

Sulla legittimità dei controlli difensivi del datore di lavoro pubblico in un caso di accesso abusivo alla banca dati dell'ente

di D. Serra - 9 Maggio 2024

Un dipendente dell'I.N.P.S. venne licenziato, all'esito di un procedimento disciplinare in cui gli erano stati contestati numerosi accessi non autorizzati, avvenuti in un periodo di tempo di circa sei mesi, alla banca dati informatica dell'Istituto, per estrarre informazioni sui conti e sulle prestazioni previdenziali riguardanti persone ivi inserite, effettuati su richiesta di due funzionari di banca, amici del dipendente.

Il lavoratore in questione, ritenendo illegittima la sanzione disciplinare, si rivolse al Tribunale di Ancona, in funzione di giudice del lavoro, il quale, però, nell'instaurato contraddittorio con il datore di lavoro, respinse la domanda.

Il lavoratore impugnò, successivamente, pertanto, la sentenza di primo grado davanti alla Corte d'Appello di Ancona, la quale rigettò l'appello e confermò la decisione del Tribunale, accogliendo anche l'appello incidentale dell'I.N.P.S., contro la parziale inutilizzabilità dei documenti posti a fondamento della contestazione disciplinare, che era stata affermata dal primo giudice: la Corte territoriale ha ritenuto legittimi i controlli effettuati dall'I.N.P.S. sugli accessi del suo dipendente alla banca dati, rilevando che si tratta dei c.d. controlli difensivi, finalizzati – non a verificare l'esatto adempimento della prestazione lavorativa, ma – ad accertare condotte illecite lesive del patrimonio aziendale ovvero pericolose per la sicurezza del luogo di lavoro.

Contro la sentenza della Corte territoriale il lavoratore ha proposto, poi, ricorso per cassazione.

Il ricorso è stato rigettato con sentenza n. 7272 del 19 marzo 2024, che qui si segnala.

Occorre, innanzitutto, rammentare che, nella versione originaria (prima delle modifiche introdotte dal d.lgs. n. 151 del 2015 e dal d.lgs. n. 185 del 2016), l'art. 4 dello statuto dei lavoratori, disposizione che è sempre stata il punto di riferimento per la tutela del lavoratore di fronte al potere di controllo datoriale, faceva divieto dell'adozione di impianti audiovisivi e di altre apparecchiature che consentissero il controllo a distanza, tranne che fossero richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro: in tal caso la loro installazione ed il loro impiego doveva essere oggetto di accordo con le rappresentanze sindacali aziendali o, in mancanza, con la commissione interna; in difetto di accordo, su istanza del datore di lavoro, provvedeva il Servizio Ispezione del lavoro dell'Ispettorato territoriale del lavoro, che dettava le modalità d'uso dei medesimi.

La formulazione dell'art. 4 non aveva, tuttavia, impedito alla giurisprudenza di interpretare la disposizione in senso evolutivo, sia nella direzione di includere nel suo ambito di applicazione

qualsiasi strumento, anche informatico, mediante il quale fosse possibile un controllo, sia rispetto all'ammissibilità dei controlli difensivi.

A partire dal 2002, la Suprema Corte aveva ritenuto che i controlli difensivi fossero ammissibili senza limitazioni, non rientrando essi nell'ambito di operatività dell'art.4, perché diretti ad accertare condotte illecite dei dipendenti (Cass.3 aprile 2002, n. 4746).

Negli ultimi anni, tuttavia, la Suprema Corte, anche sulla scorta di alcune pronunce di merito, aveva mutato orientamento ed era arrivata ad assoggettare i controlli difensivi alla stessa disciplina di quelli preterintenzionali, cioè ai limiti di cui all'art. 4, comma 2, statuto dei lavoratori, atteso che l'esigenza di evitare condotte illecite ad opera dei dipendenti non avrebbe potuto assumere una portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore.

La Cassazione, comunque, non escludeva in assoluto l'esistenza di controlli difensivi sottratti all'art. 4 statuto dei lavoratori: tale disposizione, infatti, non avrebbe trovato applicazione nel caso di controlli diretti a tutelare beni estranei al rapporto di lavoro e non diretti a verificare l'esatto adempimento delle obbligazioni di lavoro: la disciplina dei controlli tecnologici difensivi era foriera, nella pratica, di probabili violazioni della dignità e riservatezza dei lavoratori, ciò soprattutto in quanto la liceità del controllo risultava accertabile solamente *ex post*, ad attività lavorativa già avvenuta, con inevitabile violazione del divieto di cui all'art. 4, comma 1, statuto dei lavoratori e della riservatezza del lavoratore.

Con l'art. 23 del d.lgs. n. 151 del 2015(c.d. decreto sulle semplificazioni) è stato sostituito il testo dell'art. 4 dello statuto dei lavoratori: la nuova formulazione ribadisce, anzitutto, che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere installati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, previo accordo collettivo stipulato dalla r.s.u. o dalla r.s.a.; in alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale; in mancanza di accordo essi possono essere installati previa autorizzazione dell'Ispettorato territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del ministero del lavoro.

L'accordo e l'autorizzazione, ed è questa la novità del provvedimento, non sono richiesti per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per gli strumenti di registrazione degli accessi e delle uscite: l'affidamento al lavoratore, per lo svolgimento dell'attività di lavoro, di strumenti come gli smartphone o i tablet non necessita di alcuna preventiva autorizzazione amministrativa o di accordo sindacale.

Le informazioni raccolte attraverso tali strumenti ben possono essere utilizzate dal datore di lavoro, anche a fini disciplinari, purché venga data al lavoratore adeguata informazione delle loro modalità d'uso e di effettuazione dei controlli e pur sempre nel rispetto della disciplina sulla c.d. *privacy*(di cui al d.lgs. n. 196 del 2003): sono, pertanto, vietati i controlli occulti, dovendo il lavoratore essere sempre previamente informato del controllo tecnologico;

qualora il lavoratore non sia adeguatamente informato dell'esistenza e delle modalità d'uso delle apparecchiature di controllo e delle modalità di effettuazione dei controlli, i dati raccolti non sono utilizzabili a nessun fine, nemmeno a fini disciplinari.

Adesso, si chiarisce che i controlli difensivi sono controlli preterintenzionali e, come tali, per essere effettuati, necessitano dei predetti accordi o autorizzazioni, a tutela della dignità dei dipendenti.

Il nuovo articolo 4 statuto dei lavoratori ha destato dubbi soprattutto rispetto alla sopravvivenza di residue aree di controlli difensivi totalmente esclusi dai limiti dei controlli preterintenzionali: su tale punto si confrontano due opposti orientamenti dottrinari.

Secondo un primo orientamento, tutti i controlli difensivi sarebbero oggi assorbiti da quelli preterintenzionali, non residuando alcuna possibilità di controlli esclusi dalla necessità di raggiungere un accordo sindacale o di ottenere una autorizzazione amministrativa.

Un secondo orientamento, invece, lascia spazio a controlli difensivi leciti anche in mancanza degli accordi e autorizzazioni di cui all'art. 4 statuto dei lavoratori: secondo una posizione il controllo difensivo non sarebbe soggetto alle tutele di quello preterintenzionale se diretto ad accertare comportamenti che attentino all'integrità del patrimonio aziendale o all'incolumità delle persone, ossia quelle condotte riconducibili alla categoria civilistica degli atti di aggressione contro l'altrui diritto, che potrebbero avere rilevanza tanto penale quanto essere inadempimenti contrattuali o extracontrattuali e rispetto ai quali il datore potrebbe reagire con il controllo in applicazione del principio di legittima difesa nel settore civilistico, ai sensi del combinato disposto degli artt. 2044 c.c. e 52 c.p.; altri, invece, preferiscono limitare la categoria dei controlli a distanza sempre consentiti ai casi in cui la condotta del lavoratore o del terzo integri una fattispecie penalmente rilevante.

Nella pronuncia *de qua*, si evidenzia che la Corte di Cassazione si è già occupata in più occasioni dei c.d. controlli difensivi del datore di lavoro, molto spesso collegati al tema delle indagini sull'uso, da parte del dipendente, di strumenti per la navigazione in *internet* e per la comunicazione telematica in ambito lavorativo (v., tra le altre, Cass. nn. 13266/2018; 25731/2021; 25732/2021; 34092/2021; 18168/2023). Tale giurisprudenza, si legge sempre nella sentenza qui annotata, si è fatta carico del problema di assicurare un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, e le imprescindibili tutele della dignità e della riservatezza del lavoratore, affermando, tra l'altro, il principio che il controllo difensivo in senso stretto deve essere mirato ed attuato *ex post*, ossia a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto.

La Corte d'Appello di Ancona aveva accertato che il lavoratore era stato preventivamente informato delle modalità d'uso degli strumenti e di effettuazione dei controlli e che gli accertamenti erano stati eseguiti solo *ex post*, dopo la segnalazione, da parte della Direzione Centrale Risorse Umane I.N.P.S., del numero anomalo di accessi informatici effettuati con le credenziali del ricorrente.

Il caso in questione, per la Suprema Corte, è sensibilmente diverso rispetto a quelli affrontati nei citati precedenti, che sono incentrati sul bilanciamento tra esigenze di protezione di interessi e beni aziendali e imprescindibili tutele della dignità e della riservatezza del lavoratore.

In questo caso, i controlli preventivi effettuati dall'I.N.P.S. non solo non erano finalizzati al controllo dell'adempimento della prestazione del lavoratore, ma nemmeno erano volti alla protezione di interessi e beni aziendali.

L'I.N.P.S., infatti, quale gestore e responsabile della banca dati in cui sono racchiuse informazioni riservate che riguardano i soggetti iscritti, ha effettuato i doverosi controlli preventivi sugli accessi a tutela delle persone interessate alla corretta gestione di quei dati.

La tutela della *privacy*, puntualizzano i giudici di legittimità, viene sicuramente in rilievo nel caso di specie, ma si tratta della *privacy* delle persone che sono iscritte a vario titolo all'I.N.P.S. e inserite nella banca dati, non quella del lavoratore dipendente, di cui non è stato attinto alcun dato personale, se non quello, appunto, dell'accesso non autorizzato alla banca dati.

I casi affrontati nei citati precedenti sono, si legge nella sentenza *de qua*, significativamente diversi, trattandosi di accertamenti finalizzati a tutelare il datore di lavoro contro danneggiamenti alle sue dotazioni provocate da *virus* informatici (Cass. n. 25732/2021), oppure contro la fuoriuscita di informazioni commerciali riservate (Cass. n. 34092/2021) o ancora contro illeciti contatti di un dipendente con imprese concorrenti (18168/2023). E, per accertare siffatti comportamenti, il datore di lavoro aveva visionato e utilizzato gli accessi del dipendente ai siti *internet* oppure il contenuto di conversazioni tra il dipendente e soggetti terzi, avvenute via *e-mail* o in *chat*.

Nel caso di specie, prosegue il Collegio, invece, i controlli automatici effettuati dall'I.N.P.S., all'esito dei quali si è sostanzialmente fondato sospetto di un illecito disciplinare, da un lato, erano volti alla doverosa tutela di soggetti terzi (gli interessati, le cui informazioni personali sono inserite nella banca dati); dall'altro lato, non hanno comportato alcuna indagine sulle abitudini, sui gusti e sulle comunicazioni del lavoratore dipendente.

Non era quindi obbligatoria alcuna comunicazione preventiva al dipendente del fatto che l'I.N.P.S. esercita un doveroso controllo – non sull'operato dei propri dipendenti, ma – sulla regolarità degli accessi alla banca dati di cui è responsabile, né tale controllo rientra tra i controlli difensivi in senso stretto, che il datore di lavoro può adottare a tutela dei propri interessi e beni aziendali, alle condizioni indicate nella giurisprudenza citata.

La Cassazione, con la pronuncia in esame, evidenzia, inoltre, che la Corte territoriale ha fatto buon governo dell'art. 7 dello Statuto dei lavoratori (e, più propriamente, dell'art. 55-*bis* d.lgs. n. 165 del 2001), secondo cui la contestazione disciplinare deve contenere le indicazioni necessarie ed essenziali per individuare, nella sua materialità, la condotta addebitata, con la precisazione che l'accertamento relativo al requisito della specificità, riservato al giudice di merito, va condotto considerando che in sede disciplinare la contestazione non obbedisce ai rigidi canoni che presiedono alla formulazione dell'accusa nel processo penale né si ispira ad uno schema preconstituito, ma si modella in relazione ai principi di correttezza che informano il rapporto esistente fra le parti, sicché ciò che rileva è l'idoneità dell'atto a soddisfare l'interesse

dell'incolpato ad esercitare pienamente il diritto di difesa(Cass. 23771/2018; che cita, a sua volta, Cass. nn. 6099/2017; 4622/2017; 3737/2017; 619/2017; 6898/2016; 10662/2014; 27842/2009).

I giudici di legittimità, infine, precisano, con riferimento al motivo di ricorso con cui viene contestata l'appropriatezza della sanzione espulsiva, che per costante orientamento della Corte la giusta causa di licenziamento integra una clausola generale che l'interprete deve concretizzare tramite fattori esterni relativi alla coscienza generale e principi tacitamente richiamati dalla normativa e, quindi, mediante specificazioni di natura giuridica, la cui disapplicazione è deducibile in sede di legittimità come violazioni di legge, mentre l'accertamento della concreta ricorrenza, nel fatto dedotto in giudizio, degli elementi integranti il parametro normativo costituisce un giudizio di fatto, demandato al giudice di merito ed incensurabile in cassazione se privo di errori logici o giuridici(di recente: Cass. n. 7029/2023).

Dionisio Serra, cultore di diritto del lavoro nell'Università degli Studi di Bari "Aldo Moro"

Visualizza il documento: [Cass., 19 marzo 2024, n. 7272](#)