ALERT MEMORANDUM

Controlli difensivi: la Corte di Cassazione chiarisce gli oneri a carico del datore di lavoro

13 novembre 2023

Con sentenza n. 18168 del 26 giugno 2023, la Sezione Lavoro della Corte di Cassazione ha fornito chiarimenti sui "controlli difensivi" del datore di lavoro.

Sotto il profilo sostanziale, nel confermare la distinzione tra "controlli a tutela del patrimonio aziendale" soggetti all'art. 4 della legge n. 300 del 1970 (lo Statuto dei Lavoratori) e controlli difensivi (a cui tale norma non si applica), la Corte di Cassazione ha dettagliatamente articolato i requisiti di questi ultimi.

Sotto il profilo processuale, la Corte di Cassazione si è poi espressa in tema di onere della prova e utilizzabilità delle risultanze dei controlli difensivi.

La sentenza è un importante punto di approdo nell'elaborazione giurisprudenziale sui controlli difensivi. Nello specifico, pur onerando il datore di lavoro della prova della legittimità dei controlli, la sentenza fornisce a quest'ultimo utili elementi per valutare quando e come far ricorso ai controlli difensivi nonché per prepararsi preventivamente, al fine di massimizzare le possibilità che il giudice ritenga legittimi i controlli in sede di impugnativa dell'eventuale licenziamento disciplinare.

Per domande relative ai temi discussi in questa nota, potete contattare qualsiasi avvocato del nostro studio con cui siete abitualmente in contatto o gli autori di seguito indicati.

ROMA

Giuseppe Scassellati-Sforzolini
+39 06 6952 2220
gscassellati@cgsh.com

Andrea Mantovani
+39 06 6952 2804
amantovani@cgsh.com

Marco Accorroni
+39 06 6952 2320
maccorroni@cgsh.com

MILANO

Elena Galimberti
+39 02 7260 8670
egalimberti@cgsh.com

1. I CONTROLLI DIFENSIVI

La sentenza in esame costituisce un significativo arresto del filone giurisprudenziale[1] che consente forme di monitoraggio del datore di lavoro svincolate dalle formalità previste, a tutela del dipendente, dall'art. 4 dello Statuto dei Lavoratori.

Tale disposizione fu introdotta nell'ordinamento per (i) vietare l'uso di strumenti di monitoraggio per finalità di controllo a distanza dell'attività dei dipendenti e, al contempo, (ii) disciplinare l'uso di questi strumenti ove "*richiesto da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro*", sebbene da tale uso possa derivare, come conseguenza accidentale, il controllo a distanza dell'attività dei dipendenti (cc.dd. controlli preterintenzionali). In particolare, l'art. 4 prevedeva (e tutt'ora prevede) che i controlli preterintenzionali possano avvenire soltanto a seguito di accordo collettivo o, in mancanza, di autorizzazione dell'Ispettorato Nazionale del Lavoro.

Tuttavia, nel tempo è sorta l'esigenza di sottrarre dall'ambito di operatività dell'art. 4 dello Statuto dei Lavoratori i controlli effettuati allo specifico fine di accertare comportamenti illeciti del lavoratore, specie se lesivi del patrimonio o dell'immagine aziendale. Infatti, la necessità di procedere a una negoziazione sindacale (dai tempi potenzialmente lunghi e con esiti incerti) o di ottenere un'autorizzazione (con anche il rischio di imposizione di eccessivi vincoli e condizioni) appariva in contrasto con l'interesse datoriale di accertare e sanzionare illeciti dei dipendenti in maniera tempestiva ed efficace.

Per questo, la giurisprudenza ha elaborato la categoria dei controlli difensivi[2], sottraendola ai vincoli dell'art. 4 dello Statuto dei Lavoratori e individuandone progressivamente i profili di disciplina mediante il richiamo ai principi di buona fede e correttezza nonché a quelli di adeguatezza e proporzionalità quali limiti alla condotta datoriale[3].

I controlli difensivi possono essere di vario genere. La Corte di Cassazione ha ad esempio qualificato come controlli difensivi:

(a) il controllo della casella e-mail aziendale[4];

(b) l'utilizzo di registrazioni video[5];

(c) la verifica delle connessioni ad internet[6];

(d) il controllo dei dati di traffico contenuti nel *browser* del pc aziendale[7];

(e) il controllo delle presenze registrate tramite *badge* aziendale[8].

La sopravvivenza della categoria dei controlli difensivi è stata messa in dubbio a seguito del c.d. *Jobs Act*[9], posto che, con tale riforma, l'art. 4 dello Statuto dei Lavoratori veniva a ricomprendere anche i controlli preterintenzionali sorretti proprio dall'esigenza di "*tutela del patrimonio aziendale*" [10].

La Corte di Cassazione ha tuttavia di recente rigettato questa interpretazione, rinvenendo una residua operatività della categoria dei controlli difensivi mediante la distinzione tra controlli difensivi "*in senso lato*" e controlli difensivi "*in senso stretto*" [11].

Secondo la Corte di Cassazione, i controlli difensivi "*in senso lato*" (ossia i controlli a tutela del patrimonio aziendale) riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della normale prestazione lavorativa, qualora essa ponga i lavoratori a contatto con il patrimonio aziendale stesso. Alla luce della riforma operata dal *Jobs Act*, questi controlli rimangono soggetti alle garanzie *ex* art. 4 dello Statuto dei Lavoratori.

I controlli difensivi "*in senso stretto*" sono invece quelli diretti ad accertare specifiche condotte

[1] Si veda, da ultimo, Cass. Civ., Sez. Lav., 20 luglio 2023, n. 21681.
[2] Si veda, già Cass. Civ., Sez. Lav., 3 aprile 2002, n. 4746.
[3] Si veda, *ex multis*, Cass. Civ., 27 maggio 2015, n. 10955; Cass. Civ., Sez. Lav., 10 novembre 2017, n. 26682.
[4] Da ultimo, si veda la sentenza in commento.
[5] Cass. Civ., Sez. Lav., 8 novembre 2016, n. 22662.
[6] Cass. Civ., Sez. Lav., 15 giugno 2017, n. 14862.
[7] Cass. Civ., Sez. Lav., 22 settembre 2021, n. 25732.
[8] Cass. Civ., Sez. Lav., 21 agosto 2018, n. 20879.
[9] Legge n. 183/2014.
[10] Si veda, l'art. 23 del d.lgs. 14 settembre 2015, n. 151 (in attuazione della legge di delega 10 dicembre 2014, n. 183).
[11] Cass. Civ., Sez. Lav., 22 settembre 2021 n. 25732 e Cass. Civ., Sez. Lav., 12 novembre 2021, n. 34092; *contra* Trib. Milano, 31 marzo 2004; Trib. Milano, 11 aprile 2005; Trib. Roma, 4 giugno 2005.

illecite ascrivibili a singoli dipendenti. Non avendo ad oggetto la "*normale attività del lavoratore*", i controlli difensivi vengono considerati al di fuori del campo di applicazione dell'art. 4 dello Statuto dei Lavoratori[12]. Tuttavia, essi sono legittimi soltanto in presenza di un "*fondato sospetto*" di illecito e devono essere proporzionati al fine datoriale[13]. L'assenza di uno di tali requisiti comporta la "*radicale inutilizzabilità*" per fini disciplinari delle informazioni assunte con i controlli[14].

La sentenza in esame richiama tale giurisprudenza e fornisce ulteriori chiarimenti sul tema. In particolare, la sentenza (i) chiarisce la nozione di "fondato sospetto" a giustificazione dei controlli e (ii) stabilisce i criteri da applicare nel giudizio di bilanciamento tra esigenze del datore di lavoro e diritto alla riservatezza del dipendente.

La sentenza inoltre (i) precisa che l'onere della prova della legittimità dei controlli difensivi nell'ambito di un procedimento di impugnativa del licenziamento spetta al datore di lavoro e (ii) afferma che il relativo inadempimento comporta l'inutilizzabilità per finalità disciplinari delle risultanze dei controlli nonché degli atti basati su tali risultanze.

2. IL CASO DECISO

Il giudizio deciso dalla sentenza in esame trae origine dall'impugnazione di un licenziamento per giusta causa. Il lavoratore lamentava, tra l'altro, che gli elementi di prova addotti dal datore di lavoro a fondamento delle contestazioni disciplinari erano stati raccolti mediante attività investigativa illegittima. Il giudice di merito ha accolto l'impugnativa del lavoratore, ritenendo illegittimi (i) il controllo della casella e-mail aziendale in assenza di specifica motivazione, nonché (ii) i pedinamenti del dipendente, posto che essi trovavano giustificazione soltanto alla luce della corrispondenza e-mail acquisita illegittimamente.

Il controllo della casella e-mail del lavoratore è stato altresì ritenuto sproporzionato rispetto allo scopo perseguito dal datore di lavoro, avendo riguardato indistintamente tutte le comunicazioni presenti nel pc aziendale e non avendo il datore di lavoro dimostrato di aver preventivamente informato il dipendente della possibilità del monitoraggio né tantomeno della sua portata.

La Corte di Cassazione, nel rigettare il ricorso del datore di lavoro, ha ritenuto che il giudice di merito avesse correttamente deciso in conformità ai principi che informano la materia.

3. REQUISITI DI LEGITTIMITÀ

La Corte di Cassazione sottopone i controlli difensivi a due requisiti di legittimità, ossia (i) alla sussistenza di *presupposti giustificativi* del controllo e (ii) al suo svolgimento con *modalità* rispettose della riservatezza del lavoratore.

Infatti, la categoria dei controlli difensivi pone il rischio di forme surrettizie di monitoraggio illecito dell'esatto adempimento della prestazione lavorativa e, in assenza delle garanzie di cui all'art. 4 dello Statuto dei Lavoratori, potrebbe altresì giustificare monitoraggi altrimenti lesivi della dignità e della riservatezza del lavoratore.

3.1. SUSSISTENZA DI PRESUPPOSTI GIUSTIFICATIVI: IL "FONDATO SOSPETTO"

La Corte di Cassazione precisa che il datore di lavoro può effettuare controlli difensivi soltanto in presenza di "*concreti indizi*" che facciano sorgere il "*fondato sospetto*"[15] che sia stato tenuto un comportamento illecito (pp. 7, 9)[16]. Non è pertanto sufficiente il "*puro convincimento soggettivo*" del datore di lavoro, essendo necessario "*un riscontro oggettivo dell'autenticità dell'intento difensivo del controllo*" (p. 9). In altri termini, in linea con la giurisprudenza della Corte Europea dei Diritti dell'Uomo ("Corte EDU") in materia di controlli sui dipendenti, gli indizi devono essere "*materiali e riconoscibili*", tanto da far sospettare una persona ragionevole che il dipendente da sottoporre a

[12] Cass. Civ., Sez. Lav., 22 settembre 2021 n. 25732, paragrafo 32.
[13] *Ibid*., paragrafo 35.
[14] Cfr., *ex multis*, Cass. Civ., Sez. Lav., 5 ottobre 2016, n. 19922; Cass. Civ., Sez. Lav., 1 ottobre 2012, n. 16622.
[15] Per quanto attiene alla ricerca di indizi a fondamento del fondato sospetto, si segnala la recente emanazione da parte del Comitato Tecnico ISO/TC 309 della "Linea guida ISO/TS 37008:2023", luglio 2023 ("Internal investigations of organisations - Guidance") e, in particolare, il relativo paragrafo. 8.8 ("Evidence").
[16] *Contra*, Cass. Civ., Sez. Lav., 2 maggio 2017, n. 10636, secondo cui è sufficiente la mera ipotesi che illeciti siano in corso di esecuzione.

controllo abbia commesso un illecito (p. 11)[17].

Inoltre, un'eventuale carenza di indizi al momento in cui vengono effettuati i controlli non può essere sopperita da elementi acquisiti successivamente.

3.2. PROPORZIONALITÀ DEL CONTROLLO E RISPETTO DEGLI ALTRI PRINCIPI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

La Corte di Cassazione precisa altresì che i controlli difensivi devono essere svolti nel rispetto del diritto del lavoratore alla riservatezza ai sensi dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU).

Di conseguenza, prima decidere se effettuare dei controlli difensivi e determinarne forma, oggetto e durata, sarà necessario procedere a un bilanciamento tra gli interessi datoriali messi in pericolo dalla condotta del dipendente e la dignità e riservatezza del dipendente stesso. La preventiva valutazione richiesta al datore di lavoro dovrà avere anche ad oggetto la verifica del rispetto dei principi di proporzionalità, minimizzazione, non eccedenza in relazione a un legittimo scopo, trasparenza e correttezza di cui al Regolamento Generale sulla Protezione dei Dati (Regolamento UE n. 2016/679; "GDPR").

L'esito positivo del predetto giudizio di bilanciamento, da cui risulti la prevalenza dell'interesse del datore di lavoro sui confliggenti interessi o diritti e libertà fondamentali degli interessati, può consentire al datore di lavoro di invocare, quale base giuridica del trattamento dei dati personali dei dipendenti nel contesto del controllo, il proprio legittimo interesse *ex* art 6(1)(f) del GDPR[18].

Per converso, la legittimità dei controlli difensivi potrà essere contestata ove, tenuto conto di "*tutte le circostanze del caso concreto*" (p. 15), tali principi risultino violati. Per orientare i giudici di merito in tale giudizio, la Corte di Cassazione ha richiamato gli elementi che già la Corte EDU aveva elencato ai fini della valutazione della conformità all'art. 8 CEDU di misure di sorveglianza da parte del datore di lavoro. Nello specifico, i giudici di merito dovranno valutare:

i. se il lavoratore sia stato informato in anticipo e in modo chiaro circa la possibilità che il datore di lavoro adotti misure di monitoraggio;

ii. se i controlli siano eccessivamente invasivi della sfera privata del dipendente, tenuto conto della natura, del luogo in cui essi si svolgono, della loro durata e del numero di persone che hanno accesso ai loro risultati;

iii. se la causa addotta dal datore di lavoro sia sufficientemente grave da giustificare la misura di controllo posta in essere;

iv. se lo scopo perseguito dal datore di lavoro avrebbe potuto essere raggiunto in altro modo meno invasivo;

v. se il datore di lavoro abbia utilizzato le informazioni ricavate dal controllo per i soli fini strettamente necessari a raggiungere lo scopo dichiarato;

vi. se il datore di lavoro abbia fornito al dipendente garanzie sufficienti sul grado di invasività delle misure di controllo, mediante preventive informazioni ai lavoratori interessati, ai loro rappresentanti o a un organismo indipendente o mediante la previsione di meccanismi di reclamo[19].

Va ricordato che la stessa normativa in tema di protezione dei dati personali onera il datore di lavoro di informare i propri dipendenti *ex* art. 13 GDPR circa la possibilità di effettuazione di tali controlli, in conformità con il principio di trasparenza di cui all'art 5(1)(a) del GDPR.

4. ONERE DELLA PROVA

Secondo la Corte di Cassazione, l'onere di allegazione e della prova degli elementi di fatto dai quali scaturisce il "fondato sospetto" che legittima i controlli difensivi nell'ambito di un giudizio di impugnativa di licenziamento grava sul datore di lavoro, avendo questi, in conformità al principio di

[17] Corte Europea dei Diritti dell'Uomo, Grande Camera, *Lopez Ribalda et al. c. Spagna*, 17 ottobre 2019.

[18] L'art. 6(1)(f) del GDPR permette il trattamento dei dati personali se "*necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali* […]".

[19] Corte Europea dei Diritti dell'Uomo, Grande Camera, *Bărbulescu c. Romania,* 5 settembre 2017.

vicinanza della prova, maggiori possibilità di conoscerli in via diretta o indiretta.

E' quindi onere del datore di lavoro provare le circostanze che abbiano giustificato il controllo in assenza delle generali garanzie altrimenti spettanti al dipendente *ex* art. 4 dello Statuto dei lavoratori, essendo questi, del resto, tenuto a provare il complesso degli elementi che giustificano il licenziamento del dipendente ai sensi dell'art. 5 della legge n. 604/1966.

La sentenza non fornisce invece esplicite delucidazioni in merito alla ripartizione dell'onere di provare il rispetto del principio di proporzionalità e degli altri principi a tutela della riservatezza del dipendente. Tuttavia, la Corte di Cassazione parrebbe ritenere anche tale onere a carico del datore di lavoro[20]. Invero, l'assenza di prova di talune circostanze (tra cui la preventiva informazione sul controllo) è stata considerata dalla Corte di Cassazione per confermare la pronuncia di merito anche nella parte in cui ha ritenuto che i controlli difensivi fossero stati svolti in violazione dei principi a tutela della riservatezza del lavoratore.

5. CONSEGUENZE DELLA VIOLAZIONE DEI REQUISITI DI LEGITTIMITÀ DEI CONTROLLI

La Corte di Cassazione chiarisce altresì che la sanzione processuale della violazione dei requisiti di legittimità dei controlli difensivi è la medesima che la giurisprudenza di legittimità applica ai controlli a tutela del patrimonio aziendale, e cioè la "*radicale inutilizzabilità*" (p. 13) per fini disciplinari delle informazioni assunte con i controlli [21]. Ne discende che, secondo un meccanismo riconducibile alla dottrina del *fruit of the poisonous tree*, gli elementi probatori tratti da controlli difensivi illegittimi non possono essere utilizzati per dimostrare l'esistenza di un "fondato motivo" che giustifichi ulteriori controlli svolti dal datore di lavoro[22].

6. CONCLUSIONI

La sentenza in esame fornisce indicazioni molto importanti per orientare le attività del datore di lavoro che intenda tutelarsi nei confronti di illeciti disciplinari del proprio dipendente.

In particolare, la Corte di Cassazione ha ribadito che il mancato assoggettamento dei controlli difensivi "in senso stretto" alle garanzie di cui all'art. 4 dello Statuto dei Lavoratori comporta l'imposizione di stringenti doveri in capo al datore di lavoro. In sede di impugnativa di licenziamento, a tali doveri corrispondono specifici oneri probatori in capo al datore di lavoro.

Alla luce di quanto sopra, è necessario che si proceda a controlli difensivi soltanto dopo aver valutato attentamente, sulla base di tutte le informazioni disponibili, la sussistenza dei presupposti indicati dalla sentenza in esame, *in primis* il "fondato sospetto" di illecito.

Se all'esito di tale attività emergono indizi concreti a fondamento del sospetto di illecito, il datore

[20] Si veda, Corte d'Appello Roma, 19 gennaio 2022, n. 67.

[21] Cfr. *supra*, nota 14.

[22] Nell'affermare la radicale inutilizzabilità delle informazioni assunte in violazione della disciplina a tutela della riservatezza del lavoratore, la sentenza richiama l'art. 11 comma 2, del d.lgs. n. 196 del 2003 (il "Codice Privacy"), "*nella formulazione vigente all'epoca dei fatti*", secondo cui "[i] *dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*". Tuttavia, a seguito della riforma del Codice Privacy operata con d.lgs. 10 agosto 2018, n. 101, la materia è ora disciplinata dall'art. 2-*decies* del Codice Privacy. Tale disposizione conferma la sanzione dell'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina, facendo però "*salvo quanto previsto dall'articolo 160*-bis" del Codice Privacy secondo cui "[l]*a validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali*".
Dato che il codice di procedura civile non sancisce l'inutilizzabilità di prove precostituite formatesi in violazione di una norma di legge, in base alle citate disposizioni attualmente vigenti, il dato probatorio inutilizzabile al di fuori del processo parrebbe invece utilizzabile in un successivo giudizio civile. La questione è tuttavia ancora aperta. Invero, se da un lato alcuni orientamenti affermano che "*la violazione della regola di condotta ai fini della privacy non si riverbera sull'inutilizzabilità dei dati"* (Trib. Perugia, Sez. Lavoro, 13 aprile 2021, n. 112)*,* dall'altro lato, la Sezione Lavoro della Corte di Cassazione non ha ancora chiarito la propria posizione in merito (cfr., da ultimo, Cass. Civ., Sez. Lav., 11 ottobre 2023, n. 28378, che, pur sollevando la questione, ha ritenuto che non occorresse "*esaminar*[la] funditus […] *poiché la portata della novella del 2018 non rileva*[va] ratione temporis *nel caso in esame*").

di lavoro dovrebbe poi valutare se l'illecito possa essere accertato mediante controlli generalizzati nei quali sarebbero rispettate le garanzie di cui all'art. 4 dello Statuto dei Lavoratori. Ove così non fosse, il datore di lavoro dovrà scegliere le misure di controllo e le relative modalità di attuazione che consentano di accertare l'illecito con il minor livello di invasività possibile della riservatezza del dipendente, tenuto conto delle circostanze in cui il controllo si inserisce e della gravità dell'illecito.

Inoltre, considerata l'importanza riconosciuta dalla Corte di Cassazione all'informazione preventiva al dipendente, il datore di lavoro dovrebbe dotarsi di documenti che permettano ai dipendenti di conoscere le possibili forme di controllo e le garanzie previste a loro tutela.

Si pensi, ad esempio, proprio ai controlli realizzati su strumenti informatici e dispositivi aziendali in dotazione al dipendente (quali pc portatili e *smartphone*) oggetto del caso deciso dalla Corte di Cassazione.

In vista di tali controlli, il datore di lavoro dovrebbe dotarsi di una *policy* che disciplini l'uso degli strumenti in dotazione ai dipendenti, facendo menzione, nell'informativa fornita ai dipendenti ai fini del rispetto del GDPR, della possibilità che tali controlli siano effettuati in caso di fondato sospetto di illeciti disciplinari.

…

CLEARY GOTTLIEB