SCHEDA 16 Febbraio 2021

CONTROLLO A DISTANZA DEL LAVORATORE E RISCHIO PENALE

Emanuele Birritteri

Cass., Sez. III, sent. 14 dicembre 2020 (dep. 27 gennaio 2021), n. 3255, Pres. Andreazza, est. Corbo

1. Come noto, la possibilità a determinati fini**[1]** per il datore di lavoro di introdurre in azienda dei meccanismi di **controllo a distanza dei lavoratori** è subordinata, ai sensi dell'art. 4 dello Statuto dei lavoratori (l. n. 300 del 1970)**[2]**, alla sussistenza di un **accordo sindacale** o, in mancanza, all'**autorizzazione** della sede territoriale dell'**Ispettorato del lavoro**, con ulteriori disposizioni che, peraltro, condizionano la possibilità di utilizzare le informazioni così raccolte – a tutti i fini connessi al rapporto di lavoro – alla

previa informativa al lavoratore sulle modalità d'uso degli strumenti di vigilanza e di effettuazione dei controlli, nel rispetto della disciplina sulla ***privacy***.

La normativa si muove dunque in una duplice direzione regolando: a) le **condizioni di legittimità** del **controllo**; b) le **modalità d'uso** delle **informazioni** raccolte, subordinando la possibilità per il datore di avvalersi dei dati così registrati all'adempimento dei predetti oneri**[3]**.

Dalla prospettiva del penalista tale norma assume interesse, anzitutto, in relazione alle conseguenze penali che determina la violazione di tali regole da parte del datore del lavoro.

Invero, per quanto qui interessa, l'art. **171** del **codice in materia di protezione dei dati personali** (d.lgs. n. 196 del 2003) sancisce che la **violazione**, in particolare, delle regole prima citate ***sub* a)** – relative, cioè, alle condizioni di legittimità del controllo sancite dal comma 1 del detto art. 4 – è punita con le **sanzioni** di cui all'**art. 38** della legge n. 300 del 1970. Norma, quest'ultima, che appunto – disciplinando una contravvenzione passibile di oblazione c.d. facoltativa – prevede la pena alternativa dell'ammenda da 154 a 1549 euro o dell'arresto da 15 giorni ad un anno**[4]**.

L'illecito penale qui svolge il ruolo ancillare – ricorrente nella legislazione complementare – di mero presidio sanzionatorio del rispetto della disciplina di regolazione del settore, secondo uno schema operativo ben noto (e criticato a livello dogmatico), che di solito non pone particolari problemi interpretativi nella prassi applicativa, al netto delle criticità in punto di effettività e deterrenza di tale modello punitivo**[5]**.

Tuttavia, negli anni è emersa la questione legata alla possibilità per il **datore di lavoro**, specie in presenza di **indizi** concreti di **illeciti in atto** da parte dei dipendenti a danno del patrimonio aziendale, di effettuare comunque una **sorveglianza occulta** sul luogo di lavoro per fugare il dubbio sulla sussistenza o meno di tali condotte, anche **senza** aver preventivamente dato corso ai necessari **adempimenti** imposti dalla disciplina **giuslavoristica** in tema di controllo a distanza dei lavoratori.

In tali casi, invero, vanno bilanciate due esigenze contrapposte: da un lato, quella dell'**impresa** di prevenire la commissione di reati e di avviare indagini interne a tutela del **patrimonio aziendale**; dall'altro, quella legata alla necessaria protezione del **lavoratore** rispetto a forme di **sorveglianza generalizzata** (e incontrollata).

È evidente del resto che, ad esempio, imporre al datore di lavoro, in simili ipotesi, un preventivo accordo sindacale o la previa informativa al lavoratore sull'effettuazione del controllo comprometterebbe le intuibili esigenze di segretezza e celerità delle **indagini interne** che, per poter raggiungere il loro scopo, devono potersi svolgere "a sorpresa".

Di contro, però, tali situazioni non devono rappresentare l'occasione per predisporre in pianta stabile in azienda dei sistemi di controllo aggirando ed **eludendo**, di fatto, le regole che subordinano la possibilità di utilizzare tali sistemi alla sussistenza delle dette condizioni (in particolare richiedendo l'accordo sindacale o, in mancanza, l'autorizzazione dell'Ispettorato del lavoro).

Su tali temi, qui ricostruiti nelle loro linee essenziali, si è di recente pronunciata la Grande Camera della **Corte EDU** nel caso **Lopez Ribalda[6]**.

Nel bilanciare i detti interessi contrapposti, in particolare, i giudici di Strasburgo hanno in sostanza ritenuto legittima la **sorveglianza occulta** effettuata dal datore sul luogo di lavoro anche in assenza del **previo rispetto** delle disposizioni in tema di controllo a distanza dei lavoratori, a condizione, tuttavia, che possa ritenersi **proporzionata**, valorizzando la sussistenza nel caso concreto di alcune **condizioni** così sintetizzabili: a) la preventiva emersione di concreti **indizi** tali da segnalare la presenza di illeciti in atto da parte dei dipendenti; b) l'effettuazione del controllo al limitato e **unico scopo** di **accertare** gli **illeciti** in atto, e con modalità **proporzionate** e coerenti con tale esclusiva finalità; c) l'**interruzione** della sorveglianza occulta una volta terminata l'indagine.

2. La sentenza della Cassazione qui segnalata si inserisce esattamente nel solco di tale indirizzo interpretativo, avendo ad oggetto la contestazione al titolare di un esercizio commerciale della detta sanzione prevista dall'art. 38 dello Statuto dei lavoratori per aver installato un impianto di **video sorveglianza** in azienda volto al controllo a distanza dei dipendenti, **senza** tuttavia aver richiesto **preventivamente** l'**accordo** con le rappresentanze sindacali o l'**autorizzazione** dell'Ispettorato del lavoro.

Il titolare dell'attività economica in questione ricorre quindi per Cassazione rilevando come gli impianti video fossero stati predisposti al solo scopo di tutelare il **patrimonio aziendale** a seguito – ed è questo un punto chiave alla luce di quanto prima rilevato – di alcuni **precedenti episodi** ove era stata riscontrata la mancanza di merce in magazzino, e non già con la finalità di

controllare i dipendenti (dato peraltro confermato, nell'impostazione difensiva, dal fatto che le telecamere erano rivolte soltanto verso la cassa e le scaffalature).

La Cassazione ritiene il ricorso fondato, anzitutto facendo leva su una serie di precedenti giurisprudenziali, emersi anche in sede civile nonché rispetto al tema dell'**utilizzabilità processuale** degli esiti di tali attività di sorveglianza, che in diverse riprese hanno sancito la legittimità dei **c.d. controlli difensivi** volti ad accertare condotte illecite del lavoratore, ritenuti invero estranei al campo di applicazione dell'art. 4 della legge n. 300 del 1970. Il diverso scopo di quest'ultima disposizione, si spiega, è infatti quello di proteggere la **riservatezza** del lavoratore**[7]**.

La Corte, inoltre, richiama anche un precedente giurisprudenziale della Corte EDU relativo al caso **Barbulescu**, che confermerebbe come tale soluzione ermeneutica sia coerente con i principi sanciti dall'art. 8 della Convenzione, che consente simili controlli, nelle dette situazioni, se proporzionati e ragionevoli rispetto ai richiamati scopi**[8]**.

La Suprema Corte ritiene allora di aderire a tali impostazioni, affermando come debba **escludersi** la configurabilità della predetta **contravvenzione** in virtù, appunto, della legittimità di una sorveglianza non previamente autorizzata che sia strettamente funzionale alla tutela del patrimonio aziendale e che ***non*** si declini, per usare le parole del collegio, in un «...**significativo controllo** sull'ordinario svolgimento dell'attività lavorativa», oltre a rimanere necessariamente **"riservata"** «...per consentire l'accertamento di gravi **condotte illecite** degli stessi».

Rispetto a tale versante, peraltro, la Corte attribuisce anche rilievo al fatto che i dispositivi installati, essendo rivolti alle casse e agli scaffali, avrebbero potuto controllare solo in via del tutto

occasionale l'attività del singolo dipendente.

Nel caso di specie, tuttavia, la Corte annulla con rinvio la sentenza impugnata per un nuovo giudizio, evidenziando come la decisione di merito non avesse chiarito «...se l'installazione del sistema di videosorveglianza rilevato fosse strettamente funzionale alla tutela del patrimonio aziendale, né se l'utilizzo del precisato impianto comportasse un controllo non occasionale sull'ordinario svolgimento dell'attività lavorativa dei dipendenti, o, comunque, dovesse restare necessariamente "riservato" per consentire l'accertamento di gravi condotte illecite di questi ultimi».

Pur non richiamando espressamente la più recente pronuncia della Corte EDU nel caso Lopez Ribalda, quindi, la Cassazione giunge qui a esiti tutto sommato in linea con l'autorevole precedente in questione.

3. Ci sembra che un "confronto diretto" con tale pronuncia avrebbe forse consentito alla Corte di chiarire – in modo più esplicito di quanto può leggersi tra le righe della sentenza qui commentata – che la sorveglianza occulta non previamente autorizzata è sì possibile per la tutela del patrimonio aziendale, ma a condizione che possano valorizzarsi precisi elementi che segnalino la **proporzionalità** della misura: la preventiva sussistenza di **indizi** concreti di illeciti da parte dei dipendenti; il fatto che la sorveglianza occulta sia **limitata** esclusivamente ad accertare tali illeciti; l'**interruzione** del controllo una volta terminata l'indagine interna. E ciò anche considerato che i detti requisiti sembrano sussistere nel caso di specie (per quanto sull'ultimo tra quelli appena menzionati la decisione non si soffermi).

La sentenza, peraltro, ci pare offra l'occasione per un ulteriore spunto di riflessione che ci sembra possa essere segnalato pur tenendo conto che l'argomento meriterebbe un grado di approfondimento che esula dall'economia del presente lavoro.

Al di là del tema della responsabilità penale del datore di lavoro per i controlli a distanza dei dipendenti direttamente affrontato dalla decisione in commento, infatti, la disposizione di cui all'art. 4 dello Statuto dei lavoratori rappresenta un importante punto di riferimento sistematico anche per valutare le condizioni di **legittimità** dell'**uso** di alcuni strumenti di **automazione** della ***compliance*** penale adottati dagli enti collettivi nelle attività di controllo interno legate all'*enforcement* del d.lgs. n. **231** del **2001**.

Si pensi, ad esempio, ai diversi ***software*** che le aziende iniziano ad utilizzare per processare i **dati** che "transitano" nei processi aziendali in modo da identificare ***pattern*** di comportamento anomali rispetto alle ordinarie attività dell'ente e altri ***red flags*** segnalanti il rischio, da indagare ulteriormente, di azioni illecite in atto in grado di radicare la responsabilità da reato dell'ente collettivo**[9]**.

Il fatto che, come visto, la non corretta gestione di tali strumenti comporti la possibile contestazione di violazioni penalmente rilevanti, allora, deve indurre a interrogarsi sulla **razionalità** complessiva di un sistema che, da un lato, chiede all'impresa di investire significative **risorse** per la **prevenzione** del rischio reato e, dall'altro, espone chi la gestisce a un **rischio punitivo** in caso di non conformità a una disciplina che – ci pare sia questo il punto cruciale – è stata pensata ad **altri fini** dal legislatore, e non certo per regolare le attività di *compliance* penale e le ***internal investigation*** svolte dagli enti collettivi.

Con ciò non vogliamo certo affermare che l'attribuzione di un compito di autocontrollo all'impresa debba legittimare forme di sorveglianza "senza limiti" a danno dalla riservatezza dei lavoratori.

Tutt'altro. Intendiamo piuttosto evidenziare come – anche alla luce delle lacune che i processualpenalisti più accorti hanno evidenziato in punto di **garanzie difensive** oggi esistenti nel nostro ordinamento per i soggetti coinvolti dalle investigazioni interne delle società**[10]** – il legislatore debba finalmente farsi carico dell'esigenza di regolare ***direttamente*** tali attività di *compliance* e **controllo interno**, garantendo sì l'interesse dell'impresa di avvalersi dei più moderni ed efficienti strumenti di prevenzione del reato, ma avendo cura di contenere l'impatto che simili attività producono sui **diritti fondamentali** dei singoli interessati**[11]**.

[1] Le finalità in tal senso elencate dall'articolo 4 della l. n. 300 del 1970 sono le seguenti: esigenze organizzative e produttive; sicurezza del lavoro; tutela del patrimonio aziendale.

[2] Così come riformato da ultimo con il d.lgs. n. 151 del 2015 e con il d.lgs. n. 185 del 2016. Peraltro, la disposizione in parola, precisa che tali disposizioni non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

[3] Sul tema v. di recente, senza pretesa di esaustività: G. Proja, *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza*, in *Riv. it. dir. lav.*, 2016, 4, 547 ss.; L. Tebano, *Employess' Privacy and employers' control between the Italian legal system and European sources*, in *Labour & Law Issues*, 2017, vol. 3, 2, 1 ss.

[4] Peraltro, il secondo comma dell'art. 38 della legge n. 300 del 1970 prevede che nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente, impedendo così l'applicazione dell'istituto dell'oblazione. Il terzo comma della disposizione, poi, sancisce che allorquando, per le condizioni economiche del reo, l'ammenda del primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.

[5] Sul diritto penale sanzionatorio v. in generale, per tutti, M. Catenacci, *La tutela penale dell'ambiente. Contributo all'analisi delle norme penali a struttura 'sanzionatoria'*, Padova, 1996, *passim*.

[6] Corte EDU, Grande Camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019.

[7] In merito agli orientamenti qui richiamati si vedano da ultimo, *ex multis*: Cass. pen., Sez. II, 16 gennaio 2015 (dep. 22 gennaio 2015), n. 2890, in *Dir. prat. lav.*, 2016, 12, 769 ss., con nota di S. Servidio, *Controllo dei dipendenti e difesa del patrimonio aziendale*; Cass. pen., Sez. III, 15 dicembre 2006 (dep. 27 febbraio 2007), n. 8042, in *Dir. prat. lav.*, 2007, 12, 816 ss. Nella giurisprudenza civile v., di recente, tra le molte, Cass. Civ., Sez. L., 25 maggio 2018, n. 13266 in *C.E.D. Cass.* n. 649009-01.

[8] Corte EDU, Grande Camera, Barbulescu c. Romania, 5 settembre 2017.

[9] Sulle interazioni tra IA e diritto penale, anche rispetto alla prevenzione del rischio reato, v. da ultimo, diffusamente, C. Burchard, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in *Riv. it. dir. proc. pen.*, 2019, 4, 1909 ss. Sull'utilizzo di sistemi di intelligenza artificiale nelle attività *compliance* si vedano da ultimo W.S. Laufer, *The*

Missing Account of Progressive Corporate Criminal Law, in *New York University Journal of Law & Business*, 2017, vol. 14, 1, 71 ss., nonché gli studi di Deloitte, ***Compliance modernization is no longer optional: How evolved is your approach?***, 2017, e Ey, ***Integrity in the spotlight. The future of compliance***, 15th Global Fraud Survey, 2018.

[10] Si vedano sul punto: E.M. Mancuso, *Le investigazioni interne nel sistema processuale italiano: tra vuoto normativo e prassi applicative incerte*, in F. Centonze, M. Mantovani (a cura di), *La responsabilità «penale» degli enti. Dieci proposte di riforma*, Bologna, 2016, 217 ss.; F. Nicolicchia, Corporate Internal Investigations *e diritto dell'imputato del reato presupposto nell'ambito della responsabilità «penale» degli enti: alcuni rilievi sulla base della "lezione americana"*, in *Riv. trim. dir. pen. econ.*, 2014, 3-4, 781 ss. Nella letteratura internazionale in argomento v., per tutti, A. Nieto Martin, I*nternal Investigations, Whistle-Blowing and Cooperation: The Struggle for Information in the Criminal Process*, in S. Manacorda, F. Centonze, G. Forti (a cura di*), Preventing Corporate Corruption: The Anti-Bribery Complicane Model*, Londra, 2014, 69 ss.

[11] Per ogni approfondimento e per tutti i relativi riferimenti bibliografici in merito agli spunti qui da ultimo richiamati sia consentito rinviare a E. Birritteri, **Big Data Analytics *e* compliance *anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri***, in *Dir. pen. cont. – Riv. trim.*, 2019, 2, 289 ss.