



LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione

CARLO COLAPIETRO

Università degli studi Roma Tre

ANDREA GIUBILEI

Università degli studi Roma Tre

vol. 7, no. 2, 2021

ISSN: 2421-2695



Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione

CARLO COLAPIETRO

Università degli Studi Roma Tre
Ordinario di Istituzioni di Diritto pubblico
carlo.colapietro@uniroma3.it

ANDREA GIUBILEI

Università degli Studi Roma Tre
Assegnista di ricerca in Istituzioni di Diritto pubblico
andrea.giubilei@uniroma3.it

ABSTRACT

This essay analyzes one of the latest and most important decisions of the Italian Supreme Court on workplace controls. The judgment makes it possible to overcome the doubts that still exist on the possibility for the employer to use the information collected through new means for exercising remote control over the worker for disciplinary purposes.

In fact, technological progress ensures to use very invasive tools for the worker's privacy, capable of carrying out an obscure control, where it is difficult to distinguish between information on work activity and information on the employee's personal life. An example is precisely the one on which the sentence of the Supreme Court focuses: the control of data on the worker's internet browsing, carried out on the computer made available by the company.

In the essay, the authors focus on the compatibility of such checks with the guarantees provided for by art. 4 of the law n. 300 of 1970, adopting an approach focused on protecting the dignity and privacy of the worker.

Keywords: employer's monitoring powers; privacy; employee's dignity; new technologies; working tools.

[https://doi.org/ 10.6092/issn.2421-2695/14118](https://doi.org/10.6092/issn.2421-2695/14118)

Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione (*)

SOMMARIO: 1. Premessa. – 2. L'utilizzo a fini disciplinari dei dati sulle attività informatiche del lavoratore: la questione sottoposta alla Cassazione. – 2.1. L'evoluzione normativa e giurisprudenziale dei controlli difensivi. – 3. Le condizioni di legittimità per l'utilizzo dei dati informatici del lavoratore individuate dalla Cassazione. 4. – Considerazioni conclusive: un bilanciamento a favore della dignità e della riservatezza del lavoratore.

1. Premessa

Con la sentenza 22 settembre 2021, n. 25732, la Corte di Cassazione è tornata ad occuparsi di uno dei bilanciamenti più delicati che si riscontrano nell'ambito del contesto lavorativo. Si tratta dell'ipotesi che vede potenzialmente contrapposti, da una parte, i poteri del datore di lavoro per monitorare e, conseguentemente, proteggere la propria attività d'impresa e, dall'altra, la tutela della dignità e della riservatezza del lavoratore ⁽¹⁾. Con la decisione in esame, infatti, la Cassazione si è pronunciata sulla legittimità del controllo dei dati informatici effettuato dal datore di lavoro sugli strumenti forniti al lavoratore e

(*) Il presente lavoro è frutto della riflessione comune e della collaborazione dei due Autori, tuttavia, i paragrafi 1, 3 e 4 sono stati redatti da Carlo Colapietro ed i paragrafi 2 e 2.1 da Andrea Giubilei.

(¹) Non vi è dubbio che il contesto lavorativo rappresenti una delle principali “formazioni sociali” in cui l'individuo svolge la propria personalità – per richiamare quanto disposto dall'art. 2 Cost. – e in cui esso risulta titolare di diritti in una dimensione relazionale, in cui si trova, in primo luogo, il datore di lavoro. Ed è proprio all'interno di tale dimensione, dal contatto con gli altri, che possono derivare le minacce più insidiose alla propria sfera della personalità, imponendo un bilanciamento tra diritti o interessi potenzialmente contrapposti. Come si vedrà, nel caso in esame, su un piatto della bilancia si trovano i poteri datoriali, sull'altro la riservatezza del lavoratore, che rischia quotidianamente di essere mortificata dalle diverse forme di controllo esercitate dal datore di lavoro. Si rende allora indispensabile la ricerca di un punto di equilibrio, di un ragionevole bilanciamento, tra l'interesse del datore all'esercizio di un proprio potere di controllo ed «i valori di riservatezza e dignità di chi implica in qualche misura nella prestazione lavorativa la propria persona»: così R. De Luca Tamajo, *I controlli sui lavoratori*, in G. Zilio Grandi (a cura di), *I poteri del datore di lavoro nell'impresa. Atti del Convegno di studi (Venezia, 12 aprile 2002)*, Cedam, 2002, 27. Più in generale, sulla riservatezza quale presupposto, non solo per coltivare il proprio privato, ma anche la pienezza della propria sfera pubblica, si veda S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, RCDP, 1997, 601 s.

sull'utilizzabilità di tali dati a fini disciplinari ⁽²⁾. In questo modo, la Suprema Corte ha ridefinito i confini dei “controlli difensivi” e individuato le condizioni per la loro compatibilità con l'attuale assetto normativo, delineato, *in primis*, dall'art. 4 della l. n. 300 del 1970 (per come modificato a seguito dei più recenti interventi legislativi) e dal d.lgs. n. 196 del 2003 (c.d. Codice *privacy*).

Com'è noto, questa tipologia di controlli è frutto dell'elaborazione giurisprudenziale sull'art. 4 dello Statuto dei lavoratori ⁽³⁾, che disciplina l'utilizzo di «Impianti audiovisivi e altri strumenti di controllo» ⁽⁴⁾ nell'ambito dell'attività lavorativa, a partire dai più “classici” impianti di video registrazione, fino ai nuovi strumenti dell'*information end communications technology* che consentono un controllo costante e pervasivo della vita dal lavoratore ⁽⁵⁾.

A tal riguardo, può immaginarsi anzitutto l'ipotesi del controllo del lavoratore fine a sé stesso, fattispecie che – da sempre – si considera in ogni caso vietata. Il problema, tuttavia, si pone per quelle forme di monitoraggio che, sebbene siano astrattamente predisposte per esigenze organizzative e produttive, o per garantire la sicurezza sul luogo di lavoro, implicino indirettamente il controllo dell'attività dei lavoratori. Il legislatore del 1970 ha

⁽²⁾ Sul punto si veda, per tutti, P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017.

⁽³⁾ Sull'evoluzione giurisprudenziale in materia di controlli difensivi si tornerà più approfonditamente *infra*, § 2.1.

⁽⁴⁾ Tale rubrica originariamente faceva riferimento ai soli «Impianti audiovisivi» e, successivamente, è stata ampliata includendo anche «[...] altri strumenti di controllo» ad opera dell'art. 23, d.lgs. n. 151 del 2015 (nell'ambito della più ampia riforma del c.d. *Jobs Act*). A ben vedere, tale ampliamento si è reso necessario a fronte dell'introduzione di nuovi e più sofisticati mezzi – anche tra quelli dati in uso al lavoratore – che consentono il monitoraggio dell'attività lavorativa: sul punto, cfr. E. Dagnino, *Tecnologie e controlli a distanza*, *DRI*, 2015, 4, 988 ss.; P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in Id. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017, 6-9; ed R. Di Meo, *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, *LLI*, 2018, IV, 1, 3 ss.

⁽⁵⁾ Si pensi, ad esempio, al controllo che il datore di lavoro può effettuare sui *social network* del dipendente, «che permettono di individuare da quale luogo e in quale fascia oraria l'utente è connesso, consentono di incamerare tracce, indizi e di procurarsi prove dell'adempimento o dell'inadempimento del lavoratore», indipendentemente dal fatto che la persona si serva di un *device* di proprietà aziendale: così A. Ingraio, *Il controllo a distanza realizzato mediante Social network*, *LLI*, 2016, II, 1, 105 ss., spec. 108. Ma si pensi, per fare un diverso esempio, all'ipotesi analizzata da R. Di Meo, *op. ult. cit.*, 11 ss., che approfondisce il tema del braccialetto elettronico che Amazon utilizza per monitorare le attività dei propri dipendenti. Tale strumento – evidenzia l'Autrice – giunge fino a «far capire all'azienda dove sono le mani del dipendente»; consente di geolocalizzarlo e, tramite un conto alla rovescia, «gli fornisce il tempo massimo per raggiungere la postazione del prossimo prodotto da prendere dagli scaffali»; o, ancora, «fornisce il tempo massimo della pausa» che l'azienda ha stabilito a seconda della tipologia di esigenza indicata dal lavoratore». La medesima vicenda è analizzata anche da A. Ingraio, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, *DRI*, 2019, 3, 895 ss.

imposto, per simili circostanze, la necessaria conclusione di un accordo preventivo con le rappresentanze sindacali aziendali (o con l'Ispettorato del lavoro) e il rispetto dei conseguenti obblighi informativi, quali condizioni per l'installazione e l'uso legittimo delle apparecchiature in questione.

Tuttavia, sotto la vigenza dell'originaria formulazione dell'art. 4, la giurisprudenza di legittimità aveva escluso l'applicabilità di tali limiti e condizioni qualora i controlli a distanza fossero volti a monitorare comportamenti illeciti del lavoratore per tutelare il patrimonio aziendale, elaborando – per l'appunto – la categoria dei cc.dd. “controlli difensivi” (6).

Sul punto, è poi intervenuto il legislatore, che, con l'art. 23 del d.lgs. n. 151 del 2015, ha modificato l'art. 4 dello Statuto includendo espressamente le finalità di tutela del patrimonio aziendale tra le ipotesi che impongono la previa autorizzazione degli impianti (7). Tale intervento normativo è risultato particolarmente divisivo, tanto in dottrina quanto nella giurisprudenza, poiché ha posto un interrogativo sulla possibile permanenza di una categoria di controlli a distanza che potesse essere legittimamente effettuata in deroga alle condizioni previste dall'art. 4 dello Statuto dei lavoratori (8).

Proprio con la citata sentenza n. 25732 del 2021, che qui si commenta, la Cassazione ha fatto chiarezza su questo nodo ancora in parte irrisolto, individuando, non solo le forme di controllo che possono ancora collocarsi al di fuori del perimetro applicativo dell'art. 4 dello Statuto dei lavoratori, ma soprattutto le condizioni affinché le informazioni ottenute risultino legittimamente utilizzabili a fini disciplinari.

Sin d'ora può anticiparsi come la decisione in esame abbia il merito di aver posto al centro la tutela della dignità e della riservatezza del lavoratore, che oggi risulta sempre più vulnerabile. Infatti, nell'evoluzione dei modelli produttivi e organizzativi dell'impresa, la diffusione su larga scala delle moderne tecnologie informatiche ha attribuito al potere di controllo del datore di lavoro contorni

(6) In tal senso, si segnala, sin d'ora, Cass. 17 luglio 2007, n. 15892, con commenti di R. Staiano, *In tema di apparecchiature di controllo a distanza*, *DI*, 2008, 1, 31 ss. e A. Bellavista, *Controlli a distanza e necessità del rispetto della procedura di cui al co. 2 dell'art. 4 Stat. Lav.*, *RIDL*, 2008, 2, 794 ss.

(7) Attualmente, infatti, l'art. 4, co. 1, l. n. 300/1970 dispone: «gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali» (corsivi aggiunti).

(8) Cfr. M. Marazza, *I controlli a distanza del lavoratore di natura “difensiva”*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, 27 ss.

nuovi. «La trasformazione digitale ha, infatti, contribuito in larga misura a raffinare le tecniche di sorveglianza sui dipendenti»⁽⁹⁾. Ormai vi è un ventaglio tecnologico ampio e in continua evoluzione, capace di realizzare forme di monitoraggio del lavoratore subordinato sempre più penetranti e insidiose rispetto al modello classico del controllo “in presenza”. In principio, infatti, il controllo datoriale poteva avvenire quasi esclusivamente all’interno dell’azienda, ad esempio con l’installazione di impianti di ripresa audiovisiva o con il monitoraggio dei flussi telefonici. Ma il controllo è ormai diventato costante, capillare, pervasivo, indiscriminato e, soprattutto, è diventato delocalizzato e, quindi, oscuro⁽¹⁰⁾. Basti pensare alla possibilità – astratta – di controllare le mail in entrata e uscita, o anche la messaggistica, del lavoratore; di monitorare la navigazione sul *web*; di aprire file archiviati su disco (dai documenti ai file multimediali); di seguire la posizione geografica del dipendente tramite GPS (ad esempio nelle vetture aziendali); o, addirittura, di interagire con i *social network* dei propri dipendenti⁽¹¹⁾. Tutti strumenti da cui è possibile trarre informazioni rientranti, non solo nella sfera *lavorativa*, ma anche in quella *personale* del dipendente.

Questa invasività del controllo e soprattutto la sua natura occulta e remota comprimono fortemente i diritti del lavoratore. Il rischio di una indebita

⁽⁹⁾ Così A. Ingraio, *Il bracciale elettronico tra privacy e sicurezza del lavoratore*, cit., 895 s., che prosegue osservando come «qualsiasi *device* permette di visualizzare con un’indagine retrospettiva ben distinte categorie di dati, prescelti in base all’orario, al contenuto, al luogo di immagazzinamento e così via. Così ciascun dispositivo costituisce una miniera d’informazioni, attinenti alla sfera sia lavorativa sia personale, la cui conservazione nel tempo e nello spazio può costituire un pericolo per il lavoratore».

⁽¹⁰⁾ Cfr. G. Ziccardi, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, LLI, 2016, II, 1, 48 ss., il quale osserva come si sia passati da un controllo classico «in puro stile orwelliano» ad un «controllo di tipo kafkiano, estremamente frammentato, complesso, labirintico, oscuro e burocratizzato, composto da dati che si incrociano – lavorativi e privati – e da problemi tecnici difficilmente comprensibili per il lavoratore [...]».

⁽¹¹⁾ Sul controllo dei *social network* del lavoratore, si vedano, tra tutti, A. Ingraio, *Il controllo a distanza realizzato mediante Social network*, cit., 105 ss., M. Forlivesi, *Il controllo della vita del lavoratore attraverso i social network*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017, 37 ss., ed E. Dagnino, *Controlli social dei lavoratori: un’interessante pronuncia della Cassazione*, DRI, 2015, 3, 833 ss. Quest’ultimo – a commento di Cass. 27 maggio 2015, n. 10955 – analizza una vicenda particolarmente rappresentativa della pervasività e oscurità che possono caratterizzare alcuni controlli datoriali oggi. In detta occasione, infatti, un’azienda aveva autorizzato il proprio responsabile delle risorse umane a creare un profilo falso su un *social network*, utilizzato anche da un proprio dipendente, per dialogare con quest’ultimo e verificare, così, l’uso del dispositivo mobile personale durante l’orario di lavoro. È interessante constatare come la Suprema Corte abbia incluso una simile operazione nell’alveo dei controlli difensivi, riconoscendo la legittimità del comportamento attuato dalla società.

invasione della propria sfera intima, al di fuori del contesto lavorativo, potrebbe dissuadere l'individuo dal compiere quelle scelte esistenziali attraverso le quali esercita il proprio diritto all'autodeterminazione⁽¹²⁾. Ed è per questo che un'adeguata protezione della sua riservatezza, *anche* nel luogo di lavoro, può rappresentare la garanzia “presupposto” dell'esercizio di molti altri diritti fondamentali⁽¹³⁾.

2. L'utilizzo a fini disciplinari dei dati sulle attività informatiche del lavoratore: la questione sottoposta alla Cassazione

La decisione in esame trae origine dal ricorso di una lavoratrice sanzionata con licenziamento per giusta causa a seguito di alcuni accertamenti effettuati dalla Fondazione per cui prestava la propria attività lavorativa. I controlli erano stati giustificati dalla diffusione di un *virus* nella rete locale, effettivamente risultato correlato ad un *file* rinvenuto nel computer aziendale in uso alla lavoratrice che, dai suoi *download*, aveva iniziato a propagarsi nella rete della Fondazione, criptando file all'interno di vari dischi di rete, rendendoli illeggibili e inutilizzabili. Secondo quanto emerge dalla sentenza, in occasione dei controlli effettuati dall'amministrazione del sistema informatico, «venivano in rilievo numerosi accessi – da parte della lavoratrice – a siti che all'evidenza erano stati visitati per ragioni private, per un tempo lungo, tale da integrare una sostanziale interruzione della prestazione lavorativa»⁽¹⁴⁾.

A ben vedere, tali circostanze sono riconducibili ad alcuni dei controlli più pervasivi e lesivi della sfera personale del lavoratore, vale a dire quelli del computer in uso (anche se appartenente all'azienda), della posta elettronica, della

⁽¹²⁾ Questa considerazione trova le sue radici nella nota decisione della Corte costituzionale federale tedesca sull'autodeterminazione informativa, la nota *Volkszählungsurteil* o “sentenza sul censimento” (*Bundesverfassungsgericht*, 15 dicembre 1983, 1BvR 209/83). Secondo la Corte tedesca, il timore circa la possibilità che comportamenti anomali vengano ogni volta annotati e schedati, con la possibilità di una successiva trasmissione od uso, porta necessariamente a due conseguenze: o quella di nascondere tali atteggiamenti, o quella di rinunciare ad essi. In questo modo, però, come è evidente, vi è un enorme pregiudizio delle possibilità di espressione e di libertà. Per un approfondimento su tale decisione, si veda G. Sartor, *Tutela della personalità e normativa per la “protezione dei dati”. La sentenza della Corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del Datenschutz*, ID, 1986, XII, 3, 95 ss.

⁽¹³⁾ Cfr. sul punto M. Aimo, *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, 2003, 36. Per un approfondimento, sia consentito un rinvio a C. Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, GDLRI, 2017, 155, 439 ss., spec. 451.

⁽¹⁴⁾ Cass. 22 settembre 2021, n. 25732, par. 2 dei *Fatti di causa*.

cronologia di internet: «strumenti che non distinguono, e non separano, attività lavorativa da attività personale, e che possono intercettare ogni azione (anche, ad esempio, eventuali e-mail personali presenti sul computer fornito dal datore di lavoro)»⁽¹⁵⁾. Si tratta di contesti in cui è assai facile che i dati privati dell'utente-lavoratore possano intrecciarsi con quelli attinenti all'attività lavorativa, consentendo (potenzialmente) al datore di lavoro di adottare criteri di differenziazione del trattamento giuridico del lavoratore a carattere illecito e discriminatorio o, come nel caso di specie, di utilizzare i risultati del controllo a fini disciplinari.

Solo tramite l'analisi delle attività informatiche e telematiche della lavoratrice, infatti, la Fondazione ha potuto contestarle – oltre ai danni causati all'azienda per l'indisponibilità della rete – l'utilizzo «a soli fini privati» dei mezzi informatici messi a disposizione e la sostanziale interruzione dell'attività lavorativa, visti tempi e quantità di navigazione «per fini privati». A ben vedere, quindi, lo stesso datore di lavoro ha avuto la consapevolezza della natura delle informazioni raccolte. D'altronde, l'analisi della cronologia o, in generale, dell'attività svolta sul *web* rappresenta un tipo di controllo che implica strutturalmente la necessità di conoscere i fini per i quali è stata utilizzata la rete. È evidente, allora, che ciò consentirà al datore di lavoro di avere accesso, anche solo indirettamente o non intenzionalmente, a una mole significativa di informazioni attinenti alla sfera più intima della persona⁽¹⁶⁾. Per di più – e come

(15) Così G. Ziccardi, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, cit., 57. In tal senso, si vedano, altresì, M. Del Conte, *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, *DI*, 2007, 3, 497 ss. ed A. Sitzia, *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, *ADL*, 2017, 3, 804 ss.

(16) Cfr. G. Ziccardi, *op. ult. cit.*, 55 ss., spec. 57, il quale evidenzia come la tipologia di controllo in esame operi «a strascico», «carpendo tutti i dati e lasciando al controllore il compito di separare le informazioni, e in maniera indiscriminata». L'Autore prende in considerazione proprio alcune delle ipotesi venute in rilievo nella fattispecie in esame, tra cui il controllo del computer aziendale e/o delle attività in rete di un dispositivo fisso o mobile, evidenziando come, molto spesso, il dispositivo sia «preparato» e programmato dal datore di lavoro e dai suoi tecnici e fornito al lavoratore, cui non sono lasciate possibilità di disattivazione degli strumenti di controllo o di modifiche ulteriori al dispositivo (ad esempio: per cancellare alcune tracce). Sul punto, può considerarsi quanto prospettato da E.O. Policella, *Il monitoraggio elettronico dei dipendenti per scopi difensivi*, *DI*, 2007, 1, 83 ss., che, richiamando i suggerimenti elaborati dal Gruppo dei Garanti europei nel «Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro» (29 maggio 2002 - WP 55), evidenzia come risulti senz'altro più opportuno assicurare l'utilizzo di dispositivi di *blocco* e non di *controllo*. Ci si riferisce, in particolare, all'utilizzo di «software che bloccano l'accesso dei siti al fine di prevenire eventuali abusi del dipendente nonché rilasciare agli utenti, in caso di richiesta di accesso a siti bloccati dall'azienda, un'avvertenza automatica». Il documento di lavoro WP

si vedrà questo rappresenta un aspetto centrale – anche relative a momenti antecedenti a quello in cui è sorta l'esigenza di effettuare il controllo, in cui il soggetto era inevitabilmente inconsapevole e non adeguatamente informato circa la vulnerabilità dei propri dati personali.

Simili circostanze pongono «un lacerante dilemma circa i confini del diritto alla riservatezza garantito ai lavoratori dal nostro ordinamento»⁽¹⁷⁾. Non a caso, nella vicenda in esame, la dipendente si era rivolta anzitutto all'Autorità Garante per la protezione dei dati personali con ricorso presentato ai sensi dell'art. 145 del d.lgs. n. 196 del 2003⁽¹⁸⁾. Il Garante aveva ordinato alla Fondazione di astenersi dall'effettuare qualsiasi ulteriore trattamento dei dati acquisiti dalla cronologia dei *browser* utilizzati dalla ricorrente, eccettuata la mera conservazione degli stessi ai fini della loro eventuale acquisizione da parte giudiziaria. Così, successivamente, il Tribunale adito in sede di opposizione aveva ritenuto che la delibera del Garante *privacy* non ostava all'utilizzazione nel processo dei dati estratti dal computer aziendale e che la loro acquisizione non si era risolta in un controllo a distanza vietato dall'art. 4 dello Statuto dei lavoratori. I controlli, infatti, erano rivolti più che altro a bonificare il sistema

55/2002 è disponibile sul sito istituzionale del Garante *privacy*: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1609517>.

⁽¹⁷⁾ Così A. Sitzia, *Il diritto alla privacy nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, 2013, 139.

⁽¹⁸⁾ Nella direzione di assicurare la piena applicazione della disciplina a tutela dei dati personali nell'ambito dei rapporti di lavoro vanno numerosi interventi del Garante e, in particolare, le «Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati» (delib. 23 novembre 2006, n. 53, in www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939), nonché le «Linee guida per l'utilizzo di internet e della posta elettronica nei posti di lavoro» (delib. 1° marzo 2007, n. 13, in www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522).

Entrambi i provvedimenti muovono dal presupposto che le informazioni relative all'attività dei lavoratori devono essere raccolte ed eventualmente utilizzate dal datore di lavoro nel rispetto delle disposizioni previste dal d.lgs. n. 196 del 2003 e, soprattutto, che le stesse possono riguardare, non solo l'attività lavorativa, ma anche la sfera intima e privata del lavoratore o di soggetti terzi: da ciò l'esigenza di garantire che il trattamento di tali dati personali si svolga nel rispetto della riservatezza e della dignità degli interessati (art. 2, d.lgs. n. 196 del 2003). Per un'analisi sui contenuti delle linee guida del Garante si vedano I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, LLI, 2016, II, 1, 3 ss., spec. 31 ss.; M. Del Conte, *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, cit., 497 ss.; G. Finocchiaro, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017, 51 ss., spec. 56 s.; P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, RIDL, 2009, 3, 323 ss.

informatico dal *virus* e non a sorvegliare l'adempimento della prestazione lavorativa della dipendente.

Anche la Corte d'appello di Roma – investita del reclamo della Fondazione, avendo il Tribunale accordato alla lavoratrice la tutela reintegratoria – non si è discostata da simili valutazioni. Tuttavia, a differenza del Tribunale, aveva ritenuto la sanzione inflitta proporzionata alla condotta della dipendente, poiché i numerosi accessi ad internet di natura ludica e privata (e, quindi, per fini personali) avrebbero frammentato indebitamente la prestazione lavorativa, resa in maniera discontinua.

Sulla base delle argomentazioni contenute in tale decisione, la dipendente ha deciso di rivolgersi alla Corte di Cassazione, lamentando anzitutto l'illegittimità dell'utilizzo a fini disciplinari delle informazioni raccolte ⁽¹⁹⁾. In particolare, essa ritiene che la mancanza di un'adeguata informazione sulle modalità di effettuazione dei controlli non consentirebbe al datore di lavoro di fondare la propria sanzione disciplinare su simili dati. Secondo la ricorrente, infatti, la loro inutilizzabilità si estenderebbe fino al piano della prova dell'illecito, che ne risulterebbe illegittimamente raccolta.

Come evidenziato dalla stessa Corte di Cassazione, tali aspetti risultano di «indubbio rilievo nomofilattico» ⁽²⁰⁾, proprio perché consentono l'adozione di una pronuncia sulla compatibilità dei cc.dd. “controlli difensivi” con l'attuale tessuto normativo.

2.1. L'evoluzione normativa e giurisprudenziale dei controlli difensivi

Come anticipato, il tema dei “controlli difensivi” si fonda sulla necessità di bilanciare adeguatamente due interessi contrapposti, ma parimenti bisognosi di riconoscimento e protezione. Da una parte vi è il diritto del datore di lavoro di tutelare il proprio patrimonio e la propria attività imprenditoriale, funzionalmente collegata, in maniera diretta, con il lavoro svolto dai propri dipendenti. Dall'altra vi è il rispetto dei valori di riservatezza e dignità di chi implica la propria persona nella prestazione lavorativa.

⁽¹⁹⁾ Si tratta dell'unico motivo di ricorso su cui la Cassazione deciderà di concentrarsi ai fini della decisione, ritenendo assorbiti i successivi (relativi, più che altro, alla corretta applicazione della disciplina del licenziamento o ad aspetti procedurali). Per tale ragione, nel presente scritto, ci si concentrerà esclusivamente sul primo motivo di ricorso.

⁽²⁰⁾ Così Cass. 22 settembre 2021, n. 25732, par. 8 delle *Ragioni della decisione*.

Non vi è dubbio che anche l'attività imprenditoriale rappresenti un interesse di importanza primaria nel nostro ordinamento, in quanto tale ampiamente tutelato dalla Costituzione. Di certo viene in rilievo, anzitutto, il riconoscimento della libertà di iniziativa economica privata di cui all'art. 41 Cost.; ma il potere di controllo del datore di lavoro potrebbe essere diretto anche alla tutela di altri diritti fondamentali: i *devices* elettronici, come il computer, potrebbero costituire strumenti per la commissione di reati informatici, per i quali è prevista (anche) la responsabilità degli enti collettivi, con il conseguente onere del datore di lavoro di predisporre adeguati strumenti di prevenzione; o, ancora, un uso scorretto delle attrezzature informatiche da parte dei dipendenti potrebbe dar luogo a comportamenti lesivi della sfera personale e morale di altri lavoratori, come nel caso di *mobbing*, molestie o *stalking* e, anche in questo caso, si potrebbe concretizzare una responsabilità del datore di lavoro per non aver impedito il fatto.

Sono tutti esempi di quanto sia delicato e complesso contemperare le esigenze di controllo datoriale con il rispetto della *privacy* del singolo. Un bilanciamento, quest'ultimo, richiesto anzitutto dallo stesso art. 41 Cost., che, se riconosce la libertà dell'iniziativa economica privata, allo stesso tempo impone che essa non si svolga in modo da recare danno alla sicurezza, alla libertà, alla dignità umana ⁽²¹⁾.

Sulla base di tali premesse, il legislatore ha indicato nell'art. 4 della legge n. 300 del 1970 la direttrice regolativa della materia ⁽²²⁾. La sua originaria formulazione prevedeva, anzitutto, un divieto assoluto di utilizzazione di impianti audiovisivi o di altre apparecchiature per il controllo dell'attività del

⁽²¹⁾ In questo modo, il Costituente ha voluto escludere che i valori inerenti alla dignità del lavoratore venissero coinvolti nell'esplicazione del rapporto di lavoro. Così, con l'approvazione della l. 300/1970, il legislatore ha dato attuazione a questo disegno costituzionale, perseguendo l'idea-madre secondo cui «l'organizzazione deve modellarsi sull'uomo e non viceversa»: così L. Mengoni, *Diritto e valori*, Il Mulino, 1985, 379 e 400, ed Id., *Le modificazioni del rapporto di lavoro alla luce dello Statuto dei lavoratori*, in Aa. Vv. (a cura di), *L'applicazione dello Statuto dei lavoratori. Tendenze e orientamenti*, Giuffrè, 1973, 17 ss.

⁽²²⁾ Cfr. A. Levi, *Il controllo informatico sull'attività del lavoratore*, Giappichelli, 2013, 11, che rileva l'acuta percezione, da parte del legislatore dello Statuto, delle enormi potenzialità lesive del controllo a distanza dell'attività lavorativa attraverso le più svariate apparecchiature, che «per sua natura è perdurante, continuativo, subdolo». Difatti, come messo in luce dall'Autore, la libertà, la dignità e la personalità morale del lavoratore risulterebbero lese mediante un controllo continuativo sull'attività lavorativa da parte dell'imprenditore, la cui iniziativa economica privata è addirittura costituzionalmente vincolata, ai sensi dell'art. 41, co. 2, Cost., al rispetto del limite della dignità umana (oltre che della libertà e della sicurezza). Tali aspetti sono stati oggetto di approfondimento già in C. Colapietro, *Digitalizzazione del lavoro e tutela della riservatezza della persona*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi di tutela*, Giappichelli, 2017, 21 ss., spec. 27 ss.

lavoratore fine a sé stesso. In questo modo si voleva limitare l'esercizio del potere organizzativo e direttivo dell'imprenditore, nella misura in cui le relative modalità potessero incidere negativamente sulla sfera intima della persona.

Il secondo comma dell'articolo 4 consentiva, tuttavia, di installare strumenti di controllo dell'attività lavorativa a due condizioni: *a)* dovevano esservi esigenze organizzative, produttive o di sicurezza sul lavoro tali da giustificare l'installazione di un meccanismo audiovisivo di monitoraggio; *b)* era necessario un accordo preventivo con le rappresentanze sindacali (o con l'Ispettorato del lavoro). In questo modo, il secondo comma rendeva possibili – circondandoli di garanzie procedurali – i cosiddetti “controlli preterintenzionali”, cioè quei controlli che il datore di lavoro esercita per esigenze organizzative e produttive o per assicurare la sicurezza del lavoro, ma dai quali può derivare, come conseguenza accidentale, la possibilità di controllo a distanza dell'attività dei lavoratori ⁽²³⁾.

Fattispecie diversa da quella in esame è, invece, quella dei controlli difensivi ⁽²⁴⁾. Come anticipato, è stata la giurisprudenza a farsi carico del corretto inquadramento di tali controlli a distanza, funzionali alla tutela del patrimonio aziendale e aventi ad oggetto comportamenti illeciti del lavoratore, ipotesi operante al di fuori del perimetro della previgente formulazione dell'art. 4 dello Statuto. Secondo tale orientamento giurisprudenziale, questo tipo di controlli era dunque escluso dalle garanzie ivi previste, in particolare dalla procedura

⁽²³⁾ Come, d'altronde, si evince dalla lettera della precedente formulazione dell'art. 4 dello Statuto, che si riferiva a impianti e strumenti richiesti da esigenze organizzative e produttive o per assicurare la sicurezza sul lavoro «dai quali derivi *anche* la possibilità di controllo a distanza dell'attività dei lavoratori» (corsivo aggiunto).

⁽²⁴⁾ Tale tipologia di controlli realizzati in ambito lavorativo è da tempo oggetto di attenta analisi da parte della dottrina, che si è concentrata anche sulla sorte dei controlli difensivi a seguito della modifica legislativa intervenuta nel 2015. Tra tutti, si vedano I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, cit., 3 ss.; L. Cairo, *Controlli a distanza: passato e presente di un tema ancora controverso*, LG, 2018, 2, 147 ss.; M.T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il “Jobs Act” (art. 23 D.Lgs. 151/2015): spunti per un dibattito*, LLI, 2016, II, 1, III ss.; C. Coscia, *Le modifiche all'art. 4 Stat. lav.: dignità e riservatezza del lavoratore continuano a prevalere sulla tutela del patrimonio aziendale*, DPP, 2018, 7, 871 ss.; R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, RIDL, 2016, 1, 77 ss.; A. Ingraio, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, RIDL, 2017, 1, 46 ss.; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, 1 ss.; G. Proia, *Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza*, RIDL, 2016, 4, 547 ss.; A. Sitzia, *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso del lavoratore*, LLI, 2016, II, 1, 83 ss.; A. Trojsi, *Al cuore del nuovo art. 4, co. 2, St. lav.: la delimitazione della fattispecie degli «strumenti utilizzati per rendere la prestazione lavorativa»*, RIDL, 2017, 2, 317 ss.; P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, cit., *passim*.

negoziale e dalle autorizzazioni sindacali richieste dal secondo comma. Alla luce di questa interpretazione, la riservatezza del dipendente doveva essere controbilanciata e, quindi, poteva considerarsi recessiva, a fronte dell'esigenza di prevenire la commissione di illeciti ⁽²⁵⁾.

In tal senso, può considerarsi la sentenza 3 aprile 2002, n. 4746, con cui la Cassazione ha affermato che, ai fini dell'operatività del divieto di cui all'art. 4 dello Statuto dei lavoratori, «è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, [...] gli apparecchi di rilevazione di telefonate ingiustificate» ⁽²⁶⁾.

Sulla base di queste circostanze, nel tempo, la giurisprudenza si è occupata di individuare ulteriori condizioni per ritenere legittimi i controlli difensivi. Anzitutto, si riteneva presupposto necessario che i controlli fossero stati disposti *ex post*, vale a dire in un momento successivo al verificarsi del comportamento illecito attribuito al dipendente, in modo da evitare che l'attività di controllo risultasse, in realtà, un mero monitoraggio sull'esecuzione della prestazione lavorativa svolta ⁽²⁷⁾. In secondo luogo, era stata individuata, quale ulteriore condizione per l'esercizio dei controlli difensivi, la circostanza secondo cui gli illeciti da accertare dovevano essere lesivi del patrimonio o dell'immagine aziendale ⁽²⁸⁾.

Proprio quest'ultimo aspetto risulta tra gli elementi centrali dell'intervento legislativo con cui il Governo – nell'ambito della più ampia

⁽²⁵⁾ Per il corretto inquadramento dei comportamenti rientranti o meno nell'ambito dell'art. 4, St. Lav., si veda Cass. 17 luglio 2007, n. 15892. In tale occasione, la Corte ribadisce il principio secondo cui l'esigenza di evitare condotte illecite da parte dei dipendenti non possa assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore. Tale esigenza, infatti, non consente di espungere dalla fattispecie di cui all'art. 4 i casi dei cc.dd. controlli difensivi «ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori quando tali comportamenti riguardino [...] l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro». A ben vedere, quindi, i controlli attuati per far fronte a comportamenti illeciti del lavoratore possono prescindere dalle condizioni di cui all'art. 4 dello Statuto solo qualora gli illeciti abbiano ad oggetto «beni estranei» al rapporto di lavoro.

⁽²⁶⁾ Cass. 3 aprile 2002, n. 4746, in *Mass. Giur. it.*, 2002. In tal senso, più recentemente, cfr. Cass. 28 maggio 2018, n. 13266 (ordinanza relativa ad una vicenda in cui risultava applicabile ancora la precedente formulazione dell'art. 4, St. lav.).

⁽²⁷⁾ Cfr. Cass. 5 ottobre 2016, n. 19922.

⁽²⁸⁾ Cfr. Cass. 23 febbraio 2012, n. 2722.

riforma attuata tramite il *Jobs Act* – ha aggiornato la disciplina dei controlli di cui all'art. 4 dello Statuto dei lavoratori, con l'art. 23 del d.lgs. n. 151 del 2015 (in attuazione della legge di delega n. 183 del 2014). Nella sua attuale formulazione, l'art. 4 non contempla più espressamente il divieto assoluto di utilizzare impianti audiovisivi o altre apparecchiature elettroniche per finalità di controllo a distanza dell'attività dei lavoratori ⁽²⁹⁾. Questo solo perché si afferma implicitamente la regola secondo cui il controllo a distanza dell'attività dei lavoratori (fine a sé stesso) non è legittimo se non risulta sorretto dalle esigenze indicate dallo stesso art. 4 dello Statuto.

Oltre a ciò, il legislatore ha stabilito che per l'utilizzo degli strumenti che servono al lavoratore per rendere la prestazione lavorativa (come computer, *tablet* e cellulari) e per l'installazione di strumenti di registrazione degli accessi e delle presenze (*badge*) non è necessaria la procedura di accordo sindacale o di autorizzazione ⁽³⁰⁾. Su questo punto, tuttavia, il Ministero del Lavoro ha subito precisato che, se i suddetti *devices* vengono modificati con apposite funzionalità

⁽²⁹⁾ Sul punto, si veda A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, cit., 4 ss., il quale osserva come, pur in mancanza di una disposizione analoga a quella presente nell'originaria versione dell'art. 4, co. 1, il testo attuale comunque vieti al datore di lavoro di avvalersi di strumenti tecnologici per controllare a distanza la prestazione del dipendente. Questo perché – osserva l'Autore – la norma ammette i controlli esclusivamente per esigenze organizzative e produttive, per la sicurezza sul lavoro e per tutelare il patrimonio aziendale. Dunque, per converso, i controlli devono considerarsi «vietati in ogni altro e diverso caso». Sul punto, l'Autore conclude osservando come il mantenimento del divieto in questione e, quindi, l'esclusione di un ampliamento tecnologico del potere di controllo del datore di lavoro devono essere ricondotte e motivate «con l'esigenza di bilanciamento tra l'interesse del datore di lavoro di verificare l'esatta esecuzione della prestazione lavorativa, da un parte, e, dall'altra, la condizione di subordinazione del dipendente destinata altrimenti ad accentuarsi in forme più invasive e, per di più, connotate dal permanente disvalore per i controlli tecnologici realizzati *dalla macchina sull'uomo*».

⁽³⁰⁾ Cfr. P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?*, in Id. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, 97 ss., spec. 107 ss., che nell'analizzare le novità introdotte in tema di controlli sugli strumenti per eseguire la prestazione lavorativa, mette in luce come le incertezze che connotavano la previgente normativa si siano ora spostate, per l'appunto, «lungo il discrimine – non scritto eppure, in qualche misura, sottinteso – tra le tecnologie di controllo e quelle prestazionali». Tuttavia, secondo l'Autrice, si tratterebbe di un discrimine sottile e incontrovertibile e, in alcuni casi, inesistente, «come accade per gli strumenti informatici intrinsecamente e volutamente polifunzionali: nella migliore delle ipotesi, sarà possibile un giudizio di prevalenza o di preponderanza circa l'utilizzo per scopi lavorativi. A meno di voler ritenere – magari seguendo il consiglio dell'esperienza – che nel dubbio al datore convenga rispettare la disciplina della prima parte dell'art. 4 St. lav.».

per il controllo a distanza del lavoratore, torna ad essere necessaria la previa procedura di accordo sindacale ⁽³¹⁾.

Il terzo e ultimo comma dell'art. 4, inoltre, prevede che tutte le informazioni raccolte dal datore di lavoro tramite questa categoria di strumenti sono utilizzabili «a tutti i fini» connessi al rapporto di lavoro, purché il lavoratore sia adeguatamente informato tanto delle modalità d'uso degli strumenti e di effettuazione dei controlli e a condizione che ciò avvenga nel rispetto di quanto disposto dal Codice della *privacy* ⁽³²⁾. Tale richiamo – letto assieme all'utilizzabilità delle informazioni raccolte per tutti i fini connessi all'attività lavorativa, tra cui quello disciplinare – impone che, qualora «il trattamento sia rivolto alla tutela del patrimonio aziendale, il datore dovrà specificarlo nell'informativa, che dovrà anche contenere, a pena di inutilizzabilità, l'indicazione delle conseguenze disciplinari che il datore si riserva di trarre in caso di accertamento di un comportamento illecito» ⁽³³⁾.

Tuttavia, tra le maggior novità della riforma, vi è la nuova formulazione del primo comma dell'art. 4 dello Statuto. Si ribadisce la necessità di avviare e concludere procedure di autorizzazione sindacale per l'installazione degli strumenti di monitoraggio e si stabilisce che il controllo è ammesso, non più solo per esigenze organizzative, produttive o di sicurezza, ma anche per la tutela del patrimonio aziendale contro attività illecite del lavoratore.

Lungi dal rappresentare una soluzione circa il corretto inquadramento dei controlli difensivi, l'intervento legislativo da ultimo citato ha solamente

⁽³¹⁾ Si veda il Comunicato stampa del Ministero del Lavoro e delle politiche sociali, «Controlli a distanza: Ministero del Lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy», 18 giugno 2016 in www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx.

⁽³²⁾ Su quest'ultimo punto, cfr. A. Ingraio, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, RIDL, 2017, 1, 46 ss., che evidenzia come il riferimento alla normativa in tema di *privacy*, più che «un *escamotage* per i dipendenti disonesti», debba essere inteso come il fondamento per imporre «la definizione di una misura equilibrata e graduale del controllo informatico», ispirata ai principi di correttezza, trasparenza, liceità e necessità individuati dal Garante *privacy*. A tal riguardo – come sottolinea anche l'Autore – non può non tenersi conto del contributo offerto dall'approvazione del Regolamento UE 2016/279 in materia di protezione dei dati personali (c.d. GDPR). Più in generale, sull'impatto del Regolamento nel campo delle attività lavorative, cfr. A. Donini, *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, DRI, 2018, 1, 222 ss.; C. Del Federico, *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017, 61 ss.; A. Maresca – S. Ciucciovino – I. Alvino, *Regolamento UE 2016/679 e rapporto di lavoro*, in C. Colapietro – L. Califano (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, 2017, 310 ss., spec. 345 ss.; C. Ogriseq, *Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, LLI, 2016, II, 2, 29 ss.

⁽³³⁾ Così ancora A. Ingraio, *op. ult. cit.*, 46 ss.

ampliato le divisioni dottrinarie e giurisprudenziali in tema di controlli difensivi. Come è stato osservato, «da un lato, c'è chi ritiene che i controlli difensivi siano stati ormai pienamente assorbiti nella nuova regolamentazione legale, con la conseguenza che gli stessi sono consentiti solo tramite impianti debitamente autorizzati, quando necessario, e comunque nel rispetto degli obblighi informativi. Dall'altro chi, invece, propone un aggiornamento del concetto di controllo a distanza al fine di sostenerne la sopravvivenza, in deroga all'art. 4 dello Statuto, in una prospettiva di ineliminabile bilanciamento dei contrapposti interessi»⁽³⁴⁾.

È proprio nel solco di questa divisione che si colloca la sentenza n. 25732 del 2021, con cui la Cassazione ha chiarito quale sia la sorte dei controlli difensivi a seguito del citato intervento legislativo, specificando, altresì, le condizioni per poter legittimamente utilizzare a fini disciplinari i dati raccolti con l'attività di controllo.

3. Le condizioni di legittimità per l'utilizzo dei dati informatici del lavoratore individuate dalla Cassazione

Per stabilire quale tipologia di controlli a distanza possa ancora collocarsi al di fuori del perimetro tracciato dal (nuovo) art. 4 dello Statuto dei lavoratori, la Cassazione propone un'ulteriore suddivisione, tra “controlli difensivi” *in senso lato* e *in senso stretto*. I primi consisterebbero nei controlli «a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto di tale patrimonio»; data la loro natura, essi richiedono necessariamente il rispetto delle previsioni di cui all'art. 4 dello Statuto (per come novellato nel 2015). Invece, i secondi, cioè i controlli difensivi in senso stretto, sarebbero quelli «diretti ad accertare specificamente condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro»⁽³⁵⁾.

Ebbene, secondo la Suprema Corte, sono proprio questi ultimi controlli che, anche quando vengono svolti con strumenti tecnologici, «non avendo ad oggetto la normale attività del lavoratore, si [situano], anche oggi, all'esterno del perimetro applicativo dell'art. 4»⁽³⁶⁾. Sul punto, la Corte prosegue osservando

⁽³⁴⁾ Così M. Marazza, *I controlli a distanza del lavoratore di natura “difensiva”*, cit., 30.

⁽³⁵⁾ Cass. 22 settembre 2021, n. 25732, par. 31 delle *Ragioni della decisione*.

⁽³⁶⁾ Cass. 22 settembre 2021, n. 25732, par. 32 delle *Ragioni della decisione*.

come l’istituzionalizzazione della procedura di accordo con le rappresentanze sindacali – coinvolte per consentirgli di verificare l’effettiva esigenza di installare strumenti di controllo – sembrerebbe necessaria solo per le scelte che riguardano l’intera organizzazione dell’impresa. Al contrario, avrebbe meno senso prevedere la medesima procedura rispetto ad eventi straordinari ed eccezionali, correlati alla necessità di accertare e sanzionare gravi illeciti di un singolo lavoratore.

Tale chiarimento sembrerebbe mettere un punto sull’effettiva “sopravvivenza” dei controlli difensivi, anche a seguito delle modifiche introdotte con il *Jobs Act*. Tuttavia, ciò che la Corte si premura di sottolineare è la necessità che il datore di lavoro, pur in presenza di un sospetto di attività illecita, agisca nel perseguimento di determinati principi e al verificarsi di determinate condizioni.

Tra i primi, viene annoverato, anzitutto, quello secondo cui «in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e della riservatezza del lavoratore»⁽³⁷⁾. A sostegno di tale conclusione, già ampiamente consolidata, la Corte richiama anche le considerazioni emerse nell’ambito giurisprudenza della Corte Europea dei diritti dell’Uomo, in particolare quella formatasi sull’art. 8 della CEDU. Quest’ultimo, com’è noto, sancisce il «Diritto al rispetto della vita privata e familiare», un ambito che deve essere interpretato – secondo la Corte di Strasburgo – in maniera estensiva, al punto da includervi senz’altro anche la “vita professionale”⁽³⁸⁾. Per tale ragione, pur nel riconoscimento in capo al datore di lavoro di poteri finalizzati alla protezione dei propri interessi imprenditoriali, essi devono sempre essere bilanciati con il diritto alla riservatezza dei lavoratori ed esercitati alla luce dei principi di proporzionalità e di minimizzazione del controllo⁽³⁹⁾.

⁽³⁷⁾ Cass. 22 settembre 2021, n. 25732, par. 37 delle *Ragioni della decisione*. Qui la Corte evidenzia come si tratti di un principio già ampiamente consolidato nella propria giurisprudenza formatasi nel vigore della precedente formulazione dell’art. 4 dello Statuto dei lavoratori. Vengono richiamati numerosi precedenti in tal senso, primo tra tutti la già citata sentenza n. 15892 del 2007, fino alla più recente Cass. 19 settembre 2016, n. 18302.

⁽³⁸⁾ Come evidenzia parte della dottrina, infatti, «la nozione di “vita privata” ex art. 8 CEDU è particolarmente fluida e non si presta a una definizione esaustiva: si tratta di un concetto che copre l’integrità fisica e psicologica di una persona e, in una certa misura, il diritto di stabilire e sviluppare relazioni con altri esseri umani, potendo abbracciare aspetti dell’identità fisica e sociale di un individuo»: così F. Persano, *Sull’accertamento della violazione dell’art. 8 CEDU da parte dei giudici nazionali nella recente giurisprudenza della Corte di Strasburgo*, RCP, 2018, 1, 126 ss.

⁽³⁹⁾ In tal senso, la Cassazione richiama la sentenza della Corte EDU del 5 settembre 2017, sul caso *Barbulescu c. Romania*, (ric. n. 61496/08), in cui si ritiene che, sebbene il controllo della posta elettronica aziendale del lavoratore da parte del datore di lavoro possa dar luogo ad una lesione dell’art. 8 della CEDU (mediante tale monitoraggio l’imprenditore era venuto a

La Cassazione prosegue, poi, individuando in maniera puntuale le condizioni che devono sussistere affinché i controlli di natura difensiva “in senso stretto” possano essere esercitati legittimamente: deve trattarsi di un controllo mirato ed attuato *ex post*, ossia solo dopo che nel datore di lavoro sia sorto il sospetto della commissione di un atto illecito da parte del lavoratore. In altri termini, può «parlarsi di controllo *ex post* solo ove, a seguito del fondato sospetto del datore circa la commissione di illeciti ad opera del lavoratore, il datore stesso provveda, *da quel momento*, alla raccolta delle informazioni» (40).

L'elemento determinante, dunque, consiste nell'arco temporale a cui i dati si riferiscono: l'attività di controllo è legittima solo se verte su informazioni riferite a fatti avvenuti a partire dal momento in cui il datore di lavoro ha motivo di dover accertare la commissione di un illecito e non su informazioni che si riferiscono ad un periodo antecedente. In quest'ultimo caso, i dati risulterebbero acquisiti in violazione delle prescrizioni di cui all'art. 4 dello Statuto e sarebbero, dunque, inutilizzabili.

Se così non fosse – osserva la Corte – l'area del controllo difensivo si estenderebbe a dismisura, potendosi volgere a ritroso lungo tutto il rapporto di dipendenza del soggetto, purché, in un certo momento, sorga il sospetto della commissione di un illecito (41). In questo caso, però, il controllo non potrebbe definirsi effettivamente “*ex post*”, poiché, in realtà, è iniziato prima, con la raccolta delle informazioni: «quella che viene effettuata *ex post* è solo un'attività successiva di lettura e analisi che non ha, a tal fine, una sua autonoma rilevanza» (42).

Sul punto, la Cassazione conclude riportando tali considerazioni all'ipotesi di specie, evidenziando come, nel «classico esempio dei dati di traffico contenuti nel *browser* del pc in uso al dipendente, potrà parlarsi di controllo *ex*

conoscenza di notizie relative alla salute e alla vita sessuale del suo dipendente), i giudici rumeni, nel non condannare l'imprenditore, avevano effettuato un «*fair balance*» tra il diritto alla vita privata dell'impiegato e gli interessi del primo a verificare un uso corretto dei mezzi aziendali, alla luce dei principi di proporzionalità, minimizzazione dei controlli datoriali e previa informativa del lavoratore sugli stessi. Per un approfondimento su tale decisione, cfr. G. Consonni, *Il caso Barbulescu c. Romania e il potere di controllo a distanza dopo il Jobs Act: normativa europea e italiana a confronto*, DRI, 2016, 4, 1771 ss.

(40) Così Cass. 22 settembre 2021, n. 25732, par. 44 delle *Ragioni della decisione*.

(41) La Corte precisa che, in questo modo, il datore di lavoro «potrebbe, in difetto di autorizzazione e/o di adeguata informazione delle modalità d'uso degli strumenti di effettuazione dei controlli, nonché senza il rispetto della normativa sulla *privacy*, acquisire per lungo tempo ed ininterrottamente ogni tipologia di dato, provvedendo alla relativa conservazione, e, poi, invocare la natura mirata (*ex post*) del controllo incentrato sull'esame ed analisi di quei dati»: così Cass. 22 settembre 2021, n. 25732, par. 42 delle *Ragioni della decisione*.

(42) Così Cass. 22 settembre 2021, n. 25732, par. 43 delle *Ragioni della decisione*.

post solo in relazione a quelli raccolti dopo l'insorgenza del sospetto di avvenuta commissione di illeciti ad opera del dipendente, non in relazione a quelli già registrati»⁽⁴³⁾.

4. Considerazioni conclusive: un bilanciamento a favore della dignità e della riservatezza del lavoratore

La sentenza 22 settembre 2021, n. 25732, della Corte di Cassazione ha il merito di aver fatto maggiore chiarezza sui confini dei controlli datoriali, in un periodo storico in cui la riservatezza del lavoratore risulta attaccata su (almeno) due fronti, diversi ma intimamente connessi.

Il primo riguarda il mutamento dei modelli organizzativi e produttivi. Infatti, nelle società contemporanee, in cui i dati svolgono un ruolo determinante, soprattutto per l'attività d'impresa, anche la sfera personale del lavoratore risulta più vulnerabile. In particolare, a questa inedita centralità del patrimonio informativo degli individui, corrisponde, in ambito lavorativo, un cambiamento della gestione del personale. Non può non constatarsi, infatti, come i processi di identificazione, selezione, ripartizione e valutazione dei candidati e dei lavoratori si stiano orientando «verso l'abbandono dei metodi tradizionali, basati su giudizi soggettivi, per essere fondati sull'analisi (tendenzialmente automatizzata) di una enorme mole di dati, che vengono incamerati e analizzati al fine di conoscere al meglio i processi produttivi e le performance dei lavoratori, di prevedere le potenzialità di un candidato o la possibile resa di un lavoratore all'interno di un gruppo di lavoro o i comportamenti futuri»⁽⁴⁴⁾.

Il secondo fronte che rende la sfera personale del lavoratore più vulnerabile è quello del progresso tecnologico. Perché, se è vero che con le nuove tecnologie si ricerca una piena – o quantomeno maggiore – realizzazione

⁽⁴³⁾ Così Cass. 22 settembre 2021, n. 25732, par. 45 delle *Ragioni della decisione*.

⁽⁴⁴⁾ A. Sitzia, *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, cit., 3, 804 ss. In tal senso, si veda anche A. Donini, *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, cit., 222 ss., secondo cui «tecniche di *deep e predictive learning*, *machine reasoning*, *sentiment analysis* e altre applicazioni di *artificial intelligence* permettono ai datori di lavoro di raccogliere e trattare in maniera innovativa i dati derivanti dall'uso professionale e personale del web. Attraverso la combinazione di diverse tipologie di dati in un contenuto informativo sintetico sono fornite rappresentazioni e proiezioni del comportamento dei lavoratori e delle loro caratteristiche personali o professionali (reputazione, professionalità e anche abitudini di consumo, affidabilità creditizia, rischi per la salute)». Sul punto, cfr. anche Id., *Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy*, LLI, 2017, III, 1, 37 ss.

della personalità umana, esse potrebbero determinare il consolidamento di posizioni di privilegio, diseguaglianze e asimmetrie di potere all'interno della società (45). Così, proprio per scongiurare quest'ultima eventualità, l'attenzione dei giuristi si è posta soprattutto sull'esigenza di tutelare adeguatamente il patrimonio informativo degli individui. Le nuove tecnologie, infatti, tendono a frantumare la personalità umana che viene ridotta ad un'informazione parziale, non deliberatamente data e, viceversa, resa acquisibile inconsapevolmente per mezzo di strumenti elettronici. Alla frammentazione della persona umana, della sua autenticità, si accompagna una moltiplicazione delle «persone elettroniche», tante quante sono gli archivi o banche che custodiscono i diversi dati rilevanti (46). Una siffatta «deriva tecnologica» che comporta questa nostra nuova condizione di «donne e uomini di vetro» o, *rectius*, di «lavoratrici e lavoratori di vetro» (47), non può che concretizzarsi in una minaccia per i diritti fondamentali dell'individuo – e, per quanto qui interessa – del lavoratore, in particolare per la sua riservatezza, identità personale ed autodeterminazione.

Ebbene, può affermarsi – con la dovuta cautela che deve accompagnare l'adozione di una pronuncia ancora recente – che la riservatezza del lavoratore risulti rafforzata dal principio contenuto nella sentenza 22 settembre 2021, n. 25732. Vero è che la Cassazione ha chiarito come, anche dopo la riforma dell'art. 4 dello Statuto dei lavoratori, residuino ancora degli spazi per l'esercizio dei controlli difensivi da parte del datore di lavoro; ma è altrettanto vero che i margini operativi per compiere azioni lesive della sfera personale del lavoratore risultano ben circoscritti. Da un lato, ciò è dovuto alla preventiva individuazione delle condotte del lavoratore che possono legittimare controlli a distanza al di fuori delle garanzie di cui all'art. 4 dello Statuto dei lavoratori, con cui la Cassazione ha consentito di superare alcune delle perplessità interpretative che caratterizzavano la riforma della disciplina dei controlli a distanza. (48). Dall'altro, perché la Suprema Corte ha indicato chiaramente quali sono i principi e le condizioni che devono caratterizzare i singoli controlli concreti.

A parere di chi scrive, è proprio quest'ultimo l'elemento di maggiore novità. La pronuncia della Cassazione, infatti, tenta di porre al riparo la sfera

(45) Cfr. G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di eguaglianza*, PD, 2019, 2, 199 ss.

(46) A tal riguardo, cfr. S. Rodotà, *Diritto, diritti, globalizzazione*, RGL, 2000, 1, 768, nonché R. Buttarelli, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Giuffrè, 1997.

(47) Cfr. M. Aimò, *Privacy, libertà di espressione e rapporto di lavoro*, cit., 38.

(48) Come anticipato, deve trattarsi di condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti. Sul punto, v. *supra*, § 3.

personale del lavoratore da quelle indebite intromissioni del datore di lavoro che i nuovi mezzi tecnologici renderebbero, oggi, facilmente realizzabili. Ciò è possibile garantendo un controllo mirato e soprattutto attuato *ex post*, cioè – come ha chiarito la Corte – incentrato esclusivamente su dati che si riferiscono ad un momento successivo rispetto all’insorgere del sospetto circa la commissione di un illecito da parte del lavoratore. In questo modo, si circoscrive l’attività di controllo solo a quei dati strettamente necessari per tutelare gli interessi aziendali e non si consente l’accesso a tutte quelle informazioni superflue e personali che il lavoratore rischia di disseminare nel tempo e che gli strumenti dell’era digitale incamerano e memorizzano durante il rapporto di dipendenza.

Da questo punto di vista, la Cassazione sembrerebbe aver individuato un equo bilanciamento tra i contrapposti interessi che vengono in rilievo nell’ambito dei controlli difensivi, assicurandosi che sia preso adeguatamente in considerazione il peso di una potenziale lesione della dignità e della riservatezza del lavoratore. D’altronde, come già acutamente osservava autorevole dottrina, i diritti fondamentali non possono subire, all’interno dell’azienda, «altre limitazioni al loro esercizio che non siano quelle strettamente indispensabili per il normale esplicamento della prestazione lavorativa», dal momento che il problema delle libertà fondamentali non riguarda solo il rapporto tra cittadino e poteri pubblici ma, soprattutto, le relazioni tra privati ⁽⁴⁹⁾.

⁽⁴⁹⁾ In tal senso, V. Crisafulli, *Diritti di libertà e poteri dell'imprenditore*, RGL, 1954, 1, 69.

Bibliografia

- Aimo M., *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, 2003.
- Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *LLI*, 2016, II, 1.
- Bellavista A., *Controlli a distanza e necessità del rispetto della procedura di cui al co. 2 dell'art. 4 Stat. Lav.*, in *RIDL*, 2008, 2.
- Buttarelli R., *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Giuffrè, 1997.
- Cairo L., *Controlli a distanza: passato e presente di un tema ancora controverso*, in *LG*, 2018, 2.
- Carnici M.T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito*, in *LLI*, 2016, II, 1.
- Colapietro C., *Digitalizzazione del lavoro e tutela della riservatezza della persona*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi di tutela*, Giappichelli, 2017.
- Colapietro C., *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *GDLRI*, 2017, 155.
- Consonni G., *Il caso Barbulescu c. Romania e il potere di controllo a distanza dopo il Jobs Act: normativa europea e italiana a confronto*, in *DRI*, 2016, 4.
- Coscia C., *Le modifiche all'art. 4 Stat. lav.: dignità e riservatezza del lavoratore continuano a prevalere sulla tutela del patrimonio aziendale*, in *DPP*, 2018, 7.
- Crisafulli V., *Diritti di libertà e poteri dell'imprenditore*, in *RGL*, 1954, 1.
- Dagnino E., *Controlli sociali dei lavoratori: un'interessante pronuncia della Cassazione*, in *DRI*, 2015, 3
- Dagnino E., *Tecnologie e controlli a distanza*, in *DRI*, 2015, 4.
- De Luca Tamajo R., *I controlli sui lavoratori*, in G. Zilio Grandi (a cura di), *I poteri del datore di lavoro nell'impresa. Atti del Convegno di studi (Venezia, 12 aprile 2002)*, Cedam, 2002.
- Del Federico C., *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017
- Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, in *RIDL*, 2016, 1.
- Di Meo R., *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *LLI*, 2018, IV, 1.
- Donini A., *Profiliazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy*, in *LLI*, 2017, III, 1.
- Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *DRI*, 2018, 1.
- Finocchiaro G., *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017.
- Forlivesi M., *Il controllo della vita del lavoratore attraverso i social network*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017
- Ingrao A., *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in *DRI*, 2019, 3.
- Ingrao A., *Il controllo a distanza realizzato mediante Social network*, in *LLI*, 2016, II, 1.
- Ingrao A., *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, in *RIDL*, 2017, 1.
- Levi A., *Il controllo informatico sull'attività del lavoratore*, Giappichelli, 2013.
- Marazza M., *I controlli a distanza del lavoratore di natura "difensiva"*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017.

- Maresca A. – Ciucciovino S. – Alvino I., *Regolamento UE 2016/679 e rapporto di lavoro*, in C. Colapietro – L. Califano (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, 2017.
- Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017.
- Mengoni L., *Diritto e valori*, Il Mulino, 1985.
- Mengoni L., *Le modificazioni del rapporto di lavoro alla luce dello Statuto dei lavoratori*, in Aa. Vv. (a cura di), *L'applicazione dello Statuto dei lavoratori. Tendenze e orientamenti*, Giuffrè, 1973.
- Ogriseg C., *Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in LLI, 2016, II, 2.
- Persano F., *Sull'accertamento della violazione dell'art. 8 CEDU da parte dei giudici nazionali nella recente giurisprudenza della Corte di Strasburgo*, in RCP, 2018, 1.
- Policella E.O., *Il monitoraggio elettronico dei dipendenti per scopi difensivi*, in DI, 2007, 1.
- Proia G., *Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza*, in RIDL, 2016, 4.
- Resta G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di eguaglianza*, in PD, 2019, 2.
- Rodotà S., *Diritto, diritti, globalizzazione*, in RGL, 2000, 1
- Rodotà S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in RCDP, 1997.
- Sartor G., *Tutela della personalità e normativa per la “protezione dei dati”. La sentenza della Corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del Datenschutz*, in ID, 1986, XII, 3.
- Sitzia A., *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso del lavoratore*, in LLI, 2016, II, 1.
- Sitzia A., *Il diritto alla “privacy” nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, 2013.
- Sitzia A., *Personal computer e controlli “tecnologici” del datore di lavoro nella giurisprudenza*, in ADL, 2017, 3.
- Staiano R., *In tema di apparecchiature di controllo a distanza*, in DI, 2008, 1.
- Trojsi A., *Al cuore del nuovo art. 4, co. 2, St. lav.: la delimitazione della fattispecie degli «strumenti utilizzati per rendere la prestazione lavorativa»*, in RIDL, 2017, 2.
- Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017.
- Tullini P. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017.
- Tullini P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in RIDL, 2009, 3.
- Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?*, in Id. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017
- Tullini P., *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in Id. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017.
- Ziccardi G., *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in LLI, 2016, II, 1.