanti rappresenta una significativa novità, che ha sollevato interrogativi sul rapporto tra la nuova disciplina e la figura dei controlli difensivi, di elaborazione giurisprudenziale.

Una delle innovazioni più rilevanti è contenuta nel c. 2, art. 4, che introduce una disciplina speciale per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per gli strumenti di registrazione degli accessi e delle presenze. Per tali categorie di strumenti, la norma non richiede né l'accordo sindacale né l'autorizzazione amministrativa, riconoscendo la peculiarità di dispositivi ormai indispensabili per lo svolgimento dell'attività lavorativa contemporanea, quali computer, tablet, smartphone aziendali, badge elettronici e sistemi di timbratura.

Questa disposizione risponde alla necessità di adeguare la disciplina alle trasformazioni del mondo del lavoro, in cui gli strumenti tecnologici costituiscono ordinariamente il mezzo attraverso cui si realizza la prestazione. La loro capacità tecnica di consentire anche forme di controllo a distanza dell'attività lavorativa non può impedirne l'utilizzo, pena la paralisi dell'organizzazione aziendale.

Tuttavia, il legislatore ha subordinato l'utilizzabilità dei dati raccolti attraverso tali strumenti a 2 condizioni fondamentali. In primo luogo, il datore di lavoro deve fornire al lavoratore un'adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli. Tale

obbligo informativo costituisce un presidio essenziale della trasparenza e consente al lavoratore di conoscere preventivamente le regole di utilizzo degli strumenti, le tipologie di controlli possibili, i dati conservati e i soggetti abilitati ad accedervi. L'informativa deve essere chiara, completa e facilmente accessibile, solitamente attraverso l'adozione di policy aziendali che disciplinino analiticamente l'uso degli strumenti di lavoro e le conseguenze derivanti dalla violazione delle regole stabilite. La predisposizione di tali policy rappresenta una prassi ormai consolidata nelle organizzazioni aziendali e costituisce il presupposto imprescindibile per la legittimità dei controlli.

In secondo luogo, il c. 2, art. 4 richiama espressamente il rispetto della normativa in materia di protezione dei dati personali, stabilendo un necessario coordinamento tra la disciplina lavoristica e quella sulla privacy. Tale rinvio impone l'osservanza dei principi fondamentali del trattamento dei dati, quali necessità, proporzionalità, pertinenza, minimizzazione e limitazione della conservazione, come previsti dal Regolamento (UE) 2016/679 (GDPR).

Il c. 3, art. 4 precisa che le informazioni raccolte ai sensi dei cc. 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro, inclusi quelli disciplinari, a condizione che siano rispettate le garanzie procedimentali previste dalla disciplina del potere disciplinare. L'utilizzabilità a fini disciplinari rappresenta un elemento di continuità rispetto alla previgente formulazione della norma, confermando che il rispetto delle procedure di installazione degli strumenti di controllo o l'esenzione da tali procedure per gli strumenti di lavoro rende legittimo l'utilizzo dei dati raccolti anche per sanzionare comportamenti illeciti del lavoratore.

La riforma ha dunque delineato un sistema normativo più flessibile e maggiormente rispondente alle esigenze dell'organizzazione aziendale moderna, pur mantenendo saldi i presidi di tutela della dignità e della riservatezza dei lavoratori attraverso gli obblighi informativi e il richiamo alla disciplina della protezione dei dati personali.

1.2 GDPR e Codice Privacy: il bilanciamento secondo la giurisprudenza

La disciplina dei controlli tecnologici sul lavoro non può essere compresa senza considerare il quadro normativo in materia di protezione dei dati personali, che si pone in rapporto di necessaria integrazione con l'art. 4 dello Statuto dei Lavoratori. Il Regolamento (UE) 2016/679, noto come GDPR (*General Data Protection Regulation*), applicabile dal 25.05.2018, ha profondamente innovato la materia della protezione dei dati personali, introducendo principi e obblighi vincolanti per tutti i soggetti che trattano dati personali, ivi inclusi i datori di lavoro.

Il dato personale è definito dall'art. 4, par. 1 GDPR come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*". La nozione è volutamente ampia e comprende non solo dati sensibili o particolari, ma potenzialmente ogni tipo di informazione, oggettiva o soggettiva, che si riferisca a una persona fisica e consenta di identificarla, direttamente o indirettamente, attraverso riferimenti quali nome, numero di identificazione, dati di ubicazione, identificativi online o elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Nel contesto lavorativo, costituiscono dati personali del lavoratore, tra gli altri, le informazioni relative agli orari di lavoro, alle presenze e assenze, alle comunicazioni effettuate tramite posta

elettronica aziendale, ai dati di navigazione internet, alle informazioni di geolocalizzazione, nonché ogni altra informazione raccolta attraverso gli strumenti tecnologici utilizzati per la prestazione.

Il GDPR stabilisce all'art. 5 i principi fondamentali che devono governare ogni trattamento di dati personali. Il principio di liceità richiede che il trattamento si fondi su una delle basi giuridiche previste dall'art. 6 del Regolamento. Nel rapporto di lavoro, la base giuridica più frequentemente invocata è la necessità del trattamento per l'esecuzione del contratto di lavoro o per adempiere un obbligo legale cui è soggetto il datore di lavoro.

Principio di correttezza	Impone che il trattamento sia trasparente nei confronti dell'interessato e rispettoso delle sue legittime aspettative. Il principio di trasparenza si traduce nell'obbligo di fornire all'interessato, ai sensi dell'art. 13 GDPR, un'informativa completa e comprensibile sulle modalità di trattamento dei dati, sulle finalità perseguite, sui tempi di conservazione, sui diritti esercitabili e sull'identità del titolare del trattamento e, se designato, del responsabile della protezione dei dati.
Principio di minimizzazione	Richiede che i dati trattati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono raccolti. Nel contesto dei controlli tecnologici, ciò comporta che il datore di lavoro non può raccogliere e conservare dati in misura eccedente rispetto agli scopi legittimi perseguiti, dovendo selezionare le modalità di controllo meno invasive tra quelle idonee a conseguire l'obiettivo.
Principio di limitazione della conservazione	Impone che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità. Una volta esaurita la finalità del trattamento, i dati devono essere cancellati o resi anonimi.
Principio di integrità e riservatezza	Obbliga il titolare ad adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio, proteggendo i dati da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentale.

L'art. 88 GDPR riconosce che gli Stati membri possono prevedere, attraverso la legge o i contratti collettivi, norme più specifiche per garantire la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei lavoratori. Tale disposizione legittima il permanere di discipline nazionali speciali, come l'art. 4 dello Statuto dei Lavoratori, che si pongono in rapporto di complementarità con il quadro generale del GDPR.

Il D.Lgs. 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali), come modificato dal D.Lgs. 10.08.2018, n. 101, contiene all'art. 88 disposizioni specifiche sul trattamento dei dati dei lavoratori. La norma ribadisce che il trattamento dei dati deve avvenire nel rispetto dei principi di necessità, correttezza, pertinenza e non eccedenza, richiamando il necessario bilanciamento tra le esigenze organizzative e produttive del datore di lavoro e i diritti e le libertà fondamentali dei lavoratori.

L'art. 114 del Codice Privacy disciplina specificamente il controllo a distanza degli strumenti di lavoro, stabilendo che le modalità di utilizzo e le informazioni raccolte sono trattate nel rispetto del GDPR e delle disposizioni dello Statuto dei Lavoratori, confermando il rimando a quest'ultimo e il necessario coordinamento tra le due discipline.

Centro Studi Castelli S.r.l. – *Riproduzione vietata*

Il bilanciamento tra le esigenze datoriali di controllo e tutela del patrimonio aziendale e i diritti fondamentali dei lavoratori alla dignità, alla riservatezza e alla protezione dei dati personali costituisce il nucleo centrale della disciplina. Tale bilanciamento non può essere operato in astratto, ma richiede una valutazione caso per caso, tenendo conto delle circostanze concrete, della natura dell'attività svolta, del tipo di strumenti utilizzati, delle modalità e dell'intensità del controllo.

La giurisprudenza, come vedremo in seguito, ha progressivamente delineato i criteri guida per operare tale bilanciamento, riconoscendo che i diritti fondamentali dei lavoratori, pur non avendo carattere assoluto, devono essere compressi solo nella misura strettamente necessaria al perseguimento di finalità legittime e proporzionate. Eventuali limitazioni devono essere previste dalla legge, rispettare il contenuto essenziale dei diritti coinvolti e rispondere ai requisiti di necessità e proporzionalità rispetto all'obiettivo perseguito.

La Carta dei diritti fondamentali dell'Unione Europea (Gazzetta ufficiale delle Comunità Europee 2000/C 364/01) riconosce all'art. 7 il diritto al rispetto della vita privata e familiare e all'art. 8 il diritto alla protezione dei dati personali come diritti distinti ma interconnessi. Il diritto alla protezione dei dati personali non si esaurisce nella dimensione negativa del diritto alla riservatezza, ma assume anche una dimensione positiva, traducendosi in un insieme di regole e principi che disciplinano le modalità del trattamento.

Nel contesto lavorativo, il bilanciamento deve tenere conto della posizione di particolare vulnerabilità del lavoratore rispetto al datore di lavoro, derivante dalla subordinazione inerente al rapporto di lavoro. L'apparente consenso del lavoratore al trattamento dei propri dati non può essere considerato come base giuridica sufficiente, in quanto viziato dalla disparità di potere contrattuale. Per questa ragione, il trattamento dei dati dei lavoratori deve fondarsi sulla necessità per l'esecuzione del contratto o sull'adempimento di obblighi legali, e deve essere circoscritto a quanto strettamente indispensabile.

Il Garante per la protezione dei dati personali ha più volte evidenziato che il datore di lavoro, nel predisporre sistemi di controllo tecnologico, deve privilegiare soluzioni tecniche che minimizzino l'impatto sulla sfera privata dei lavoratori, adottando modalità che consentano il perseguimento delle finalità legittime con il minor sacrificio possibile dei diritti fondamentali. Ad esempio, laddove sia possibile conseguire l'obiettivo attraverso il trattamento di dati aggregati o anonimi, deve essere esclusa la raccolta di dati che consentano l'identificazione del singolo lavoratore.

L'obbligo di informativa previsto dall'art. 13 GDPR assume nel rapporto di lavoro una funzione particolarmente rilevante, in quanto consente al lavoratore di conoscere preventivamente le modalità e l'estensione dei controlli cui può essere sottoposto, adeguando conseguentemente il proprio comportamento. L'informativa deve essere fornita al momento dell'instaurazione del rapporto e deve essere aggiornata in caso di modifiche sostanziali delle modalità di trattamento.

1.3 Controlli difensivi e investigativi

Accanto alla disciplina generale dei controlli tecnologici delineata dall'art. 4 dello Statuto dei Lavoratori, si colloca la figura dei controlli difensivi, di elaborazione giurisprudenziale, che ha conosciuto una significativa evoluzione a seguito della riforma del Jobs Act. I controlli difensivi

rappresentano una categoria peculiare di controlli finalizzati non già alla verifica dell'adempimento della prestazione lavorativa, ma all'accertamento di condotte illecite dei lavoratori lesive del patrimonio aziendale o comunque costituenti violazioni degli obblighi contrattuali di fedeltà e diligenza.

La distinzione fondamentale elaborata dalla giurisprudenza è quella tra controlli preventivi, diretti a verificare in via generale e continuativa il corretto svolgimento della prestazione da parte della generalità o di gruppi di lavoratori, e controlli successivi o investigativi, attivati in presenza di un fondato sospetto circa la commissione di specifici illeciti da parte di determinati lavoratori.

Nella vigenza della formulazione originaria dell'art. 4 dello Statuto dei Lavoratori, la giurisprudenza aveva affermato che i controlli difensivi, in quanto estranei alla finalità di controllo dell'attività lavorativa e rivolti invece all'accertamento di comportamenti illeciti, si collocavano al di fuori dell'ambito di applicazione della norma e non richiedevano pertanto né l'accordo sindacale né l'autorizzazione amministrativa.

Tale orientamento si fondava sulla considerazione che l'art. 4, nella sua formulazione originaria, vietava i controlli finalizzati a verificare l'esecuzione della prestazione lavorativa, mentre rimanevano estranei al suo perimetro applicativo i controlli volti a tutelare il datore di lavoro da condotte illecite, espressione del legittimo diritto di difesa del patrimonio aziendale e della libertà di iniziativa economica.

La riforma del 2015, inserendo espressamente tra le esigenze legittimanti l'installazione di strumenti di controllo a distanza la tutela del patrimonio aziendale, ha sollevato il problema della permanente autonomia della categoria dei controlli difensivi rispetto alla disciplina dell'art. 4 riformato.

La giurisprudenza successiva alla riforma ha confermato la sopravvivenza dei controlli difensivi in senso stretto, distinguendo tra controlli a difesa del patrimonio aziendale rivolti alla generalità dei dipendenti o a gruppi di dipendenti, che devono essere effettuati nel rispetto delle procedure previste dall'art. 4, e controlli difensivi in senso proprio, diretti ad accertare specifici illeciti ascrivibili a singoli lavoratori sulla base di concreti indizi, che si collocano al di fuori del perimetro applicativo della norma statutaria.

I controlli difensivi in senso stretto presentano caratteristiche peculiari che ne giustificano l'esenzione dalle procedure dell'art. 4. In primo luogo, essi presuppongono l'esistenza di un fondato sospetto circa la commissione di un illecito da parte di uno o più lavoratori determinati. Il sospetto deve basarsi su elementi concreti e non su mere congetture o sospetti generici, e deve essere antecedente rispetto all'attivazione del controllo.

In secondo luogo, i controlli difensivi hanno carattere successivo rispetto al comportamento illecito sospettato, nel senso che vengono attivati dopo l'insorgere del sospetto e sono finalizzati alla raccolta di elementi probatori in ordine a fatti già verificatisi o in corso di realizzazione. La loro natura *ex post* li differenzia dai controlli preventivi e continuativi sulla generalità dei lavoratori.

In terzo luogo, i controlli difensivi sono caratterizzati dalla specificità e dalla limitazione temporale, essendo circoscritti all'accertamento di determinati fatti illeciti e cessando una volta conseguita la prova o esclusa la fondatezza del sospetto.

L'esenzione dei controlli difensivi dalle procedure dell'art. 4 non significa tuttavia che il datore di lavoro possa attivarli in modo del tutto discrezionale e senza limiti. Anche i controlli difensivi

devono rispettare i principi fondamentali di tutela della dignità e della riservatezza del lavoratore, nonché la disciplina della protezione dei dati personali. In particolare, deve essere assicurato un corretto bilanciamento tra le esigenze di protezione degli interessi e dei beni aziendali, correlate alla libertà di iniziativa economica, e le tutele della dignità e della riservatezza del lavoratore. Tale bilanciamento non può prescindere dalle circostanze del caso concreto e deve tenere conto della natura dell'illecito sospettato, dell'invasività delle modalità di controllo, della durata e dell'estensione dell'attività investigativa.

Il datore di lavoro rimane tenuto all'obbligo di informativa previsto dal GDPR, dovendo comunicare al lavoratore, anche in occasione dell'attivazione di controlli difensivi, le modalità di trattamento dei dati raccolti, fermo restando che tale informativa può essere fornita anche successivamente all'avvio del controllo, laddove un'informazione preventiva rischierebbe di pregiudicarne l'efficacia.

I controlli difensivi devono inoltre rispettare i principi di necessità, pertinenza e proporzionalità del trattamento dei dati personali. Il datore di lavoro deve adottare le modalità investigative meno invasive tra quelle idonee a conseguire l'obiettivo di accertamento dell'illecito, evitando forme di controllo che eccedano quanto strettamente necessario.

Particolare delicatezza assumono i controlli investigativi che comportino l'accesso alla corrispondenza elettronica del lavoratore o ai dati di navigazione internet. In questi casi, il bilanciamento deve tenere conto della legittima aspettativa di riservatezza del lavoratore sulle comunicazioni effettuate, anche attraverso strumenti aziendali, e può giustificare l'accesso ai contenuti solo in presenza di gravi indizi di illeciti rilevanti e dopo aver esperito forme di controllo meno invasive.

La distinzione tra controlli difensivi legittimi e controlli illegittimi si fonda dunque su una pluralità di elementi quali la sussistenza di un fondato sospetto antecedente, la natura *ex post* del controllo, la specificità e limitazione temporale dell'attività investigativa, la proporzionalità tra gravità dell'illecito sospettato e invasività del controllo, il rispetto dei principi di protezione dei dati personali e della dignità del lavoratore.

1.4 Potere disciplinare e proporzionalità della sanzione

Il legittimo esercizio del potere di controllo da parte del datore di lavoro costituisce il presupposto per l'eventuale irrogazione di sanzioni disciplinari in caso di accertamento di comportamenti illeciti del lavoratore. Tuttavia, l'accertamento dell'illecito non è di per sé sufficiente a giustificare qualsiasi tipo di sanzione, dovendo il datore di lavoro rispettare il principio di proporzionalità tra gravità dell'infrazione e severità della reazione disciplinare.

Il potere disciplinare del datore di lavoro trova il proprio fondamento normativo nell'art. 2106 c.c., che riconosce al datore il potere di irrogare sanzioni disciplinari "*secondo la gravità dell'infrazione*". Tale disposizione codifica il principio di proporzionalità, richiedendo che la sanzione sia commisurata all'entità della violazione commessa.

L'art. 7 dello Statuto dei Lavoratori disciplina le procedure che il datore di lavoro deve osservare nell'esercizio del potere disciplinare, stabilendo garanzie procedimentali a tutela del lavoratore. In particolare, il codice disciplinare deve essere portato a conoscenza dei lavoratori

mediante affissione in luogo accessibile a tutti; le sanzioni devono essere proporzionate alla gravità dell'infrazione; non possono essere disposte sanzioni che comportino mutamenti definitivi del rapporto di lavoro; deve essere contestato specificamente al lavoratore l'addebito e deve essere consentita la difesa, eventualmente assistita da un rappresentante sindacale; non può tenersi conto delle sanzioni disciplinari decorsi 2 anni dalla loro applicazione.

La valutazione di proporzionalità della sanzione costituisce un momento essenziale del corretto esercizio del potere disciplinare e può formare oggetto di sindacato giudiziale. Il giudice, nel verificare la legittimità del licenziamento disciplinare o di altre sanzioni conservative, deve accertare non solo la sussistenza dell'elemento oggettivo dell'illecito contestato, ma anche l'adeguatezza e la proporzionalità della sanzione irrogata rispetto alla gravità della condotta.

La valutazione di proporzionalità si articola su un duplice piano, oggettivo e soggettivo. Sotto il profilo oggettivo, deve essere considerata la gravità intrinseca del fatto commesso, tenendo conto della natura della violazione, dell'entità del pregiudizio arrecato agli interessi datoriali, delle modalità di realizzazione della condotta illecita e delle sue eventuali conseguenze.

Sotto il profilo soggettivo, devono essere valutati l'elemento psicologico del comportamento (dolo o colpa, e l'intensità dell'uno o dell'altra), le circostanze personali del lavoratore (quali l'anzianità di servizio, l'assenza di precedenti disciplinari, il comportamento complessivamente tenuto nel corso del rapporto), il grado di affidamento richiesto dalle specifiche mansioni svolte, e ogni altra circostanza rilevante del caso concreto.

La giurisprudenza ha elaborato una serie di indici sintomatici che orientano la valutazione di proporzionalità. Tra questi, assume particolare rilievo il comportamento complessivo del lavoratore nel corso del rapporto, sicché l'assenza di precedenti disciplinari e un lungo periodo di servizio caratterizzato da correttezza e diligenza possono attenuare la gravità di una condotta illecita isolata, rendendo sproporzionata l'applicazione della sanzione espulsiva.

Al contrario, la reiterazione di condotte illecite o l'esistenza di precedenti disciplinari possono aggravare la valutazione della condotta contestata, denotando una persistente inosservanza degli obblighi contrattuali e la scarsa affidabilità del lavoratore.

Particolare rilevanza assume la natura fiduciaria del rapporto di lavoro e il grado di affidamento richiesto dalle mansioni svolte. Per determinate categorie di lavoratori, quali dirigenti, addetti alla gestione di valori o denaro, personale con funzioni di controllo o vigilanza, la violazione degli obblighi di fedeltà e correttezza assume maggiore gravità in ragione della posizione di particolare fiducia rivestita. Il principio di proporzionalità impone inoltre che il licenziamento disciplinare, quale sanzione più grave e definitiva, sia irrogato solo in presenza di condotte che determinino un'effettiva lesione del vincolo fiduciario, rendendo impossibile la prosecuzione anche provvisoria del rapporto. La sussistenza della giusta causa di licenziamento presuppone che il comportamento del lavoratore sia di gravità tale da non consentire la prosecuzione del rapporto, neppure in via provvisoria (art. 2119 c.c.).

La valutazione della gravità della condotta ai fini della configurabilità della giusta causa deve essere compiuta non in astratto, ma in concreto, tenendo conto di tutte le circostanze del caso. Una medesima condotta può assumere diversa gravità in relazione al contesto in cui si inserisce, alle modalità di realizzazione, alle conseguenze prodotte e alle caratteristiche soggettive del lavoratore.

Il rispetto del principio di proporzionalità richiede inoltre che il datore di lavoro valuti l'opportunità di irrogare sanzioni conservative in luogo del licenziamento, laddove la gravità della condotta non sia tale da escludere in radice la possibilità di prosecuzione del rapporto. La scel-

ta tra sanzione conservativa e licenziamento deve essere adeguatamente motivata, dovendo emergere le ragioni per cui il datore ha ritenuto inidonea una sanzione meno afflittiva.

La necessità di una motivazione puntuale e coerente della scelta sanzionatoria costituisce un presidio essenziale del corretto esercizio del potere disciplinare. La contestazione disciplinare deve specificare con precisione i fatti addebitati, le circostanze di tempo e di luogo, le norme violate e le ragioni per cui il datore ritiene che tali fatti integrino l'illecito contestato e giustifichino la sanzione irrogata. L'inadeguatezza della motivazione può costituire vizio autonomo di legittimità della sanzione, impedendo al lavoratore l'esercizio effettivo del diritto di difesa e precludendo al giudice la verifica della proporzionalità della reazione datoriale.

Nel caso di licenziamento fondato su elementi probatori raccolti attraverso controlli tecnologici, il rispetto del principio di proporzionalità si intreccia con la verifica della legittimità delle modalità di acquisizione della prova. L'utilizzo di dati raccolti in violazione dell'art. 4 dello Statuto dei Lavoratori o della disciplina sulla protezione dei dati personali determina l'inutilizzabilità degli stessi a fini disciplinari, con conseguente illegittimità del licenziamento fondato su tali elementi.

Anche laddove i controlli siano stati legittimamente effettuati, il giudice deve verificare che la sanzione irrogata sia proporzionata alla gravità della condotta accertata, potendo sostituire il licenziamento con una sanzione conservativa ove ritenga che le circostanze del caso concreto non giustifichino la recisione del rapporto.

Il principio di proporzionalità opera, dunque, come limite interno al potere disciplinare, imponendo al datore di lavoro una valutazione articolata e bilanciata che tenga conto di tutti gli elementi rilevanti del caso concreto e garantisca una reazione sanzionatoria adeguata, senza eccessi né difetti, alla gravità dell'infrazione commessa.