

La comunicazione digitale nel lavoro subordinato tra regole di conservazione dei metadati e tutela della segretezza



Alessandra Ingrao

Associata di Diritto del lavoro
Università degli Studi di Milano

Marco Peruzzi

Associato di Diritto del lavoro
Università degli Studi di Verona

Abstract: La comunicazione digitale del lavoratore — dall'e-mail alle chat fino ai social network — rappresenta oggi uno snodo decisivo nel rapporto tra poteri datoriali e diritti fondamentali. L'analisi ricostruisce le linee di frizione e convergenza tra diritto del lavoro e GDPR, anche alla luce delle indicazioni del Garante e dell'integrazione di sistemi di intelligenza artificiale nelle infrastrutture aziendali. Viene quindi esaminata la tutela costituzionale della segretezza della corrispondenza e l'utilizzabilità probatoria delle comunicazioni digitali nel procedimento disciplinare, alla luce dell'evoluzione giurisprudenziale sull'art. 15 Cost., con l'obiettivo di delineare un equilibrio tra poteri organizzativi e diritti fondamentali.

Parole chiave: Metadati della posta elettronica - Controlli a distanza - Segretezza della corrispondenza - Protezione dei dati personali - Utilizzabilità probatoria delle comunicazioni digitali - Monitoraggio algoritmico e intelligenza artificiale

Digital Communication in employment relations: Between Metadata Retention Rules and Privacy Protection

Employees' digital communication — from email and messaging apps to social networks — has become a pivotal point of tension in the relationship between managerial powers and fundamental rights. The analysis reconstructs the areas of convergence and friction between labour law and the GDPR, also in light of the guidance issued by the Italian Data Protection Authority and the integration of artificial intelligence systems into workplace infrastructures. It then examines the constitutional protection of secrecy of correspondence and the evidentiary admissibility of digital communications in disciplinary proceedings, in light of the evolving case law on Article 15 of the Italian Constitution, with a view to defining a balanced framework between managerial powers and fundamental rights

Keywords: Email metadata - Remote monitoring of employees - Secrecy of correspondence - Personal data protection - Evidentiary admissibility of digital communications - Algorithmic monitoring and artificial intelligence:

ISSN: 3103-4721

Copyright © 2026 Alessandra Ingrao e Marco Peruzzi

The text is licensed under the Creative Commons BY 4.0 International License <https://creativecommons.org/licenses/by/4.0/>

SOMMARIO. 1. Introduzione. — 2. La posta elettronica tra limiti al controllo a distanza e protezione dei dati personali: impostazione e criticità delle indicazioni del Garante sui metadati. — 2.1. Una riflessione a partire dal confronto con le indicazioni del Garante sui metadati, nella prospettiva dell’insediamento di sistemi di IA in azienda. — 3. Segretezza della corrispondenza e rilievo probatorio delle comunicazioni digitali nel rapporto di lavoro. — 3.1. I percorsi della giurisprudenza di merito. — 3.2. La segretezza della corrispondenza digitale nella interpretazione della giurisprudenza della Corte Costituzionale e della Cassazione. — 3.3. I recenti arresti della Corte di Cassazione. — 4. Una proposta interpretativa per sciogliere il nodo irrisolto dei post sui profili chiusi dei social network. Verso una “segretezza ragionevole” della comunicazione digitale.

1. Introduzione

La comunicazione digitale del lavoratore — dalla posta elettronica alle chat di messaggistica, fino ai social network — è oggi uno snodo decisivo del rapporto tra poteri datoriali e diritti fondamentali dei lavoratori subordinati.

In ambito aziendale, l’e-mail è al contempo strumento di lavoro e canale di scambio potenzialmente riservato; senza considerare che la sua infrastruttura tecnica genera contenuti e dati “esteriori” (log e metadati) che possono rendere l’attività lavorativa osservabile e, quindi, controllabile dal datore di lavoro. Per questa ragione, la disciplina della posta elettronica rappresenta un terreno privilegiato per mettere a fuoco l’intreccio tra l’art. 4 St. lav. sui controlli a distanza e la protezione dei dati personali: le informazioni ricavabili dall’uso degli strumenti digitali, quando riferibili anche indirettamente al dipendente, integrano dati personali, e la loro raccolta e conservazione impongono trasparenza, proporzionalità e limiti coerenti con le garanzie statutarie. Su questo sfondo, il § 2 ricostruisce le linee di frizione e convergenza tra diritto del lavoro e GDPR, anche alla luce delle indicazioni del Garante sui metadati e delle nuove potenzialità connesse all’integrazione di sistemi di intelligenza artificiale nelle infrastrutture aziendali: l’attenzione si sposta dal “mezzo” alle finalità del trattamento e ai rischi di una trasformazione degli strumenti di lavoro in vettori di monitoraggio.

Il § 3 di questo scritto sposta poi il baricentro dal tema del controllo datoriale a quello, distinto ma contiguo, della tutela costituzionale della segretezza della corrispondenza e del rilievo probatorio delle comunicazioni digitali nel procedimento disciplinare e nel processo. La questione diventa se, e a quali condizioni, e-mail e messaggi scambiati in chat ove il datore di lavoro non è un destinatario diretto, possano essere conosciuti e utilizzati dallo stesso (ad esempio perché “inoltrati” da un collega). Ci si interroga, inoltre,

sulla distinzione, ai fini della disciplina sulla utilizzabilità disciplinare, tra tali comunicazioni a destinatario circoscritto (mail, chat, ecc.) e i contenuti diffusi dai lavoratori in ambienti digitali strutturalmente più esposti, come i social network. In questa prospettiva, l'analisi segue l'evoluzione giurisprudenziale che, aggiornando la nozione di corrispondenza ai sensi dell'art. 15 Cost., ridefinisce i confini tra comunicazione riservata e comunicazione potenzialmente pubblica, incidendo direttamente sulle possibilità d'azione del potere disciplinare.

2. La posta elettronica tra limiti al controllo a distanza e protezione dei dati personali

La disciplina dell'utilizzo della posta elettronica da parte del lavoratore in ambito aziendale ha da sempre rappresentato un punto di osservazione privilegiato per analizzare — e mettere sotto tensione — l'interazione tra il sistema delle garanzie statutarie in materia di controllo a distanza e la normativa in tema di protezione dei dati personali¹. È sufficiente rilevare come la riformulazione dell'art. 4 St. lav. operata nel 2015 riproduca, nel dettato del terzo comma, alcune indicazioni enucleate nelle Linee guida in materia di posta elettronica e Internet adottate dal Garante per la protezione dei dati personali nel 2007. In tale sede, infatti, l'Autorità aveva evidenziato come, quale diretta proiezione del principio di correttezza del trattamento — secondo cui le caratteristiche essenziali dello stesso devono essere portate a conoscenza dei lavoratori — «grav[i] sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli»².

L'interazione tra disciplina lavoristica e protezione dei dati personali si impone, anzitutto, in ragione del fatto che le informazioni relative all'attività lavorativa, ove intercettate mediante strumenti idonei a consentire un controllo a distanza, costituiscono dati personali ai sensi del GDPR ogniqualvolta il lavoratore interessato risulti anche solo indirettamente identificabile.

L'ampia nozione di dato personale accolta dall'art. 4, n. 1, GDPR attrae, infatti, nel proprio perimetro qualsiasi informazione che possa riguardare

¹ Sul tema dell'interazione tra art. 4 St. lav. e normativa in materia di protezione dei dati personali, cfr. *ex multis* (Bellavista 2023), (Proia 2022), (Trojsi 2022), (Sartori 2020), (Ingrao 2018), (Nuzzo 2018), (Tullini 2017), (Califano 2017), (Marazza 2016).

² Garante per la protezione dei dati personali, *Linee guida per posta elettronica e internet*, n. 13 del 01.03.2007, par. 3.1. Cfr. al riguardo (Del Conte 2007), (Alvino 2014). Il profilo evidenziato nel testo è segnalato da (Marazza 2016).

una persona fisica non soltanto in ragione del suo contenuto intrinseco, ma anche in funzione della finalità del trattamento o del potenziale impatto che essa è idonea a produrre sull'interessato, purché sia possibile tracciare o ricostruire il collegamento tra l'informazione e il soggetto cui essa si riferisce, tenendo conto di tutti i mezzi ragionevolmente utilizzabili alla luce dell'evoluzione tecnologica³.

Ne consegue che assumono natura personale anche i dati relativi all'uso di una macchina o di uno strumento di lavoro, riconducibili a un determinato lavoratore anche solo mediante l'incrocio con i dati dei turni, nella misura in cui risultino potenzialmente utilizzabili per valutarne la produttività, le prestazioni o, più in generale, per l'adozione di decisioni o misure incidenti sulle sue condizioni di lavoro. Rientrano in tale nozione, pertanto, per restare nella prospettiva d'analisi che ci occupa, tanto le informazioni direttamente attinenti all'attività comunicativa del dipendente (dalle battute di tastiera al te-

³ Nella sentenza *EDPS vs SRB* (C. giust.04.09.2025, C-413/23), la Corte di giustizia ha chiarito che, ai fini della qualificazione di un'informazione come dato personale, non rileva l'esistenza in sé di informazioni aggiuntive detenute da terzi potenzialmente idonee alla re-identificazione, bensì la possibilità concreta e ragionevolmente probabile, avuto riguardo alle circostanze del caso, che il titolare del trattamento o un terzo dispongano di, o possano accedere a, mezzi idonei a identificare la persona fisica. Ne discende che il requisito dell'anonimizzazione non deve necessariamente sussistere in modo assoluto ed *erga omnes*, potendo invece assumere carattere relativo, ossia essere riferito a determinati soggetti che, in concreto, anche alla luce del contesto normativo e organizzativo in cui il trattamento si colloca — inclusi eventuali vincoli contrattuali che impediscano lo scambio o l'incrocio di informazioni tra soggetti diversi — non dispongono né possono ragionevolmente disporre dei mezzi per identificare l'interessato. Tale impostazione trova oggi un significativo riscontro anche a livello normativo nella proposta *Omnibus* digitale della Commissione europea (COM(2025) 837 final del 19.11.2025, art. 3, par. 1), che, intervenendo sulla relativa disposizione del GDPR, si pone a recepimento di questa lettura funzionale e relazionale della nozione di dato personale. La modifica proposta nell'*Omnibus* è stata fortemente contestata dal Comitato europeo per la protezione dei dati (EDPB) e dal Garante europeo della protezione dei dati (EDPS), che nell'opinione congiunta del 10.02.2026 rilevano, anzitutto, si tratti di «una codificazione selettiva» volta a recepire «soltanto un singolo elemento tratto da una sola sentenza» senza il necessario contesto e senza la prospettiva dell'intero corpus giurisprudenziale della Corte (par. 15). Ritengono altresì che la proposta non rifletta accuratamente quanto detto nella pronuncia *EDPS vs SRB*, in particolare nell'ultima frase, in cui si specifica che «tali informazioni non diventano dati personali per tale entità per il solo fatto che un potenziale destinatario successivo disponga di mezzi ragionevolmente suscettibili di essere utilizzati per identificare la persona fisica cui le informazioni si riferiscono». Nella citata sentenza, la Corte ha invece confermato che «dati altrimenti impersonali possono acquisire natura personale quando sono messi a disposizione di un destinatario (qualsiasi destinatario) che disponga di mezzi ragionevolmente suscettibili di essere utilizzati per identificare un interessato. La CGUE ha confermato che, in tali casi, tali dati costituiscono dati personali sia per il destinatario sia, indirettamente, per l'entità che li mette a disposizione di quest'ultimo» (par. 16 dell'Opinione congiunta; parr. 84 e 85 della pronuncia).

sto di una e-mail), quanto gli elementi tecnici che accompagnano o documentano la comunicazione: dalle intestazioni necessarie al trasporto del messaggio (c.d. *envelope*: mittente e destinatario, informazioni di instradamento, identificativi di consegna), fino alle informazioni automaticamente registrate nei *log* dei sistemi server di gestione e smistamento della posta elettronica (mittente, destinatario, orari, server coinvolti, dimensioni e stato della consegna).

In secondo luogo, se, da un lato, le informazioni raccolte attraverso uno strumento che consente il controllo a distanza sono da tutelare ai sensi del GDPR, dall'altro, lo stesso art. 4 St. lav. si configura come fonte del medesimo sistema normativo di tutela. Esso costituisce, segnatamente, una delle «norme più specifiche» dirette ad assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro, ai sensi dell'art. 88 GDPR⁴. La sua violazione incide, quindi, sulla liceità del trattamento dei dati personali raccolti e/o trattati mediante lo strumento installato senza rispetto delle garanzie statutarie.

Su un piano ulteriore, ma strettamente connesso, il fatto che il dato sia raccolto tramite uno strumento idoneo a consentire il controllo a distanza dell'attività lavorativa assume rilievo, per il GDPR, anche sotto il profilo dell'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati (DPIA). Ai sensi dell'art. 35, par. 4, GDPR, infatti, il Garante per la protezione dei dati personali, con il provvedimento n. 467/2018 (All. 1), ha incluso tra i trattamenti soggetti obbligatoriamente a DPIA quelli «effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici [...] dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti». Massima espressione dell'approccio *risk-based* e del connesso principio di *accountability*, tale processo impone di verificare la necessità e la proporzionalità dei trattamenti rispetto alle finalità perseguite, di valutare i rischi per tutti i diritti e le libertà degli interessati, nonché di indicare le misure tecniche e organizzative previste per affrontare tali rischi e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati. Di centrale rilievo, ai fini del discorso qui sviluppato, è la previsione secondo cui «se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti» (art. 35, par. 9, GDPR). Le linee guida europee invitano a interpretare tale disposizione nel senso che il titolare è tenuto a richiedere il parere degli interessati o dei loro rappresentanti, salvo che ritenga tale consultazione non appropriata (ad esempio perché spropor-

⁴ Con comunicazione del 03.09.2019, l'Italia ha inviato alla Commissione una tabella di sintesi contenente, per quanto attiene all'attuazione a livello interno dell'art. 88 GDPR, il riferimento ad alcune disposizioni del d.lgs. n. 196/2003, in particolare l'art. 114, che fa salva la normativa sul controllo a distanza, rinviando all'art. 4 St. lav.

zionata, impraticabile o idonea a compromettere la riservatezza dei piani aziendali), dovendo però documentare puntualmente le ragioni della mancata consultazione. Analogamente, qualora il parere sia stato richiesto ma il titolare decida di discostarsene, egli è tenuto a motivare e documentare tale scelta⁵.

È significativo osservare come la Direttiva (UE) 2024/2831 in materia di lavoro su piattaforma digitale, all'art. 8, introduca per tale settore una disciplina rafforzata, che avvicina il processo di valutazione del rischio della DPIA alla dimensione partecipata che connota il sistema prevenzionistico in tema di salute e sicurezza: la consultazione delle rappresentanze diviene obbligatoria e la valutazione deve essere messa a disposizione delle stesse. Si tratta di una soluzione che certamente, a livello normativo, è circoscritta al perimetro applicativo della direttiva. Deve tuttavia tenersi in considerazione che la stessa potrebbe essere replicata, in altri ambiti, attraverso la contrattazione collettiva, facendo leva sull'art. 88 GDPR quale base giuridica per introdurre per via pattizia garanzie procedurali ulteriori nel contesto del rapporto di lavoro.

Tornando ora specificamente al trattamento dei dati derivanti dall'uso della posta elettronica, giova anzitutto ricordare che nelle citate linee guida del 2007, il Garante evidenziava che il contenuto della posta elettronica del lavoratore, così come i dati esteriori delle comunicazioni e i file allegati, sono assistiti da garanzie di segretezza tutelate anche a livello costituzionale (sul punto v. anche *infra*). In tal senso, per dirla con le parole delle linee guida europee, «il controllo della corrispondenza di un lavoratore [...] può ritenersi necessario unicamente in circostanze eccezionali»⁶. In questo quadro, la liceità del trattamento dei dati richiede, a monte, l'adozione di un duplice ordine di misure: da un lato, policy aziendali e informative idonee a evitare la formazione, in capo al lavoratore, di una legittima aspettativa di riservatezza e confidenzialità rispetto all'uso degli strumenti di comunicazione aziendali; dall'altro, accorgimenti organizzativi e tecnici volti a prevenire trattamenti in violazione dei principi di pertinenza e non eccedenza, nonché inutili intrusioni nella sfera personale dei lavoratori.

Tali indicazioni trovano traduzione in misure operative concrete, quali, a titolo esemplificativo: la predisposizione di caselle e-mail condivise tra più lavoratori, riferite a funzioni aziendali e non a soggetti individuali; l'assegna-

⁵ Gruppo di lavoro sulla protezione dei dati – Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati*, wp248rev., adottate il 04.04.2017, come modificate e adottate da ultimo il 04.10.2017.

⁶ Gruppo di lavoro sulla protezione dei dati – Articolo 29, *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, adottato il 29.05.2002, WP 55, p. 13.

zione a ciascun dipendente di un indirizzo di posta elettronica aggiuntivo ad uso privato, distinto da quello professionale, destinato a configurare uno spazio personale al quale il datore di lavoro non può accedere in alcuna circostanza; nonché la previsione di meccanismi di delega, in forza dei quali il lavoratore individua un altro dipendente (fiduciario) incaricato di verificare i messaggi ricevuti e di inoltrare al titolare del trattamento quelli strettamente rilevanti per lo svolgimento dell'attività lavorativa, in caso di assenza improvvisa o prolungata e di improrogabili esigenze organizzative.

A ciò si aggiungono le raccomandazioni relative all'applicazione del principio di proporzionalità e alla graduazione dei controlli: deve essere, per quanto possibile, privilegiato un controllo preliminare su dati aggregati, riferiti all'intera struttura organizzativa o a sue specifiche aree. Il controllo anonimo può eventualmente concludersi con un avviso generalizzato circa un utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite, anche limitatamente ai dipendenti afferenti all'area o al settore interessato dall'anomalia. In assenza di ulteriori irregolarità, non risulta di regola giustificato procedere a controlli su base individuale.

2.1. Una riflessione a partire dal confronto con le indicazioni del Garante sui metadati, nella prospettiva dell'inserimento di sistemi di IA in azienda

Alle linee guida dedicate ricordate nel precedente paragrafo è utile affiancare le precisazioni offerte dal Garante in merito alla qualificabilità del sistema di posta elettronica in termini di strumento di lavoro ai fini dell'operatività dell'art. 4, comma 2, St. lav. che, come noto, prevede che lo strumento sia dato in dotazione al prestatore previa adeguata informazione e senza necessità di un accordo sindacale o, in sua assenza, di un'autorizzazione amministrativa dell'Ispettorato.

All'indomani della riforma della disposizione statutaria del 2015, il Garante è intervenuto sull'ambito di applicazione della deroga, rilevando come ai fini della qualificazione di uno strumento come di lavoro sia necessario verificarne la stretta funzionalità alla prestazione lavorativa, anche sotto il profilo della sicurezza. In tale prospettiva, ha richiamato espressamente, come esempio, «il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale)», con la precisazione che a ricadere nell'ambito del secondo comma sono anche «i sistemi e le misure che [...] consentono il fisiologico e sicuro funzionamento» dello strumento di lavoro, in quanto ne «costituiscono parte integrante». Tra questi: i «sistemi di *logging* per il corretto esercizio del servizio di posta elettronica, con conservazione

dei soli dati esteriori, contenuti nella cosiddetta “*envelope*” del messaggio, per una breve durata non superiore comunque ai sette giorni⁷. È sì vero che quest’ultima precisazione presenta *in nuce* alcuni elementi che il Garante ha sviluppato, poi, nel contestato Documento di indirizzo di dicembre 2024/giugno 2025, ragionando *a contrario* con riguardo alla disciplina dei metadati di sistema. Tanto più che già qui si segnala la necessità che addirittura gli stessi dati di *envelope* siano conservati per non più di una settimana. Pare, tuttavia, significativo notare come all’interno del documento del 2016 sia comunque ancora individuata come *discrimen* ai fini dell’applicazione della deroga la funzionalità dello strumento alla resa della prestazione lavorativa, ovvero la funzionalità di eventuali strumenti/misure collegati a consentirne il fisiologico e sicuro funzionamento. Tale funzionalità viene esclusa solo se il sistema *software* — che consente il controllo a distanza — opera «con modalità non percepibili dall’utente (c.d. in *background*) e in modo del tutto indipendente rispetto alla normale attività dell’utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente) operazioni di “monitoraggio”, “filtraggio”, “controllo” e “tracciatura” costanti ed indiscriminati degli accessi a internet o al servizio di posta elettronica»⁸.

Il profilo è centrale perché, nel Documento di indirizzo sui metadati della posta elettronica⁹, il Garante per la protezione dei dati personali non mette in discussione che i metadati di sistema — al pari di quelli ricavabili dall’*envelope* — siano informazioni fisiologicamente generate dall’utilizzo del servizio di posta elettronica e, in primo luogo, funzionali ad «assicurare il funzionamento delle infrastrutture» dello strumento. Ciò emerge con particolare evidenza nel passaggio in cui l’Autorità analizza la proiezione di tale funzione sotto il profilo del principio di conservazione dei dati, richiedendo che per detta finalità i dati non siano conservati per più di 21 giorni. Il Garante, tuttavia, concentra e circoscrive la propria attenzione su due profili, strutturando attorno ad essi il proprio ragionamento. Da un lato, insiste sul fatto che

⁷ Garante per la protezione dei dati personali, *Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro*, provvedimento n. 303 del 13.07.2016, par. 4.3.

⁸ Provvedimento n. 303 del 13.07.2016 - *Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro*.

⁹ Provvedimento n. 364 del 06.06.2024 - *Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*. Il Documento segue il periodo di consultazione pubblica avviata dopo le richieste di chiarimento avanzate rispetto al precedente Provvedimento del n. 642 del 21.12.2023. Come evidenziato da (Tebano 2024), rimane d’altra parte «inalterata l’insolita prospettiva adottata dal Garante per risalire alla natura dello strumento» (p. 292). Rispetto al provvedimento conseguentemente adottato dal Garante nel confronto della Regione Lombardia (n. 243 del 29.04.2025), cfr. (D’Arcangelo 2025).

la raccolta di tali informazioni avvenga «indipendentemente dalla percezione e dalla volontà dell'utilizzatore». È una caratteristica che connota specificamente i metadati registrati nei *log* dei server di gestione e smistamento della posta, distinguendoli dalle informazioni contenute nell'*envelope*, che, invece, sottolinea il documento, rimangano «sotto l'esclusivo controllo dell'utente» e «nella disponibilità dell'utente/lavoratore, all'interno della casella di posta elettronica attribuitagli». Dall'altro lato, individua come dirimente il fatto che, pur essendo originariamente raccolti per una funzione di supporto tecnico fisiologico al funzionamento del sistema, tali dati, per le modalità della loro registrazione e conservazione, possano potenzialmente prestarsi al perseguimento di finalità diverse e ulteriori rispetto a quelle strettamente tecniche che ne giustificano la generazione.

Se, dunque, nel documento del 2016 rimaneva ancora decisivo, ai fini dell'esclusione dal concetto di “strumento di lavoro”, il fatto che il funzionamento e l'impiego del sistema fossero del tutto indipendenti dall'attività del lavoratore e privi di qualunque impatto o interferenza su di essa, nel successivo documento di indirizzo si assiste a un passaggio concettuale diverso.

Emerge, infatti, una stretta convergenza tra la funzione per cui lo strumento è stato inserito e installato nell'organizzazione datoriale e le finalità con cui sono utilizzati successivamente i dati raccolti attraverso di esso. Come sottolineato in dottrina, il Garante «passa, con eccessiva disinvoltura, dalla funzione dello strumento alla funzione della conservazione» (Tebano 2024, p. 292). La funzionalità dello strumento può dirsi collegata alla resa della prestazione, ai fini dell'art. 4, comma 2, St. lav., soltanto nella misura in cui le finalità del trattamento dei dati generati restino circoscritte alla stretta operatività fisiologica dello strumento stesso (con corrispondente delimitazione dei tempi di conservazione, nel caso dei metadati 21 giorni).

Laddove, invece, la base giuridica del trattamento includa finalità ulteriori — ancorché in sé legittime — lo strumento, pur continuando a essere utilizzato dal lavoratore per rendere la prestazione, cessa di essere “solo” strumento di lavoro. In virtù della multifunzionalità che le finalità del trattamento dei dati raccolti attraverso di esso finiscono per imprimere allo strumento, esso fuoriesce dall'ambito di applicazione della deroga e diventa soggetto alle garanzie procedurali (autorizzazione sindacale o amministrativa) di cui all'art. 4, comma 1, St. lav.

Si tratta di una linea di lettura che trova riscontro in dottrina, laddove alcuni autori ritengono che la polifunzionalità dello strumento, a prescindere dalla sua immediata finalizzazione alla resa della prestazione lavorativa, ne determini una «proiezione superindividuale», con conseguente sconfinamento in una più ampia funzione di carattere organizzativo-produttivo, tale da trascinarlo al di fuori dell'ambito di applicazione della deroga. In questa prospettiva, tali autori rilevano che, quanto più si diffonderanno e si consoli-

deranno tecnologie sofisticate strutturalmente idonee ad abilitare dette polifunzionalità¹⁰, tanto più risulterà circoscritto il novero delle ipotesi cui la deroga potrà applicarsi, pena il rischio di trasformare gli strumenti di lavoro in un vero e proprio «cavallo di Troia del controllo tecnologico digitale» (Sartori 2020, p. 246).

Si ritiene, tuttavia, che l'operazione interpretativa compiuta dal Garante nel raccordo tra garanzia statutaria e principi di protezione dei dati personali realizzi un'osmosi tra i due sistemi normativi, dando luogo a un indebito condizionamento bidirezionale.

È certamente vero che la legittimità del trattamento dei dati personali raccolti attraverso uno strumento di lavoro risulta condizionata, a monte, dal rispetto delle garanzie statutarie previste in sede di installazione dello strumento stesso, quali fonti di norme speciali in materia di privacy dei lavoratori. Appare invece discutibile ritenere, in via speculare, che le condizioni che legittimano, a valle, l'utilizzo del dato raccolto, ai sensi del GDPR, possano risalire il cordone normativo fino a conformare anche le condizioni che legittimano l'installazione dello strumento di raccolta a norma dell'art. 4 St. lav.

Occorre, infatti, mantenere distinti i due piani e i due momenti, il primo riferito all'apprestamento delle garanzie che filtrano l'introduzione nell'organizzazione di uno strumento potenzialmente idoneo alla raccolta di dati, anche personali, il secondo all'individuazione della base giuridica di liceità del trattamento del dato così raccolto.

Ai fini dell'applicazione della deroga di cui al secondo comma, ciò che rileva non dovrebbe essere tanto la modalità di utilizzo del dato raccolto, quanto piuttosto la funzione che giustifica l'inserimento nell'organizzazione datoriale dello strumento che apre alla raccolta di quel dato. Se tale funzione è la realizzazione della prestazione lavorativa – anche dal punto di vista legale, pensiamo all'obbligo di installare sistemi di geolocalizzazione sui veicoli addetti al trasporto di rifiuti pericolosi¹¹ – l'ingresso dello strumento be-

¹⁰ Cfr. (Tullini 2017a); l'Autrice segnala che «la rivoluzione digitale sembra in grado di svalutare e di rendere meno incisivo anche il debole meccanismo dell'autorizzazione sindacale o amministrativa ex art. 4, co. 1, St. lav.»; «nella *smart factory* pressoché tutti gli apparati tecnologici sono finalizzati alla realizzazione dell'attività lavorativa e 'utilizzati per rendere la prestazione', potendo così fruire dell'esonero dai vincoli posti all'esercizio del potere datoriale» (Tullini 2017b, p. 18).

¹¹ La lettura proposta nel testo si confronta quella più restrittiva adottata dall'INL. Anzitutto, nella nota prot. n. 831 del 28.01.2026, l'ispettorato ha sì escluso che l'installazione di sistemi di geolocalizzazione sui veicoli addetti al trasporto di rifiuti pericolosi, obbligatoria a norma dell'art. 188bis del d.lgs. n. 152/2006 alla lettera b), richieda l'autorizzazione sindacale/amministrativa a norma dell'art. 4 St. Lav., ma non perché attratta nell'ambito di applicazione della deroga di cui al secondo comma: la «prescrizione, prevista da una norma di carattere speciale, costituisce condizione di esercizio dell'attività d'impresa e pertanto si esula dal

neficerà della deroga; tornerà operativa, invece, la necessità di autorizzazione sindacale o amministrativa qualora la raccolta dell'informazione richieda il ricorso a uno strumento ulteriore. Una volta che il dato sia legittimamente raccolto, le modalità del suo utilizzo attengono alla disciplina della protezione dei dati personali e non risalgono sino ad incidere sulla fase di installazione dello strumento, che resta regolata in funzione della ragione organizzativa che, come detto, ne giustifica l'introduzione.

Proprio in tale prospettiva, non dovrebbero incidere sull'esigenza di impiego né sulla funzione dello strumento il tipo di tecnologia applicata, il suo livello di autonomia o la sua capacità computazionale, inferenziale o di gestione di relazioni e modelli complessi nei dati. Si pensi, in particolare, all'inserimento di sistemi di intelligenza artificiale nell'infrastruttura dei dispositivi, degli impianti e degli strumenti impiegati dal datore di lavoro e/o utilizzati dal lavoratore: si tratta di elementi che abilitano nuove potenzialità di utilizzo dei dati raccolti, ma che incidono su una fase logico-temporale successiva rispetto alla funzione organizzativa che giustifica, a monte, l'introduzione dello strumento, pur ora potenziato, "aumentato" o aggiornato a tecnologia avanzata.

Si pensi, per restare al caso della posta elettronica, a sistemi di IA assistiva integrati nel *client* di posta a supporto diretto dell'utente, in grado di fornire suggerimento di risposte, riformulazione o miglioramento del tono del discorso, sintesi di e-mail particolarmente articolate, traduzione automatica o rilevazione della priorità dei messaggi. Ovvero ancora a software di *workflow* che classificano automaticamente le e-mail (per cliente, pratica o grado di

campo di applicazione dell'art. 4 [St. lav.] in quanto non sussistono in capo al datore di lavoro le ragioni legittimanti previste dal comma 1, né il sistema gps può essere considerato uno strumento necessario alla prestazione lavorativa, che può essere svolta anche in assenza del sistema». Ancora, nella nota prot. n. 1511 del 16.02.2026, l'Ispettorato ha affermato che i sistemi di geolocalizzazione installati sulle dotazioni delle guardie giurate a norma del d.m. 269/2010, allegato A, non possono essere equiparati a strumenti di lavoro, posto che la stessa norma regolamentare contempla soluzioni alternative (ad es. l'attivazione di centri di comunicazione o centrali operative distaccati) e la scelta datoriale di utilizzare il gps risponde a finalità tecniche e organizzative (garantire ad es. interventi più tempestivi) riconducibili alle ragioni tipizzate di cui all'art. 4, primo comma, St. lav. Ne consegue la necessaria applicazione delle garanzie procedurali ivi previste. La lettura restrittiva dell'Ispettorato si differenzia da quella sviluppata dalla giurisprudenza di legittimità, secondo cui deve ritenersi riconducibile alla nozione di strumento di lavoro non solo quello indispensabile per assenza di alternative, ma anche quello funzionale a incrementare l'efficienza della prestazione. In tal senso, in Cass. 3.06.2024, n. 15391, la Suprema Corte ha affermato che «il telepass, se installato su auto aziendali destinate allo svolgimento di specifici servizi, si deve considerare uno strumento direttamente funzionale all'efficienza della singola prestazione, oltre che ormai fortemente compenetrato con essa nell'odierna pratica lavorativa, sicché il telepass così contestualizzato rientra nell'ambito applicativo del comma 2 dell'art. 4 L. n. 300/1970 novellato».

urgenza) e generano *task*, ovvero a sistemi di sicurezza finalizzati alla rilevazione di *phishing* e *malware* e alla prevenzione di fughe di dati.

Peraltro, appare significativo richiamare, nella costruzione di questa riflessione, l'osservazione formulata dalla Cassazione nella sentenza n. 15391/2024 in ordine alla qualificabilità del telepass quale strumento di lavoro: esso, infatti, oltre a essere «direttamente funzionale all'efficienza della singola prestazione», risulta «ormai fortemente compenetrato con essa nell'odierna pratica lavorativa». È lecito domandarsi se il medesimo inquadramento non possa essere prospettato anche con riferimento all'intelligenza artificiale, in un orizzonte temporale che potrebbe rivelarsi non solo prossimo, ma quasi immediato, alla luce dell'accelerazione con cui i sistemi di IA si innervano nei dispositivi e nei processi organizzativi e del progressivo processo di normalizzazione del loro utilizzo.

Il ragionamento può essere esteso ai dispositivi introdotti ai sensi dell'art. 4, comma 1, Stat. lav., quale, ad esempio, un sistema di registrazione delle telefonate di un call center, aggiornato mediante l'integrazione di un *co-pilot* basato su IA, destinato a supportare e guidare il lavoratore nella gestione del cliente, anche attraverso forme di *sentiment analysis* di quest'ultimo. Analogamente si pensi a un impianto di videocamere già introdotte per finalità di tutela della salute e sicurezza dei lavoratori, ora divenute *smart* e in grado di consentire in modo automatico l'accertamento di anomalie, l'assenza o la non corretta posizione dei DPI rispetto alla sagoma della persona, la caduta di oggetti dall'alto, nonché in linea generale tutte le potenziali situazioni di pericolo, con analisi delle immagini e invio di apposite notifiche al personale addetto.

Restano ferme in questa prospettiva due considerazioni.

Anzitutto, l'approdo del discorso cambia se ad essere introdotti — anche già al momento dell'installazione dello strumento cui sono applicati, con una funzione inferenziale strutturale — sono sistemi che, anziché operare come semplici moduli accessori volti a migliorare l'efficienza dello strumento che raccoglie il dato, configurano uno strato applicativo autonomo, che attinge ai dati raccolti, li rielabora e produce per inferenza informazioni nuove, anche relative all'attività lavorativa. Si prenda l'esempio di un sistema di *people analytics* applicato alla posta elettronica: tale strumento, pur attingendo a dati e metadati provenienti dal sistema di posta, non ne costituisce una componente funzionale, operando su un piano distinto, con finalità ulteriori e autonome rispetto a quelle comunicative. In questi casi, il potenziale di controllo non deriva dai dati raccolti dal sistema e-mail in quanto tale, bensì dalla loro rielaborazione algoritmica, che genera per inferenza informazioni

nuove, a loro volta configurabili come dati personali¹². Si pensi al rilevamento di pattern comunicativi atipici, ricostruiti attraverso il confronto statistico con il gruppo di riferimento e idonei a generare segnalazioni di anomalia; alla produzione di indicatori di affidabilità operativa, ricavati dalla correlazione tra volumi di messaggi, tempi di risposta e rispetto delle scadenze interne; ovvero alla costruzione di indici predittivi di stress o burnout, desunti dall'intensità, dalla frammentazione e dalla collocazione temporale delle comunicazioni elettroniche.

In secondo luogo, l'introduzione di un sistema di IA non richiede necessariamente il passaggio dall'art. 4 St. lav., trovando questa applicazione solo laddove vi sia una raccolta di dati relativi all'attività lavorativa dei lavoratori. Così, laddove un sistema di *sentiment analysis* sia applicato esclusivamente nella fase di ricezione delle telefonate, al solo fine di analizzare il cliente — con riguardo al contenuto della richiesta e all'atteggiamento manifestato — per classificarle e consentirne l'instradamento e il riparto strategico tra i diversi operatori del call center, e non comporti la raccolta o l'elaborazione di dati relativi all'attività svolta dai lavoratori, tale sistema non rientrerà nell'ambito di applicazione delle garanzie statutarie.

Non si vuole con la lettura proposta dell'art. 4 St. lav. indirizzare verso una compressione del ruolo delle parti sociali né del confronto sindacale, ritenendosi che anzi questi dovrebbero essere pienamente valorizzati nella fase di utilizzo del dato, anche attraverso forme di partecipazione alla DPIA, auspicabilmente rafforzate da fonti pattizie che ricalchino le previsioni della direttiva sulle piattaforme. Tale coinvolgimento si rivela tanto più necessario qualora la base giuridica di liceità del trattamento dei dati sia individuata nell'interesse legittimo del titolare del trattamento, posto che tale interesse, ai sensi dell'art. 6 GDPR, deve essere oggetto di un bilanciamento con i diritti e le libertà fondamentali degli interessati e proprio la consultazione dei rappresentanti dei lavoratori costituisce in tale bilanciamento una misura idonea a garantire una tutela effettiva dei diritti dei soggetti interessati¹³. Analogo rilievo assume il coinvolgimento sindacale nella fase di trasparenza richiesta in presenza di sistemi integralmente automatizzati di monitoraggio, in base agli obblighi informativi previsti dall'art. 1-bis del d.lgs. 152/1997.

Sarebbe tuttavia necessario, in termini più generali, considerare come nella prospettiva dell'IA i sistemi tecnologici manifestino, in una crescente

¹² Per una qualificazione dei dati derivati o desunti in merito a persone fisiche come «dati personali “nuovi”» cfr. *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, WP 251 rev.0, p. 10

¹³ Cfr. al riguardo Gruppo di lavoro sulla protezione dei dati – Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, WP 217, adottato il 09.04.2014.

logica di commistione dei poteri (Tebano 2020), una capacità sempre più marcata di innervarsi nel potere direttivo e di assumere, in tutto o in parte, profili decisionali. Ne deriva l'esigenza che l'attenzione per il confronto sindacale e per la dimensione della contrattazione collettiva non si fermi alla prospettiva di presidiare l'introduzione delle tecnologie rispetto alle derive della sorveglianza (cercando il proprio varco d'accesso solo nelle maglie del dettato normativo statutario sul controllo a distanza), ma si sviluppi anche rispetto alla dimensione dei processi decisionali algoritmici che i sistemi di IA – in rapida evoluzione e di prevedibile diffusione su scala più ampia, anche in prospettiva agantica – possono supportare o, in taluni casi, contribuire a determinare. Il risultato, altrimenti, è un governo negoziale dell'IA non adeguatamente attrezzato per incidere sulle logiche attraverso le quali le tecnologie possono, a vario titolo, partecipare alla determinazione del contenuto e dell'esercizio di tutti i poteri datoriali¹⁴.

In tale prospettiva, non si possono che salutare con favore alcune traiettorie regolative sviluppate dalla più recente contrattazione collettiva di settore: si pensi al rinnovo del CCNL TLC dell'11 novembre 2025, ove – a traduzione della proposta avanzata in dottrina di istituire per via contrattuale una figura di rappresentanza specifica, ossia il rappresentante dei lavoratori per la privacy (Ingrao 2023) – si è previsto che «nell'ambito delle attività dell'Osservatorio sulle Nuove Tecnologie e tutela dei diritti dei lavoratori, potranno essere individuate figure che, in relazione all'esperienza maturata sugli ambiti di attività interessati, possano offrire il proprio contributo ai lavori dell'Osservatorio medesimo. Analoghe figure potranno essere previste da specifici accordi aziendali, nell'ambito delle rappresentanze dei lavoratori»¹⁵.

¹⁴ Cfr. le *Linee guida per l'implementazione dell'IA nel mondo del lavoro*, adottate dal Ministero del lavoro con d.m. n. 180 del 17 dicembre 2025, nelle quali si evidenzia come il coinvolgimento attivo di lavoratori, rappresentanze sindacali e comitati di sicurezza aziendale costituisca un elemento essenziale per la buona riuscita della mappatura dei sistemi di IA utilizzati in azienda. Tale mappatura è intesa come ricognizione sistematica diretta a individuare dove e come l'IA sia impiegata all'interno dell'organizzazione, quali dati utilizzi, quale livello di autonomia decisionale presenti e quale impatto produca su lavoratori, processi e risultati. Il processo è qualificato come attività cruciale per valutare il livello di esposizione al rischio, distinguere i sistemi ad alto rischio ai sensi dell'*AI Act*, assicurare la conformità normativa e prevenire discriminazioni, violazioni della privacy o criticità in materia di sicurezza.

¹⁵ Per una riflessione più ampia sui profili di intervento sviluppati nella contrattazione collettiva di secondo livello, cfr. (Peruzzi 2025). Nella prospettiva della partecipazione organizzativa, si può segnalare che la l. n. 76/2025 prevede, all'art 7, l'istituzione da parte delle aziende delle commissioni paritetiche, «composte in eguale numero da rappresentanti dell'impresa e dei lavoratori, finalizzate alla predisposizione di proposte di piani di miglioramento e di innovazione dei prodotti, dei processi produttivi, dei servizi e dell'organizzazione del lavoro»; all'art. 12, stabilisce che «ai fini dello sviluppo delle conoscenze e delle competenze tecniche, specialistiche e trasversali, per i rappresentanti facenti parte delle commis-

3. Segretezza della corrispondenza e rilievo probatorio delle comunicazioni digitali nel rapporto di lavoro

L'impiego da parte dei lavoratori di mezzi di comunicazione digitale, si pensi a WhatsApp o alle chat dei social networks e alle più tradizionali e-mail, ha sollevato nuove questioni che si stanno progressivamente affiancando alle più tradizionali che concernono i limiti al potere di controllo a distanza del datore di lavoro sulla posta elettronica e la perimetrazione del diritto di critica del lavoratore subordinato espresso con comunicazioni digitali. La problematica nuova di cui si discuterà nel prosieguo riguarda l'estensione della garanzia di segretezza della corrispondenza di cui all'art. 15 Cost. alle forme di comunicazione digitale del lavoratore subordinato.

Come noto l'art. 15 Cost. garantisce la libertà e la segretezza di ogni forma di comunicazione, ivi inclusa la corrispondenza, che ne costituisce una *species*, tutelando l'individuo nella sfera più intima delle relazioni interpersonali¹⁶. Si tratta di un diritto che, in quanto espressione del nucleo essenziale dei valori della personalità di cui all'art. 2 Cost., partecipa alla categoria dei principi supremi dell'ordinamento e, come tale, non può essere oggetto di revisione o limitazione se non per il perseguimento di un interesse pubblico primario, nei soli limiti e con le garanzie procedurali che la stessa disposizione costituzionale prevede¹⁷.

Il diritto alla segretezza delle comunicazioni e della corrispondenza assume perciò un rilievo preminente anche nel rapporto di lavoro, non potendo restare confinato ai rapporti tra cittadino e pubblici poteri.

Nelle pagine che seguono, si indagheranno i limiti alla possibilità giuridica del datore di lavoro di utilizzare, nel procedimento disciplinare e nel successivo ed eventuale processo, i contenuti delle comunicazioni digitali inviati in gruppi o chat di messaggistica ai quali non partecipa e che siano stati a lui "inoltrati" dal collega "spione" del lavoratore malcapitato.

Delineare tali limiti di utilizzabilità probatoria presuppone l'analisi dei percorsi della giurisprudenza di merito e di legittimità che, negli ultimi dieci anni, ha affrontato *funditus* la questione, muovendosi lungo due direttrici sostanziali. Infatti, se in una prima fase, un orientamento, prevalentemente espresso dai giudici di merito, era incline a valorizzare l'utilizzabilità probatoria del dato digitale nelle condizioni sopradette; più di recente, un'opera di sistematizzazione condotta dalla Corte di Cassazione, ha rivoluzionato i confini entro cui la libertà e la segretezza della corrispondenza possono essere

sioni paritetiche, [...] è prevista una formazione, anche in forma congiunta, di durata non inferiore a dieci ore annue».

¹⁶ (Pace 1992 e 1977).

¹⁷ Corte cost., n. 366 del 1991. In dottrina, (Troisio 1988) e (Italia 1963).

effettivamente garantite ai lavoratori anche in riferimento alle comunicazioni digitali.

3.1. I percorsi della giurisprudenza di merito

Sul versante della giurisprudenza di merito si è registrata, negli ultimi anni, una tendenza piuttosto costante a riconoscere l'utilizzabilità probatoria delle comunicazioni digitali private, anche nel caso in cui il datore di lavoro non fosse tra i diretti destinatari. Il criterio dirimente, in tali pronunce, non è tanto il titolo soggettivo di chi accede alla comunicazione, quanto la *disponibilità materiale del contenuto* da parte di almeno uno dei partecipanti e la sua successiva trasmissione volontaria al datore.

Così, il Tribunale di Fermo¹⁸ aveva ritenuto legittima la produzione di un messaggio inviato via WhatsApp da un dirigente alla moglie dell'amministratore unico della società, nel quale si esprimevano valutazioni fortemente critiche verso la direzione aziendale, idonee a compromettere il vincolo fiduciario e dunque a sorreggere un licenziamento per giusta causa. Una logica analoga informa la decisione del Tribunale di Vicenza¹⁹, che ha ammesso l'utilizzo, nel procedimento disciplinare, di messaggi scambiati in una *chat* tra medici ospedalieri, successivamente inoltrati al datore da uno dei colleghi coinvolti. Il contenuto della conversazione — incentrato su pratiche inadeguate nei confronti dei pazienti — è stato ritenuto rilevante sotto il profilo dell'inadempimento degli obblighi professionali e del danno all'immagine dell'ente sanitario. Parimenti, il Tribunale di Bergamo²⁰ ha ritenuto legittima l'esclusione da una cooperativa e il conseguente licenziamento di un socio-lavoratore che, in una chat WhatsApp condivisa con altri soci, aveva istigato al boicottaggio dell'attività produttiva, promuovendo condotte conflittuali con gli interessi aziendali.

In tutti questi casi, l'assunto implicito è che la trasmissione della comunicazione a un terzo partecipante alla chat, anche senza il consenso dell'autore che confidava nella riservatezza dei contenuti immessi, valga a escludere l'aspettativa di segretezza della corrispondenza, rendendo il contenuto conoscibile anche a chi non è destinatario della comunicazione digitale che diviene quindi potenzialmente utilizzabile senza limiti di sorta in sede probatoria. Tale impostazione, tuttavia, solleva interrogativi rilevanti rispetto al fondamento costituzionale della tutela della corrispondenza e della sua se-

¹⁸ T. Fermo, 30.09.2017, n. 1973.

¹⁹ T. Vicenza, 14.12.2017, n. 778.

²⁰ T. Bergamo, 07.06.2018, n. 424.

gretezza, di cui all'art. 15 Cost. che ha infatti imposto una più compiuta riflessione sistematica da parte della Corte di Cassazione.

3.2. La segretezza della corrispondenza digitale nella interpretazione della giurisprudenza della Corte Costituzionale e della Cassazione

A fronte dell'orientamento di merito tendenzialmente aperto all'utilizzabilità probatoria delle comunicazioni digitali, la giurisprudenza di legittimità ha progressivamente affinato i criteri di delimitazione tra comunicazione privata e comunicazione potenzialmente esposta a un pubblico indiscriminato²¹.

È proprio il *criterio selettivo dell'accessibilità* ad assumere un ruolo centrale nella distinzione, ai fini dell'integrazione dell'illecito disciplinare²², tra una comunicazione destinata a un contesto chiuso e determinato, e viceversa una comunicazione idonea, per struttura e modalità di diffusione, a raggiungere un pubblico indeterminato. Infatti, la segretezza della corrispondenza di cui all'art. 15 Cost. si distingue dalla libertà di manifestare il pensiero di cui all'art. 21 Cost., proprio perché, nel primo caso, l'espressione comunicativa del pensiero è intenzionalmente riservata ad un numero determinato e circoscritto di soggetti, mentre, nel secondo caso, l'espressione è diffusa presso una platea indeterminata di destinatari.

Tale distinzione tra comunicazione "chiusa" e comunicazione "aperta" si innesta, peraltro, nel più ampio processo di rilettura costituzionale della nozione di "corrispondenza", reso necessario dalla transizione digitale dei mezzi di comunicazione.

La Corte Costituzionale con la sentenza n. 170/2023 – resa in giudizio per conflitto di attribuzione tra poteri statutali – ha fornito una lettura "aggior-

²¹ Una significativa attestazione in tal senso si rinviene in Cass., 10.09.2018, n. 21965, nella quale è stato riconosciuto il carattere riservato e segreto ex art. 15 Cost. di una *chat* Facebook composta esclusivamente da iscritti a una specifica sigla sindacale, qualificata come «luogo digitale di dibattito e scambio di opinioni» funzionale esclusivamente ad un confronto interno riservato ai soli membri ammessi alla chat e, sottratto, in quanto tale, alla logica alla pubblica esposizione.

²² Il punto è stato ulteriormente chiarito da Cass. n. 33074/2024, che, richiamando i precedenti del 2018 e del 2021 (rispettivamente, nn. 21965 e 27939), ha escluso la ricorrenza della giusta causa di licenziamento per espressioni offensive rivolte al datore di lavoro, allorché esse risultino confinate all'interno di una *mailing list* chiusa, ossia indirizzate a un gruppo definito e identificabile di destinatari. In questa prospettiva, la valutazione dell'idoneità del mezzo di comunicazione a generare una circolazione incontrollata del messaggio diventa elemento dirimente nella ricostruzione della lesione alla fiducia datoriale. Ma si tratta di un accertamento che resta, come ribadito dalla Corte, riservato al giudice di merito, implicando un apprezzamento complesso, tanto sul piano fattuale quanto su quello relazionale.

nata” dell’art. 15 Cost., affermando che la nozione di corrispondenza non si esaurisce alle più tradizionali forme di comunicazione epistolari o alla corrispondenza cartacea, ma ricomprende «ogni comunicazione di pensiero umano tra due o più persone determinate (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza». Come precisato anche dalla successiva sentenza della Corte Costituzionale n. 2 del 2023, la garanzia prevista dalla Carta si estende a «ogni strumento che l’evoluzione tecnologica metta a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti al momento della sua adozione».

Ne deriva che strumenti come l’e-mail e la messaggistica istantanea rientrano a pieno titolo nel perimetro della tutela costituzionale dell’art. 15 Cost. perché sono assimilabili a lettere sigillate che veicolano messaggi e contenuti accessibili unicamente dal destinatario, protetti da credenziali personali o da dispositivi di identificazione, finalizzati a circoscrivere gli accessi alla corrispondenza o alla comunicazione (di contenuti foto, video o audio) ivi contenute. Di tal che diviene irrilevante il luogo virtuale dello scambio della comunicazione o della corrispondenza, ma ciò che conta è che queste *siano trasmesse a soggetti determinati con mezzi idonei a sottrarle alla conoscenza dei terzi*, senza che siano però necessarie particolari precauzioni per assicurarne la segretezza.

La lettura estensiva del concetto di corrispondenza di cui all’art. 15 Cost. costituisce senza dubbio una interpretazione adeguatrice dell’ambito oggettivo di applicazione della norma incontrovertibile. Maggiori dubbi invece sono stati sollevati in dottrina sul limite temporale della tutela alla segretezza della corrispondenza²⁵.

Una prima impostazione aveva infatti ritenuto che la garanzia costituzionale si esaurisse con la ricezione del messaggio, trattandosi di una tutela “dell’atto del corrispondere”; una seconda, più convincente e poi accolta dalla giurisprudenza costituzionale appena citata, riconosce che la riservatezza perdura finché il contenuto della comunicazione mantenga un interesse alla protezione, cessando solo nel momento in cui si trasformi in documento storico, privo di attualità e di carica relazionale.

Quest’ultima lettura è stata fatta propria dalla Corte Costituzionale nella stessa sentenza n. 170/2023, la quale ha ribadito che il contenuto della corrispondenza continua a essere protetto anche dopo la ricezione da parte del destinatario, in coerenza con la sua funzione di garanzia della dignità e della libertà personale.

²⁵ (Orofino 2021) e (C. Caruso 2013).

Un orientamento, peraltro, in linea con quanto stabilito dalla Corte EDU in applicazione dell'art. 8 e 10 CEDU, e recentemente riaffermato anche dalla Cassazione penale, sent. n. 25549/2024, che ha esteso la tutela alla dimensione “statica” delle comunicazioni digitali, riconoscendone la protezione anche in fase successiva alla trasmissione.

3.3. I recenti arresti della Corte di Cassazione

Le più recenti pronunce della Corte di Cassazione sembrano consolidare l'indirizzo volto a riconoscere una effettiva tutela alla segretezza delle comunicazioni digitali nel contesto del rapporto di lavoro.

In particolare, le sentenze del 28 febbraio 2025, n. 5334 e del 6 marzo 2025, n. 5963²⁴ escludono in radice che i messaggi scambiati dal lavoratore mediante il proprio dispositivo personale, e indirizzati a un numero determinato di destinatari in una chat virtuale, possano essere legittimamente reperiti e utilizzati dal datore di lavoro a fini disciplinari.

A fondamento di tale conclusione, la Corte valorizza non già il mezzo tecnico impiegato, ma la *volontà chiaramente manifestata dal mittente di mantenere la comunicazione in una dimensione segreta*. Il contenuto comunicativo viene così a collocarsi all'interno della sfera di protezione dell'art. 15 Cost., il quale, in tale prospettiva, si conferma presidio della dignità individuale anche nelle sue proiezioni digitali.

La già citata sentenza n. 5963/2025 contribuisce a definire in termini più articolati il perimetro della nozione di “segretezza” applicabile alle comunicazioni digitali.

Il punto di partenza è rappresentato dall'idea secondo cui la nozione di “corrispondenza” deve intendersi in senso estensivo, comprensivo di ogni forma di comunicazione digitale tra soggetti determinati.

Ciò che assume rilievo, nella prospettiva della tutela, non è tanto la forma del mezzo impiegato, quanto la presenza di cautele idonee a escludere l'accesso dei terzi alla comunicazione. La riservatezza discende, in altri termini, dall'esistenza di modalità tecniche o convenzionali che consentano di riconoscere il carattere “chiuso” dello scambio comunicativo: come accade per le

²⁴ Con nota critica di (Chiaromonte 2025) per il quale «il diritto alla libertà e segretezza della corrispondenza, sia quello di critica, tuttavia, non possono essere intesi quali situazioni giuridiche assolute. Essi devono, pertanto, essere esercitati alla luce dei limiti rilevanti in quanto discendenti da interessi e beni protetti dalla stessa Costituzione».

e-mail accessibili solo tramite credenziali personali o per le chat protette da sistemi di autenticazione.

Non rileva, invece, che il datore di lavoro sia venuto in possesso del contenuto senza porre in essere un'attività d'indagine intrusiva, ciò che conta è che la comunicazione fosse concepita *ex ante* come riservata, ossia destinata a un circuito definito e non aperto. Né tantomeno rilevante risulta il contenuto diffamatorio o denigratorio delle esternazioni del lavoratore, dal momento che la segretezza della comunicazione costituisce un limite assoluto alla stessa possibilità datoriale di venire a conoscenza del messaggio, almeno sul piano giuridico²⁵.

Infine, la Corte ha chiarito che la protezione accordata dall'art. 15 Cost. non si esaurisce nel momento della ricezione del messaggio, ma perdura nel tempo, fintanto che la comunicazione conservi un interesse alla segretezza. Solo quando il contenuto perda ogni connotazione personale o relazionale, assumendo rilievo storico, la tutela viene meno.

Nel bilanciamento tra poteri datoriali e diritti fondamentali del lavoratore, la dimensione digitale della comunicazione non implica un venir meno delle tradizionali categorie del diritto del lavoro e del diritto costituzionale. Essa esige, piuttosto, un loro riadattamento interpretativo, in cui la garanzia della persona che lavora non sia sacrificata a una concezione meramente espansiva del potere organizzativo e disciplinare datoriale.

4. Una proposta interpretativa per sciogliere il nodo irrisolto dei post sui profili chiusi dei social network. Verso una “segretezza ragionevole” della comunicazione digitale

La crescente attenzione della giurisprudenza al tema della segretezza della corrispondenza digitale ha condotto a risultati di significativa apertura sul versante della messaggistica interpersonale. È ormai acquisito che le comunicazioni tramite e-mail, WhatsApp o mailing list chiuse – ove siano presenti cautele tecniche (quali credenziali d'accesso) e volontà soggettiva di limitare la platea dei destinatari – rientrino nel perimetro applicativo dell'art. 15 Cost. In questa prospettiva, il diritto alla riservatezza è letto come presidio della dignità individuale e come garanzia non solo della libertà comunicativa, ma della sua intangibilità rispetto a interferenze esterne. La Corte costituzionale

²⁵ Ma v. *contra* (Chiaromonte 2025, p. 280 laddove afferma che «la natura confidenziale e riservata della comunicazione non implica necessariamente la liceità del comportamento tenuto dal lavoratore. La riservatezza della comunicazione in particolare di per sé non esclude, né tantomeno legittima, la diffamazione, che mantiene comunque evidenti risvolti disciplinari».

(sent. n. 170/2023) ha valorizzato, in tal senso, un'idea di “corrispondenza” che, pur nata in un contesto cartaceo, si estende oggi a ogni forma di scambio tra soggetti determinati, anche attraverso strumenti impensabili al tempo della redazione della Carta.

Tuttavia, questo processo di riconoscimento non ha trovato, finora, un equivalente sviluppo in relazione ai contenuti (post, commenti e like) veicolati mediante social network, anche laddove tali contenuti siano condivisi in spazi digitali delimitati e tecnicamente “chiusi”, come i profili accessibili solo a una cerchia ristretta di amici o contatti.

La domanda, allora, si impone: per quale ragione la comunicazione privata su WhatsApp sarebbe segreta e tutelata dall'art. 15 Cost., mentre un post pubblicato in un profilo Facebook con accesso limitato ad un numero determinato di utenti non meriterebbe la medesima protezione?

Su questo punto, la maggior parte della giurisprudenza di merito e di legittimità si è mostrata piuttosto prudente, se non addirittura restrittiva. La Corte di appello di Torino²⁶ ha affermato che i social network, anche se impostati come “privati”, sono da considerarsi luoghi pubblici, giacché la possibilità tecnica di rilancio dei contenuti da parte degli utenti renderebbe potenzialmente illimitato il numero dei destinatari. Di qui, l'irrilevanza della scelta operata dall'utente in merito alle impostazioni di visibilità: ciò che conta, secondo questa lettura, è l'idoneità strutturale della piattaforma a rendere il contenuto accessibile a terzi. Lo stesso orientamento si ritrova nella giurisprudenza di Cassazione²⁷, la quale ha ritenuto che un commento diffamatorio postato su Facebook costituisca giusta causa di licenziamento, valorizzando non tanto l'intento soggettivo del lavoratore, quanto presumendo che il mezzo utilizzato fosse idoneo a determinare l'effettiva diffusione su larga scala.

²⁶ Corte d'Appello Torino, n. 599/2017. Si veda altresì Trib. Bergamo, 14.09.2016, in *ADL*, 2017, n. 2, con nota di Cusumano, secondo cui la condivisione di immagini o espressioni attraverso un profilo social impostato come pubblico comporta, da parte dell'autore della pubblicazione, l'accettazione del rischio che il contenuto venga liberamente visualizzato da una cerchia indeterminata di soggetti. In tale prospettiva, la natura “aperta” del profilo esclude ogni legittima aspettativa di riservatezza, legittimando la possibile acquisizione del materiale diffuso anche ai fini probatori. *Contra*, Tribunale di Ascoli Piceno 19.11.2013 per cui è illegittimo per violazione del principio di proporzionalità il licenziamento intimato per giusta causa a un lavoratore per aver pubblicato sulla propria pagina Facebook una critica alla clientela del proprio datore di lavoro (vaff... di cuore ai clienti che oggi sono venuti a comprare le vitarelle a Brico invece di fare la scampagnata di Pasquetta!!!), quando questa costituisca uno sfogo, pur volgare ed inelegante, e risulti visibile soltanto ad un numero ristretto di persone e per un breve lasso di tempo (aveva cancellato dopo 20 minuti il post).

²⁷ Cass. 26.04.2018, n. 10280.

Questo approccio sembra tuttavia appiattare la questione sul solo piano tecnico-formale, trascurando una serie di fattori che l'evoluzione giurisprudenziale e dottrinale ha invece posto al centro dell'analisi. Una parte della riflessione costituzionale, infatti, ha suggerito di distinguere, all'interno dell'art. 15 Cost., due posizioni concettualmente autonome: la libertà di comunicare e la segretezza delle comunicazioni. Se la prima può, in talune ipotesi, essere compressa (es. fermo della corrispondenza per ragioni di giustizia), la seconda postula una tutela assoluta, salvo autorizzazione dell'autorità giudiziaria. Ma soprattutto, nella realtà digitale contemporanea, ciò che qualifica una comunicazione come riservata non è (più) il mezzo in sé, bensì la combinazione tra le caratteristiche dello strumento tecnico utilizzato, l'intento del mittente e la delimitazione – anche ragionevolmente presumibile – dei destinatari.

Ne consegue che non può escludersi aprioristicamente la garanzia costituzionale di segretezza per il solo fatto che una comunicazione sia veicolata tramite una piattaforma social, almeno quando l'architettura tecnica della stessa consenta all'utente di predeterminare le impostazioni di *privacy* del proprio profilo, garantendo in buona sostanza il diritto all'autodeterminazione informativa²⁸. L'aspettativa di riservatezza può sussistere anche in questi contesti, purché siano ravvisabili indici oggettivi (e non meramente soggettivi) di esclusione del pubblico: ad esempio, un numero ristretto e identificabile di destinatari, l'uso di impostazioni di *privacy* restrittive, la natura del contenuto e l'assenza di intenzione divulgativa. Si tratta, in altre parole, di adottare un criterio elastico e funzionale, che tenga conto sia dell'idoneità tecnica del mezzo a garantire la riservatezza, sia della finalità perseguita dal mittente.

Il rischio, altrimenti, è quello di una indebita attrazione nell'alveo dell'art. 21 Cost. – con le sue diverse condizioni di tutela e con un regime di limiti più ampio (buon costume, ordine pubblico) – di comunicazioni che, per struttura e contenuto, restano ancorate al paradigma della corrispondenza riservata. Ma una simile sovrapposizione può generare incertezze applicative e svuotare la garanzia dell'art. 15 Cost., riducendone la portata a fronte della metamorfosi digitale della comunicazione.

²⁸ Non così è per esempio per il social Twitter che ha funzione di diffondere le manifestazioni di opinioni che l'utente pubblica, cfr. Tribunale di Busto Arsizio 20.02.2018 n. 62 per il quale è garantito il diritto di esprimere il dissenso rispetto alle scelte della società senza toni ingiuriosi, ma il fatto sussiste perché l'insulto postato su *Twitter* è potenzialmente capace di raggiungere un numero indeterminato comunque quantitativamente apprezzabile di persone.

In conclusione, la questione dell'utilizzabilità a fini disciplinari dei post pubblicati su profili social chiusi rappresenta oggi un terreno interpretativo ancora irrisolto, che sollecita una riflessione sistematica più profonda. Occorre interrogarsi se sia davvero coerente con i principi costituzionali negare tutela alla comunicazione solo in ragione del mezzo impiegato, senza considerare le sue caratteristiche funzionali e contestuali. Il riconoscimento di una "segretezza ragionevole", fondata su indici oggettivi e intenzionali, potrebbe offrire una via interpretativa più rispettosa della dignità del lavoratore e più aderente alla complessità delle relazioni comunicative nella società digitale.

Riferimenti bibliografici

- Alvino I. (2014), *L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica*, in *DRI*, 4, p. 999 ss.
- Bellavista A. (2023), *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, in *LDE*, 1.
- Califano L. (2017), *Tecnologie di controllo del lavoro, diritto alla riservatezza e orientamenti del Garante per la protezione dei dati personali*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli.
- Caruso C (2013), [La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale](#), in *Forum Quaderni Costituzionali*.
- Chiaromonte W. (2025) «What happens in whatsapp stays in whatsapp»: illegittimo il licenziamento determinato dalla diffusione di messaggi denigratori via chat, in *RGL*, 3, p. 275 ss.
- D'Arcangelo L. (2025), *I limiti del Garante al controllo degli strumenti di lavoro*, in *LG*, 11, p. 984 ss.
- Del Conte M. (2007), *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, in *Dir. inf.*, 3, p. 497 ss.
- Ingrao A. (2018), *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci.
- Ingrao A. (2023), *Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *LLI*, 1, p. I.101 ss.
- Italia V. (1963), *Libertà e segretezza della corrispondenza e delle comunicazioni*, Giuffrè.
- Marazza M. (2016), *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *Biblioteca '20 Maggio' – 1/2016*, p. 289 ss.
- Nuzzo V. (2018), *La protezione del lavoratore dai controlli impersonali*, Ed. Scientifica.
- Orofino M. (2021), *Sub art. 15*, in F. Clementi, L. Cuocolo, F. Rosa, G.E. Vigevani (a cura di), *La costituzione italiana. Commento articolo per articolo*, Il Mulino.
- Pace A. (1977), *Sub art. 15*, in G. Branca, A. Pizzorusso (a cura di), *Commentario della Costituzione*, Zanichelli.
- Pace A. (1992), *Problematica delle libertà costituzionali*, vol. II, Cedam.
- Peruzzi M. (2025), *Governare l'IA nei luoghi di lavoro: traiettorie della contrattazione collettiva aziendale e territoriale*, in *LLI*, 2, p. 53 ss.

- Proia G. (2022), *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione)*, in C. Pisani, G. Proia, A. Topo (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè.
- Sartori A. (2020), *Il controllo tecnologico sui lavoratori*, Giappichelli.
- Tebano L. (2020), *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale scientifica.
- Tebano L. (2024), *Ancora sulla gestione della posta elettronica nel contesto lavorativo: conservazione dei metadati e natura dello strumento*, in *RIDL*, 2, p. 291 ss.
- Troisio C. (1988), voce *Corrispondenza (Libertà e segretezza della)*, in *Enc. Dir.*, vol. IX, Istituto dell'enciclopedia italiana.
- Trojci A. (2022), *La sorveglianza digitale del datore di lavoro*, in A. Bellavista, R. Santucci, (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Giappichelli.
- Tullini (2017a), *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli
- Tullini P. (2017b), *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli.