CONTRIBUTO DIVULGATIVO

I poteri di controllo del datore di lavoro tra cybersecurity e tutela della privacy: i limiti ai controlli difensivi e il caso dei metadati

The employer´s control powers between cybersecurity and privacy protection: the limits to defensive controls and the case of metadata

Federico Palumbo

Avvocato · Università degli Studi di Roma La Sapienza

IDENTIFICATIVO
Contributo n. 11853
ISSN 2421-7123

LICENZA
Accesso aperto · gli autori conservano i propri diritti

STORIA EDITORIALE
Pubblicato il 30 giugno 2026
Contributo divulgativo

COME CITARE
FEDERICO PALUMBO, *I poteri di controllo del datore di lavoro tra cybersecurity e tutela della privacy: i limiti ai controlli difensivi e il caso dei metadati*, in Riv. Cammino Diritto, ISSN 2421-7123.

ABSTRACT

Il saggio indaga la tensione tra prerogative di controllo datoriali (controlli difensivi) e diritto alla riservatezza del lavoratore (art. 15 Cost., art. 8 CEDU). Attraverso l´esame della recente giurisprudenza di legittimità (Cass. nn. 807/2025 e 24204/2025) e dei Provvedimenti del Garante Privacy (nn. 243 e 250 del 2025), si delinea il perimetro di liceità nell´acquisizione di metadati e log di navigazione. Lo studio traccia i delicati confini tra l'adempimento degli obblighi di cybersecurity (Direttiva NIS2) e il divieto di monitoraggio massivo, analizzando le conseguenze patologiche – come l'inutilizzabilità processuale e l'illegittimità del licenziamento – che derivano da accessi abusivi e indagini retrospettive sproporzionate.

The essay investigates the tension between employer´s control prerogatives (defensive controls) and the worker´s right to privacy (Art. 15 Const., Art. 8 ECHR). Through the examination of recent Supreme Court case law (Cass. nos. 807/2025 and 24204/2025) and the measures of the Privacy Guarantor (nos. 243 and 250 of 2025), the perimeter of lawfulness in the acquisition of metadata and navigation logs is outlined. The study traces the delicate boundaries between the fulfillment of cybersecurity obligations (NIS2 Directive) and the prohibition of massive monitoring, analyzing the pathological consequences – such as procedural unusability and the illegitimacy of dismissal – deriving from abusive access and disproportionate retrospective investigations.

SOMMARIO

1. Introduzione: il complesso rapporto tra cybersecurity aziendale e poteri datoriali; 2. La natura della posta elettronica aziendale e la tutela della segretezza; 2.1. L'inviolabilità della corrispondenza: gli artt. 15 Cost. e 8 CEDU; 2.2. L'accesso abusivo agli account aziendali dei dipendenti; 3. I controlli difensivi: ratio e confini operativi; 3.1. La distinzione giurisprudenziale tra controlli difensivi in senso stretto e in senso lato; 3.2. Il requisito temporale: l'esclusiva legittimità dei controlli difensivi ex post; 4. Il caso dei metadati di posta e dei file di log di navigazione; 4.1. L'impostazione rigorosa del Garante Privacy sui tempi di conservazione; 4.2. Il bilanciamento tecnico: minimizzazione, accountability e DPIA; 5.

Profili patologici: le conseguenze processuali dei controlli illegittimi; 5.1. L'inutilizzabilità probatoria e l'illegittimità del licenziamento disciplinare; 6. Considerazioni conclusive: verso un equilibrio sostenibile.

1. Introduzione: il complesso rapporto tra cybersecurity aziendale e poteri datoriali

L'evoluzione tecnologica dei luoghi di lavoro ha progressivamente sgretolato i confini fisici e temporali della prestazione subordinata, inaugurando una stagione in cui la digitalizzazione assume i tratti di un'infrastruttura ubiqua. In questo panorama, il datore di lavoro si trova a fronteggiare minacce cibernetiche di natura sistemica, come le frodi informatiche, i *ransomware* e le violazioni strutturali dei database aziendali, note come *data breach*. Di fronte a tali minacce, non di rado si assiste al tentativo, talvolta pernicioso, di declinare le ordinarie prerogative di controllo, sancite in via generale dall'art. 2104 del Codice Civile e, nello specifico, dall'art. 4 della Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), in una chiave prettamente preventiva ed esplorativa.

La recente Direttiva (UE) 2022/2555, comunemente conosciuta come direttiva NIS2, ha ulteriormente innalzato il livello di guardia nel panorama continentale, imponendo obblighi stringenti e sanzioni di vasto raggio in capo agli operatori economici al precipuo scopo di garantire la resilienza delle reti e dei sistemi informativi. Il legislatore europeo postula, dunque, l'adozione di un approccio di tipo proattivo alla sicurezza, imperniato in modo sistematico sull'*accountability* e sull'analisi costante e predittiva del rischio, per far fronte a minacce come lo spionaggio industriale o i furti massivi di identità. Ciononostante, tale pur legittima e doverosa spinta alla messa in sicurezza del perimetro aziendale finisce, sovente, per collidere frontalmente con la sfera di riservatezza, libertà e dignità del lavoratore dipendente. Le *policy* di *cybersecurity* finiscono talora per trasformarsi in uno strumento distorsivo del potere organizzativo e direttivo.

La criticità ermeneutica di fondo risiede nella tentazione, sempre più radicata da parte dell'imprenditore, di sottoporre a un monitoraggio massivo, occulto o indiscriminato le attività digitali del prestatore di lavoro, adducendo astratte e generiche ragioni di difesa del patrimonio informatico o materiale. Emerge, in tutta la sua dirompente attualità, la necessità di tracciare un rigoroso bilanciamento, su cui l'interprete è chiamato a esercitare una funzione nomofilattica: se da un lato la *cybersecurity* non è più qualificabile come una mera opzione strategica ma assurge a obbligo giuridico ineludibile, dall'altro lato le garanzie statutarie poste a baluardo della persona non tollerano interpretazioni abrogatrici di fatto. Un siffatto *modus operandi* convertirebbe il sistema di rete in un apparato di controllo continuo o *panoptico* della prestazione.

L'impiego massiccio di software di monitoraggio continuo e lo *screening* automatizzato di *file di log*, di comunicazioni in entrata e in uscita, pur se teoricamente funzionali all'individuazione di potenziali vulnerabilità del network aziendale, impattano prepotentemente sull'aspettativa di riservatezza che il lavoratore ripone nel normale svolgimento della propria prestazione, ancor più qualora resa in regime di *smart working* o lavoro agile, ove le barriere tra vita privata e sfera lavorativa divengono irrimediabilmente labili. Proprio in tali congiunture, il quadro normativo nazionale, corroborato dai recenti e decisi interventi della giurisprudenza di legittimità e del Garante per la Protezione dei Dati Personali, si erge a difesa di prerogative invalicabili. Il presente saggio intende, pertanto, mappare i limiti insormontabili di questi controlli, definendone le ricadute non solo in termini sanzionatori e amministrativi ma anche, e soprattutto, sul piano della validità delle indagini aziendali nel processo del lavoro.

2. La natura della posta elettronica aziendale e la tutela della segretezza

Il nucleo originario e paradigmatico del conflitto tra le istanze di controllo datoriale e il diritto alla riservatezza del prestatore d'opera si condensa ineluttabilmente attorno all'utilizzo della posta elettronica istituzionale. Per lungo tempo, le corti di merito e parte della dottrina hanno dibattuto sull'effettiva sussistenza di un'aspettativa di segretezza da parte del dipendente, qualora egli si avvalesse, per inviare e ricevere missive, degli apparati tecnologici (*hardware* e *software*) messi a sua esclusiva disposizione dal datore di lavoro per fini prettamente lavorativi. La giurisprudenza di legittimità, in questo specifico e scivoloso ambito, ha tuttavia compiuto un salto evolutivo di vitale importanza. È stata definitivamente rigettata e destituita di fondamento la tesi - un tempo capillarmente radicata - secondo cui l'impiego e lo sfruttamento di risorse informatiche di pacifica proprietà dell'azienda degraderebbe automaticamente i dati ivi transitanti a mero "patrimonio aziendale", rendendoli un archivio aperto e liberamente ispezionabile senza filtri da parte del *management*[1].

2.1. L'inviolabilità della corrispondenza: gli artt. 15 Cost. e 8 CEDU

Questa epocale svolta nomofilattica trae origine da una rigorosa rilettura, costituzionalmente e convenzionalmente orientata, del medesimo concetto giuridico di corrispondenza. La garanzia e lo scudo offerto dall'art. 15 della Carta fondamentale prescindono in radice dalla "materialità" del mezzo tecnico adoperato. L'alveo applicativo dell'articolo 15 abbraccia con forza ogni forma di comunicazione dinamica, telematica e fluttuante tipica dell'epoca contemporanea. Pertanto, i messaggi di posta elettronica, del tutto assimilabili a lettere chiuse per il loro contenuto e per le modalità della loro trasmissione, non smarriscono la propria intima e strutturale vocazione alla segretezza nel momento in cui vengono instradati, processati o salvati sui *server* o nei *cloud* del datore di lavoro.

L'orientamento del Giudice delle Leggi si è d'altronde sedimentato e consolidato attingendo a piene mani dall'immutato quadro giurisprudenziale della Corte Europea dei Diritti dell'Uomo. La giurisprudenza sovranazionale, a partire dal celebre caso *Bărbulescu v. Romania*, non ha mai palesato tentennamenti nell'includere a pieno titolo le *e-mail* dei dipendenti sotto il robusto ombrello protettivo offerto dall'art. 8 della CEDU, che tutela il rispetto della vita privata e familiare. Ne discende il granitico principio per cui, finanche nel perimetro spaziale e temporale dell'orario di lavoro e ancorché l'attività si dipani su *device* rigorosamente aziendali (computer, *smartphone*, tablet), il dipendente matura una inossidabile e "ragionevole aspettativa di privacy" rispetto alla corrispondenza che intercorre con terzi o con i colleghi[2].

Di assoluto e dirimente rilievo è, inoltre, l'approdo giurisprudenziale relativo alla qualificazione temporale: l'e-mail conserva inalterata la sua natura costituzionale di "corrispondenza" - e dunque non decade al più modesto rango di mero documento storico, come tale liberamente acquisibile e consultabile - fintanto che essa mantenga un'attualità e un persistente interesse per i soggetti corrispondenti (mittente e destinatario), impedendo l'accesso indiscriminato a chiunque non vi sia ricompreso, compreso il formale titolare dell'infrastruttura di rete.

1. *In questo senso si è lungamente e uniformemente espresso l'orientamento consolidato che rifugge da indefiniti e fluidi poteri ispettivi in via di assoluta deroga. Sul punto, essenziale, per un accuratissimo, strutturale e prezioso approccio metodologico e dogmatico ai controlli di tipo esclusivamente protettivo, cfr.* inter plurimos *M. MARAZZA,* I controlli a distanza del lavoratore di natura difensiva, *in* Controlli a distanza e tutela dei dati personali del lavoratore, *Torino, 2017, p. 38 ss.*

2. *È da ritenersi ormai pacifico e incontestabile nel panorama nomofilattico che la solenne e perentoria garanzia posta dall'art. 15 della Costituzione italiana abbracci e assorba la dinamica e complessa dimensione telematica in tutte le sue molteplici forme e sfaccettature telematiche e digitali.*

2.2. L'accesso abusivo agli account aziendali dei dipendenti

Il principio assoluto di segretezza e inviolabilità delle comunicazioni si ripercuote in maniera dirimente, deflagrante e quasi sempre letale sulla legittimità delle indagini aziendali interne, laddove queste ultime varchino i confini del controllo formale per addentrarsi nel vivo dei contenuti. Emblematica e tranciante, a tale proposito, risulta la recentissima e incisiva pronuncia della Suprema Corte (Cass. Civ., sez. lav., sentenza 29 agosto 2025, n. 24204), la quale ha dovuto dipanare il caso, assai frequente nella prassi aziendale, di un datore di lavoro che, al fine di rintracciare e cristallizzare prove schiaccianti in merito a presunti, infedeli atti di concorrenza sleale e sviamento di clientela perpetrati da alcuni dirigenti e collaboratori di vertice, aveva forzato l'accesso alla loro posta elettronica personale aziendale. Tale irruzione digitale, materialmente compiuta incaricando un perito informatico di *bypassare* le credenziali di autenticazione e creare copie forensi delle caselle *Outlook*, si era verificata in un momento in cui i dipendenti in questione avevano peraltro già formalmente rassegnato le proprie dimissioni, interrompendo il rapporto sinallagmatico.

La Suprema Corte, confermando senza esitazioni e avallando in toto le ponderate argomentazioni sviluppate dalla Corte di merito territoriale, ha sancito un principio che scolpisce nel marmo il confine del potere datoriale: la mera circostanza materiale per cui una specifica casella di posta elettronica (seppur nomenclata con l'estensione nominale dell'azienda, es. *nome.cognome@azienda.it*) sia fisicamente ospitata e allocata su un *server* pagato e gestito dall'azienda medesima non elide, né tanto meno attenua in alcun modo, la sua insostituibile e originaria natura privata.

Il corollario penalistico di tale postulato è di immensa portata: l'introduzione non autorizzata, forzosa o furtiva del datore di lavoro all'interno di un *account* telematico per accedere al quale è necessaria una *password* o l'utilizzo di una *username* personale si configura, a tutti i fini ed effetti di legge, come un vero e proprio accesso abusivo a sistema informatico o telematico, ai sensi e per gli effetti dell'art. 615-*ter* del codice penale. Quest'ultimo reato concorre, naturalmente, con le concomitanti e ulteriori fattispecie di violazione, sottrazione e soppressione di corrispondenza, gettando un'ombra di gravissima illiceità *ab origine* sull'intera catena investigativa interna all'azienda.

3. I controlli difensivi: *ratio* e confini operativi

Se, da un lato, il divieto generale di indagini ostruzionistiche o non pertinenti in ambito lavorativo (sancito dall'art. 8 dello Statuto dei Lavoratori) e le stringenti regole in merito ai controlli a distanza ex art. 4, comma 1, Stat. Lav. impongono proceduralizzazioni e autorizzazioni vincolanti e pressoché inderogabili, dall'altro lato, la giurisprudenza - chiamata a mediare tra le istanze di sicurezza aziendale e la *privacy* - ha da lungo tempo e faticosamente elaborato la fondamentale categoria dogmatica dei cosiddetti controlli difensivi. Tali ispezioni sono concepite e teleologicamente orientate a escludere che l'ombrello di tutela offerto al lavoratore e alla sua dignità possa surrettiziamente tramutarsi in uno scudo di impunità, sotto il quale celare e reiterare condotte gravemente illecite e palesemente lesive del patrimonio, tanto materiale quanto immateriale o reputazionale, dell'azienda stessa.

La *ratio* dei controlli difensivi, secondo una prospettazione avallata da un consolidato filone giurisprudenziale, rinviene la sua giustificazione ultima nell'esigenza vitale per l'imprenditore di difendere l'azienda non da un semplice inadempimento (il lavoratore lento o disattento), ma da un vero e proprio "attacco" al patrimonio sociale. La tutela della struttura e dei beni aziendali trascende le ordinarie dinamiche di sinallagmaticità, assurgendo a interesse preminente laddove si consumino fattispecie di reato

o illeciti extracontrattuali. Il nodo gordiano, tuttavia, rimane l'individuazione di quel labile confine oltre il quale il lecito e doveroso potere di controllo protettivo sfocia nel ben più opprimente - e inesorabilmente vietato - sindacato massivo e indiscriminato sulla persona e sull'opera del dipendente.

3.1. La distinzione giurisprudenziale tra controlli difensivi in senso stretto e in senso lato

Per venire a capo di questo groviglio interpretativo, la giurisprudenza ha stratificato un'architettura concettuale fondata su una dicotomia cruciale: la distinzione sistematica tra i controlli "in senso lato" e quelli "in senso stretto". Questa linea di demarcazione costituisce la bussola per orientarsi nella liceità delle acquisizioni istruttorie aziendali.

I controlli difensivi "in senso lato" si identificano con quelle attività di monitoraggio e ispezione dirette o indirette volte precipuamente ad accertare la corretta, puntuale e diligente esecuzione dell'obbligazione lavorativa principale, ovverosia l'esatto adempimento qualitativo e quantitativo della prestazione promessa nel contratto. Poiché ineriscono organicamente alla misurazione della *performance* e alle modalità con le quali il dipendente eroga le proprie energie lavorative, tali controlli ricadono inesorabilmente - senza alcuna possibilità di elusione - sotto la scure procedurale e democratica dell'art. 4, comma 1, dello Statuto dei Lavoratori. Essi postulano, a pena di totale illegittimità, il preventivo accordo stipulato con le Rappresentanze Sindacali Unitarie (RSU) o le Rappresentanze Sindacali Aziendali (RSA), o, in difetto di concertazione sindacale, la tempestiva autorizzazione rilasciata dall'Ispettorato Territoriale del Lavoro competente. In assenza di tali validazioni, le indagini tese a valutare se il lavoratore abbia sprecato tempo lavorativo o navigato su internet per finalità ludiche restano precluse.

Radicalmente differente ed ontologicamente autonomo si staglia il perimetro dei controlli difensivi "in senso stretto". Quest'ultima tipologia di ispezioni è preordinata e diretta non già a misurare la *performance*, l'impegno o la diligenza contrattuale del lavoratore subordinato, bensì ad accertare in via esclusiva e oggettiva l'esistenza di condotte manifestamente illecite (che spesso travalicano nell'alveo del rilievo penale, annoverando, tra gli altri, episodi di furto, frode, appropriazione indebita, storno sistematico di clientela o spionaggio industriale a vantaggio di *competitors*). Tali azioni colpiscono e mettono a repentaglio l'integrità del patrimonio (tecnologico, materiale o informativo) o la stessa immagine commerciale dell'azienda all'esterno. Questi gravissimi comportamenti, pur se materialmente posti in essere in costanza di rapporto e fisicamente in occasione della prestazione lavorativa (all'interno dei locali aziendali o dai terminali messi a disposizione), possiedono una loro spiccata autonomia lesiva e una sostanziale estraneità ontologica rispetto al normale, fisiologico e quotidiano decorso del sinallagma contrattuale che lega l'impresa al dipendente. Per tale ragione formidabile, i controlli difensivi in senso stretto si pongono in una zona "franca", o per meglio dire *extra-statutaria*, sottraendosi al vaglio procedurale e all'*imprimatur* sindacale di cui all'art. 4 dello Statuto.

3.2. Il requisito temporale: l'esclusiva legittimità dei controlli difensivi *ex post*

Se è pur vero che l'esenzione dalle pastoie autorizzative rende il controllo difensivo in senso stretto uno strumento di indubbia efficacia investigativa, tale esenzione non può e non deve in alcun modo essere interpretata come un "assegno in bianco" siglato a favore dell'arbitrio e dell'ingerenza del potere datoriale. Le coordinate ermeneutiche tracciate dalla giurisprudenza esigono il rigoroso rispetto di un limite invalicabile: il requisito della posteriorità temporale.

Come puntualmente e brillantemente statuito, da ultimo, dalla fondamentale ordinanza della Corte di Cassazione n. 807 del 13 gennaio 2025, affinché il datore di lavoro possa agire legittimamente al di fuori delle strettoie garantiste dell'art. 4, comma 1, Stat. Lav., è considerato imprescindibile e dirimente che l'attività di controllo sia materialmente avviata e attuata in una fase rigorosamente successiva, ovvero *ex post*. Ciò comporta che la raccolta dei metadati, l'estrazione delle stringhe o l'analisi dei tracciamenti e dei dati debba fisiologicamente iniziare soltanto posteriormente all'insorgere di un fondato, ragionevole e oggettivo sospetto, basato su elementi indiziari chiari e preesistenti (come ammanchi di cassa, anomalie contabili o fughe conclamate di notizie riservate), circa la probabile commissione di atti illeciti perpetrati da parte di un determinato e specifico lavoratore, o al massimo di un gruppo circoscritto e chiaramente individuabile.

Risulta, per converso, palesemente illegittima (e, inesorabilmente foriera di disastrose conseguenze sul piano processuale) ogni forma di acquisizione e controllo retrospettivo e aspecifico dei dati, finalizzata alla genesi del sospetto stesso. Il datore di lavoro, in ossequio ai supremi precetti di liceità, non può attivare un'indagine "pescando a strascico" all'interno di sterminati archivi, *log* o memorie (ad esempio incrociando i *file* di *log* dei *proxy*, le cronologie di navigazione dell'ultimo anno o le miriadi di metadati delle conversazioni *e-mail*) che siano stati deliberatamente accumulati in maniera continuativa, *ex ante*, massiva e indiscriminata nel corso dei mesi o degli anni, quando alcun indizio di reato, malversazione o illecito si era mai affacciato all'orizzonte.

Un siffatto e sproporzionato controllo "preventivo" - il cui unico effetto pratico è quello di porre i lavoratori in un perpetuo e strisciante stato di soggezione silente e di assoggettamento incondizionato alla tecnologia - concretizza in maniera drammatica e speculare esattamente quella temibile lesione alla riservatezza personale e alla serenità relazionale che il lungimirante legislatore statutario del 1970 ha inteso categoricamente estirpare dalle moderne logiche di produzione[3]. L'implementazione latente di tali strumenti, sebbene ammantata dalle più nobili esigenze di *data protection*, rievoca lo spettro del controllo occulto, e perciò stesso viola l'art. 4 nella sua essenza più profonda.

4. Il caso dei *metadati* di posta e dei *file* di *log* di navigazione

Nel complesso ecosistema dell'architettura tecnica e dell'ingegneria delle comunicazioni aziendali, un ruolo di spessore e importanza sempre più preminente - e per ciò stesso potenzialmente invasivo o finanche intrusivo - è ormai indiscutibilmente rivestito dai cosiddetti "*metadati*" (i *log*, i *record* temporali e i minutissimi tracciamenti di connessione ai nodi di rete). Queste asettiche stringhe numeriche, pur non essendo finalizzate a veicolare o esplicitare in alcun modo in chiaro il contenuto semantico o testuale del messaggio o la stringa specifica di *URL* della pagina visitata (e sottraendosi, dunque, a una palese ed epidermica intromissione nel *corpus* della conversazione), descrivono e delineano nondimeno, con fedeltà quasi millimetrica e con insidiosissima capillarità, il traffico in entrata e in uscita, le tempistiche di risposta, l'allocazione temporale, il peso e le dimensioni digitali e, soprattutto, la cadenza e la frequenza delle complesse interazioni digitali intrecciate quotidianamente dai prestatori di lavoro. Tali dati esteriori delle comunicazioni "definiscono i profili temporali (come la data e l'ora di invio/ricezione) nonché gli aspetti quali-quantitativi anche in ordine ai destinatari", profilando inevitabilmente la vita lavorativa e di relazione del dipendente.

3. *A tale irrinunciabile proposito, si veda l'illuminante, capillare e minuziosa ricostruzione storico-giuridica operata in tempi recentissimi da Cass. Civ. Sez. Lav. Ord., 13 gennaio 2025, n. 807, oggetto di denso ed encomiabile commento sistematico in M. CAPECE,* Controlli difensivi: illegittimo il licenziamento basato su dati acquisiti antecedentemente all'insorgere del sospetto, *in* Il lavoro nella giurisprudenza, *anno 2025, fasc. 10, p. 915 ss.*

4.1. L'impostazione rigorosa del Garante *Privacy* sui tempi di conservazione

L'Autorità Garante per la Protezione dei Dati Personali, con l'intento di arginare le derive e prevenire la stratificazione occulta di archivi sterminati, è recentemente intervenuta in maniera drastica tramite due provvedimenti di rilievo storico, speculari fra di loro (i Provvedimenti nn. 243 e 250 del 2025). L'obiettivo precipuo del Collegio dell'*Authority* era quello di perimetrare in maniera del tutto rigorosa, certa e non equivocabile gli angusti limiti e la giustificazione causale della ritenzione sistematica di tali delicate informazioni informatiche.

La portata dell'intervento regolatorio emerge plasticamente nel caso analiticamente esaminato e vagliato dal Provvedimento n. 250. In tale congiuntura, il Garante ha sanzionato con estrema asprezza e senza mezzi termini l'amministrazione regionale della Lombardia, colpevole di aver posto in essere un trattamento massivo, continuativo e sistematico di conservazione occulta. La sanzione è scaturita dal fatto oggettivo che l'Ente lombardo conservava i *metadati* di posta elettronica dei dipendenti per un periodo assai cospicuo pari a 90 giorni, estendendo al contempo la ritenzione dei file di *log* relativi alla navigazione *internet* quotidiana all'esorbitante termine di 365 giorni.

Una siffatta persistenza e tenuta informativa dei *record* è stata censurata alla luce di una manifesta sproporzione teleologica. Attraverso le proprie Linee Guida di recente aggiornamento, l'Autorità aveva infatti ormai tracciato un confine netto, superato il quale scatta un *vulnus* strutturale. La conservazione cd. "fisiologica", ritenuta indispensabile ed essenziale per il mero mantenimento, l'ordinaria garanzia di operatività delle infrastrutture di *routing* aziendale e la pedissequa continuità qualitativa del servizio informatico (incluse le fisiologiche esigenze di *debug*, tracciamento degli errori e ripristino di sistema), non deve valicare o oltrepassare l'angusto termine di 21 giorni. Superata e infranta tale predeterminata soglia cronologica temporale, la passiva attività di memorizzazione digitale dei dati esteriori trasmoda surrettiziamente, slittando e trasformandosi da un'innocua e tecnica "esigenza infrastrutturale" a una forma di penetrante "controllo a distanza indiretto", capace di fotografare per intero la vita digitale del prestatore d'opera. È il superamento del tempo fisiologico a convertire l'esigenza informatica in monitoraggio umano.

Ne deriva, quale corollario sistematico, che, qualora il datore di lavoro nutra la fondata intenzione di protrarre e mantenere in vita tali immensi archivi ben oltre la barriera dei 21 giorni (ad esempio, paventando ipotetiche e future ragioni difensive), lo stesso è tenuto e obbligato, ai sensi del perentorio combinato disposto normativo discendente dagli artt. 4, comma 1, della citata Legge 300/1970 e dell'art. 114 del novellato Codice della Privacy (D.Lgs. 196/2003, in aderenza all'art. 88 del GDPR), a incamminarsi sui binari della trasparenza. Egli dovrà dunque stipulare il prescritto e vincolante accordo sindacale preventivo con le RSU/RSA ovvero, in via residuale, munirsi di formale autorizzazione amministrativa preventiva rilasciata per iscritto dall'Ispettorato[4].

4.2. Il bilanciamento tecnico: minimizzazione, *accountability* e *DPIA*

Sotto il prisma della sovrastante disciplina eurounitaria imperante in materia di *data protection*, giova ricordare che il GDPR non avalla in alcun modo un divieto assoluto, cieco o dogmatico al controllo per ragioni di sicurezza, ma piuttosto costruisce e incardina un ben più virtuoso e sfidante paradigma di

4. *Sulla perentoria e gravosa sanzione irrogata dal Garante della Privacy per evidente e patologico sforamento delle tempistiche ordinarie di conservazione massiva, si veda specificamente e in dettaglio Provvedimento Garante Privacy 29 aprile 2025, n. 250, analiticamente esaminato in L. D'ARCANGELO,* I limiti del Garante al controllo degli strumenti di lavoro, *in* Il lavoro nella giurisprudenza, *anno 2025, fasc. 11, p. 984 ss.*

responsabilizzazione giuridica. Al principio fondamentale di *accountability* (art. 5, par. 2, GDPR) si affianca, in maniera complementare e indissolubile, la stringente e ineluttabile necessità di perimetrare in modo analitico i rischi, operando a monte e preliminarmente la cosiddetta Valutazione d'Impatto (la cd. DPIA, esplicitamente sancita e imposta dall'art. 35 del GDPR), considerata l'intrinseca vulnerabilità sociale del prestatore di lavoro in seno all'organizzazione produttiva aziendale.

Laddove l'esigenza impellente di una conservazione più estensiva e cospicua dei metadati ritrovi e reperisca un suo solido, coerente e plausibile fondamento in virtù delle categoriche imposizioni di natura puramente securitaria discendenti, ad esempio, dalle previsioni precettive della direttiva NIS2, essa deve comunque incanalarsi rigorosamente verso binari leciti. Questa traduzione tecnica deve obbligatoriamente sostanziarsi nell'attuazione progettuale (*privacy by design* e *by default*) di misure tecniche e organizzative dal sapore strettamente minimizzante. Il datore non può sfuggire al principio sancito dall'art. 5 par. 1 lett. c) del Regolamento Europeo.

Come lucidamente delineato anche a corollario del parere dottrinale (M. Liotta) sul Provv. 243/2025[5], il datore di lavoro risulta integralmente gravato dell'onere ineludibile di approntare e implementare tempestivamente ogni possibile accorgimento tecnologico che consenta di ottemperare ai principi di minimizzazione e *privacy by design*. Le misure tecniche adottate devono evitare di rendere i dati massivamente tracciabili o indebitamente conservati oltre le tempistiche strettamente necessarie, non appena siano venute meno le immediate, stringenti ed incombenti urgenze informatiche di sicurezza ordinaria per le quali il log aveva inizialmente un senso sistematico.

L'architettura europea esige l'assenza di automatismi e scorciatoie interpretative: anche qualora l'impresa sia mossa dall'imperativo categorico di sventare o prevenire un devastante attacco tramite *malware*, le contromisure e i presidi difensivi tecnici adottati a salvaguardia devono categoricamente attestarsi su una dimensione e su un raggio strettamente pertinenti e funzionali alla reazione all'attacco cibernetico. Non è concesso, per difendere la rete o adempiere ai diktat della compliance europea della NIS2, sconfinare, scivolando nell'erroneo ed illecito abuso, tramite un sistematico spionaggio finalizzato all'esplorazione generalizzata, all'indicizzazione e all'archiviazione di tutti i contenuti, i *link* falliti e le corrispondenze personali e non lavorative che compongono il traffico digitale di rete dei propri lavoratori. Il monitoraggio si arresta lì dove comincia il privato.

5. Profili patologici: le conseguenze processuali dei controlli illegittimi

Cosa accade nel momento, patologico per antonomasia, in cui l'azienda o l'imprenditore decide di derogare deliberatamente o colposamente a questi rigidi parametri normativi (sia statutari che garantisti) al mero fine di acquisire ed estrapolare le stringenti prove necessarie a innescare e sostanziare un procedimento o un illecito disciplinare a carico del dipendente? Il cortocircuito normativo che si innesca sfocia inevitabilmente e inesorabilmente nella delicatissima dimensione processuale. La patologia genetica dell'acquisizione del dato o dell'informazione digitale non resta infatti confinata nel perimetro amministrativo e non si esaurisce nell'irrogazione di eventuali sanzioni irrogate dall'autorità indipendente, bensì si riverbera e travolge il cuore del processo del lavoro, intaccando le fondamenta dell'utilizzabilità

5. *Sull'esame e sui rilevantissimi e assai attuali profili di complessa interoperabilità pratica e normativa tra stringenti obblighi europei di cui alla direttiva NIS2 in tema di* cybersecurity *e tracciamento massivo e invisibile dei* metadati *dei dipendenti, nonché sull'imperatività assoluta sancita dal Provvedimento Garante n. 243/2025, si veda estensivamente e diffusamente in dottrina M. LIOTTA,* I dipendenti e il trattamento dei metadati: la cybersecurity e la tutela dei dati personali, *in* Giornale di diritto amministrativo, *2026, n. 3, p. 390 ss.*

della prova e conducendo in maniera fulminea alla successiva, inevitabile declaratoria di illegittimità del provvedimento espulsivo datoriale.

5.1. L'inutilizzabilità probatoria e l'illegittimità del licenziamento disciplinare

L'orientamento ormai granitico della Suprema Corte non lascia alcuno spazio interpretativo e si staglia in maniera lapidaria e inflessibile: qualsivoglia prova materiale (siano esse plurime corrispondenze estrapolate da *account* privati aziendali, intere catene di e-mail lette, scansionate o copiate da periti informatici in palese difetto di una pregressa e trasparente *policy* aziendale sul corretto utilizzo degli strumenti in comodato, o ancora miriadi di preziose informazioni disciplinari tratte a piene mani da occulti e persistenti tracciamenti di navigazione esorbitanti i ristretti e inderogabili limiti temporali stabiliti di concerto dal Garante per la Privacy) deve essere irrimediabilmente spunta dal processo.

Nel momento in cui si accerta storicamente, tramite le rituali indagini del CTU, che la fonte di tale prova si è andata formando o è stata estrapolata in spregio o in palese e stridente contrasto con il coacervo sistematico delle rigide disposizioni poste dall'art. 4 dello Statuto dei Lavoratori, dall'art. 8 della medesima legge e con le vincolanti normative generali di salvaguardia eurounitaria delineate dal GDPR e dai conseguenti interventi attuativi del Garante nazionale, detta "prova" patisce senza appello la radicale sanzione della più totale e incondizionata inutilizzabilità processuale. Il precetto stabilito dall'art. 2-*decies* del Codice Privacy sancisce a chiare lettere e con formula draconiana l'inutilizzabilità totale e assoluta dei dati personali oggetto di qualsivoglia trattamento sistematico o occasionale che si sia estrinsecato in aperta violazione e palese inosservanza della preordinata disciplina statale ed europea di protezione.

La ricaduta sul piano sostanziale giuslavoristico è del tutto palese, lampante e deflagrante[6]. Un pur apparentemente ben motivato licenziamento per giusta causa (ex art. 2119 cod. civ.) ovvero per giustificato motivo soggettivo, che sia stato materialmente intimato e strutturato in via fondativa sulla scorta esclusiva di report periodici, file di *log* retrospettivi o *metadati* massivi acquisiti subdolamente o abusivamente a seguito di una perizia informatica disposta solo successivamente ma inerente, come nel caso esaminato nell'ordinanza poc'anzi citata, all'intero trascorso del dipendente prima ancora che venisse in essere ed emergesse il necessario, oggettivo e preesistente "fondato sospetto" su fatti già di rilievo, è fatalmente destinato al disconoscimento e al totale travolgimento giudiziale.

Come è stato lucidamente, puntualmente ed esaustivamente evidenziato e argomentato dalla migliore e più attenta dottrina formatasi in questa fluida materia nel corso degli ultimi e recenti decenni, la profonda e imprescindibile dimensione "umana" del rapporto di lavoro subordinato non può in alcuna fattispecie essere svilita, annientata o soverchiata dalle crescenti pulsioni panottiche alimentate dalle nuove, potentissime tecnologie di monitoraggio e controllo capillare. Né l'indubbia, seppur puramente civilistica ed economica, istanza securitaria posta alla base delle moderne esigenze di continuità operativa del *management* d'impresa può arbitrariamente assurgere, nel delicato perimetro del nostro bilanciato ordinamento costituzionale, a inedita ed aberrante "esimente" di natura giurisprudenziale idonea a fungere da scudo per indiscriminati, penetranti e continui accessi e sondaggi telematici della sfera più intima del lavoratore[7]. Le conseguenze di tali atti sproporzionati e illeciti si rivelano sempre distruttive non soltanto per l'indagine stessa, ma inficiano integralmente la legittimità costitutiva di ogni successiva

6. *A questo delicatissimo proposito, la Cassazione del lavoro non arretra di un singolo millimetro nell'alveo della sua rigorosa giurisprudenza difensiva: per l'inoppugnabile inutilizzabilità in ambito probatorio e processuale e il strettamente e funzionalmente correlato concorso nel grave delitto di accesso abusivo al sistema informatico finalizzato alla repressione di specifiche intrusioni e incursioni datoriali in* account *e domini telematici rigidamente protetti, si veda Cass. Civ. Sez. Lav. Sent., 29 agosto 2025, n. 24204, a cura e nota di L. D'ARCANGELO.*

determinazione o comminazione disciplinare, costringendo l'impresa alle non irrilevanti conseguenze in tema di reintegrazione o risarcimento del danno previste dall'art. 18 dello Statuto dei Lavoratori e dalle più recenti previsioni normative in tema di tutele crescenti.

6. Considerazioni conclusive: verso un equilibrio sostenibile

Alla luce dell'incessante e rapida evoluzione tanto legislativa quanto pretoria e regolamentare sin qui minuziosamente esplorata e sviscerata, la fuorviante ed errata narrazione di stampo eccessivamente manicheo che vedrebbe in perenne, drammatica e insanabile antitesi e collisione l'intangibile e sacra libertà del singolo lavoratore, da un lato, e la vitale e strategica messa in sicurezza cibernetica dell'intera struttura e architettura dell'impresa aziendale, dall'altro, deve essere inesorabilmente destituita di ogni e qualsivoglia residuale fondamento sistematico. L'ordinamento esige, al contrario, che l'esercizio e l'espressione di entrambe tali istanze, pacificamente tutelate da norme e precetti di rango costituzionale e convenzionale (il diritto d'iniziativa economica ex art. 41 Cost. da un lato, la dignità, la libertà personale e la segretezza delle comunicazioni degli artt. 2, 13 e 15 Cost. dall'altro), vengano ricondotte alacremente e saldamente nei più quieti, equilibrati e rigorosi binari del contemperamento proporzionato e di un armonico e non eludibile bilanciamento.

A fondato giudizio di chi scrive, le rigide e prescrittive, nonché spesso contestate, tempistiche stringenti in tema di ritenzione dei *log* minuziosamente calibrate e dettate dall'Autorità Garante per la Protezione dei Dati Personali (nel suo più recente statuto regolatorio e giurisprudenziale delineato con i Provvedimenti nn. 243 e 250 del 2025), così come il granitico orientamento in ordine all'esigenza ineliminabile di una specifica e fattuale "preventiva genesi fenomenica del sospetto" lucidamente elaborata dalla Corte di Cassazione, non costituiscono in alcuna maniera una *deminutio* né tendono a comprimere indebitamente o a menomare fittiziamente il fisiologico e ordinario potere ispettivo e direttivo riservato al datore di lavoro. Al contrario, queste formidabili demarcazioni normative ed ermeneutiche, lungi dal rappresentare dei meri fardelli burocratici, ne elevano tangibilmente, e doverosamente, il livello sistematico e lo straordinario tasso di civiltà giuridica applicata.

La prospettiva di una fruttuosa coabitazione tra esigenze ispettive ed estrinsecazione della dignità professionale passa, dunque, unicamente per il canale e il crisma della limpida trasparenza e dell'assunzione formale di responsabilità condivisa. Il tempestivo e consapevole ricorso a una solida, palese ed inequivocabile *policy* aziendale di stampo prettamente e convintamente preventivo, se posta in aperta e matura sinergia con la feconda stipula di mirati e lungimiranti accordi collettivi di secondo livello che traccino in modo lapalissiano e trasparente l'orizzonte, le concrete modalità, gli specifici *trigger* attivanti e le coordinate spaziali e temporali di impiego dei complessi sistemi e applicativi informatici e di controllo, rappresenta indiscutibilmente, alla prova dei fatti e dell'esperienza forense, l'unico ed esclusivo *driver* organizzativo che si riveli concretamente capace, in ultima analisi, di scongiurare sul nascere possibili nullità processuali in sede di contenzioso giuslavoristico. Tale virtuosa architettura di procedure partecipate si erge, contestualmente, a primario scudo atto a tutelare in via eminentemente e

7. *Si veda diffusamente in merito V. MAIO,* La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica, *in* Arg. dir. lav., *anno 2015, p. 1199 ss.* ***Bibliografia*** *M. CAPECE,* Controlli difensivi: illegittimo il licenziamento basato su dati acquisiti antecedentemente all'insorgere del sospetto, *in Il lavoro nella giurisprudenza, 2025, 10, 915 ss. L. D'ARCANGELO,* Controlli difensivi, inviolabilità delle e-mail personali e inutilizzabilità processuale, *in Il lavoro nella giurisprudenza, 2026, 3, 270 ss. L. D'ARCANGELO,* I limiti del Garante al controllo degli strumenti di lavoro, *in Il lavoro nella giurisprudenza, 2025, 11, 984 ss. M. LIOTTA,* I dipendenti e il trattamento dei metadati: la cybersecurity e la tutela dei dati personali, *in Giornale di diritto amministrativo, 2026, 3, 390 ss. V. MAIO,* La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica, *in Argomenti di diritto del lavoro, 2015, p. 1199 ss. M. MARAZZA,* I controlli a distanza del lavoratore di natura difensiva, *in Controlli a distanza e tutela dei dati personali del lavoratore, Torino, 2017, 38 ss.*

modernamente proattiva l'integrità profonda dell'inestimabile patrimonio informativo dell'azienda dinanzi alle crescenti e minacciose insidie della mutevole e incerta epoca digitale contemporanea.