amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Marco Cardilli

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 1/2020

estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Vincenzo Caputi Jambrenghi, Enrico Carloni, Guido Clemente di San Luca, Andry Matilla Correa, Gianfranco D'Alessio, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Salvatore Bonfiglio, Vinicio Brigante, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Gaetano Natullo, Carmen Pérez González, Marcin Princ, Giuliano Taglianetti, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

La tutela della privacy nell'esercizio del potere datoriale

di Filippo Lore'

(Docente a contratto Università degli studi di Bari "A. Moro")

Sommario

1. Il rapporto tra diritto alla riservatezza e il potere di controllo datoriale - 2. Brevi cenni ai primi atti di indirizzo del Garante per la protezione dei dati personali - 3. I recenti orientamenti delle Corti europee tra riconoscimento del diritto alla riservatezza ed esercizio del potere datoriale

Abstract

This article examines the aspects relating to the protection of worker confidentiality and the exercise of the employer's control power in the context of guarantees provided by national labor legislation.In particular, recent decisions of the European Courts on the recognition of the private sphere of the worker will be examined.

1. Il rapporto tra diritto alla riservatezza e il potere di controllo datoriale.

L'attività di analisi dei dati assume fondamentale rilevanza per le imprese che desiderano trarre vantaggi sul mercato, in ottica di posizionamento. Sul fronte organizzativo, interno all'ambito lavorativo, si parla di *data driven management*, approccio che consente di ottimizzare, anche mediante sistemi di intelligenza artificiale e di *machine learning*, la gestione delle risorse umane nel corso delle diverse fasi del rapporto di lavoro, dal processo di selezione del personale alla riorganizzazione degli uffici, dai trasferimenti alla variazione delle mansioni del singolo lavoratore, dalla verifica delle prestazioni alle promozioni di carriera.

La tutela dei dati personali richiamata dal Regolamento UE 2016/679 e, in ambito nazionale, dal D. Lgs n. 196/2003 e s.m.i., impattano fortemente sulla disciplina del rapporto di lavoro, in considerazione del fatto che sempre più numerosi e tecnologicamente avanzati sono i dispositivi messi a disposizione dal datore al dipendente. Tale materia, negli ultimi tempi, è risultata essere oggetto di attenzione da parte della Giustizia europea e nazionale, con decisioni contrastanti. Ai diversi indirizzi forniti dai giudici, si deve altresì considerare un ulteriore elemento: l'utilizzo delle nuove tecnologie, che aggiungono aspetti di criticità legati al bilanciamento tra riservatezza dei lavoratori e potere di controllo in capo al datore di lavoro[1]. L'impiego di strumenti quali personal computer, tablet, altri devices e la rete internet se da un lato rappresentano idonei elementi per incrementare la produttività, dall'altro evidenziano rischi in ordine al corretto assolvimento della prestazione lavorativa e, contestualmente, al godimento dei diritti dei lavoratori[2]. Se ne deduce, quindi, che un potenziale controllo del datore di lavoro sul proprio dipendente, in connessione con il potere disciplinare, possono configurare un serio rischio al libero godimento del diritto alla riservatezza dei lavoratori[3].

La normativa, storicamente, ha sancito un generale divieto dell'esercizio dei controlli da remoto del lavoratore, successivamente attenuato da specifici interventi legislativi intervenuti a dettare casistiche per le quali, al ricorrere di determinate condizioni, si sarebbe resa possibile l'attività di controllo datoriale. Con riferimento al quadro di tutele normative, la prima norma di riferimento è la L. n. 330/1970, art. 4[4], che, nella

[1] Audizione di Antonello Soro, Presidente del Garante per la protezione dei dati personali, in tema di utilizzo delle metodologie di data mining per eseguire visite mediche di controllo nei confronti dei lavoratori del settore pubblico presso la 11ª Commissione permanente (Lavoro, previdenza sociale) del Senato della Repubblica (18 settembre 2018).

[2] M. G. Stanzione, *Il Regolamento Europeo sulla Privacy: origini e ambito di applicazione*, Europa e diritto privato, 2016, 4, pp. 1249-1264.

[3] R. Lattanzi, *Dallo statuto dei lavoratori alla disciplina di protezione dei dati personali*, RIDL, 2011, I, 151.

[4] Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale (Adottata dal Comitato dei Ministri il 1 aprile 2015, nel corso della 1224ma seduta dei

formulazione originale, prevedeva un categorico divieto del monitoraggio della prestazione lavorativa. Lo stesso articolo, al comma 2, sanciva comunque la possibilità per il datore di lavoro di derogare al divieto previsto dal richiamato comma 1, per motivi legati alle "*esigenze organizzative e produttive ovvero dalla sicurezza del lavoro*" attraverso la definizione di un accordo con le rappresentanze sindacali, o in assenza, mediante espressa autorizzazione dell'Ispettorato del Lavoro. Il quarto comma dello stesso articolo guardava al regime da adottare per quegli impianti che erano stati installati prima dell'entrata in vigore dello Statuto, mentre l'ultimo comma stabiliva che "*contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo articolo 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale*"[5].

Preme ricordare che il quadro di tutela normativa non si esauriva solo con la previsione di garanzie per l'installazione di sistemi di videosorveglianza, bensì ricomprendeva la componente *software*, così come richiamato, poi, dalle "Linee guida del Garante per posta elettronica e internet" (così si pronunciava l'Autorità di controllo "*Le informazioni di carattere personale trattate possono riguardare, oltre all´attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell´uomo, può essere tracciata a volte solo con difficoltà*"). Nonostante la stringente previsione normativa, l'orientamento giurisprudenziale, sempre in ottica di bilanciamento degli interessi in gioco tra la riservatezza del lavoratore e il potere di controllo del datore di lavoro, ha di fatto introdotto l'istituto dei c.d. "controlli difensivi", intesi in una prima fase solo per le fattispecie che risiedevano fuori dall'ambito di applicazione dell'art. 4 dello Statuto dei Lavoratori e, quindi, solo per perseguire potenziali comportamenti illeciti

---

rappresentanti dei Ministri). 15. Sistemi informativi e tecnologie per la sorveglianza dei dipendenti, compresa la videosorveglianza

15.1. Non dovrebbe essere consentito introdurre e utilizzare sistemi informativi e tecnologie aventi per scopo diretto e primario la sorveglianza dell´attività e del comportamento dei dipendenti. Se l´introduzione e l´utilizzazione di tali sistemi e tecnologie per altri scopi legittimi, quali la tutela dell´attività produttiva, della salute e della sicurezza, o l´efficace gestione di un´azienda o di un ente, comportano indirettamente la possibilità di sorvegliare l´attività dei dipendenti, esse dovrebbero essere soggette alle ulteriori salvaguardie previste nel Principio 21, ed in particolare alla consultazione di rappresentanti dei dipendenti.

15.2. Sistemi informativi e tecnologie che comportino indirettamente la sorveglianza di attività e comportamenti dei dipendenti dovrebbero essere progettati su base specifica e posizionati in modo da non compromettere i diritti fondamentali dei dipendenti stessi. In nessun caso è consentito ricorrere alla videosorveglianza di luoghi che appartengono alla sfera più privata della vita dei dipendenti.

15.3. In caso di controversie o procedimenti giudiziari, i dipendenti dovrebbero avere la possibilità di ottenere copie delle registrazioni effettuate, se del caso e conformemente al diritto interno. La conservazione di eventuali registrazioni dovrebbe essere soggetta ad un limite temporale.

[5] A. Bellavista, Il *controllo sui lavoratori, Torino, 1995; A. TROISI, Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013, pp. 17 e ss.

dei lavoratori ed estranei dalla prestazione lavorativa intesa, in senso stretto, allo scopo di tutelare il patrimonio aziendale. A questi, devono annoverarsi, altresì, i c.d. controlli difensivi occulti, che non necessitano *tout court* di preventivo accordo sindacale (o di altra specifica autorizzazione), come si desume dalla lettura della Sentenza n. 10636/2017 della Corte di Cassazione[6], emessa in materia di videosorveglianza sui luoghi di lavoro, nella quale si affronta il ricorso di un dipendente contro il licenziamento disciplinare subito. Più dettagliatamente, il lavoratore in oggetto si era reso colpevole, sulla base della rilevazione video, di un comportamento illecito, in violazione degli obblighi connessi alla propria mansione e del dovere di custodia dei beni aziendali. Se ne desume che la Corte, nella sentenza richiamata, ha ritenuto che si esulasse dal campo di operatività dell'art. 4 Statuto dei Lavoratori, trattandosi di telecamere poste in area alla cui gestione era addetta una ditta esterna all'organizzazione aziendale, al solo fine di sorvegliare un unico ripiano sul quale erano stati disposti specifici prodotti, ragion per cui il controllo non si estrinsecava, in alcun modo, in un controllo sull'adempimento della prestazione lavorativa[7]. Invero, secondo la Corte, tali controlli sono da intendersi leciti, in piena aderenza all'art. 4 dello Statuto dei Lavoratori, purché vi sia un corretto contemperamento tra diversi diritti, in un quadro di garanzia dei principi di ragionevolezza e proporzionalità.

Ulteriore caso, meritevole di approfondimento, riguarda una decisione del Tribunale di Roma, chiamato ad esprimersi sul licenziamento intimato da un'Azienda ad un dipendente, provvedimento scaturito dalle indagini circa l'utilizzo dell'applicativo software denominato "Blue's 2002", in grado di estrarre, esclusivamente, il numero di telefono del chiamante, l'ora della telefonata e la sua durata, in assenza di ulteriore informazione circa il contenuto della chiamata e della possibilità di controllo circa l'effettiva prestazione lavorativa. Il datore di lavoro rilevava che il dipendente, durante la prestazione di lavoro, aveva sostenuto conversazioni telefoniche (anche per scopi personali) con centinaia di soggetti, per una durata inferiore ai quindici secondi per ogni singolo contatto, arco di tempo non sufficiente ad evadere, in maniera esaustiva, eventuali reclami e segnalazione degli utenti. Il Tribunale interessato, all'esito del processo, rigettava la domanda del lavoratore, il quale provvedeva, successivamente, ad adire la Corte di Appello di Roma che, con sentenza n. 1970 del 12 novembre 2009, *"in via preliminare rigettava l'eccezione di improcedibilità dell'appello e, nel merito, riteneva, come già il giudice di primo grado, che il sistema di rilevamento delle telefonate attraverso il software Blue's 2002 non fosse in*

[6] M. Di Francesco, *Licenziamento per giusta causa e controlli difensivi occulti*, Diritto & Pratica del Lavoro, n. 34-35/2017, Settimanale Ipsoa, settembre 2017.

[7] Corte di Cassazione, Sezione Lavoro Civile, con la sentenza del 2 magio 2017, n. 10636, mediante la quale ha rigettato il ricorso e confermato quanto già deciso, nel caso de quo, dalla Corte d'appello di Perugia.

contrasto con l'art. 4 dello Statuto dei lavoratori, in quanto relativo al c.d. controllo difensivo".

La Corte di Cassazione, Sezione Lavoro, con sentenza depositata il 1° ottobre 2012, n. 16622, ha definitivamente archiviato il contenzioso, considerando illegittimo l'utilizzo del software "Blue's 2002", con conseguente inutilizzabilità dei dati acquisiti attraverso lo stesso per provare l'inadempimento del lavoratore, motivando tale decisione con la tesi secondo cui *"(I)l divieto di controlli a distanza ex art. 4, della L. n. 300 del 1970, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico Blue's 2002, ricadono nell'ambito della L. n. 300 del 1970, art. 4, comma 2, e, fermo il rispetto delle garanzie procedurali previste, non possono impingere la sfera della prestazione lavorativa dei singoli lavoratori; qualora interferenze con quest'ultima vi siano, e non siano stati adottati dal datore di lavoro sistemi di filtraggio delle telefonate per non consentire, in ragione della previsione dell'art. 4, comma 1, di risalire all'identità del lavoratore, i relativi dati non possono essere utilizzati per provare l' inadempimento contrattuale del lavoratore medesimo*".

Ancora, La Corte Suprema di Cassazione con sentenza 17 luglio 2007, n. 15892 ha precisato, proprio in riferimento all'utilizzo di informazioni che derivano da apparecchiature per il controllo a distanza dell'attività dei lavoratori, che la rilevazione dei dati di entrata e di uscita dall'azienda attraverso il sistema di controllo organizzato dal datore di lavoro, benché finalizzato a perseguire una condizione di favore per gli stessi lavoratori, comporta una attività di controllo sull'osservanza dell'orario di lavoro e, quindi, anche della correttezza dell'esecuzione della prestazione lavorativa. Tale apparecchio, utilizzato per giungere al licenziamento di un dipendente, non era stato concordato con le rappresentanze sindacali, né oggetto di autorizzazione amministrativa dall'Ispettorato del lavoro e, per questo, rientrante nella fattispecie prevista dal secondo comma dell'art. 4 dello Statuto dei lavoratori. Il caso riportato e oggetto di decisione analizzava il dispositivo di sicurezza, in entrata e in uscita dagli uffici, predisposto nelle aree dedicate al parcheggio delle vetture dei dipendenti durante l'orario di lavoro. Quest'ultimo si avviava con un tesserino personale di cui era in possesso ogni dipendente, tracciando ogni singolo passaggio dello stesso[8]. Ne deriva che la necessità di prevenire condotte illecite da parte dei lavoratori non può rivestire forza tale da giustificare un pregiudizio al libero godimento di diritti fondamentali, quali la dignità e la riservatezza del lavoratore stesso. Il bilanciamento di interessi tra le pretese datoriali e la tutela della riservatezza del prestatore di lavoro incontrano un punto di

[8] Costituisce strumento di controllo "preterintenzionale" a distanza dell'attività dei lavoratori, soggetto alla disciplina dell'art. 4, comma 2, l. 300/1970, un'apparecchiatura di rilevamento delle presenze attivata mediante tessere magnetica (badge), sicché, in caso di mancato esperimento della procedura di cui all'art. 4 c. 2 St. Lav., non sono utilizzabili in sede disciplinare i dati acquisiti tramite la stessa. (Trib. Napoli 29/9/2010, Giud. Vargas, con nota di Federico Fusco, "Il pomo della discordia: il badge come strumento di controllo a distanza?", 31)

equilibrio nel principio di proporzionalità, in forza del quale l'attività di controllo risulta possibile previa valutazione degli interessi contrapposti e, comunque, cercando di preservare le libertà fondamentali degli interessati.

Sempre con riferimento ai controlli difensivi occulti, una pronuncia della Corte di Cassazione n.10955/2015 si è occupata del caso di un datore di lavoro, resosi protagonista della creazione di un falso profilo sulla piattaforma social *Facebook*, allo scopo di verificare gli accesi del dipendente in orario di lavoro e la relativa condotta illecita[9]. Più dettagliatamente, la Suprema Corte nel rilevare che "*la creazione del falso profilo facebook non costituisce, di per sé, violazione dei principi di buona fede e correttezza nell'esecuzione del rapporto di lavoro, attenendo ad una mera modalità di accertamento dell'illecito commesso dal lavoratore, non invasiva né induttiva all'infrazione, avendo funzionato come mera occasione o sollecitazione cui il lavoratore ha prontamente e consapevolmente aderito*", ha sancito che l'indagine svolta con l'attivazione di un falso profilo non integrava l'attività di controllo datoriale (ex art. 4, comma 2 dello Statuto dei Lavoratori), riconoscendo la piena legittimità e utilizzabilità dei dati e delle informazioni raccolte, anche a fini disciplinari[10].

La Sezione Lavoro della Cassazione, con sentenza 23 febbraio 2012, n. 2722, ha poi stabilito un rilevante orientamento secondo il quale il generale divieto del controllo datoriale sulla posta elettronica e sulla navigazione in rete del lavoratore può essere attenuato, *ex post*, qualora risulti necessario assicurare l'avvio di una indagine retrospettiva utile ad individuare eventuali condotte illecite del lavoratore[11]. Il caso di specie riguarda il dipendente di un istituto di credito, destinatario di un provvedimento di licenziamento "*per giusta causa*", che, in forza della posizione ricoperta all'interno dell'Istituto, inviava, a terzi non autorizzati, comunicazioni riservate mediante l'utilizzo della posta elettronica aziendale anche al fine di consentire, agli stessi soggetti terzi, operazioni finanziare vantaggiose. Alla luce della situazione instauratasi, secondo la Corte di Cassazione il licenziamento del dipendente non configurerebbe un controllo a distanza del lavoratore e, quindi, una violazione dello Statuto dei Lavoratori, avendo, l'istituto di credito, subito un danno in termini di immagine, e più precisamente *"[…] entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale"* [12].

---

[9] Newsletter n. 437 del 26 gennaio 2018, relativa alla legittimità da parte del datore di lavoro del controllo sui telefoni aziendali dei dipendenti (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7570001#3).

[10] P. Tullini, M. Marazza, *Controlli a distanza e tutela dei dati del lavoratore*, Giappichelli Editore, 2017, pp.37-40.

[11] M. Talarico, *Art. 4, co. 3, L. n. 300/1970: sulle condizioni di utilizzabilità dei dati derivanti da impianti audiovisivi e strumenti di controllo, Personale e lav.*, 2016, n. 576, 14.

[12] A. Levi, *Il controllo informatico sull'attività del lavoratore*, Giappichelli, 2013.

Come riferito in precedenza, lo sviluppo delle nuove tecnologie ha condotto ad un cambiamento dell'organizzazione del lavoro, anche nella concezione del potere direttivo del datore[13]. Il momento di svolta è rappresentato dalla Legge del 10 dicembre 2014, n. 183, con cui è stata delegata al Governo l'attività di potenziamento delle opportunità di ingresso nel mondo lavoro per i cittadini in cerca di occupazione mediante la "*revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore*"[14]. Tale delega, attuata successivamente con il D. Lgs n. 151/2015, art. 23, ha riformato il testo dell'art. 4 dello Statuto dei Lavoratori, lì dove, sotto il profilo sostanziale, prevede una distinzione tra "*impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza*" (comma 1) e sugli "*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*" (comma 2)[15]. Per la prima classe, resta intatto l'obbligo della preventiva autorizzazione sindacale e amministrativa al fine di accertare il legittimo interesse del datore di lavoro all'installazione dei sistemi; per la seconda classe, invece, tale legittimazione viene meno per gli strumenti necessari all'assolvimento della prestazione, in dotazione al lavoratore, quali pc, telefoni cellulari e altri *devices*. La Circolare esplicativa n. 5/2018 diramata dall'Ispettorato Nazionale del Lavoro, condivisa con il Ministero del lavoro, specifica che le richieste di autorizzazione all'installazione di impianti audiovisivi devono, necessariamente, essere corredate da effettive esigenze di carattere organizzativo e produttivo, di sicurezza del lavoro e di tutela del patrimonio e che, successivamente, l'utilizzo dei predetti strumenti deve essere riservato alla specifica finalità che si intende perseguire. A tal fine, si riporta recente sentenza della Corte Suprema di Cassazione[16], lì dove viene ulteriormente rafforzata l'inibizione, secondo quanto previsto dall'art. 4, comma 1 dello Statuto dei Lavoratori e dagli artt. 114 e 171 del D.Lgs n.196/2003, modificato dal D.Lgs n. 101/2018, all'installazione degli strumenti di videosorveglianza a distanza in assenza delle intese con le rappresentanze dei lavoratori o della autorizzazione rilasciata dall'Ispettorato del Lavoro. Secondo la Corte, non rileva alcun effetto la comunicazione trasmessa dal datore all'Ispettorato del lavoro, nel giorno immediatamente successivo a quello in cui si verificava la presenza dell'impianto di videosorveglianza, con la quale, in forza dell'art. 50 del

[13] M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in Centre for the study of European Law "Massimo d'Antona", Working Papers, n. 300/2016.
[14] Il Garante per la protezione dei dati personali, Audizione sugli schemi di decreti legislativi attuativi del c.d. Jobs Act, presso la Commissione Lavoro della Camera dei Deputati (9 luglio 2015) e la Commissione Lavoro del Senato (14 luglio 2015).
[15] M.T. Salimbeni, *La riforma dell'art. 4 dello Statuto dei Lavoratori: l'ambigua risolutezza del legislatore*, Rivista di Diritto del lavoro, 2015, I, 589;
[16] Sentenza Cassazione n. 50919-19.

Codice penale, i lavoratori sollevavano il datore di lavoro dagli adempimenti richiamati dall'art. 4 dello Statuto. Il Collegio, non condividendo l'orientamento di altre autorevoli decisioni[17], ritiene che "*il consenso in qualsiasi forma prestato dai lavoratori non valga a scriminare la condotta del datore di lavoro che abbia installato i predetti impianti in violazione delle prescrizioni dettate dalla fattispecie incriminatrice*", dovendosi considerare tale manifestazione di volontà non pienamente libera in ragione del rapporto di squilibrio intercorrente tra datore e lavoratore, accogliendo, altresì, il sempre valido orientamento della Corte di Cassazione, Sezione Lavoro, del 16 settembre 1997, n. 9211, secondo cui l'installazione in azienda di impianti audiovisivi deve essere preceduta dall'accordo con le rappresentanze sindacali e la relativa violazione comporta le conseguenze previste dall'art. 28 dello Statuto dei Lavoratori[18].

Sempre l'art. 4 dello Statuto dei Lavoratori, al comma 3, sancisce la possibilità di utilizzare le informazioni raccolte, richiamate dai commi sopra rammentati, per gli scopi connessi al rapporto di lavoro. Tale disposizione è condizionata, però, al rispetto di due criteri, quali l'adeguata informazione al lavoratore in ordine alle modalità d'uso degli strumenti e dei possibili relativi controlli, e il rispetto di quanto disposto dal D.Lgs n. 196/2003, oggi da considerare come rimando al Regolamento UE 2016/679, al D. Lgs n.196/2003 con s.m.i e agli atti di indirizzo delle singole Autorità di controllo e del Comitato europeo per la protezione dei dati personali[19].

Come riferito in precedenza, l'art. 4, comma 3 dello Statuto dei Lavoratori sancisce che "*sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazioni dei controlli*" (oggi da leggere, pertanto, alla luce dei *cc.dd.* principi di trasparenza, di limitazione delle finalità e di minimizzazione, espressamente previsti dall'art. 5, paragrafo 1, lett. a) del Regolamento UE 2016/679), e lascia aperti margini di interpretazione in ordine ai limiti entro i quali il potere datoriale può essere esercitato sugli strumenti, sulla prestazione lavorativa e sul relativo utilizzo dei dati, anche di carattere sensibile, del lavoratore[20]. Risulta, pertanto, di tutta evidenza come

---

[17] Corte di Cassazione, Sezione III Penale, 11 giugno 2012, n. 22611. In tale decisione, la Cassazione rileva che "*la disposizione di cui all'art. 4 intende tutelare i lavoratori contro forme subdole di controllo della loro attività da parte del datore di lavoro e che tale rischio viene escluso in presenza di un consenso di organismi di categoria rappresentativi (RSU o commissione interna), a fortiori, tale consenso deve essere considerato validamente prestato quando promani proprio da tutti i* dipendenti".

[18] Il Giudice ribadisce come la condotta del datore di lavoro costituisca un comportamento antisindacale reprimibile con la speciale tutela approntata dall'art. 28 dello Statuto del Lavoratori. Tale disposizione è utile per evidenziare ancora una volta come l'assenso delle rappresentanze sindacali è previsto per legge come uno dei momenti essenziali dell'intera procedura volta all'installazione degli impianti, derivando da ciò l'inderogabilità e la tassatività sia dei soggetti legittimati che della procedura autorizzativa di cui all'art. 4 dello Statuto dei Lavoratori.

[19] In ultimo, *Guidelines 3/2019 on processing of personal data through video devices*, diramate il 22 gennaio 2020 dall'European Data Protection Board.

[20] Il Garante per la protezione dei dati personali nelle *Linee guida per posta elettronica e internet*, punto 3.1., rilevava come "*Grava quindi sul datore di lavoro l´onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali*

l'informazione fornita al lavoratore sia da calibrare in base al caso specifico, avendo comunque cura di specificare gli strumenti presenti in azienda, quelli utilizzati direttamente o indirettamente dal dipendente, le modalità con le quali è fatta salva la possibilità di utilizzare tali strumenti (anche per eventuali finalità personali) e in quale maniera potranno essere compiuti i richiamati controlli.
Con riferimento all'interpretazione delle disposizioni contenute nello Statuto dei Lavoratori e delle relative decisioni assunte dai Giudici nazionali, risulta opportuno soffermarsi sulla sentenza della Sezione Lavoro del Tribunale di Torino, n. 1664, pronunciata in data 18 settembre 2018[21], secondo cui il mancato rispetto delle condizioni di legittimità previste dallo Statuto conducono all'inutilizzabilità del dei dati acquisiti e alla conseguente illegittimità del licenziamento. Il Giudice, nel caso di specie, è chiamato ad esprimersi in merito all'adozione di un provvedimento di licenziamento nei confronti di un lavoratore resosi protagonista, in seguito a controlli disposti dal datore di lavoro sul personal computer aziendale, di consultazione, per fini personali, di pagine web aventi ad oggetto contenuti legati al mondo della borsa e della finanza e, quindi, per finalità slegate dalla prestazione lavorativa[22]. Il Tribunale interessato, nella formulazione delle motivazioni prodotte, rileva che il personal computer aziendale, da intendersi quale strumento di lavoro, è dispositivo utile a configurare un'attività di controllo a distanza sulla prestazione del lavoratore e che, più specificamente, il *proxy* di navigazione è mezzo attraverso il quale operare un controllo diretto e, quindi, riconducibile direttamente all'art. 4, comma 1 dello Statuto dei Lavoratori[23]. Ulteriore elementi ravvisati dal Giudice del Lavoro riguardano, rispettivamente, l'inidonea informativa fornita al lavoratore circa le modalità di controllo datoriali preclude l'utilizzo delle informazioni raccolte attraverso gli strumenti di lavoro affidati al dipendente, anche di quelle raccolte

---

siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali. Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative".

[21] R. Del Punta, La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d. lgs. 151/2015) in Riv. It. Dir. Lav. 2016, I, 99); A. Ingrao, Il controllo disciplinare e la privacy del lavoratore dopo il Jobs act in Riv. It. Dir. Lav. 2017, I, 46; Tribunale di Roma 13.6.2018 n. 57668 in Wikilabour.it; Tribunale di Torino 19.9.2018 n. 1664 in Il Giustavorista.it, 2018;; in senso contrario Tribunale di Roma 24.3.2017 in Bollettino Adapt, Home, Mercato del Lavoro; Tribunale di Padova, ordinanza 19.1.2018, in Il Caso.it, sez. Giurisprudenza, 19948, pubb. 14/6/2018.

[22] G. Proia, *Trattamento dei dati personali, rapporto di lavoro e l'impatto della nuova disciplina dei controlli a distanza*, in Riv. It.Dir. Lav., fasc. 4, 2016, pag. 547.

[23] Rivista telematica del diritto del lavoro. Anche per i cd. controlli difensivi trovano applicazione le garanzie dell'art. 4, c. 2, St. lav.; ne consegue che se, per l'esigenza di evitare attività illecite, il datore di lavoro installa senza autorizzazione impianti e apparecchi di controllo che rilevino anche dati relativi alla attività lavorativa dei dipendenti, tali dati non possono formare oggetto di prova. (Cass. 24/5/2017, n. 13019, Pres. Napoletano Est. De Marinis, in Riv. Giur. Lav. prev. soc. 2017, con nota di M. E. Sauro, "I controlli difensivi e l'(in)utilizzabilità della prova", 588).

mediante l'impiego di strumenti tecnologici, come il proxy di navigazione[24], e comporta, poi, l'esclusione, dai predetti obblighi informativi, del Modello di Organizzazione e Gestione, adottato in ottemperanza al D. Lgs n. 231/2001[25]. Secondo l'orientamento del Giudice, dunque, il predetto Modello non riveste alcuna finalità informativa, così come intesa dall'art. 4, comma 3 dello Statuto dei Lavoratori, bensì, risulta essere prova utile all'implementazione di un sistema di prevenzione, il cui scopo è quello di sensibilizzare il personale in ordine al rischio di incorrere in sanzioni anche in capo all'azienda presso cui la prestazione lavorativa viene resa[26].
Tenendo fermi gli obblighi informativi, anche il Garante per la protezione dei dati personali, con Provvedimento dell'8 marzo 2018, ha raccolto una segnalazione pervenuta da un'organizzazione sindacale e da alcuni operatori di una Società, con la quale si lamentava una potenziale lesione dei diritti tutelati dalla disciplina in materia di protezione dei dati personali in seguito all'installazione di un nuovo gestionale. I segnalanti, nel dettaglio, rilevavano che il sistema era stato introdotto dalla Società con avvisi, mediante *pop up*, visualizzabili al momento dell'accesso all'applicativo ormai in disuso, in assenza di idonei elementi informativi previsti dalla normativa privacy e senza ulteriore chiarimento del datore di lavoro, il quale disattendeva la richiesta di incontro urgente avanzata dall'organizzazione sindacale. Alla luce della documentazione rilevata in sede istruttoria dall'Autorità di controllo nazionale, si evidenziava che il sistema di *Customer Relationship Management* (CRM) permetteva di ricostruire, anche indirettamente, la prestazione lavorativa di centinaia di lavoratori, di raccogliere informazioni personali della clientela e degli operatori addetti al servizio di call center (codice operatore, il tipo di operazione svolta, la durata della chiamata, data e orario di termine della chiamata), configurando, potenzialmente, controllo indiretto all'attività lavorativa degli interessati[27]. Agli stessi

[24] P. LAMBERTUCCI, *I poteri del datore di lavoro nello Statuto dei lavoratori dopo l'attuazione del c.d. jobs act del 2015: primi spunti di riflessione*, ADL, 2016, 514.
[25] T. E. Romolotti, *Cybersecurity: un ponte tra GDPR e d.lgs. 231/2001 alla luce del d.lgs. 101/2018*, Rivista 231, numero 2 – 2019.
[26] A. Jannone e I. Ciarletta Guzzo, *231: gestione "post evento e controlli sui dipendenti – Limiti e utilizzabilità a fini probatori*, *Resp. amm. società e enti*, 2015, n. 3, 245.
[27] Nel Provvedimento del Garante per la protezione dei dati personali, con riferimento all'informativa relativa al trattamento dei dati personali stabilisce "*A tal proposito, si osserva che il documento denominato "Informativa ai dipendenti di Sky Italia Network Service S.r.l. ai sensi dell´art. 4, comma 3 l. 20/5/1970 n. 300 (cfr. p. 7 all. n. 4 verbale 21.06.2017, cit.) si compone di due parti. La prima contiene le istruzioni e le modalità d´uso del sistema di gestione che viene qualificato "strumento per rendere la prestazione lavorativa" nella quale vengono sinteticamente indicate le principali caratteristiche nell´interfaccia con il cliente, per semplificare la relazione tra il chiamante e l´operatore e gestire più efficacemente i rapporti contrattuali in essere; in tale sezione del documento, tuttavia, non si menzionano le funzionalità del sistema "lato operatore" e le specifiche operazioni di trattamento che riguardano, come invece verificato nel corso degli accertamenti, i dati personali riferiti agli operatori addetti al call center. Nella seconda parte del documento la società rende note ai dipendenti le specifiche attività di controllo che si riserva di effettuare sulla loro attività, prefigurandone modalità e procedure in vista del successivo utilizzo dei dati raccolti mediante il sistema "per tutte le finalità connesse al rapporto di lavoro" ai sensi e per gli effetti dell´art. 4, comma 3 della legge n. 300/1970 (es: "estrazione di dati attraverso le funzioni di interrogazione del Sistema"; "raccolta, analisi ed elaborazione dei dati relativi all´attività di gestione degli abbonati e verifica*

dipendenti, dedicati alla gestione delle richieste dei clienti, inoltre, sulla base degli elementi istruttori forniti dalla Società al Garante, non risultava presentata alcuna informativa privacy circa le modalità di raccolta, le finalità di trattamento e ogni ulteriore cenno a quanto espressamente previsto dalla normativa in materia di protezione dati personali. Il sistema in esame, pertanto, risulta essere annoverato tra gli strumenti utili a soddisfare esigenze organizzative e produttive del datore di lavoro dai quali, inevitabilmente, può derivare il controllo a distanza dei lavoratori. Alla luce di quanto sin qui espresso, la Società avrebbe dovuto adottare idonee misure previste dallo Statuto dei lavoratori, quali l'accordo sindacale o, in assenza, l'autorizzazione amministrativa delle Direzioni territoriali del lavoro[28], configurando così, secondo quanto riscontrato dall'Autorità di controllo, violazione della disciplina lavoristica nazionale e, contestualmente, della normativa a tutela della riservatezza, dell'identità personale e della protezione dei dati personali[29].
Ne deriva che l'introduzione della tecnologia all'interno degli ambienti di lavoro deve necessariamente ispirarsi ai principi di privacy by design e by default che impongono al titolare del trattamento, fin dalla fase di progettazione, l'organizzazione di regole a tutela della protezione dei dati dei lavoratori nell'ambito dell'utilizzo della strumentazione aziendale e, conseguentemente, a mantenerle per tutto il ciclo di vita dei trattamenti[30]. La regolazione europea in materia di privacy, inoltre, chiama il datore di lavoro ad eseguire e attuare una valutazione d'impatto sulla protezione dei dati, vale a dire una valutazione documentata delle potenziali conseguenze pregiudizievoli per i diritti e le libertà fondamentali delle persone fisiche interessate dal trattamento[31].

2. Brevi cenni ai primi atti di indirizzo del Garante per la protezione dei dati personali

---

della correttezza delle stesse rispetto alle procedure stabilite in materia per le attività di retention, prevention, commerciale, extra, tecnica, back-office e teleselling ed agli standard qualitativi ed operativi previsti"; "raccolta analisi di ed elaborazione dei dati quantitativo relativi alle attività di gestione degli abbonati e confronto degli stessi con gli obiettivi di volume e con gli indici di performance periodica stabiliti a livello aziendale per le attività di retention…etc.."), così presupponendo la raccolta di informazioni riferibili agli operatori, senza tuttavia darne specifica evidenza".

[28] Si vedano, a tal riguardo, i Provvedimenti del Garante per la protezione dei dati personali, Provv. 1° febbraio 2018, n.53; Provvedimenti 19 marzo 2015, doc. web n. 4039439, 20 febbraio 2014, doc. web n. 3115239 e 4 giugno 2009, doc. web n. 1629029

[29] Newsletter 29/03/18 - *Customer care, no a software che controlla operatori - Lavoro: vietato controllo massivo* email, www.garanteprivacy.it.

[30] S. Wachter, B. Mittelstadt, *A Right to Reasonable inferences: Re-Thinking Data Protection Law in the Age of Big Data and A.I.*, in Columbia Business Law Review, 2019, n. 1, 1 ss.

[31] *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679* - WP248rev.01

Le Linee guida del Garante sull'utilizzo della posta elettronica e di internet del 2007[32], poi arricchite con il Vademecum *Privacy e Lavoro*[33], si sono rese necessarie a seguito di numerosi reclami, segnalazioni e quesiti pervenuti all'attenzione del Garante per la protezione dei dati nel corso degli anni, dai quali risultava l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie e opportune, per conformare, alle disposizioni vigenti, il trattamento di dati personali effettuato al fine di verificare il corretto utilizzo, nell'ambito del rapporto di lavoro, dei devices informatici affidati, del servizio di posta elettronica e della rete Internet. Proprio la navigazione in rete da parte dei lavoratori può, infatti, costituire oggetto di analisi, di profilazione e di integrale ricostruzione delle attività mediante l'elaborazione di file log della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni; allo stesso modo, i servizi di posta elettronica, parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di verifiche, possono consentire al datore di lavoro di condurre un controllo del contenuto della corrispondenza elettronica, fattispecie ancor più rilevante quando le informazioni in oggetto toccano, oltre a quella lavorativa, la sfera personale e la vita privata di lavoratori e di soggetti terzi[34]. Nell'ambito delle predette Linee guida, il Garante, muovendo i passi dalle disposizioni contenute nella vecchia formulazione del D.lgs n.196/2003, oggi da intendere come rimando al Regolamento UE 2016/679 e al D.Lgs n. 196/2003 e s.m.i., indica i dettami fondamentali cui i titolari del trattamento devono attenersi nelle operazioni di trattamento: il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l´utilizzazione di dati personali e identificativi e sempre in relazione alle finalità perseguite, il principio di correttezza, sulla base del quale le caratteristiche essenziali dei trattamenti devono essere analiticamente rese note ai lavoratori, in virtù anche del fatto che lo sviluppo delle tecnologie dell´informazione permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all´attività lavorativa[35]. Tale situazione può verificarsi in assenza di una adeguata consapevolezza dei lavoratori, in contrasto anche con il principio di trasparenza. Tenendo ferme le

[32] SI vedano, a tal riguardo, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico* e *Linee-guida per il trattamento di dati dei dipendenti privati*, www.garanteprivacy.it

[33] Garante per la protezione dei dati personali, *Privacy e Lavoro. Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati*, 2015, www.garanteprivacy.it.

[34] C. Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, Giornale di diritto del lavoro e di relazioni industriali, 155/2017, 445.

[35] Il Considerando n. 39 al Regolamento UE 2016/679 sancisce che "*qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*"

ulteriori raccomandazioni di massima fornite dall'Autorità, il trattamento di dati personali deve essere ispirato e concretizzato per finalità determinate, esplicite e legittime, in piena adesione al principio di pertinenza e non eccedenza, motivo per cui al datore di lavoro è demandato il compito di trattare informazioni personali "*nella misura meno invasiva possibile*"[36] (oggi minimizzazione del dato). Il Garante, inoltre, ha specificato che nell'ambito dell'organizzazione lavorativa è opportuno adottare un disciplinare interno, redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna aziendale o mediante affissioni sui luoghi di lavoro) e da sottoporre ad aggiornamento periodico; a tale documento è affidato il compito di riportare, in maniera puntuale, quali condotte siano contemplate rispetto alla navigazione in Internet (ad es., il download di software o di file musicali), l'eventuale tenuta di file nella rete interna, quali informazioni risultino memorizzate temporaneamente (ad esempio, le componenti di file di log eventualmente registrati), i soggetti (risiedenti anche all´esterno dell'organizzazione) che possono accedere legittimamente, nonché quali informazioni sono eventualmente custodite, i relativi tempi di conservazione e l'eventualità che i dati risiedano in forma centralizzata o decentralizzata. Ancora, dovrebbe essere precisata la riserva, per il datore di lavoro, di eseguire controlli in conformità alla legge, periodici o occasionali, indicando, all'uopo, gli interessi legittimi per i quali verrebbero effettuati, le relative modalità e le conseguenze, sotto il profilo disciplinare, in caso di utilizzo indebito dei predetti strumenti da parte del lavoratore[37]. Ulteriore casistica specificamente rilevata dal Garante per la protezione dei dati personali riconduce alla fattispecie per la quale al datore, al fine di garantire la continuità dell'attività lavorativa in caso di assenza del lavoratore (anche ripetuta nel tempo, come nel caso di permessi consentiti dalla legge), spetta l'ulteriore compito di concordare forme di cooperazione con gli interessati, in un'ottica di bilanciamento tra l'esigenza di garantire la regolare prosecuzione dell'attività lavorativa (e produttiva) e la tutela della sfera di riservatezza del lavoratore. Con specifico riferimento al principio della trasparenza, altresì previsto dall'art. 5, par. 1 del Regolamento UE 2016/679, l'Autorità di controllo rileva che il datore di lavoro, al fine di coniugare esigenze organizzative, produttive e di sicurezza, deve informare preventivamente, e in modo chiaro, gli interessati rispetto a potenziali controlli cui possono essere sottoposti, sulle finalità per le quali il trattamento di dati personali si

[36] Linee guida del Garante per posta elettronica e internet, Gazzetta Ufficiale n. 58 del 10 marzo 2007, *2.3. Principi del Codice, c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere "mirate sull´area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, cit., punti 5 e 12).*

[37] F. Ciccotti, *Diritto di accesso del lavoratore di lavoro e diritto alla riservatezza del lavoratore,* Diritto del Lavoro, Vol. 69, Fasc. 2, 1995.

rende necessario e sulla possibilità di esercitare i diritti degli interessati, previsti dalla normativa rilevante in materia di protezione dei dati personali. La nota informativa, pertanto, deve avere cura di specificare la tipologia degli strumenti presenti in azienda, l'utilizzo, diretto o indiretto, degli stessi da parte del lavoratore, dai quali possa derivare attività di controllo a distanza dell'attività lavorativa, le modalità attraverso le quali risulti possibile l'impiego di dispositivi forniti dal datore di lavoro anche, eventualmente, per scopi personali. Con riguardo, invece, alle apparecchiature preordinate al controllo a distanza, il Garante afferma, in ossequio ai principi sanciti dagli artt. 2086, 2087 e 2104 del codice civile, che il datore di lavoro può riservarsi il diritto di verificare (direttamente o attraverso la propria struttura) l´effettivo adempimento della prestazione lavorativa, il corretto utilizzo degli strumenti di lavoro e, che nell´esercizio di tale prerogativa, occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "*apparecchiature per finalità di controllo a distanza dell´attività dei lavoratori*" (art. 4, primo comma, L. n. 300/1970, poi modificato dal "Jobs Act"), tra cui sono certamente comprese componenti hardware e software mirate al controllo dell´utente di un sistema di comunicazione elettronica. In aderenza con quanto oggi stabilito dall'art. 5, par. 1, lett. c) del Regolamento UE 2016/679, l'Autorità di controllo afferma che il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all´adozione di misure "repressive") e, comunque, a "minimizzare" l´uso di dati riferibili ai lavoratori. Dal punto di vista organizzativo, invero, il Garante impone di valutare prudentemente l´impatto sui diritti dei lavoratori, prima dell´installazione di apparecchiature che consentono il controllo a distanza, e, successivamente, di adottare tutte le misure tecnologiche volte a ridurre l´utilizzo di dati identificativi (c.d. *privacy enhancing technologies–PETs*)[38]. Nonostante tali prescrizioni, nuovi controlli delle attività dei lavoratori, e sempre più pervasivi, sono stati messi in atto dai datori di lavoro nel corso degli anni, chiamando, così, l'Autorità di controllo ad intervenire nuovamente, come nel caso del Provvedimento n. 547 del 22 dicembre 2016, per rimarcare l'assunto secondo il quale l'accesso in maniera indiscriminata, per lo più in assenza di una idonea informativa, alla posta elettronica o ai dati personali contenuti negli *smartphone* in dotazione al personale, configura un comportamento illecito[39]. Il provvedimento del Garante, emesso a seguito di un reclamo promosso da un dipendente che lamentava una presunta violazione della sfera personale derivante dalla illecita intrusione datoriale durante il transito di messaggi di posta elettronica e di conversazioni telefoniche, ha disposto l'illegittimità del comportamento di una Società multinazionale che si era resa

[38] Yu Pu, J., J. Grossklags, *Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy*, Volume 2016: Issue 2, pp. 61-81.
[39] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, RIDL, 1/2016.

protagonista del mantenimento dell'account di posta elettronica e della conservazione della predetta documentazione, anche a seguito della cessazione del rapporto di lavoro, per dieci anni, periodo nettamente superiore a quello consentito di sei mesi[40]. L'Autorità, pur riconoscendo il potere datoriale sul controllo della prestazione lavorativa e sull'utilizzo della strumentazione affidata agli interessati, ha stabilito che "*la raccolta sistematica delle comunicazioni elettroniche, la loro memorizzazione per un periodo di dieci anni e la possibilità di accedervi all'esito di una procedura, consente alla società di effettuare il controllo dell'attività dei dipendenti. Ciò risulta in contrasto con la disciplina di settore in materia di controlli a distanza. Tale disciplina, infatti, pure a seguito delle modifiche disposte con l'art. 23 del d.lgs. 14 settembre 2015 n. 151, non consente l'effettuazione di attività idonee a realizzare, anche indirettamente, il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore*". Altra casistica meritevole di opportuna menzione e affrontata dal Garante per la protezione dei dati personali nel Provvedimento del 13 luglio 2016, riguarda il trattamento illecito di un Ateneo sui dati personali del corpo amministrativo e docente di una Università italiana. Nel dettaglio, l'Autorità di controllo ha rilevato che "*verifiche indiscriminate sulla posta elettronica e sulla navigazione web del personale sono in contrasto con il Codice della Privacy e con lo Statuto dei Lavoratori*": l'infrastruttura dell'Ateneo consentiva, in assenza di idonea informativa, la raccolta e la conservazione di file di log relativi al traffico Internet, l'indirizzo IP, informazioni relative all'utilizzo della posta elettronica ed alle connessioni di rete di una serie di utenti, tra cui docenti, ricercatori, personale tecnico amministrativo, studenti, dottorandi, specializzandi, assegnisti di ricerca, professori a contratto e *visiting professor*. In particolare, il Garante per la protezione dei dati personali precisa che nella nozione di "strumenti di lavoro" di cui all'art. 4 dello Statuto dei Lavoratori, secondo comma, possono ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza[41]. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro", alla stregua della normativa sopra citata, il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui il collegamento ai siti internet, nel quale vengono ricompresi tutti i sistemi e le misure di sicurezza, quali sistemi di logging, di filtraggio anti-virus e di inibizione automatica della consultazione di alcuni contenuti. L'intervento del Garante non risolve tutte le questioni emerse, bensì occorrerà operare una valutazione, caso per caso, specificando che la "*stretta funzionalità*" di un software e di un applicativo rispetto alla

[40] Garante per la protezione dei dati personali, *Accesso alla posta elettronica dei dipendenti*, 22 dicembre 2016, Doc. web n. 5958296.
[41] L. Tebano, *Employees' Privacy and employers' control between the Italian legal systemandEuropean sources*, Labour & Law Issues, Vol. 3, no. 2, 2017, pp. 7-9.

prestazione lavorativa (anche in termini di sicurezza) non può prescindere da una verifica sulla specifica attività svolta dal lavoratore e del settore nel quale egli opera.
Prendendo sempre come riferimento gli aspetti legati al potenziale controllo datoriale sul lavoratore, la posizione del Garante per la protezione dei dati personali, a tal riguardo, si è ulteriormente rafforzata con il Provvedimento generale in materia di videosorveglianza[42], lì dove sono disposte ulteriori specificazioni in ordine al trattamento di dati personali mediante sistemi di rilevazione delle immagini[43] e che, in base a quanto disposto dall'art. 22, comma 4, del D.Lgs n. 101/2018, continuano a produrre effetti, compatibilmente con le disposizioni vigenti in materia[44]. L'Autorità di controllo, nel ribadire che le attività di raccolta, registrazione, consultazione e conservazione configurano un trattamento di dati personali, sottolinea, così come ribadito anche dall'*European Data Protection Board* nelle Linee guida in tema di videosorveglianza ("*Video surveillance measured should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of data subject*"), che il ricorso a tali sistemi deve essere consentito qualora, successivamente ad un bilanciamento di interessi, si ravvisi l'impossibilità di utilizzare sistemi meno invasivi per il raggiungimento dello scopo prefissato. Se ne desume che le operazioni di trattamento, considerate alla luce delle condizioni di liceità previste dagli artt. 6 e 9 del Regolamento UE 2016/679, e dal Provvedimento del Garante n. 146/2019, debbano essere ispirate ai principi fondamentali in materia, oggi richiamati dall'art. 5 della stessa normativa europea, ed essere garantiti da adeguate misure di sicurezza utili a garantire la riservatezza, l'integrità, la disponibilità dei dati e la resilienza dei sistemi, con il precipuo scopo di mitigare i rischi per i diritti e le libertà fondamentali degli interessati[45]. Con riferimento agli aspetti di sicurezza, in ottica di *privacy* e *security by design*, l'Autorità di controllo prima, il *Board* Europeo poi, evidenziano la necessità dell'adozione di misure tecniche ed organizzative affinché, in adesione all'art. 32 del *GDPR*, il trattamento risulti sicuro, onde prevenire potenziali episodi di perdita o manipolazione dei dati (c.d. *data breach*). Il citato Provvedimento dispone, dunque, che l´attività di videosorveglianza debba essere effettuata nel rispetto del principio di proporzionalità, nella scelta delle modalità di ripresa e dislocazione (es. tramite

[42] F. Sarzana, S. Ippolito, *La nuova videosorveglianza per gli enti locali, le imprese e i privati*, Maggioli Editore, 2010, pp. 102-105.
[43] Il Provvedimento generale del Garante per la protezione dei dati personali in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680) sostituisce il precedente Provvedimento emanato dalla stessa Autorità di controllo in data 29 aprile 2004 (doc. web n. 1003482).
[44] Art. 22, comma 4 del D.Lgs n.101/2018, "*A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto*".
[45] I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto di lavoratori e quelle del Codice della privacy*, Labour & Law Issues, 2016, No. 1, p. 30.

telecamere fisse o brandeggiabili, dotate o meno di zoom) e della limitazione delle finalità perseguite dal titolare del trattamento. Gli ulteriori principali adempimenti prescritti dal Provvedimento del Garante e dalle disposizioni del Comitato europeo per la protezione dei dati personali, richiedono l'implementazione di un modello organizzativo, l'individuazione di compiti e di responsabilità in ambito privacy (anche per i soggetti esterni al contesto lavorativo), il rispetto del principio di trasparenza e degli obblighi di informazione, mediante anche informative brevi,[46] una attenta analisi in ordine alla *data rentention*, in forza della quale i dati personali trattati con l'ausilio di *video surveillance system* devono essere conservati per il tempo strettamente necessario (stabilito finanche dagli Stati membri) rispetto alle finalità per le quali vengono raccolti, e l'adozione di un sistema utile per consentire l'esercizio dei diritti degli interessati. Quanto al rapporto di lavoro, anche nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell´attività lavorativa, pertanto è vietata l´installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l´osservanza dei doveri di diligenza stabiliti per il rispetto dell´orario di lavoro e la correttezza nell´esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge). Risulta necessario, in ambito lavorativo, operare una valutazione in ordine all'effettiva necessità di implementare un sistema di videosorveglianza che, in ogni caso, dovrà tenere in considerazione le indicazioni contenute nell'art. 4 dello Statuto dei Lavoratori.

3. I recenti orientamenti delle Corti europee tra riconoscimento del diritto alla riservatezza ed esercizio del potere datoriale

La Corte Europea dei Diritti dell'Uomo (CEDU) di recente è stata chiamata a pronunciarsi su potenziali violazioni dei diritti fondamentali dei lavoratori e sul difficile bilanciamento tra diritto alla riservatezza del lavoratore e potere di controllo del datore di lavoro, valutazione resa ancor più complicata dall'avvento delle nuove tecnologie[47]. Con sentenza depositata il 5 settembre 2017, la Grande Camera della

[46] Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, *https://www.garanteprivacy.it/Regolamentoue/diritti-degli-interessati*

[47] SI riportano, per gli aspetti legati alla protezione dei dati personali, i Considerando 6 e 7 al Regolamento UE 2016/679 che meglio illustrano la rilevanza e la portata del progresso tecnologico della Società. (6) "*La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*". (7) "*Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le*

CEDU si è pronunciata nel caso *Bărbulescu v. Romania*. L'origine della controversia risiede nelle domande inoltrate da Bogdan Mihai Bărbulescu, *sales engineer* di una Società privata di Bucarest, licenziato per motivi disciplinari a causa dell'utilizzo, per scopi personali e durante l'orario di lavoro, dell'account di messaggeria istantanea fornito dal software *Yahoo! Messenger*, originariamente creato con il precipuo scopo di assistere i clienti nelle loro diverse richieste formulate. Tale fattispecie si inseriva in un quadro di consapevolezza del lavoratore, il quale veniva informato in merito alle disposizioni contenute nel regolamento aziendale interno della Società che, per l'appunto, vietavano l'uso, per scopi personali, di risorse dell'impresa, ma, allo stesso tempo, non contemplavano la facoltà datoriale di effettuare controlli o monitorare la corrispondenza dei propri lavoratori, elemento che induceva il lavoratore a convenire in giudizio il datore di lavoro presso le Corti nazionali, lamentando la violazione del diritto alla riservatezza della corrispondenza, espressamente tutelato dall'art. 8 CEDU[48]. Il Giudice nazionale, sia in primo grado che in appello, riconosceva la legittimità del licenziamento, affermando che il software era stato messo a disposizione esclusivamente per ragioni lavorative, non rilevando alcuna violazione della sfera della riservatezza del lavoratore, il quale, avverso tali decisioni, adiva la Corte Europea dei Diritti dell'Uomo. In questa sede veniva confermato l'orientamento dei Giudici nazionali e si ribadiva la legittimità dell'attività di controllo svolta dal datore di lavoro, aderente, altresì, alle disposizioni normative in materia di protezione dei dati personali e all'art. 8 CEDU[49]. La *Grande Chambre* sovvertiva le precedenti decisioni, facendo leva su elementi normativi essenziali, quali la Risoluzione 45/95 delle Nazioni Unite, la Convezione di Strasburgo del 1981[50] e il Regolamento generale sulla protezione dei dati personali UE 2016/679[51]. Più nello specifico, la Grande Camera, nell'attività di ricostruzione dei fatti, si soffermava sull'effettivo riconoscimento del diritto alla riservatezza degli individui, prendendo come riferimento analoga autorevole decisione[52] e sostenendo che al lavoratore debba vedersi riconosciuto il diritto alla privacy. Nel caso in cui la sfera privata

persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche".

[48] F. Tumiello, *Privacy sul posto di lavoro: la Corte EDU fa marcia indietro*, Ius in Itinere – Rivista semestrale di Diritto, ISSN 2611-3202.

[49] Corte EDU, Bărbulescu c. Romania, ricorso n. 614960/08, sentenza 12 gennaio 2016 (Quarta sezione).

[50] Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, Strasburgo, 28 gennaio 1981.

[51] Si fa riferimento al Gruppo di Lavoro art. 29 e alla Corte EDU, Bărbulescu c. Romania, Quarta sezione, cit., §47, "*il semplice fatto che un'attività di controllo e sorveglianza sia funzionale agli interessi del datore di lavoro non può giustificare di per sé qualsiasi intrusione nella privacy del dipendente e che qualsiasi misura di controllo deve soddisfare quattro criteri: trasparenza, necessità, lealtà e proporzionalità*"

[52] F. Perrone, *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Bărbulescu 2*, (Köpke c. Germania, ricorso n. 420/07), Labour-Il Lavoro nel diritto, Pacini Giuridica, Diritto del lavoro comparato, internazionale e dell'Unione Europea, 2018.

debba essere soggetta a limitazione, agli interessati deve essere garantita informazione, adeguata e puntuale, sulle potenziali attività di controllo e monitoraggio[53]. Risulta di tutta evidenza come la *Grande Chambre* ravvisi una violazione dell'art. 8 CEDU, invitando le Corti nazionali al rispetto di specifici criteri[54], che riprendono anche i principi previsti dall'art. 5 del Regolamento UE 2016/679, utili a determinare la legittimità del controllo datoriale, quali l'informazione preventiva al dipendente sulla portata, la proporzionalità, la durata e le conseguenze del controllo, i soggetti che possono accedere a tali informazioni, la base giuridica utile a legittimare l'attività da parte del datore, la ponderazione, in alternativa, di strumenti meno invasivi rispetto a quelli attuati e le garanzie adottate a tutela dei diritti degli interessati[55].

Prendendo in esame altra decisione, nel caso Antovič e Mirkovič v. Montenegro, la Corte di Strasburgo, Sezione II, è chiamata ad esprimersi su una potenziale violazione della privacy dei lavoratori a seguito del controllo effettuato dal datore di lavoro mediante l'utilizzo di sistemi di videosorveglianza. Più precisamente, il Preside della facoltà della School of Mathematics dell'Università del Montenegro, previa comunicazione nel Consiglio Universitario, autorizzava l'installazione di un sistema di videosorveglianza nell'Ateneo al fine di perseguire esigenze legate alla sicurezza e alla protezione delle aree universitarie. Sulla base delle misure poste in essere dalla Scuola, i professori Antovič e Mirkovič, ritenendo lesiva dei diritti fondamentali, dei docenti e degli studenti, il sistema di riprese installato all'interno delle aule didattiche, la cui sicurezza era già garantita da misure di controllo degli accessi fisici, quale la chiusura a chiave degli Uffici, segnalavano tale situazione al Garante nazionale per la protezione dei dati personali (*Personal Data Protection Agency)*, eccependo la legittimità delle riprese. La decisione di sfavore dell'Autorità di controllo, induceva i ricorrenti a presentare ricorsi all'*Agency's Council*, confutando le indagini sin lì svolte e sostenendo, altresì, in un'ottica di minimizzazione delle misure potenzialmente lesive delle libertà, che solo la rilevazione delle immagini all'ingresso e all'uscita dei locali universitari risultava misura adeguata a garantire la sicurezza delle aree e, contestualmente, il rispetto della disciplina in materia di protezione dei dati personali. A seguito dell'accoglimento della decisione da parte del *Council* attraverso cui si imponeva all'Università la rimozione delle telecamere, Antovič e Mirkovič avviavano successivo contenzioso civile contro l'Università, l'Autorità di controllo in materia di protezione dei dati persona e lo Stato del

[53] F-46/09, V c. Parlamento europeo, 5 luglio 2011.

[54] Il Giudice Paulo Pinto de Albuquerque, in aperto contrasto con la decisione della Corte, IV Sezione, del 2016, afferma "*Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace*"

[55] A tal riguardo, G. Formici, *Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza"*, Osservatorio Costituzionale, Fascicolo 1/2018, 13 aprile 2018.

Montenegro, con lo scopo di vedere riconosciuto il danno subito in ordine al libero godimento della propria vita privata, promuovendo la causa, dopo il rigetto della Corte di Prima Istanza e della Alta Corte, dinanzi alla CEDU per violazione dell'art. 8 della Convenzione. Secondo la Corte, il fatto che queste attività siano state calate in un contesto lavorativo configurato come luogo pubblico[56] non contribuisce ad escludere l'applicabilità dell'art. 8 richiamato, bensì irrobustisce le ragioni dei due appellanti, nei termini in cui costituisce "*una considerevole ingerenza nella vita privata dei dipendenti*"[57].

La Corte EDU, muovendo dalle considerazioni prodotte dalla Grande Camera nel contezioso *Berbulescu*[58] e riconoscendo la violazione delle disposizioni contenute nel *Data Protection Act* montenegrino, evidenzia l'errata interpretazione avanzata dalle Corti nazionali nel riconoscimento della vita privata, desumibile dalla presenza di una normativa nazionale in materia di protezione dei dati personali[59] e dai criteri di legittimità tracciati dalla precedente pronuncia della Grande Camera (*Bărbulescu*).

In ultimo, la CEDU si è nuovamente pronunciata in merito ai sistemi di videosorveglianza installati sui luoghi di lavoro, per esaminare il ricorso di alcuni cassieri, impiegati presso una catena di supermercati spagnoli, destinatari di un provvedimento di licenziamento. Più nel dettaglio, il datore di lavoro, al fine di verificare discordanze tra giacenze di magazzino e ricavi conseguiti, predisponeva un sistema di videosorveglianza, collocato anche in prossimità dei varchi di entrata e uscita per i quali veniva fornita regolare informazione ai dipendenti e, in aggiunta, installava telecamere occulte, in posizione utile al controllo del personale dedicato alle operazioni di cassa, mediante le quali scopriva che cinque dipendenti si rendevano protagonisti di furto e sottrazione di denaro, anche in collaborazione tra loro.[60] I lavoratori, segnalando le modalità illecite di registrazione e l'assenza di una preventiva informazione agli interessati, ricorrevano alle Corti spagnole per lamentare la violazione dello *Estatuto dei Trabajadores* e del diritto alla privacy, altresì tutelato dall'impianto costituzionale spagnolo, vedendosi respinte, in entrambi i gradi di giudizio, le impugnative. Secondo l'orientamento della Alta Corte di Giustizia della Catalogna, infatti, pur ricorrendo i presupposti per l'irrogazione di una sanzione amministrativa in capo al datore di lavoro per omessa informazione,

---

[56] CGUE, C-342/12, *Worten – Equipamentos para o Lar SA c. Autoridade para as Condições de Trabalho (ACT)*, 30 maggio 2013, punto 19.

[57] Antovič e Mirkovič v. Montenegro, 28 novembre 2017, Sez. II, n. 70838/13, "*developing mutual relations and constructing their social identity*"

[58] A. Lombardi, *Il potere di controllo del datore di lavoro alla luce della giurisprudenza CEDU*, Ricerca del Dipartimento di Diritto Pubblico dell'Università di Perugia, 18 novembre 2017.

[59] Sezione 35 e 36 del *Personal Data Protection Act*. Nel caso di specie, l'Università non aveva considerato l'effettiva minaccia per beni e persone all'interno dei locali.

[60] *Telecamere sul luogo di lavoro: dichiarazione di Antonello Soro, Presidente del Garante per la privacy, su sentenza Corte di Strasburgo*, 2019, (*https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9164334*)

l'interferenza datoriale nella sfera di riservatezza dei lavoratori mediante videosorveglianza, anche se occulta, risultava giustificata, necessaria, proporzionata e, quindi, legittima. I successivi ricorsi in Cassazione e alla Corte Costituzionale venivano dichiarati, rispettivamente, irricevibili e inammissibili (quest'ultimo a causa della violazione degli artt. 18 e 24 della *Costituciòn*), inducendo i lavoratori ad adire la Corte di Strasburgo per violazione degli artt. 8 e 6 della Convenzione e, pertanto, ad una valutazione in ordine al corretto bilanciamento, tra i diritti contrapposti, operato dal giudice nazionale[61].

Proprio la Corte di Strasburgo, attraverso la decisione della Terza sezione, richiama la legislazione nazionale sul tema e accerta la violazione dell'art. 8 CEDU, rilevando, pertanto, la durata prolungata delle riprese video e le connesse potenzialità di controllo generalizzato per tutti i dipendenti, contestando la proporzionalità della misura e asserendo 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. Essa comporta una documentazione riproducibile della condotta di una persona sul suo posto di lavoro, che lui o lei, essendo obbligato a […] svolgere il lavoro in quel luogo, non può eludere*". [62]

A diverse conclusioni, tuttavia, è giunta la Grande Camera, lì dove prendendo spunto dai criteri stabiliti nel caso Bărbulescu, i Giudici non hanno evidenziato alcuna violazione del diritto al rispetto della vita privata di cui all'art. 8 CEDU, concludendo che l'intrusione nella sfera di riservatezza non sia stata caratterizzata da un "*livello elevato di serietà*" e che, in alternativa, una modalità di sorveglianza meno invasiva non sarebbe potuta essere adottata valutato che *"la fornitura di informazioni a qualsiasi membro del personale avrebbe potuto vanificare lo scopo della videosorveglianza, che era […] scoprire i responsabili dei furti, ma anche ottenere prove da utilizzare per i procedimenti disciplinari contro di loro*"[63]. Invero, le Corti nazionali avevano rimarcato come, alla luce dei furti subiti, il datore di lavoro avesse deciso di installare un sistema di sorveglianza occulta nelle sole aree in prossimità delle casse e, conseguentemente, quest'ultimo non avrebbe potuto informare preventivamente i suoi dipendenti o scegliere una modalità di controllo meno invasiva, tenuto conto, altresì, del fatto che le registrazioni erano state utilizzare solo per la stringente finalità di prova nel caso *de quo*.

La Corte, rimarcato il rispetto dell'art. 8 CEDU, considera la violazione da parte del datore in ordine al dovere di informazione sancito dalla Sezione 5 della Legge

[61] A. Ciriello, *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo*, Lavoro Diritti Europa, Rivista nuova di diritto del lavoro, no 3/2019.

[62] A livello nazionale si riportano le seguenti decisioni, Corte di Cassazione, Sez. L, sentenza n. 22313 del 3 novembre 2016; nello stesso senso, Corte di Cassazione, Sez. L, sentenza n. 22662 del 8 novembre 2016

[63] Corte EDU, López Ribalda e altri c. Spagna, ricorsi nn. 1874/12 e 8567/13, 17 ottobre 2019 (Grande Camera), §116.

spagnola sulla protezione dei dati personali, ma, sulla base dei criteri stabiliti nel caso Bărbulescu, tale fattispecie non svilisce la proporzionalità della misura, essendo stati rispettati gli ulteriori criteri enunciati nel caso di specie del *sales engineer* rumeno. La *Grande Chambre*, nonostante opinioni dissenzienti da parte di Giudici dello stesso Collegio giudicante[64], ha quindi deciso di imprimere maggiore rilievo alla misura di sorveglianza adottata piuttosto che operare una attenta analisi in ordine alla sua legittimità, portando alla considerazione che la possibilità di installare sistemi di sorveglianza occulti favorisce un clima che compromette, inevitabilmente, il rapporto tra datore e lavoratore.

[64] I tre giudici, Ganna Yudkivska, Yonko Grozev e Vincent A. De Gaetano, preoccupati dalla crescente ingerenza delle nuove tecnologie, hanno affermato che neanche l'esistenza del ragionevole sospetto di una grave condotta scorretta è sufficiente a giustificare l'impiego della videosorveglianza occulta sul posto di lavoro.