ISSN 2384-9169
Fascicolo n. 1 - 2020
rivista.eurojus.it

La videosorveglianza occulta sui luoghi di lavoro secondo la Corte europea dei diritti dell'uomo

DI CARMINE SANTORO*

Sommario: 1. L'art. 4 della legge n. 300/1970 (cd. "Statuto dei lavoratori"): in particolare i "controlli difensivi". – 2. Il diritto spagnolo. – 3. La sentenza della Corte. – 3.1. La pronuncia della Camera semplice e il precedente *Barbulescu*. – 3.2. La Sentenza della Grande Camera: legittimità della videosorveglianza occulta. – 3.3. L'opinione dei giudici dissenzienti. – 4. Possibili effetti della pronuncia sull'ordinamento interno.

1. Al fine di introdurre il tema trattato nella pronuncia della Corte di Strasburgo e di valutarne l'impatto sull'ordinamento interno, appare necessaria una premessa sulla disciplina nazionale dei controlli a distanza nei luoghi di lavoro[1].

A tal proposito viene in rilievo l'art. 4 della legge n. 300/1970, che, nel testo attualmente vigente dopo le modifiche introdotte dall'art. 23 del D.lgs. n. 151/2015 (c.d. *Jobs act*), dispone:

«1. 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

* Dottore di ricerca dell'Università di Bergamo, Funzionario dell'Ispettorato nazionale del lavoro. Il presente contributo è frutto esclusivo del pensiero dell'autore e non impegna l'Amministrazione di appartenenza.

[1] Per una trattazione sistematica del tema dei controlli a distanza sui luoghi di lavoro e le sue correlazioni con la riservatezza dei lavoratori, si rinvia, tra i contributi più recenti, a S. ROSSI, *Tutela della riservatezza e limiti ai controlli difensivi,* in *Giur. It*., 2019, 2, p. 390 ss.; P. LAMBERTUCCI, *I controlli del datore di lavoro e la tutela della* privacy, in G. SANTORO–PASSARELLI (a cura di), *Diritto e processo del lavoro e della previdenza sociale*, Torino, 2017, p. 873 ss.; M. MARRAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona".IT – 300/2016. Per un'analisi della riforma del D.lgs. n. 151/2015, si veda, tra gli altri, M. DAGNINO, *Tecnologie e controlli a distanza*, in M. TIRABOSCHI (a cura di), *Le nuove regole del lavoro dopo il Jobs act*, Milano, 2016, p. 107 ss..

sindacale unitaria o dalle rappresentanze sindacali aziendali. […]. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro […].

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196».

Dalle disposizioni richiamate emerge che gli impianti di controllo a distanza dei lavoratori subordinati possono essere installati per talune tassative ragioni, che non riguardano l'adempimento dell'obbligazione lavorativa. Ne deriva, implicitamente, il divieto di controllo a distanza finalizzato a verificare tale adempimento (c.d. controllo diretto). Tra le esigenze richieste dalla legge ai fini della legittimità del suddetto controllo occorre soffermare l'attenzione, in questa sede, sulla tutela del patrimonio aziendale. Attraverso questo riferimento, la recente riforma del D.lgs. n. 151/2015 cit. ha recepito l'elaborazione giurisprudenziale afferente ai c.d. controlli difensivi, cioè le verifiche disposte dal datore di lavoro al fine di individuare illeciti dei dipendenti sul proprio patrimonio[2].

Secondo questo indirizzo pretorio – formatosi nel periodo di vigenza del pregresso testo dell'art. 4 cit. – i controlli difensivi sono legittimi in quanto finalizzati non al controllo della prestazione lavorativa, vietato dalla legge, ma alla repressione di illeciti dei dipendenti. Nello specifico, la prima giurisprudenza che ha trattato della questione ha stabilito che: «Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 della l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti "controlli difensivi"), quali per esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate» (Cass. n. 4746/2002).

Secondo questo orientamento, era consentita, *ex* art. 4 cit. vecchio testo, la verifica a distanza diretta a rinvenire comportamenti illeciti del lavoratore, diversi dal mero inadempimento agli obblighi contrattuali, anche quando la stessa debordasse in controllo sull'attività lavorativa (Cass. 17 luglio 2007, n. 15892). In proposito, si era posta la questione dell'applicabilità di tale orientamento nelle ipotesi in cui non fosse agevole distinguere la finalità del controllo datoriale, a causa dell'utilizzo di strumenti di lavoro da parte dei dipendenti, come nei monitoraggi sulle telefonate ovvero sulla posta elettronica dei dipendenti. In queste eventualità, il compito dell'interprete richiedeva una complessa indagine, diretta ad

[2] Sui controlli difensivi giurisprudenza e dottrina hanno prodotto un'ampia elaborazione, di cui non è possibile in questa sede dare adeguatamente conto: si vedano in proposito, tra gli altri, i contributi di A. SITZIA, *Personal computer e controlli ''tecnologici'' del datore di lavoro nella giurisprudenza*, in *Argomenti Dir. Lav*., 2017, 3, p. 804; V. G. RECCHIA, *Controlli datoriali difensivi: note su una categoria in via di estinzione*, in *Lav. Giur*., 2017, 4, p. 348; A. BELLAVISTA, *La Cassazione e i controlli a distanza sui lavoratori*, in *Rass. Giur. Lav*., 2010, II, p. 465; V. M. FALSONE, *L'infelice giurisprudenza in materia di controlli occulti e le prospettive del suo superamento*, in *Riv. It. Dir. Lav*., 2015, II, p. 990 ss..

accertare in concreto se il controllo a distanza avesse ad oggetto l'esecuzione delle prestazioni, nel qual caso era illecito, ovvero la tutela del patrimonio aziendale, ove era invece lecito.

Ad aggravare tali perplessità, si doveva registrare che l'elaborazione pretoria menzionata era contraddetta da un'altra impostazione della stessa giurisprudenza di legittimità. In tale ambito, la Cassazione aveva affermato che la violazione del succitato art. 4 non fosse esclusa dalla circostanza che le apparecchiature di controllo fossero dirette ad evitare illeciti dei dipendenti, ove queste rendessero possibile il controllo a distanza sull'attività dei dipendenti: infatti «[…] l'eventuale motivo per cui sono state installate le telecamere non esclude l'obbligo di seguire la procedura di cui all'art. 4 legge n. 300/1970 […]» (Sentenza n. 10268 del 6 marzo 2003). Più di recente, la Suprema Corte ha stabilito il principio giurisprudenziale secondo il quale «l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i cosiddetti controlli difensivi trovino applicazione le garanzie della L. n. 300 del 1970, art. 4, comma 2; ne consegue che, se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, il datore di lavoro può installare impianti o apparecchi di controllo che rilevino anche dati relativi alla attività lavorativa dei dipendenti, tali dati non possono essere utilizzati per provare l'inadempimento contrattuale del lavoratori medesimi» (Cass. 05/10/2016, n. 19922; *ead*. n. 16622/2012 e n. 4375/2010) [3].

Sicché, i contrasti giurisprudenziali producevano notevole incertezza sull'ambito di applicabilità del modificato testo dell'art. 4 cit. e, in particolare, sulla necessità di ricorrere alle garanzie procedurali dell'accordo sindacale ovvero dell'autorizzazione dell'Ispettorato del lavoro.

Anche al fine di dirimere i dubbi giurisprudenziali, la disciplina del *Jobs act*, come detto, ha riformato l'art. 4 della legge n. 300/70, consentendo il controllo "indiretto" – quello dettato da esigenze organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale – alle condizioni procedurali dell'accordo sindacale o autorizzazione dell'Ispettorato del lavoro, e precisando che la verifica sull'impiego degli strumenti di lavoro è esclusa da qualunque restrizione e le relative risultanze sono liberamente utilizzabili dal datore per i fini connessi al rapporto di lavoro (comma 2). In tal modo, superate le incertezze relative alle finalità del controllo, si sposta l'attenzione sull'individuazione oggettiva degli strumenti di lavoro. In quest'ultima nozione rientrano i mezzi – quali, ad es., la posta elettronica, Internet o il telefono – che hanno suscitato i maggiori dubbi nel pregresso regime.

Pertanto, la legge attualmente consente il controllo indiretto e difensivo sulle prestazioni lavorative, imponendo una condizione procedurale e due sostanziali. La prima prescrive l'accordo con i sindacati aziendali e, in mancanza, l'autorizzazione dell'Ispettorato competente per territorio. La seconda prevede che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli; infine, deve essere osservato il decreto legislativo 30 giugno 2003, n. 196, che tutela –com'è noto – la riservatezza delle persone.

Nel rispetto delle suddette condizioni, le informazioni acquisite dal datore di lavoro sono «utilizzabili a tutti i fini connessi al rapporto di lavoro» e, quindi, anche a fini disciplinari.

[3] Per un commento del quadro giurisprudenziale e dell'analogo orientamento dell'Ispettorato nazionale del lavoro circa la legittimità del sistema *GPS* da parte dei datori di lavoro (Circolare n. 2 del 7 novembre 2016) sia consentito il rinvio a C. SANTORO, *Il sistema GPS costituisce controllo a distanza dei lavoratori*, in *La circolare di lavoro e previdenza*, 2016, 46, p. 7 ss..

In questa sede rileva particolarmente la sanzione prevista, *a contrario*, dalla legge per l'omessa informativa preventiva ai lavoratori e/o la mancata applicazione del D.lgs. n. 196/2003, costituita dall'inutilizzabilità dei dati acquisiti. Si deve notare, sin d'ora, come la disposizione non ponga limiti, né deroghe o eccezioni, alla propria applicabilità. Ne deriva che, secondo la disciplina nazionale richiamata, la mancata informativa ai lavoratori – o l'omessa concessione delle garanzie del Codice *Privacy* – determina *tout court* l'inutilizzabilità delle informazioni raccolte con gli strumenti di videosorveglianza. Come si vedrà meglio nel seguito della trattazione, è questo il profilo critico risultante nell'analisi del rapporto tra il *dictum* in commento, che ha stabilito l'utilizzabilità dei dati in casi eccezionali in ipotesi di omessa informativa, e la disciplina interna.

La mancata osservanza di uno o più dei requisiti richiesti dal comma 1 dell'art. 4 cit. – insussistenza delle ragioni normative dell'installazione e/o mancata osservanza delle garanzie procedurali – rende penalmente illecita la condotta datoriale e la sottopone alle sanzioni di cui all'art. 171 del D. Lgs. n. 196/2003 (c.d. Codice della *privacy*), come modificato dall'art. 15 lett. f) del D. Lgs. n. 101/2018, che a sua volta rimanda al disposto dell'art. 38 della legge n. 300 cit.[4].

2. La Costituzione spagnola stabilisce, quali diritti fondamentali, il diritto alla *privacy* della persona e il "diritto al controllo dei dati" (art. 18), demandando alla legge la previsione di limiti all'uso della tecnologia dell'informazione per garantire l'onore e la *privacy* personale e familiare dei cittadini.

La disciplina dello "Statuto dei Lavoratori" spagnolo prevede che «Il datore di lavoro può adottare le misure che ritiene più appropriate per il monitoraggio e il controllo al fine di verificare il rispetto da parte del lavoratore dei propri obblighi e doveri lavorativi, mantenendo l'adozione e applicazione dovuta alla loro dignità e tenendo conto, se del caso, della reale capacità dei lavoratori con disabilità» (art. 20.35).

Lo Statuto dei Lavoratori prevede che ogni lavoratore abbia il diritto alla propria *privacy* (art. 4.2, e). Inoltre, i lavoratori hanno il diritto alla riservatezza nell'uso dei dispositivi digitali messi a disposizione dal datore di lavoro, alla disconnessione e alla *privacy* nei confronti dell'uso di dispositivi di videosorveglianza e geolocalizzazione in materia di protezione dei dati personali e garanzia dei diritti digitali (art. 20 *bis* 8). Come si può notare la legge lavoristica iberica, al contrario di quella italiana, non impone espressamente la previa informativa al lavoratore dell'uso dei dispositivi di controllo a distanza.

Tuttavia, la disciplina sulla protezione dei dati personali vigente al tempo dei fatti cui del caso *López* (Legge 5 dicembre 1999, n.15), imponeva tale informativa al datore di lavoro «in modo espresso, preciso e inequivocabile» riguardo all'esistenza «di un archivio o un trattamento di dati personali» e, tra gli altri requisiti, «della finalità della raccolta e dei destinatari delle informazioni». Tali prescrizioni sono ora previste nella Legge del 5 ottobre 2018, n.3, sulla protezione dei dati personali, che recepisce le disposizioni del Regolamento UE 2016/679.

[4] Cfr. E. A. PITITTO, *Il "nuovo" art. 171 del Codice Privacy: oltre la razionalizzazione normativa?* in *Bollettino ADAPT*, 2018, p. 34.

Pertanto, anche l'ordinamento spagnolo prevedeva, e prevede, il previo obbligo di informativa ai dipendenti circa l'istallazione di apparecchiature dirette a controllare a distanza l'attività lavorativa.

3. Il caso sottoposto allo scrutinio della Corte di Strasburgo riguarda condotte illecite di sottrazione di beni, commesse da vari lavoratori ai danni di un supermercato spagnolo da cui quelli dipendevano. Il datore di lavoro, a seguito del riscontro degli ammanchi, disponeva l'installazione di telecamere di videosorveglianza senza fornire informazione alle rappresentanze sindacali e ai diretti interessati. I dati acquisiti con tali strumenti erano, quindi, utilizzati a fini disciplinari e i lavoratori subivano il conseguente licenziamento.

Dopo aver infruttuosamente esperito i rimedi giurisdizionali interni, dai quali risultava accertata la legittimità del comportamento datoriale, in quanto – a detta dei giudici – proporzionato e adeguato rispetto alle condotte illecite dei propri dipendenti, questi ultimi si rivolgevano alla Corte EDU. In particolare, il ricorso verteva su due profili, uno relativo alla violazione dell'art. 8 CEDU (tutela della riservatezza), l'altro all'art. 6 (diritto a un equo processo)[5].

3.1. In prima istanza, la Camera semplice, con sentenza del 9 gennaio 2018, escludeva la violazione dell'art. 6, ma accoglieva la censura relativa alla lesione della riservatezza[6].

Circa il primo punto, la Camera ritiene che i ricorrenti siano stati posti in condizione di contestare sia l'autenticità, sia l'ammissibilità della prova costituita dal filmato ottenuto per mezzo della videosorveglianza; inoltre, i giudici osservano come quest'ultima non sia stata l'unica prova su cui le corti nazionali hanno fondato la propria decisione, concludendo che non vi sia stata violazione dell'art. 6.

Riguardo al profilo della riservatezza, la Camera osserva che «il concetto di vita privata si estende agli aspetti relativi all'identità personale, come il nome o l'immagine di una persona». Tale concetto «può includere attività di natura professionale o imprenditoriale […] anche effettuate al di fuori della casa di una persona o di locali privati». Da tale assunto deriva, per la Corte, che «la videosorveglianza nascosta di un dipendente nel suo luogo di lavoro deve essere considerata, in quanto tale, una considerevole intrusione nella sua vita privata». Questa intrusione, avverte la Camera, non può essere evitata dagli interessati, essendo questi obbligati a svolgere il lavoro in quel luogo.

Secondo la Corte, l'art. 8 deve essere interpretato non solo come norma di tutela dell'individuo da illegittime ingerenze delle autorità pubbliche, ma anche come fonte di obblighi di intervento a carico dello Stato, il quale deve adottare misure necessarie ad assicurare il rispetto della *privacy* anche nei rapporti tra privati. I giudici sostengono che, nel caso di specie, non fossero state adottate tali misure dall'ordinamento spagnolo; in tal senso, non era stato garantito il giusto equilibrio tra il diritto dei lavoratori al rispetto della riservatezza e quello del datore alla tutela della proprietà, non avendo il datore di lavoro rispettato l'obbligo, sancito dalla

[5] Sull'analisi dei due articoli della Convenzione, su cui si è espressa la Corte, si rimanda a S. BARTOLE, P. DE SENA, V. ZAGREBELSKY, *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, per l'art. 6, p. 172 ss., per l'art. 8, p. 297 ss..

[6] Per un commento alla pronuncia si veda F. PERRONE, *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Bărbulescu 2*, in *rivistalabor.it*.

legge spagnola sulla protezione dei dati personali –come dall'art. 4 della legge n. 300/70 cit., come sopra osservato –, di informare gli interessati dell'attivazione di strumenti di acquisizione e trattamento dei loro dati personali. In particolare, come evidenzia la Camera, l'ordinamento iberico prevede un articolato sistema di strumenti normativi a protezione della *privacy* sul luogo di lavoro, idoneo a fondare un ragionevole affidamento di tutela da parte dei lavoratori ricorrenti.

Quanto alla proporzionalità della misura, la Corte ritiene che nel caso di specie tale attributo non sussista, attesa l'estesa durata della videosorveglianza e le sue potenzialità di controllo indiscriminato dell'intero gruppo di lavoro. Inoltre, gli interessi datoriali, in sé legittimi, avrebbero potuto essere tutelati con mezzi differenti, quale un'informazione preventiva generica dei lavoratori. Pertanto, lo Stato spagnolo, ad avviso dei giudici della Camera, non ha correttamente espletato il giudizio di bilanciamento imposto dall'art. 8, par. 2 Cedu. A breve si vedrà come tale assunto sia confutato dalla Grande Camera.

La pronuncia della Camera semplice si pone in relazione di continuità con la Sentenza *Barbulescu*[7], ove il giudice europeo aveva chiarito come l'art. 8 dovesse intendersi in senso ampio, tale da ricomprendere tutte le attività che consentono lo sviluppo della personalità e della vita di relazione, anche sul luogo di lavoro. Nella propria valutazione, la Corte non mancava di sottolineare la specialità del diritto del lavoro e la situazione di subordinazione giuridica del prestatore, che lo rendono soggetto "debole" del rapporto e quindi sempre esposto a possibili abusi (par. 117).

Affermava la Corte: «…le disposizioni del datore di lavoro non possono azzerare la vita sociale privata nel luogo di lavoro. Il rispetto per la vita privata e per la riservatezza della corrispondenza continua a sussistere, anche se può essere limitato nella misura necessaria» (par. 80). Tali considerazioni conducono i giudici ad affermare che «le comunicazioni del ricorrente nel luogo di lavoro rientrassero nelle nozioni di "vita privata" e di "corrispondenza"» (par. 81).

Nel caso di specie, il lavoratore, secondo la Corte, poteva contare su un evidente affidamento di tutela della propria riservatezza, nella misura in cui non era stata fornita informazione alcuna sul controllo delle conversazioni da parte del datore di lavoro.

Secondo il giudice di Strasburgo, le Corti nazionali non avevano operato un corretto bilanciamento fra gli interessi del datore e il diritto alla *privacy* del lavoratore. In particolare, i tribunali interni non avevano verificato se il lavoratore interessato fosse stato preliminarmente informato dal datore di lavoro della possibilità che le proprie comunicazioni avrebbero potuto essere monitorate; né hanno tenuto conto del fatto che non fosse stato informato del carattere o della portata del monitoraggio o del livello di invasività nella sua vita privata e nella sua corrispondenza.

Quindi, secondo la Corte, nella fattispecie era mancata del tutto una valutazione di bilanciamento tra gli opposti interessi delle parti, per stabilire se il lavoratore potesse ragionevolmente aspettarsi che la propria riservatezza rimanesse garantita o meno.

[7] Per un commento si rinvia a C. CARTA, *Corte europea dei diritti dell'uomo: la Grande camera torna sul (e difende il) diritto alla privacy del lavoratore*, in *www.rivistalabor.it/wpcontent/uploads/2017/09/Barbulescu.pdf*.

3.2. Nella pronuncia in commento, la Grande Camera, ribaltando l'orientamento della Camera semplice, nega la fondatezza del ricorso, tanto per l'invocata violazione dell'art. 6 quanto per quella dell'art. 8, in virtù del seguente ragionamento[8].

In ordine alla invocata violazione dell'art. 8 della Convenzione, la Corte rileva che il monitoraggio non si era esteso all'intero negozio, essendo stato specificamente diretto alle aree dove si trovavano le casse, cioè il luogo in cui era ragionevole attendersi che i furti fossero stati commessi.

I giudici evidenziano, inoltre, che le prestazioni lavorative erano adempiute in un luogo aperto al pubblico, in una posizione lavorativa a permanente contatto con i clienti. A questo proposito, la Corte osserva come sia necessario distinguere, nell'analisi della proporzionalità dell'attività di videosorveglianza, i vari luoghi in cui il monitoraggio sia stato eseguito, alla luce del grado di protezione della *privacy* che un lavoratore può ragionevolmente attendersi. Tale soglia è alta nei luoghi non esposti al pubblico, come gli uffici interni e, soprattutto, i locali naturalmente destinati a proteggere la riservatezza degli occupanti, come spogliatoi o bagni. Viceversa, essa è bassa, secondo i giudici, in luoghi che sono visibili o accessibili a colleghi oppure, come nel caso di specie, alla generalità del pubblico. In questi ultimi, secondo i giudici, i lavoratori non possono formarsi un ragionevole affidamento sulla tutela della propria *privacy*.

Da notare che in tale segmento argomentativo, i giudici, pur non contraddicendolo apertamente, ridimensionano l'assunto sostenuto nel caso *Antović e Mirković c. Montenegro* del 18 novembre 2017, ove essi avevano ampliato la nozione di "vita privata", di cui all'art. 8 cit., estendendola ai luoghi lavorativi. In tal senso, i giudici avevano affermato che la mera circostanza che la prestazione lavorativa fosse espletata in luogo aperto al pubblico non era sufficiente ad escludere l'ambito applicativo della disposizione menzionata. In tale occasione, in effetti, la Corte sosteneva che l'aspettativa di protezione del diritto alla riservatezza del lavoratore non potesse venir meno per il solo fatto che il luogo di lavoro fosse accessibile a una cerchia indeterminata di persone. Ebbene, rispetto a tale orientamento, nella sentenza in commento la Corte puntualizza che tale aspettativa deve attestarsi a un livello di modesta entità, almeno se comparato a quello che il prestatore di lavoro può avere nei siti "riservati".

Per quanto riguarda l'estensione temporale della misura di sorveglianza, la Corte rileva che la durata dell'attività di videosorveglianza si è protratta per dieci giorni, ed è cessata non appena sono stati individuati i lavoratori responsabili del fatto. Per tale motivo, la durata dell'attività di videosorveglianza non sembra ai giudici essere di per sé eccessiva. Risultava, inoltre che solo due responsabili aziendali e un rappresentante sindacale avessero preso visione delle registrazioni, prima che i ricorrenti ne fossero informati. Avuto riguardo a questi fattori, la Corte ritiene proporzionata la misura al fine che si prefiggeva e che l'intromissione nella sfera di riservatezza dei dipendenti non avesse raggiunto una soglia di significativa gravità.

[9] Per un'approfondita trattazione del tema trattato dalla Corte si vedano i contributi di A. CIRIELLO, F. ARIANTE, *Videosorveglianza "occulta" sul luogo di lavoro: il caso Lòpez Ribalda e altri c. Spagna e giurisprudenza della Corte Europea dei Diritti dell'Uomo*, e di A. SITZIA, M. I. RAMOS QUINTANA, *Sorveglianza difensiva "occulta" sui luoghi di lavoro e dignità nella prospettiva della Grande Camera della Corte EDU: la sentenza Lòpez–Ribalda,* entrambi in *Europa, lavoro, diritti*, 2019, 3, dove è possibile anche trovare ampi estratti del testo della sentenza. Per efficaci sintesi della pronuncia cfr. anche F. BUFFA, F. PERRONE, *La rilevanza dell'informazione preventiva nei controlli a distanza sul luogo di lavoro*, in *Questione giustizia.it*.; S. AURIEMMA, in *Giurisprudenza italiana*, 2019, 12, p. 2590.

La Corte osserva ancora che le informazioni raccolte per mezzo della videosorveglianza non sono state usate dal datore di lavoro per scopi differenti rispetto alla necessità di identificare il responsabile delle sottrazioni dei beni, nonché di adottare misure disciplinari contro i responsabili, né sono state rese pubbliche.

La Corte rileva anche che l'entità delle perdite economiche riscontrata dal datore di lavoro fosse tale da indurre a ritenere elevato il numero dei possibili autori dei furti, e che la comunicazione della videosorveglianza ai dipendenti ne avrebbe vanificato lo scopo. Era, inoltre, risultata l'indisponibilità di alcun altro mezzo idoneo a consentire il perseguimento dello scopo legittimo avuto di mira e che, pertanto, la misura doveva essere considerata "necessaria" alla luce della giurisprudenza della Corte Costituzionale spagnola.

I giudici osservano che né la legge spagnola, né gli orientamenti comunemente applicati nel diritto comparato impongono che sia prestato il preliminare consenso da parte del soggetto destinatario dell'attività di videosorveglianza[9], ma tuttavia è generalmente richiesto – anche dalla legge spagnola e da quella italiana come sopra osservato – che costui sia informato preventivamente circa il trattamento e la raccolta dei dati. Risultano, in questo senso, fondamentali il requisito della trasparenza e il diritto all'informazione, particolarmente nelle relazioni di lavoro, in cui il datore di lavoro esercita un significativo potere sui lavoratori. La Corte evidenzia, tuttavia, che l'obbligo di fornire preventiva informazione agli individui oggetto di monitoraggio circa l'estensione di tale monitoraggio, costituisce soltanto uno dei molteplici criteri che devono essere presi in considerazione al fine di valutare la proporzionalità della misura adottata nel caso concreto. In tale quadro, osservano i giudici, se una tale informazione preventiva risulta mancante, l'adozione di misure di salvaguardia individuabili sulla base degli ulteriori criteri di valutazione rilevanti assume una maggiore importanza ai fini della valutazione spettante alla Corte. Considerata l'importanza nel caso di specie rivestita dal diritto all'informazione preventiva, la Corte ritiene che soltanto un prevalente interesse concernente la protezione di rilevanti interessi pubblici ovvero privati può giustificare la carenza della preventiva informazione.

Nel caso di specie, avuto riguardo al grado di intrusione concretamente effettuato nella *privacy* dei lavoratori e allo scopo legittimo che ha giustificato l'installazione degli strumenti di videosorveglianza, la Corte ritiene che i giudici nazionali non abbiano oltrepassato il margine di apprezzamento che compete alle autorità nazionali nella valutazione della proporzionalità della misura adottata rispetto al fine concretamente perseguito. Pertanto, se non è accettabile la posizione secondo cui anche il minimo sospetto di appropriazione illecita possa autorizzare l'installazione di strumenti occulti di videosorveglianza, d'altra parte l'esistenza di un ragionevole sospetto circa la commissione di illeciti connotati da significativa gravità possono costituire, secondo la Corte, giustificazione legittimante, anche in relazione ai danni economici e alla generale atmosfera di sfiducia nel luogo di lavoro che possono derivarne.

La Corte osserva inoltre che i lavoratori avrebbero avuto a disposizione una serie di ulteriori strumenti di tutela, quali ad esempio il ricorso all'Autorità garante per la protezione dei dati personali spagnola, non concretamente attivati dagli stessi.

[9] Circa il consenso dei lavoratori interessati, appare utile evidenziare che esso non solo non è richiesto dalla disciplina nazionale ma, qualora prestato, resta irrilevante ai fini della configurabilità dell'illecito penale di cui all'art. 171 del D. Lgs. n. 196/2003 (cfr. da ultimo, Cass. pen. n. 1733/2020).

Avute presenti tutte queste circostanze, la Corte conclude che le autorità nazionali non hanno violato l'obbligo positivo su di esse gravante, previsto dall'articolo 8 della Convenzione, ed hanno rispettato il margine di apprezzamento loro riservato dalla Convenzione.

Circa l'invocata violazione del diritto ad un equo processo, di cui all'art. 6 della Convezione, la Corte osserva che, nel contesto del giudizio dinanzi al tribunale del lavoro nazionale, i ricorrenti hanno avuto accesso alle videoregistrazioni oggetto di contestazione e sono stati in grado di verificarne l'autenticità e di fare opposizione alla loro utilizzazione come prova in giudizio. Le corti nazionali hanno esaminato le difese dei ricorrenti con cui è stato chiesto che tali registrazioni fossero escluse dagli atti del giudizio in quanto ottenute in violazione di un diritto fondamentale, ed hanno dato ampia motivazione su tale punto. I tribunali nazionali hanno pertanto ritenuto, in linea con la giurisprudenza della Corte Costituzionale spagnola, che tale attività di videosorveglianza non sia stata posta in essere in violazione del diritto dei ricorrenti al rispetto della loro vita privata. I tribunali hanno anche ritenuto che le immagini ottenute per mezzo di tale attività di videosorveglianza non sia stata il solo mezzo di prova acquisito in atti.

La Corte nota che i ricorrenti non hanno mai contestato l'autenticità del filmato registrato per mezzo della videosorveglianza. La loro principale doglianza era invece fondata sulla mancanza di preventiva informazione circa l'installazione degli strumenti di ripresa. Le corti domestiche, da parte loro, hanno ritenuto che tali registrazioni fossero assistite da sufficiente garanzia di autenticità. Considerate tutte le circostanze in cui tali registrazioni sono state ottenute, la Corte non vede alcuna ragione per mettere in dubbio la loro autenticità ed affidabilità. I giudici, pertanto, ritengono che si tratti di una fonte di prova priva della necessità di essere corroborata da ulteriori elementi di riscontro.

La Corte evidenzia, peraltro, che le registrazioni in esame non costituiscono l'unica prova su cui le corti domestiche hanno basato le loro decisioni. Esse hanno valutato anche le dichiarazioni rese dai ricorrenti, le testimonianze rese dal direttore del supermercato, dai legali rappresentanti della società, dai rappresentanti sindacali, dinanzi ai quali i ricorrenti avevano fatto ammissione dell'illecito commesso, la consulenza tecnica che ha verificato la corrispondenza tra le immagini registrate per mezzo della videosorveglianza e il registratore di cassa.

Alla luce di quanto sopra, la Corte ritiene che l'uso come prova delle immagini ottenute per mezzo di tale videosorveglianza non abbia leso il diritto all'equo processo. Sotto tale profilo, dunque, l'assunto della Grande Camera non differisce da quello della Camera semplice, che ugualmente aveva ritenuto garantito il rispetto del diritto all'equo processo.

Con tale pronunzia la Corte EDU sembra dare continuità all'orientamento già espresso nel caso *Köpke c. Germania*, deciso con sentenza del 5 ottobre 2010, nel quale pure aveva affermato la legittimità della videosorveglianza occulta. Anche in quest'ultima fattispecie il datore di lavoro aveva videoregistrato, senza preavviso, la condotta di lavoratori sospettati di essere responsabili di una serie di furti in un supermercato. Peraltro, nel caso tedesco le attività di controllo riguardavano due lavoratori specificamente individuati, anziché –come nel caso recente– la generalità del personale aziendale.

In tale vicenda, come in quella sopra esaminata, la Corte EDU aderiva all'impostazione dei tribunali tedeschi, i quali avevano sostenuto che l'interferenza nella sfera privata dei prestatori fosse stata limitata al perseguimento dello scopo al quale la videosorveglianza era

preordinata, cioè l'identificazione dei dipendenti autori degli illeciti, e che per il datore di lavoro non vi fosse concretamente a disposizione altro mezzo di protezione del proprio diritto di proprietà. Sicché, per la Corte i giudici domestici, facendo buon uso del margine di apprezzamento loro riconosciuto, avevano individuato un giusto punto di equilibrio tra il diritto dei lavoratori al rispetto della vita privata e il diritto di proprietà del datore di lavoro.

3.3. In ultimo, appare oltremodo interessante analizzare l'opinione della minoranza dissenziente del Collegio.

I giudici di minoranza partono dall'osservazione secondo cui le moderne tecnologie consentono ai dati memorizzati di essere visualizzati da chiunque, in qualsiasi posto, in qualsiasi momento, con scarso controllo e minima traccia. In tal modo, essi contestano l'assunto della maggioranza nel caso in esame secondo cui solo poche persone –il gestore del supermercato il rappresentante legale dell'azienda e un rappresentante sindacale – hanno visionato le registrazioni ottenute attraverso la videosorveglianza contestata. Le nuove tecnologie, essi osservano, hanno reso estremamente semplici le modalità di effettuazione e trasmissione della videosorveglianza, moltiplicando in modo significativo la potenziale violazione dei diritti alla *privacy*, tutelati dall'art. 8 della Convenzione. Quindi, il disaccordo di principio con la maggioranza deriva dall'approccio di quest'ultima, inadeguato rispetto ai casi riguardanti la sorveglianza elettronica. Nel caso in esame, il quadro giuridico esistente prevedeva una specifica garanzia, vale a dire la necessità che i dipendenti ricevessero un preavviso di installazione e uso della sorveglianza, senza contemplare alcuna eccezione a quella garanzia. Questo punto, ad avviso dei giudici dissenzienti, è dirimente per un'efficace analisi del caso di specie.

Nel contesto particolare dei rapporti di lavoro, osservano ancora i giudici, il quadro giuridico riveste maggiore rilevanza, atteso che il datore di lavoro esercita significativi poteri nei confronti dei dipendenti e qualsiasi abuso di tali poteri dovrebbe essere evitato. Le informazioni sull'attuazione delle misure di sorveglianza sono essenziali affinché gli interessati possano far valere la totalità dei diritti che sono garantiti, come i diritti di accesso, di rettifica o della cancellazione in relazione ai dati personali raccolti.

I giudici richiamano un precedente della Corte (*S. e Marper c. Regno Unito* ([GC], nn. 30562/04 e 30566/04, CEDU 2008), ove è stato affermato che la protezione dei dati personali è di fondamentale importanza per il godimento del diritto al rispetto della vita privata e familiare, come garantito dall'art. 8. Ora, questo diritto non è stato garantito agli interessati in questo caso, in aperta violazione della legge spagnola sulla protezione dei dati. Se è necessario applicare l'attuale quadro normativo, quindi, un preavviso deve essere dato alle persone la cui immagine sarà raccolti e usati. Ebbene, evidenziano i giudici, nessuna opportunità del genere è stata data ai dipendenti in quanto non erano stati precedentemente informati della videosorveglianza segreta.

I giudici di minoranza ritengono insoddisfacente la valutazione effettuata dai tribunali nazionali nel determinare se la videosorveglianza occulta fosse stata, o meno, necessaria. In particolare, il Tribunale non è riuscito a considerare se una misura meno restrittiva avrebbe potuto essere utilizzata dal datore di lavoro per perseguire l'obiettivo di scoprire gli autori degli illeciti. Questa lacuna assume particolare importanza alla luce dell'assunto della maggioranza della Corte, secondo cui è necessario verificare la possibilità di istituire un sistema di

monitoraggio basato su metodi e misure meno invadenti, al fine di garantire la proporzionalità di misure segrete di videosorveglianza sul luogo di lavoro (paragrafo 116).

Il datore di lavoro aveva due scopi legittimi: in primo luogo, voleva evitare ulteriori furti, e per questo l'avvertimento dell'installazione del sistema di videosorveglianza sarebbe stato sufficiente. In secondo luogo, intendeva identificare i responsabili dei danni subiti; a tal fine, il preavviso della videosorveglianza non si sarebbe rivelato utile. Tuttavia, osservano ancora i giudici dissenzienti, poiché il furto commesso era un reato, il datore di lavoro avrebbe potuto, anzi dovuto, rivolgersi alla polizia. I giudici non esitano ad affermare che la necessità di accertare un reato non giustifica l'indagine privata, sotto forma di videosorveglianza nascosta. Non condannando tale comportamento commesso da soggetti privati la Corte, secondo i giudici minoritari, finisce per incoraggiare i datori di lavoro a farsi giustizia da sé.

In senso contrario all'assunto adottato dalla Corte, la minoranza ritiene che, in assenza di chiare garanzie procedurali, l'esistenza di un ragionevole sospetto di una condotta illecita non è sufficiente, in quanto può comportare indagini private e potrebbe essere usato come giustificazione in un numero inaccettabilmente elevato di casi. Il requisito del "ragionevole sospetto" non è, quindi, ritenuto idoneo da tali giudici a tutelare il diritto alla *privacy* di fronte alla videosorveglianza di natura occulta.

I giudici di minoranza osservano ulteriormente che, nella fattispecie in questione, tutti i dipendenti erano stati soggetti alla videosorveglianza nascosta installata dietro le casse del supermercato; inoltre, la sorveglianza è durata per l'intera giornata lavorativa e le telecamere sono state posizionate in modo tale che i lavoratori, nella loro attività di cassieri, non avrebbe potuto evitare di essere filmati. Una così vasta collezione di dati personali, relativa a tutti i dipendenti, avrebbe dovuto essere adeguatamente valutata nel determinare la proporzionalità della misura utilizzata dal datore di lavoro.

Un altro fattore che, ad avviso della minoranza, è stato sottovalutato dalla Grande Camera è costituito dalle possibili conseguenze del monitoraggio per i dipendenti ad esso soggetti. Nella fattispecie, la maggioranza ha riscontrato che, sebbene i richiedenti fossero stati licenziati a seguito dell'uso della videosorveglianza segreta, le registrazioni non sono stati utilizzate dal datore di lavoro per scopi diversi (paragrafo 127). Secondo i giudici di minoranza, tuttavia, il rischio di uso di questi dati non dovrebbe essere sottovalutato, soprattutto in considerazione della vasta gamma delle possibilità che offrono le tecnologie moderne.

In sintesi conclusiva, i giudici dissenzienti osservano che sia i tribunali nazionali sia la Grande Camera non sono riusciti a trovare un giusto equilibrio tra i diritti del datore di lavoro e i diritti dei dipendenti. Non riscontrando alcuna violazione dell'art. 8 della Convenzione, la Corte ha deciso, secondo la minoranza, di consentire l'uso illimitato della videosorveglianza segreta nei luoghi di lavoro, senza offrire garanzie giuridiche sufficienti a coloro i cui dati personali saranno raccolti e utilizzati per scopi a loro sconosciuti. Con la crescente influenza che la tecnologia ha sulla nostra società, concludono i giudici, non si può consentire alle persone di farsi giustizia da sé e di lasciare insufficientemente protetta la riservatezza delle persone, di cui all'art. 8 della Convenzione.

4. Analizzati il contesto normativo interno e il contenuto della pronuncia della Grande Camera, con le annesse contraddizioni interne, è ora possibile verificare i possibili effetti di quest'ultima sul primo.

A tal fine, bisogna precisare innanzitutto che, non essendo l'Italia parte in giudizio nella fattispecie, non può riscontrarsi il conseguente obbligo di adeguarsi alla pronuncia, ai sensi dell'art. 46 della Convenzione. Tuttavia, com'è noto, le supreme giurisdizioni, sia sovranazionali sia interne[10], sostengono la tesi dell'efficacia indiretta della sentenza, in relazione all'art. 32 della Convenzione. Secondo tale indirizzo, le decisioni della Corte di Strasburgo s'impongono a tutti gli Stati contraenti, sotto forma di interpretazione vincolante, per i giudici, delle norme applicate. Si tratta di un'efficacia che, tuttavia, non è prevista esplicitamente negli artt. 41 e 46 della Convenzione.

Sul tema si riscontra un intenso dibattito dottrinale, di cui non è possibile qui dare conto compiutamente[11]. In estrema sintesi, si possono registrare due posizioni, una che – in adesione alla giurisprudenza suddetta – afferma la sussistenza dell'efficacia *erga omnes* delle sentenze della Corte, in riferimento all'art. 32 della Convenzione, analogamente a quelle della Corte di Giustizia *ex* art. 267 TFUE[12]. L'altro indirizzo nega il monopolio interpretativo della Corte sulle disposizioni della Convenzione e il conseguente effetto vincolante per i giudici nazionali, proprio in ragione della mancanza di una norma come quella dell'art. 267 cit.[13].

Aderire all'uno o all'altro orientamento rileva in merito alla soluzione da ipotizzare sull'evidente contrasto tra il *dictum* della Corte e l'art. 4, comma 3, della legge n. 300 cit., laddove – come sopra evidenziato – quest'ultima disposizione stabilisce, a pena di inutilizzabilità dei dati acquisiti e senza limiti o deroghe, un'adeguata informazione preventiva ai lavoratori interessati.

In caso di adesione alla tesi negatrice dell'interpretazione vincolante, il giudice nazionale è libero di adeguarsi alla pronuncia, ovvero di discostarsi da essa, considerandola un mero precedente autorevole, e applicare così l'attuale formulazione dell'art. 4, comma 3 cit.. Viceversa, ove si appoggi l'opposto indirizzo, sostenuto dalla giurisprudenza dominante, il giudice è vincolato alla decisione e, alle condizioni poste dalla Corte, non può ritenere necessaria l'informazione preventiva, aprendo così la strada all'introduzione dei controlli occulti nel nostro ordinamento.

Occorre anche precisare che, in ogni caso, l'adesione alla statuizione dei giudici europei comporterebbe, per le corti nazionali, l'obbligo di sollevare la questione di legittimità costituzionale dell'art. 4, comma 3 cit., per contrasto con l'art. 117 Cost. e con la norma interposta CEDU – nella specie l'art. 8 come interpretato dai giudici di Strasburgo – secondo il ragionamento della Corte Costituzionale[14]. In questo ambito, invero, non vi è spazio per una mera disapplicazione della disposizione interna, come avviene in relazione alle decisioni della Corte di Giustizia.

---

[10] Cfr. Corte CEDU, 27 marzo 2003, Scordino c. Italia, n. 36813/97 in *D&G*, 2003, 25, p. 83 ss.; Corte Cost. sentenza nn. 311 e 317 del 2009, nonché nn. 348 e 349 del 2007, in *giurcost.org*, con relativi riferimenti di dottrina, Cass. SS.UU., nn. 1338, 1339, 1340 e 1341 del 2004.

[11] Si veda in proposito P. PIRRONE, *L'obbligo di conformarsi alle sentenze della Corte europea dei diritti dell'uomo*, Milano, 2004.

[12] G. TESAURO, *Costituzione e norme esterne*, in *Il diritto dell'unione europea*, 2009, 2, p. 219; L. MONTANARI, *Giudici comuni e Corti sovranazionali: rapporti tra sistemi*, in *rivistaaic.it*.

[13] M. LUCIANI, *Alcuni interrogativi sul nuovo corso della giurisprudenza costituzionale in ordine ai rapporti fra diritto italiano e diritto internazionale*, in *Corriere giur*., 2008, p. 204; R. GRECO, *Dialogo tra corti ed effetti nell'ordinamento interno. Le implicazioni della sentenza della Corte Costituzionale del 7 aprile 2011, n.113*, in *giustcost.org*.

[14] Sentenze nn. 348 e 349 del 2007 cit..

Peraltro, secondo gli ultimi approdi ermeneutici della Consulta[15], il vincolo dei giudici italiani alle sentenze della Corte EDU si riscontra solo nella misura in cui i principi di diritto da esse enunciate siano espressione di un «diritto consolidato, generato dalla giurisprudenza europea, che il giudice interno è tenuto a porre a fondamento del proprio processo interpretativo, mentre nessun obbligo esiste in tal senso, a fronte di pronunce che non siano espressive di un orientamento oramai divenuto definitivo» (sentenza n. 49/2015). Per di più i giudici costituzionali hanno puntualizzato che, nel progressivo adeguamento alla CEDU, non può sussistere alcun automatismo, stante il «predominio assiologico della Costituzione sulla CEDU» nell'ordinamento nazionale.

Ciò posto, nel caso di specie si deve considerare non solo che la sentenza in commento si pone quale indirizzo al momento non sufficientemente consolidato, almeno nei termini in cui è espresso, ma anche – come notato – che la decisione è risultata il frutto di un intenso dibattito non senza contrasti all'interno della Corte, per concludere che appare più che dubbio ipotizzarne effetti paralizzanti o invalidanti sulla disciplina interna. In questo quadro, sembrano degni della massima attenzione le notazioni della Camera semplice e della minoranza della Grande Camera, in merito ai rischi della raccolta dei dati con modalità occulte e, soprattutto, al pericolo di incentivare condotte di ragion fattasi.

In definitiva, appare arduo immaginare, in ragione dell'attuale posizione della giurisprudenza costituzionale, l'adesione dei giudici nazionali ad un assunto, per un verso minoritario e, per l'altro, contrastato al suo interno. Sicché, non sembra affatto scontato che la decisione in commento possa dare ingresso nel nostro ordinamento ai controlli a distanza occulti.

A conferma di tale assunto, appare utile segnalare la dichiarazione del Presidente del Garante per la protezione dei dati personali, datata 17 ottobre 2019, secondo la quale la sentenza della Grande Camera della Corte di Strasburgo, se da una parte giustifica le telecamere nascoste, dall'altra conferma il principio di proporzionalità come requisito essenziale di legittimazione dei controlli in ambito lavorativo. Il requisito essenziale perché i controlli sul lavoro, anche quelli difensivi, siano legittimi resta dunque la loro rigorosa proporzionalità e non eccedenza. Dopo aver rammentato le peculiarità del caso scrutinato dalla corte di Strasburgo, il Garante avverte che la videosorveglianza occulta è, dunque, ammessa solo quale *extrema ratio*, a fronte di "gravi illeciti" e con modalità spazio–temporali tali da limitare al massimo l'incidenza del controllo sul lavoratore e non può diventare una prassi ordinaria. La posizione del Garante assume i caratteri di un monito, rivolto ai datori di lavoro, a non ritenere la pronuncia un'illimitata autorizzazione alla sorveglianza occulta sui dipendenti.

[15] Sentenza 26 marzo 2015 n. 49, in *giurcost.org*, con ampi commenti di dottrina. Nello stesso senso, più di recente, Sentenza 13 giugno 2018, n. 120.