LaBoUR & Law Issues
Rights | Identity | Rules | Equality

L'instabile equilibrio tra controllori e controllati nello sguardo del Garante privacy

ANTONELLA FRAGASSI
Università degli Studi di Bari "Aldo Moro"

vol. 10, no. 1, 2024

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

L'instabile equilibrio tra controllori e controllati nello sguardo del Garante privacy

ANTONELLA FRAGASSI
Università degli Studi di Bari "Aldo Moro"
Dottoranda di ricerca in Diritto del Lavoro
antonella.fragassi@uniba.it

ABSTRACT

The increasing and pressing development of technology permeates every field of human activity and it is considered to have profoundly affected the labour market and workplace environment. A greater concern regarding workers' privacy and dignity has been generated by the increase of subtle and invasive controls by the employers.

This paper aims to investigate the defensive controls made by an employer to protect company assets analysing the decisions of the Italian Data Protection Authority. As a result, the principles that make these controls lawful as well as the strict bond between the privacy policy and the legislation of the Workers Statute emerge from the practical cases submitted to the Authority. Moreover, the examined cases demonstrate the unstable balance between the employer's needs and the protection of workers' rights.

Keywords: remote control; defensive controls; Italian Data Protection Authority; worker privacy; worker dignity.

https://doi.org/10.6092/issn.2421-2695/19916

L'instabile equilibrio tra controllori e controllati nello sguardo del Garante privacy

SOMMARIO: 1. Premessa. – 2. Il Garante per la protezione dei dati personali, normativa sulla privacy e disciplina lavoristica. – 3. La "giurisprudenza" del Garante della privacy sui cd. controlli difensivi. – 4. Posta elettronica e Internet. – 5. Videosorveglianza. – 6. Geolocalizzazione. – 7. Rilevazione biometrica. – 8. Conclusioni.

1. Premessa

La progressiva e incalzante invasione della tecnologia in tutte le aree dell'agire umano, e dunque anche nell'organizzazione del lavoro, ha reso sempre più forte l'esigenza di tutela della riservatezza e della dignità dei lavoratori. Le nuove tecnologie rappresentano una preziosa risorsa, ma al contempo, avendo determinato una «tecnicizzazione»([1]) del lavoro, amplificano le criticità legate al bilanciamento tra la riservatezza dei lavoratori e il potere di controllo del datore di lavoro. Di fatti, il conseguente mutamento dell'esercizio dei poteri datoriali, può costituire una pericolosa minaccia per i diritti fondamentali dei lavoratori a causa di controlli capillari, indiscriminati e delocalizzati([2]).

La Carta Costituzionale costituisce il primario fondamento normativo del diritto alla riservatezza del lavoratore, si pensi all'art. 41, secondo comma, che stabilisce che l'imprenditore-datore di lavoro non può esercitare la propria iniziativa economica in modo da ledere la sicurezza, la libertà e la dignità umana. È forte il rapporto che intercorre tra la libertà di impresa e la tutela del lavoratore così come emerge dal dettato normativo che «colloca la tutela della dignità e della libertà del lavoratore entro la stessa cornice normativa del riconoscimento costituzionale della libertà di impresa»([3]). Dunque, nel riconoscere la libertà di iniziativa economica, la Costituzione ne individua un preciso e invalicabile confine di legittimità.

Sulla base del fondamento costituzionale si innesta la disciplina dettata dallo Statuto dei lavoratori.

Il riferimento a tal proposito è all'art. 4, che nel disciplinare il potere di controllo a distanza esercitato dal datore di lavoro, si pone come strumento di garanzia della riservatezza del lavoratore.

([1]) A. Sitzia, *Lavoro e privacy: adempimenti obbligatori e procedure*, in *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, a cura di E. Barraco - A. Sitzia, Ipsoa, 2016, 112.

([2]) G. Ziccardi, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, *LLI*, 2016, vol. 2, n. 1, 48 ss.; sul tema si v. anche G. Fioriglio, *Intelligenza artificiale, privacy e rapporto di lavoro: una prospettiva informatico-giuridica*, *LDE*, 2022, n. 3, 2 ss. e V. Nuzzo, *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, 2018.

([3]) P. Chieco, *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*, Cacucci, 2000, 14.

Con la riforma dell'art. 4, operata dal legislatore del *Jobs Act*, tramite l'art. 23, comma 1, d.lgs. n. 151/2015(4) si è resa ancor più evidente l'interazione della disciplina statutaria con la disciplina in materia di privacy, essendovene l'esplicito riferimento al terzo comma della norma. Infatti, è l'integrazione tra le regole dettate dallo Statuto dei lavoratori e il complesso normativo in materia di protezione dei dati personali a rappresentare la regolazione del trattamento dei dati personali(5) nel rapporto di lavoro. Non ci si può esimere dal loro esame parallelo, poiché appare evidente che si tratti di «due centri gravitazionali che transitano uno nell'orbita dell'altro, in un rapporto quasi simbiotico e inscindibile senza, però, che il primo assorba totalmente il secondo o viceversa»(6).

La disciplina della privacy rappresenta un «quid pluris»(7), una maggiore tutela, in quanto prevede ulteriori garanzie rispetto allo Statuto dei lavoratori, infatti al suo rispetto è subordinata l'utilizzabilità(8) delle informazioni raccolte dal datore di lavoro(9).

Essa, nel meccanismo della nuova disposizione, rappresenta la fonte di difesa dell'interesse del lavoratore al rispetto della propria dignità, costituendo il limite agli antagonisti interessi del datore di lavoro: la tutela del patrimonio aziendale da un lato e la verifica al controllo del corretto adempimento della prestazione dall'altro.

2. Il Garante per la protezione dei dati personali, normativa sulla privacy e disciplina lavoristica

Nella declinazione del legame tra diritto del lavoro e disciplina sulla privacy è fondamentale il ruolo del Garante per la protezione dei dati personali, più comunemente noto come Garante della privacy (d'ora in poi Garante), che con il suo operato, "indica

(4) In attuazione della legge delega 10 dicembre 2014, n. 183, *Deleghe al Governo in materia di riforma degli ammortizzatori sociali, dei servizi per il lavoro e delle politiche attive, nonché in materia di riordino della disciplina dei rapporti di lavoro e dell'attività ispettiva e di tutela e conciliazione delle esigenze di cura, di vita e di lavoro*.

(5) Sul tema dei dati del lavoratore si v. P. Tullini, *Dati*, in *Lavoro digitale*, a cura di M. Novella - P. Tullini, Giappichelli, 2022, 105 ss.

(6) G. Busia, *Così vicini, così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente*, *LDE*, 2020, n. 3, 3.

(7) M. T. Salimbeni, *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, *RIDL*, 2015, I, 598.

(8) A tal proposito si v. M. Barbieri, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 183 ss.

(9) Era chiaro l'obiettivo della riforma così come si evince dalla nota del Ministero del Lavoro e delle Politiche Sociali del 18 giugno 2015: «Il nuovo articolo 4, peraltro, rafforza e tutela ancor meglio rispetto al passato la posizione del lavoratore, imponendo che al lavoratore venga data adeguata informazione circa l'esistenza e le modalità d'uso delle apparecchiature di controllo (anche quelle, dunque, installate con l'accordo sindacale o l'autorizzazione della DTL o del Ministero); e, per quanto più specificamente riguarda gli strumenti di lavoro, che venga data al lavoratore adeguata informazione circa le modalità di effettuazione dei controlli, che, comunque, non potranno mai avvenire in contrasto con quanto previsto dal Codice privacy».

la via" del corretto bilanciamento fra il diritto alla privacy e i poteri esercitabili dal datore di lavoro.

È un'autorità amministrativa indipendente istituita dalla l. n. 675/1996, la c.d. Legge sulla privacy, successivamente disciplinata dal d.lgs. n. 196/2003, il Codice in materia di protezione dei dati personali, così come modificato dal d.lgs. n. 101/2018.

I suoi molteplici compiti sono definiti dal Regolamento Ue 2016/679([10]) (d'ora in poi Gdpr, *General Data Protection Regulation*), dal Codice in materia di protezione dei dati personali e da atti normativi nazionali e internazionali.

È un'autorità designata al controllo della conformità dei trattamenti di dati personali a leggi e a regolamenti nazionali e al Gdpr, pocanzi menzionato, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche e di agevolare la libera circolazione dei dati personali all'interno dell'Unione([11]).

Infatti, a tal fine, prescrive ai titolari o responsabili dei trattamenti, se necessario, le misure da adottare (per realizzare il trattamento) ed eventualmente rivolge loro ammonimenti e ingiunge di conformare i trattamenti a quanto disposto dal *Gdpr*, potendo imporre limitazioni provvisorie o definitive, ordinando la rettifica o la cancellazione dei dati personali.

Può collaborare con altre autorità di controllo al fine di garantire l'attuazione coerente del Gdpr, esamina reclami, segnala alle istituzioni competenti la necessità di adottare atti normativi e amministrativi su questioni relative alla protezione dei dati personali, predispone una relazione annuale sull'attività svolta nel corso dell'anno da trasmettere al Parlamento e al Governo.

Incoraggia altresì l'elaborazione di codici di condotta, fornendo un parere su di essi e approvando quelli che offrono garanzie sufficienti e che contribuiscono alla corretta applicazione del Regolamento, a seconda delle peculiarità dei settori in cui avviene il trattamento e delle esigenze delle micro, piccole e medie imprese([12]).

Significativo a tal proposito, il Provvedimento dell'11 gennaio 2024([13]), tramite cui l'Autorità ha approvato il Codice di condotta per il settore delle Agenzie per il Lavoro, così come proposto da Assolavoro, l'Associazione Nazionale di Categoria delle Agenzie per il Lavoro, che risultava offrire in misura sufficiente, in seguito all'esame svolto dall'Autorità di controllo, garanzie adeguate a tutela degli interessati nel settore di riferimento. Con l'approvazione del Codice, il Garante ha anche disposto l'accreditamento del relativo Organismo di Monitoraggio([14]) che garantirà il rispetto

([10]) Sul punto C. Ogriseg, *Il regolamento Ue n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, *LLI*, 2016, vol. 2, n. 2, 29 ss.; A. Ingrao, *La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi*, in *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, a cura di A. Bellavista - R. Santucci, Giappichelli, 2022, 127 ss.

([11]) Si v. art. 51 del Reg. Ue. 2016/679.

([12]) Si v. artt. 57, lett. m e 40 del Reg. Ue 2016/679.

([13]) Garante della privacy, Provv. dell'11 gennaio 2024, doc. web. 9983415.

([14]) Si v. art. 41 del Reg. Ue 2016/679.

delle regole previste. È bene considerare che l'adesione ad un codice di condotta rappresenta, tra l'altro, un elemento di responsabilizzazione, di *accountability,* poiché consente di dimostrare la conformità al Regolamento dei trattamenti di dati posti in essere dai titolari o dai responsabili del trattamento che vi aderiscano.

L'Autorità coinvolge inoltre i cittadini e i soggetti interessati tramite consultazioni pubbliche di cui tiene conto al fine di adottare provvedimenti di carattere generale e ha cura di sviluppare la consapevolezza dei titolari del trattamento e del pubblico, rivolgendo un'attenzione particolare alla tutela dei minori([15]).

Il Garante, nell'espletamento dei suoi compiti, persegue un modello di comportamento improntato al rispetto dei «principi di lealtà, imparzialità, integrità, riservatezza e corretto adempimento dei doveri, nonché di prevenzione contro ogni forma di corruzione»([16]).

È fondamentale dunque il suo ruolo nel dare concreta attuazione ai principi enunciati dal Gdpr*,* il cui obiettivo principale è quello di rimediare alla frammentazione della protezione dei dati personali nel territorio dell'Unione europea determinata dalla compresenza di diversi livelli di protezione, che può rappresentare un ostacolo per la libera circolazione dei dati nell'ambito del territorio unionale([17]).

Il Gdpr, congiuntamente alla disciplina lavoristica statutaria, contribuisce alla regolazione del trattamento dei dati personali nel rapporto di lavoro. Significativo a tal proposito è l'art. 88, rubricato «Trattamento dei dati nell'ambito dei rapporti di lavoro». Esso fa salva la possibilità, per gli Stati membri, di prevedere tramite leggi o contratti collettivi, disposizioni che siano più favorevoli per i lavoratori, i cui dati personali siano oggetto di trattamento, in modo da garantire adeguata e piena tutela ai loro diritti e libertà, non gettando mai l'ombra sull'irrinunciabile diritto alla dignità umana([18]).

Il Regolamento, inoltre, enuncia una serie di requisiti che è doveroso rispettare nel caso di utilizzazione di tecnologie che compromettano la libertà e la privacy dei lavoratori([19]).

In *primis*, il trattamento dei dati deve essere conforme ai principi di liceità, correttezza, trasparenza([20]), deve rispettare il principio di «minimizzazione»([21]), per cui essi devono essere adeguati, pertinenti e proporzionati rispetto alle finalità perseguite.

([15]) Compiti del Garante, scheda di sintesi consultabile in https://garanteprivacy.it/home/autorita/compiti.

([16]) Codice etico del Garante consultabile in https://garanteprivacy.it/home/autorita/codice-etico.

([17]) Considerando n. 9 del Gdpr.

([18]) Sul punto si v. A. Sitzia, *Il decreto legislativo di attuazione del Regolamento Privacy (n. 101 del 2018): profili giuslavoristici*, *LDE*, 2018, n. 2, 3 ss.; e anche R. Fratini, *Privacy ed efficienza nel pubblico impiego*, *MGL*, 2021, n. 3, 607 ss.

([19]) Sul punto R. Fratini - R. Maurelli, *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e codice privacy*, *LPO*, 2020, 11-12, 714 ss.

([20]) V. art. 5 del *Gdpr*, par. 1, lett. a.

([21]) V. art. 5 del *Gdpr*, par. 1, lett. c.

Ulteriore requisito è la previa informativa, cioè dare «adeguata informazione ai lavoratori delle modalità d'uso degli strumenti e di effettuazione dei controlli» così come previsto dall'art. 13, Gdpr, ma anche dall'art. 4, terzo comma dello Statuto dei lavoratori.

Inoltre, è dovere del datore di lavoro, nel caso di controllo a distanza e laddove il trattamento possa determinare un rischio elevato per i diritti e le libertà del lavoratore, predisporre una valutazione d'impatto([22]) sulla protezione dei dati, cioè una descrizione dei trattamenti previsti, delle finalità perseguite, dei rischi e anche delle misure di sicurezza disposte([23]).

In vero, il Regolamento si fa portatore di due importanti principi: *privacy by design* e *privacy by default*, per cui il datore di lavoro, in quanto titolare del trattamento, deve sin dall'inizio, valutandone l'ambito applicativo e considerando le finalità e gli eventuali rischi, mettere in atto misure tecniche e organizzative volte a tutelare efficacemente i dati, in una logica preventiva([24]) e deve altresì mettere in atto misure tecniche e organizzative volte a garantire che oggetto del trattamento siano per impostazione predefinita unicamente i dati necessari per la finalità perseguita([25]).

In tal senso, il datore di lavoro «accountable»([26]) dovrà operare una scelta oculata sugli strumenti da utilizzare per il controllo, dovendo prevenire sin da subito il rischio di lesione dei diritti del lavoratore soggetto al controllo.

Tornando al ruolo del Garante, attraverso l'emanazione di provvedimenti e di Linee Guida esso ha la possibilità di fornire indicazioni per prevenire il rischio di utilizzi impropri e di ridurre l'impiego di dati riferibili ai lavoratori, valorizzando i principi di cui si è detto pocanzi, infatti la sua "giurisprudenza" è luogo di definizione di un possibile bilanciamento di interessi così come rappresentato dal nuovo art. 4([27]) dello Statuto.

Il suo contributo è fondamentale per l'armonizzazione tra la disciplina statutaria e la normativa in materia di privacy e per la costruzione di un efficace apparato di tutela della persona del lavoratore contro il dirompente potere di controllo esercitato dal datore di lavoro.

In molti dei suoi interventi e in particolare nelle Linee Guida, il Garante ha manifestato la consapevolezza che l'acquisizione e il trattamento dei dati personali dei lavoratori per il tramite di strumenti informatici, costituisce la maggiore minaccia per la

([22]) Garante della privacy, Provv. 11 ottobre 2018, Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679, doc. web. 9058979.

([23]) V. art. 35 del Gdpr.

([24]) V. art. 25, primo comma del Gdpr.

([25]) V. Art. 25, secondo comma del Gdpr.

([26]) A. Ingrao, *Controllo a distanza e privacy alla luce dei principi di finalità e proporzionalità della sorveglianza*, *LLI*, 2023, vol. 9, n. 1, 107.

([27]) M. T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro* in *Controlli a distanza e tutela dei dati personali del lavoratore*, *op. cit*., 59 s.

loro riservatezza. Per questo tra le più note e applicate prese di posizione del Garante, figurano le Linee Guida del 2007 per l'utilizzo di Internet e della posta elettronica([28]), che anche oggi costituiscono un importante punto di riferimento per tracciare i confini dell'esercizio del potere datoriale di controllo esercitabile tramite le strumentazioni informatiche, e anche il Provvedimento in materia di videosorveglianza emanato l'8 aprile del 2010, di cui si dirà più avanti.

Dunque, l'operato del Garante, attraverso la divulgazione di concrete istruzioni operative, contribuisce ad una maggiore interazione tra le norme statutarie e la disciplina generale sulla privacy, integrandone i rispettivi principi e rafforzando così il quadro regolativo.

3. La "giurisprudenza" del Garante della privacy sui c.d. controlli difensivi

Com'è noto il tema del potere di controllo a distanza esercitato dal datore di lavoro sulla condotta del lavoratore è stato oggetto di un denso dibattito in dottrina e in giurisprudenza, mai sopito, neppure con l'intervento del *Jobs Act*, che al contrario, ha alimentato gli interrogativi circa l'ammissibilità dei c.d. controlli difensivi del patrimonio aziendale e la loro conciliabilità con la disciplina dettata dallo Statuto([29]).

La categoria di controlli in esame è frutto di un'elaborazione giurisprudenziale durante la vigenza della norma statutaria, *ante* riforma del 2015, che descrive una particolare tipologia di controllo avente ad oggetto gli illeciti del lavoratore e che, essendo finalizzato alla tutela del patrimonio aziendale, si svolge in modo occulto([30]).

Ripercorrendo le tappe della produzione "giurisprudenziale" del Garante della privacy si evince chiaramente un disallineamento rispetto agli orientamenti della giurisprudenza di legittimità sul tema.

Il Garante, *ante* riforma del 2015, occupandosi del trattamento dei dati raccolti tramite l'utilizzo di strumenti elettronici, ha sempre insistito sull'illegittimità del

([28]) Sul tema *ex multis* M. Del Conte, *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, *Dir. Informatica*, 2007, fasc. 3, 497 ss.

([29]) P. Tullini, *I controlli aziendali per finalità difensive nella giurisprudenza*, *RIDL*, 2022, I, 222 ss., sul tema si v. anche M. Marazza, *I controlli a distanza del lavoratore di natura «difensiva»*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, *op. cit*., 27 ss.

([30]) Cass. 3 aprile 2002, n. 4746 inaugura i c.d. controlli difensivi. Nel caso di specie era emerso, per il tramite di un sistema di monitoraggio delle chiamate, che un lavoratore avesse effettuato da un telefono aziendale una telefonata di carattere strettamente personale. Oggetto del controllo una condotta illecita lesiva di beni estranei alla prestazione lavorativa e non l'adempimento corretto della prestazione lavorativa, per cui la procedura prevista dal secondo comma dell'art. 4 non risultava necessaria. La Suprema Corte affermava che «ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi)».

controllo a distanza attuato in violazione delle procedure previste dall'art. 4 dello Statuto dei lavoratori e dei principi dettati dalla normativa sulla privacy. Al contrario, la giurisprudenza legittimava ed esonerava dai limiti statutari i controlli difensivi, in quanto volti a tutelare il patrimonio aziendale e aventi ad oggetto gli illeciti compiuti dai lavoratori e non l'attività lavorativa. In realtà la dottrina non ha esitato a manifestare le sue perplessità sul punto, evidenziando l'«aporia logica di non poco momento»([31]), che affligge i controlli difensivi, che avrebbero inevitabilmente "colpito" l'attività svolta dal lavoratore e la loro legittimità si sarebbe rivelata solamente *ex post*, dopo il loro esercizio in concreto([32]).

Successivamente, il Garante, esprimendo la propria posizione sugli schemi dei decreti legislativi attuativi del *Jobs Act*, ha riconosciuto l'esigenza di «sincronizzazione»([33]) della norma rispetto alla realtà odierna, esigenza alla base della riforma e non è mancato il riferimento all'art. 4 come fondamentale "baluardo" della libertà del lavoratore rispetto al rischio di una sua totale espropriazione, in quanto parte debole del rapporto.

Nell'enunciazione e analisi dei profili innovativi della nuova versione della norma, vi è il riferimento all' «espressa legittimazione dei controlli c.d. difensivi, la cui disciplina è ricondotta alla procedura generale concertativo-autorizzativa»([34]), considerata l'introduzione della tutela del patrimonio aziendale tra i possibili oggetti del controllo.

La posizione del Garante appare chiara sul tema, a differenza di quanto sia invece accaduto in dottrina e in giurisprudenza in seguito alla riforma del 2015.

La dottrina si è divisa tra l'"assorbimento" dei controlli difensivi nel disposto dell'art. 4, in virtù dell'esplicito riferimento alla tutela del patrimonio aziendale nel nuovo

([31]) V. Pinto, *I controlli "difensivi" del datore di lavoro sulle attività informatiche e telematiche del lavoratore*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, *op. cit.*, 141.

([32]) M. Tufo, *Potere di controllo datoriale vs. privacy del lavoratore: alla ricerca delle coordinate di ammissibilità dei controlli occulti*, *Studium Iuris*, 2020, n. 7-8, 849, sul "paradosso" della legittimità *ex post* del controllo anche R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151 n. 151/2015), RIDL*, 2016, I, 85.

([33]) Audizione del Presidente del Garante della privacy Antonello Soro sugli schemi di decreti legislativi attuativi del c.d. Jobs Act 9 e 14 luglio 2015, doc. web. 4119045.

([34]) Audizione del Presidente del Garante della privacy, cit., par. 2, lett. b.

testo della norma([35]) e la «ridefinizione e sistematizzazione»([36]) dei controlli difensivi in modo da affermarne la sopravvivenza in deroga all'art. 4 dello Statuto.

La giurisprudenza di legittimità, malgrado le titubanze dottrinali, non sembrerebbe aver dubbi circa la sopravvivenza dei controlli difensivi, su cui si è espressa più volte anche con recentissime sentenze, facendo leva, da ultimo, sulla distinzione tra controlli in "senso lato" e controlli in "senso stretto"([37]). Concretamente pare tutt'altro che agevole definire l'esercizio del potere in senso stretto o ampio, per cui sembrerebbe meno tortuoso seguire il percorso tracciato dal Garante della privacy, che tende a ricondurre tutti gli strumenti di controllo nell'alveo dell'art. 4, sottoponendoli alla procedura codeterminativa e comprimendo così, significativamente, lo "spazio vitale" dei controlli difensivi.

Il rispetto della procedura di autorizzazione e di informazione prevista dalla norma, porrebbe il lavoratore nelle condizioni di conoscere effettivamente le modalità di effettuazione del controllo, delle finalità, dei tempi e sarebbe rigoroso il rispetto della normativa in materia di privacy, al fine di tutelare la sua riservatezza e dignità.

Peraltro, il Garante non si è sottratto dal rimarcare la stretta connessione tra la disciplina di settore (Statuto dei lavoratori) e la disciplina di protezione dei dati, con particolare riferimento all'art. 88 del Gdpr sostenendo che «il Codice» (della privacy) «confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro (artt. 113 "Raccolta dati e pertinenza" e 114 "Garanzie in

([35]) In questo senso *ex multis* P. Lambertucci, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act)*, Biblioteca "20 maggio", 1, 2015; I. Alvino, *dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, *LLI,* 2016, vol. 2, n. 1; R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151 n. 151/2015)*, *op. cit.*; M. Barbieri, *L'utilizzabilità delle informazioni raccolte,* cit.; G. A. Recchia, *Controlli datoriali difensivi: note su una categoria in via di estinzione*, *LG*, 2017, 348 ss.; A. Ingrao, *I controlli difensivi tra passato e presente: privacy del lavoratore e inutilizzabilità dei dati*, *NGCC*, 4, 2019, 652 ss.

([36]) A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. Lav.*, in *Controlli a distanza e tutela dei dati personali del lavorat*ore, *op. cit.*, 7.

([37]) Cass. 22 settembre 2021, n. 25732, Cass. 26 giugno 2023 n. 18168.

La categoria dei controlli in "senso lato", ascrivibile al regime di cui all'art. 4, ricomprenderebbe controlli volti alla «difesa del patrimonio aziendale, che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto di tale patrimonio»; la categoria dei controlli in "senso stretto" ricomprenderebbe invece i controlli «diretti ad accertare specificamente condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro» e come ritenuto dalla Corte, non avendo ad oggetto l'ordinaria attività svolta dal lavoratore esulano dall'applicazione del dettato normativo, sul punto *ex multis* si v. A. Tursi, *Note minime in tema di controlli difensivi del datore, onere della prova e utilizzabilità delle prove illecitamente acquisite nel processo*, *LLI*, 2023, vol. 9, n. 1, 85 ss.; C. Colapietro - A. Giubilei, *Controlli difensivi e tutela dei dati del lavoratore*, *LLI*, vol. 7, n. 2, 2021, 189 ss.; A. Riccobono, *Nuove tecnologie e controlli difensivi tra diritto positivo e creazionismo giudiziario*, *RIDL,* 2023, fasc. 4, 506 ss.

materia di controllo a distanza"). Per effetto di tale rinvio, e tenuto conto dell'art. 88, par. 2, del Regolamento, l'osservanza degli artt. 4 e 8 della l. 20 maggio 1970, n. 300 e dell'art. 10 del d.lgs. n. 297/2003 (nei casi in cui ne ricorrono i presupposti) costituisce una condizione di liceità del trattamento»([38]).

È stato il rispetto dei diritti, delle libertà e della dignità dei lavoratori ad aver ispirato le decisioni del Garante nel corso degli anni, anche quando, per l'inevitabile progresso tecnologico ha dovuto "scontrarsi" con dispositivi tecnologici dotati di configurazioni sempre più complesse, tali da porre nuovi problemi rispetto al passato([39]).

"Esplorando" la giurisprudenza del Garante in materia di controlli a distanza dei lavoratori, è possibile individuare quattro materie, nell'ambito delle quali è stata registrata la maggior parte delle segnalazioni: posta elettronica e Internet, videosorveglianza, geolocalizzazione e rilevazione biometrica.

4. Posta elettronica e Internet

Come già accennato, tra i più importanti punti di riferimento nella produzione "giurisprudenziale" del Garante della privacy, figurano le Linee Guida del 2007 per l'utilizzo di Internet e della posta elettronica, resesi necessarie a seguito di numerosi reclami e segnalazioni, da cui emergeva l'esigenza di prescrivere ai datori di lavoro alcune misure necessarie per adeguare alle disposizioni vigenti, il trattamento dei dati personali effettuato al fine di verificare il corretto utilizzo, nell'ambito del rapporto di lavoro, degli strumenti informatici affidati, del servizio di posta elettronica e della rete Internet([40]).

È possibile riconoscere valore vincolante alle indicazioni contenute nelle Linee guida e considerarle come "luogo" in cui è delineata la cornice nell'ambito della quale il datore di lavoro può muoversi per preservare il patrimonio aziendale, tutelando al contempo la riservatezza e la libertà dei dipendenti([41]).

([38]) Garante della privacy, Provv. 28 ottobre 2021, doc. web. 9722661, sul punto si v. A. Bellavista, *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, *LDE*, 2023, n. 1, 7.

([39]) Garante della privacy, Relazione annuale del 2020, 2 luglio 2021, doc. web. 9676435.

([40]) Sul punto *ex multis* F. Lorè, *La tutela della privacy nell'esercizio del potere datoriale*, *Amministrativamente*, 2020, n. 1, 43; E. Barraco, *Controlli tecnologici*, in *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, a cura di E. Barraco - A. Sitzia, Ipsoa, 2016, 20 ss.

([41]) V. Pinto, *I controlli "difensivi" del datore di lavoro sulle attività informatiche e telematiche del lavoratore, op. cit.*, 154, il quale ritiene che le Linee guida abbiano compiuto il bilanciamento della «libertà di iniziativa economica dei datori di lavoro e il loro diritto di utilizzare dispositivi di protezione dei sistemi informativi aziendali con la libera esplicazione della personalità del lavoratore sul luogo di lavoro e con la protezione della sua sfera di riservatezza nelle relazioni personali e professionali»; sulla natura delle Linee Guida e la loro vincolatività si v. P. Tullini, *Tecnologie informatiche in azienda: dalle linee-guida del Garante alle applicazioni concrete*, in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, a cura di P. Tullini, Cedam, 2010, 124; I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, *LLI,* 2016, vol. 2, n. 1, 31.

Il Garante, tramite esse, ha fornito concrete indicazioni sull'uso dei computer sul luogo di lavoro, ravvisando nell'utilizzo di Internet e della posta elettronica una fonte di informazioni sensibili dei lavoratori, anche di carattere personale.

Interessante notare come il Garante indichi tra le premesse la necessità di realizzare un bilanciamento tra esigenze datoriali e garanzie di libertà dei lavoratori.

È fondamentale partire dall'assunto per cui «il luogo di lavoro è considerato come una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali»([42]).

Nei principi di necessità, correttezza, pertinenza e non eccedenza, è individuato il nucleo fondante della tutela del lavoratore.

Il datore di lavoro deve indicare le modalità di utilizzo degli strumenti forniti al dipendente e di ipotetici controlli e deve predisporre misure organizzative e tecnologiche per prevenire l'utilizzo indebito di dati.

Deve essere minimizzato l'uso di dati identificativi dei lavoratori e in ogni caso sono vietate «la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore»([43]).

Eventuali controlli posti in essere dal datore di lavoro non devono essere invasivi e sono leciti solo se rispettosi dei principi di pertinenza e non eccedenza e conformi alla «normativa di settore». È esplicito il riferimento all'art. 4 dello Statuto([44]).

Nonostante le suddette prescrizioni, nel corso degli anni i datori di lavoro hanno esercitato controlli sempre più pervasivi inducendo l'Autorità di controllo ad intervenire nuovamente.

Il Garante ha insistito sull'illegittimità di un controllo a distanza effettuato tramite uno strumento fornito da una compagnia aerea ai dipendenti per l'invio di comunicazioni elettroniche e per la formazione tecnico specialistica. Nonostante le insite potenzialità di controllo, lo strumento sarebbe stato consegnato in violazione delle procedure richieste dall'art. 4 dello Statuto e in assenza dell'informativa agli interessati. È stata ravvisata l'idoneità dello strumento a controllare a distanza l'attività lavorativa dei dipendenti, in ragione delle funzioni di tracciamento e registrazione degli accessi al corso di formazione (oltre che della relativa durata) utili al monitoraggio dell'andamento del processo formativo degli interessati. Questa funzionalità è stata ritenuta compatibile con le esigenze organizzative dell'azienda, ma non avendo espletato le procedure di cui alla norma statutaria, «presupposto indefettibile per la liceità e correttezza del

([42]) Garante della privacy, Linee Guida del 1° marzo 2007, doc. web. 1387522, par. 1.2 delle premesse.

([43]) Garante della privacy, Linee Guida del 1° marzo 2007, cit., n. 3, lett. b del dispositivo.

([44]) Garante della privacy, Relazione annuale del 2007, 16 luglio 2008, 100.

trattamento dei dati», il Garante ha dovuto inibire l'ulteriore trattamento dei dati personali dei dipendenti(45).

Si è pronunciato inoltre in senso contrario sul monitoraggio costante e reiterato di una società, relativamente alla navigazione Internet di un proprio dipendente, effettuato attraverso un software in grado di memorizzare tutte le pagine web consultate, registrando anche in questo caso la mancanza dei presupposti di cui all'art. 4 e la sproporzione del controllo. Benché i dipendenti fossero stati resi edotti del divieto di navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa e della possibilità di controlli sulla propria postazione individuale, il trattamento effettuato è risultato illecito sia per violazione della normativa sulla privacy, sia perché sproporzionato rispetto alla finalità perseguita, tenuto conto della forma reiterata e costante con cui il monitoraggio era stato effettuato(46).

Meritevole di essere menzionato è un caso affrontato dal Garante all'esito del quale ha vietato la conservazione e la categorizzazione, anche su base individuale, dei dati riferiti alla navigazione Internet dei dipendenti, poiché in contrasto con la normativa sulla privacy e l'art. 4 dello Statuto.

Si trattava di una società che aveva regolato l'uso di Internet da parte dei dipendenti con appositi filtri di navigazione, possibilità peraltro suggerita dalle menzionate Linee Guida al fine di ridurre il rischio di uso improprio di Internet e di prevenire controlli successivi sul lavoratore.

I filtri venivano implementati tramite un *software* «per finalità di tutela aziendale e per poter eventualmente riferire all'Autorità Giudiziaria comportamenti anomali registrati dai sistemi». Il sistema di filtraggio non si limitava ad inibire l'accesso a siti non correlati allo svolgimento della prestazione lavorativa, ma memorizzava l'accesso e i tentativi di accesso di ogni lavoratore ai domini selezionati, acquisendo una serie di ulteriori informazioni che indicavano la macchina utilizzata, data e ora dell'accesso e utente richiedente. Peraltro, risultava che il sistema di filtraggio potesse generare quotidianamente report individuali indicando nominativamente il singolo lavoratore, dando luogo ad una vera e propria profilazione degli utenti, e che i dati acquisiti fossero oggetto di una prolungata conservazione.

Appare evidente come il trattamento effettuato fosse in violazione della norma statutaria, poiché determinava un controllo a distanza e pur volendo ricondurre il sistema di filtraggio alle «esigenze organizzative e produttive», non verrebbero meno la violazione dell'art. 4 in quanto non risultava la stipulazione di alcun accordo con le organizzazioni sindacali o l'autorizzazione dell'Ispettorato del lavoro, e la violazione

(45) Garante della privacy, Provv. del 2 aprile 2008, doc. web.1519695.
(46) Garante della privacy, Provv. del 2 aprile 2009, doc. web. 1606053.

della normativa sulla privacy poiché in contrasto con i principi di pertinenza e non eccedenza([47]).

Interessante anche il caso di un Ateneo italiano che effettuava operazioni di raccolta e conservazione, per un periodo di 5 anni, di informazioni relative all'accesso ai servizi Internet, alla posta elettronica e alle connessioni di rete di una pluralità di utenti, con la possibilità di controllarne l'attività.

I dati raccolti erano perfettamente riconducibili ai singoli utenti, anche grazie al tracciamento degli indirizzi IP dei computer assegnati ai dipendenti o utilizzati dagli utenti abilitati, potendo risalire perfino alla postazione e di conseguenza all'utente che vi operava. Il Garante ha dichiarato l'illiceità del trattamento, poiché in contrasto con i principi di necessità, pertinenza e non eccedenza e poiché effettuato in assenza della dovuta informativa e in violazione della disciplina dettata dall'art. 4([48]).

Il Garante è intervenuto ancora una volta in tema di posta elettronica ritenendo illecito il trattamento posto in essere da una società che aveva effettuato l'accesso al contenuto dei messaggi di posta elettronica scambiati da un dipendente con alcuni colleghi per un periodo di tempo piuttosto esteso, servendosene per effettuare una contestazione disciplinare.

La società insisteva sulla legittimità del trattamento effettuato «in quanto preordinato alla tutela degli interessi dell'impresa (anche di protezione del patrimonio aziendale)», ma l'Autorità Garante, ne ribadiva l'illegittimità tenendo conto dell'assenza di una previa informativa, della violazione dei principi di liceità, necessità e proporzionalità del trattamento e ravvisava anche un contrasto con la disciplina di settore in materia di controlli a distanza, che non consente di realizzare un controllo massivo, prolungato e indiscriminato sull'attività del lavoratore, perché il datore di lavoro deve in ogni caso avere cura di salvaguardarne la libertà e la dignità([49]).

Un'altra casistica sulla quale il Garante si è pronunciato più volte, è quella relativa all'accesso alla casella di posta elettronica aziendale, in seguito alla cessazione del rapporto di lavoro. Si prenda come riferimento il recente caso di una società che ha mantenuto attivo l'account di posta elettronica aziendale di una lavoratrice dopo la cessazione del rapporto di lavoro, conservando comunicazioni elettroniche per 10 anni dalla data di registrazione del messaggio nella casella di posta. Si è rilevato che l'interessata non avesse ricevuto alcuna informativa in merito al trattamento dei dati realizzato in seguito all'assegnazione di un account di posta elettronica aziendale, per cui, configurando una violazione dei principi di trasparenza e correttezza, il trattamento è stato considerato illecito. È stata accertata la violazione della disciplina dettata dall'art. 4 dello Statuto, poiché la condotta della società ha consentito di ricostruire l'attività della

([47]) Garante della privacy, Provv. del 21 luglio 2011, doc. web. 1829641, cfr. anche Provv. del 5 febbraio 2015, doc. web. 3813428.

([48]) Garante della privacy, Provv. del 13 luglio 2016, doc. web. 5408460.

([49]) Garante della privacy, Provv. del 1° febbraio 2018, doc. web. 8159221.

dipendente e di effettuare un controllo sulla stessa al di là delle finalità tassativamente ammesse dall'art. 4 e comunque in assenza delle garanzie procedurali ivi previste. Si è rilevata altresì la violazione del principio di minimizzazione dei dati richiamando l'orientamento del Garante per cui «l'adozione di appropriate misure organizzative e tecnologiche, individuare i documenti che, nel corso dello svolgimento dell'attività lavorativa, devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile» è fondamentale ai fini dell'ordinario svolgimento dell'attività aziendale, ma i sistemi di posta elettronica non consentono per la loro natura di assicurare tali caratteristiche([50]).

Altrettanto significativo un provvedimento del 1° dicembre del 2022, con cui l'Autorità ha accertato che una Regione avesse monitorato i dipendenti, che inviavano messaggi ad un determinato sindacato, conservando i metadati per finalità di sicurezza informatica per 180 giorni, violando i principi di protezione dei dati e le norme sul controllo a distanza, non essendoci validi presupposti giuridici. In questi casi, specifica il Garante, il datore di lavoro deve avviare le specifiche procedure di garanzia previste dalla legge (autorizzazione amministrativa o accordo sindacale), poiché il trattamento dei dati personali non può trovare la sua legittimazione nella teoria dei controlli difensivi([51]). Infatti, nel provvedimento si specifica di non poter accogliere la tesi difensiva presentata dalla Regione in questione, secondo cui avrebbe effettuato un controllo *ex post*, in seguito al compimento del presunto comportamento illecito, in presenza di ragionevoli sospetti, appellandosi alla giurisprudenza che qualifica i controlli difensivi come fattispecie estranea all'ambito di applicazione dell'art. 4.

Il Garante ritiene che «la c.d. teoria sui controlli difensivi, di pura creazione giurisprudenziale, è oggetto di applicazioni non univoche […] occorre ribadire, per i profili di protezione dei dati, quanto segue. I trattamenti di dati personali connessi all'impiego di strumenti dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori devono essere svolti nel rigoroso rispetto dei limiti e delle condizioni previste dalla cornice legislativa di riferimento, che ne costituisce, come detto, la base giuridica […]. Ciò, a maggior ragione, in quanto, a seguito delle modifiche apportate all'art. 4 della l. n. 300/1970 dal d.lgs. 14 settembre 2015, n. 151, anche le esigenze di tutela del patrimonio datoriale sono state espressamente incluse tra le sole finalità lecite perseguibili mediante sistemi che possono comportare il controllo indiretto

([50]) Garante della privacy, Provv. del 21 luglio 2022, doc. web. 9809466, cfr. anche Provv. del 29 settembre 2021, doc. web. 9719914, Provv. del 30 luglio 2015, doc. web. 4298277, Provv. del 20 dicembre 2019, doc.web. 9215890, Provv. del 29 ottobre 2020, doc. web. 9518890, Provv. del 16 dicembre 2021, doc. web. 9739653, Provv. del 31 agosto 2023, doc. web. 99

([51]) Garante della privacy, Relazione annuale del 2022, 6 luglio 2023, 125.

sulla generalità dei dipendenti, subordinandone l'installazione e l'utilizzazione all'accordo sindacale o, in alternativa, all'autorizzazione pubblica»([52]).

L'orientamento del Garante sull'utilizzo della posta elettronica, è stato confermato e consolidato altresì dalla recente adozione del Documento di indirizzo denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati"([53]). L'intento è quello di fornire a datori di lavoro pubblici e privati e ad altri soggetti coinvolti, indicazioni al fine di «promuovere la consapevolezza delle scelte, anche organizzative dei titolari del trattamento, nonché a prevenire iniziative e trattamenti di dati in contrasto con la disciplina in materia di protezione dei dati e le norme che tutelano la libertà e la dignità dei lavoratori» in modo che sia fatta chiarezza sulle norme e le garanzie che devono essere rispettate nell'ambito del contesto lavorativo, poste a presidio dei diritti e delle libertà dei lavoratori interessati.

L'attenzione dell'Autorità in particolare, è stata rivolta a programmi e servizi informatici per la gestione della posta elettronica, che possano raccogliere, a causa di impostazioni predefinite, i metadati relativi agli account di posta elettronica utilizzati dai dipendenti, in modo generalizzato e preventivo, conservandoli per un arco temporale piuttosto esteso.

L'intervento del Garante si è reso necessario soprattutto poiché in alcuni casi è emerso che i sistemi non consentissero ai datori di lavoro di modificare le impostazioni dei suddetti programmi informatici, non potendo così disabilitare la raccolta sistematica dei dati o ridurre il periodo di conservazione degli stessi.

Infatti, è proprio il tema della conservazione ad essere nucleo fondante del provvedimento.

Avendo sempre riguardo alla disciplina statutaria, l'attività di raccolta e conservazione dei metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, affinché ricada nell'ambito di applicazione del secondo comma dell'art. 4, «non può essere superiore di norma a poche ore o ad alcuni giorni, in ogni caso non oltre sette giorni, estensibili, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento, di ulteriori 48 ore». Al contrario, «la generalizzata raccolta e la conservazione di tali metadati, per un lasso di tempo più esteso – ancorché sul presupposto della sua necessità per finalità di sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro – potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta l. n. 300/1970»([54]).

([52]) Garante della privacy, Provv. del 1° dicembre 2022, doc. web. 9833530, nelle premesse, par. 3.5.

([53]) Garante della privacy, Provv. del 21 dicembre 2023, doc. web. 9978728.

([54]) Garante della privacy, Provv. del 21 dicembre 2023, doc. web. 9978728, par. 3.

Conseguentemente, l'impiego dei programmi e dei servizi di gestione della posta elettronica, in difetto dell'espletamento delle procedure di garanzia statutarie, prima di avviare la raccolta e la conservazione dei dati per un ampio arco temporale, esporrebbe il datore di lavoro, titolare del trattamento, ad una violazione della normativa di protezione dei dati personali e della, più volte richiamata, disciplina di settore.

Di qui, l'invito rivolto ai datori di lavoro pubblici e privati a verificare con diligenza che i servizi e programmi di gestione della posta elettronica dei dipendenti siano modificabili, in modo da impedire la raccolta dei metadati e limitare il periodo della loro conservazione([55]).

5. Videosorveglianza

Un altro punto fermo, unitamente alle Linee Guida del 2007, è rappresentato dal Provvedimento generale in materia di videosorveglianza, emanato l'8 aprile 2010, materia su cui il Garante è intervenuto più volte, in quanto tecnica di controllo a distanza più frequentemente oggetto di segnalazioni.

Il Garante, nel ribadire che la registrazione, la conservazione e l'utilizzo di immagini configura un trattamento di dati personali, insiste sulla necessità che esso avvenga nel rispetto dei principi declinati dalla normativa sulla privacy con la finalità di mitigare i rischi per i diritti e le libertà fondamentali degli interessati dal trattamento. Relativamente ai rapporti di lavoro, l'Autorità Garante precisa che nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, per cui «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). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell´art. 4, l. n. 300/1970, gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede

([55]) Non sono stati pochi i dubbi sollevati dall'adozione del Provvedimento in esame, tanto che il Garante, per rispondere alle numerose richieste di chiarimenti pervenute, ha deciso, tramite il Provvedimento del 22 febbraio 2024 (doc. web. 9987885), di differire l'efficacia del documento di indirizzo e promuovere una consultazione pubblica della durata di 30 giorni, per raccogliere dai datori di lavoro pubblici e privati e da altri soggetti interessati, informazioni, commenti, proposte su forme e modalità di utilizzo dei programmi e sistemi che renderebbero necessaria una conservazione dei metadati superiore rispetto a quella ipotizzata.

l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti"». Queste garanzie devono essere rispettate sia all'interno degli edifici, sia in altri contesti in cui è eseguita la prestazione lavorativa([56]).

Sono stati molteplici gli interventi dell'Autorità in questo ambito, relativamente a trattamenti effettuati in assenza delle garanzie dettate dall'art. 4 dello Statuto.

Nel settore alberghiero, si pensi ad una struttura, il cui sistema di videosorveglianza, installato per finalità di tutela del patrimonio aziendale, risultava idoneo ad inquadrare il personale, che eseguendo le proprie mansioni, si spostava nei diversi ambienti dell'hotel sottoposti a videosorveglianza, alcuni peraltro adibiti esclusivamente ai lavoratori. Il Garante è più volte intervenuto nel corso degli anni, per rimarcare la necessità di un'adeguata informativa indirizzata agli interessati dal trattamento anche qualora le telecamere dovessero essere disposte in aree in cui i dipendenti transitano o sostano per lo svolgimento dell'attività lavorativa([57]).

Nel caso di specie risultava che l'installazione delle telecamere non fosse avvenuta nel rispetto dei limiti dettati dalla norma statutaria e di quanto previsto dalla disciplina sulla privacy e considerato che «il divieto di controllo a distanza dell'attività lavorativa – e con esso le garanzie previste dall´art. 4, comma 2, l. n. 300/1970 – non viene meno in ragione della circostanza che lo stesso possa essere discontinuo, né per il fatto che i lavoratori siano al corrente dell´esistenza del sistema di videosorveglianza e del suo funzionamento», il Garante dichiarava illecito il trattamento([58]).

Nella casistica inoltre, spiccano vicende nelle quali è stato accertato che la ripresa delle immagini avvenisse in modo occulto([59]), all'insaputa dei lavoratori, sorvegliando la loro attività lavorativa e violando il principio di correttezza del trattamento. Si pensi al caso in cui il Garante ha dichiarato l'illiceità del trattamento effettuato da una società editoriale che «per finalità di tutela dei beni aziendali» era dotata di un impianto di videosorveglianza. Alcune delle telecamere erano nascoste nei rilevatori di fumo e nei segnali luminosi delle uscite di emergenza e due di queste in particolare posizionate all'interno di due locali dove prestavano la propria attività lavorativa i dipendenti della società. Le ragioni dell'illiceità del trattamento si possono facilmente ravvisare nella violazione del diritto alla riservatezza e della dignità dei lavoratori, del principio di correttezza, visto il carattere occulto dell'attività di videosorveglianza e nell' assenza dell'informativa ai lavoratori così come previsto dal Provvedimento generale menzionato pocanzi([60]).

([56]) Garante della privacy, Provv. dell'8 aprile 2010, doc. web. 1712680, par. 4.

([57]) A tal proposito Garante della privacy, Provv. del 16 settembre 2021, doc. web. 9719768, cfr. anche Provv. del 2 marzo 2023, doc. web. 9880398.

([58]) Garante della privacy, Provv. del 25 ottobre 2012, doc. web. 2212826, cfr. anche Provv. del 9 gennaio 2014, doc. web. 2927804.

([59]) R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151 n. 151/2015)*, *op. cit.*

([60]) Garante della privacy, Provv. del 4 aprile 2013, doc. web. 2439178.

Anche nel settore della grande distribuzione, il Garante ha ravvisato ampie aree di inosservanza della disciplina applicabile in relazione alla normativa in materia di controlli a distanza, con particolare riferimento all'installazione di telecamere, che con la finalità di tutela del patrimonio aziendale e quale deterrente per l'eventuale commissione di illeciti, realizzavano un controllo sull'attività lavorativa([61]).

L'Autorità ha anche precisato che i dati personali dei dipendenti acquisiti mediante sistemi di videosorveglianza, installati per finalità di sicurezza e tutela dei beni aziendali, non possono essere utilizzati per la contestazione di illeciti disciplinari([62]), poiché si tratterebbe di uno scopo ulteriore e diverso rispetto a quello originario, configurando così la violazione del principio di finalità del trattamento.

Al vaglio del Garante è passata anche l'installazione di un sistema di videosorveglianza di un'azienda sanitaria, dotato di telecamere posizionate in aree in cui normalmente transitano i dipendenti con la possibilità di controllarne l'attività. L'installazione era stata giustificata da esigenze di sicurezza e di tutela del patrimonio aziendale ed era avvenuta in assenza del preventivo accordo con le organizzazioni sindacali o l'autorizzazione dell'Ispettorato del lavoro. Anche in questo caso, confermando il suo precedente orientamento, il Garante ha sottolineato che «le esigenze di sicurezza e di tutela del patrimonio, pure invocate dall'Azienda, non sono, infatti, di per sé sole, sufficienti a legittimare la presenza di tali dispositivi in luoghi ove si svolge anche l'attività lavorativa, dando luogo a un trattamento di dati personali che può essere giustificato solo nel rispetto delle garanzie previste dalla legge nazionale applicabile». Pertanto, il rispetto del citato art. 4 legittima il trattamento dei dati personali([63]).

Sulla stessa scia, un recentissimo provvedimento del 1° giugno 2023 con cui il Garante è intervenuto per molteplici violazioni della privacy da parte di una società, che aveva installato un sistema di videosorveglianza trasgredendo alla procedura di garanzia descritta dall'art. 4. La società in questione difendendosi, affermava che l'autorizzazione non fosse necessaria, in quanto il sistema sarebbe stato installato in seguito ad un furto e quindi finalizzato alla tutela del patrimonio aziendale. In realtà l'Autorità ha accertato che gli strumenti operassero, di fatto, un controllo a distanza dell'attività lavorativa, per cui, l'autorizzazione al contrario sarebbe stata necessaria e fonte di legittimità dell'installazione([64]).

Sotto la "lente d'ingrandimento" del Garante vi è stato recentemente un Comune sanzionato in seguito all'installazione di una telecamera in prossimità dei dispositivi di

([61]) Garante della privacy, Provv. del 18 luglio 2013, doc. web. 2605290, cfr. anche Provv. dell'8 maggio 2014, doc. web. 3250490.

([62]) Garante della privacy, Provv. del 2 ottobre 2014, doc. web. 3534543.

([63]) Garante della privacy, Provv. del 5 marzo 2020, doc. web. 9433080.

([64]) Garante della Privacy, Provv. del 1° giugno 2023, doc. web. 9913830, cfr. anche Provv. del 18 luglio 2023, doc. web. 9931319, cfr. anche Provv. del 24 aprile 2024, doc. web.10019506.

rilevazione delle presenze dei lavoratori(65). È stata la segnalazione di una dipendente, destinataria di una contestazione disciplinare per il mancato rispetto dell'orario di servizio, ad aver "messo in moto" la procedura di accertamento dell'illecito condotta dall'Autorità. Il Comune giustificava l'installazione dell'impianto di videosorveglianza facendo leva sulla finalità di tutela del patrimonio comunale e di sicurezza dei lavoratori, in seguito ad alcune aggressioni subite da due dipendenti. Nel corso dell'istruttoria, tuttavia, il Garante ha ravvisato la violazione delle procedure di garanzia previste dalla disciplina in materia di controlli a distanza. Infatti, il trattamento dei dati personali dei lavoratori è avvenuto in assenza di un'adeguata informativa e il conseguente provvedimento disciplinare è stato adottato in una data antecedente rispetto all'ottenimento dell'autorizzazione dell'Ispettorato del lavoro. L'Autorità, peraltro, è tornata sulla teoria dei controlli difensivi sostenendo che nel caso di specie non ne ricorressero le circostanze di fatto «avendo il Comune installato la telecamera di videosorveglianza anteriormente ai fatti poi contestati alla dipendente e in maniera tale da riprendere la totalità dei lavoratori e dei visitatori transitanti nell'atrio dell'edificio»(66). Ha ribadito, in ogni caso, che pur se si fosse trattato di controlli difensivi per la tutela del patrimonio datoriale, il rispetto della disciplina dettata dallo Statuto e della normativa in materia di privacy sarebbe stato condizione fondante la liceità del trattamento.

6. Geolocalizzazione

I sistemi di localizzazione satellitare sono sempre più frequenti nel mondo del lavoro e sono generalmente installati a bordo dei veicoli impiegati dai datori di lavoro per soddisfare esigenze organizzative e produttive o di sicurezza sul lavoro e costituiscono un prezioso strumento ai fini della garanzia della sicurezza dei beni aziendali, ma allo stesso tempo possono giungere a realizzare un controllo sull'attività dei lavoratori, localizzandone la posizione.

Il Garante della privacy è stato chiamato più volte a pronunciarsi sul tema nonostante le prescrizioni generali emanate con il Provvedimento del 4 ottobre 2011, con cui si afferma che i dati relativi all'ubicazione dei veicoli, in quanto associati ai lavoratori, costituiscono informazioni personali riferite a questi ultimi e per questo è necessario il rispetto della disciplina in materia di privacy.

L'Autorità ritiene doveroso individuare le condizioni di liceità di tali trattamenti e in particolare intende, con questo provvedimento, dare attuazione, nell'ambito qui considerato, all'istituto del c.d. bilanciamento di interessi, di cui si era già detto nelle Linee Guida del 2007.

(65) Garante della Privacy, Provv. dell'11 aprile 2024, doc. web. 10013356.
(66) Garante della Privacy, Provv. dell'11 aprile 2024, cit., par. 3.3.

Il trattamento deve avvenire in modo lecito, rispettando i principi di pertinenza e non eccedenza, il principio di necessità, deve esserci l'informativa agli interessati e il rispetto della disciplina dettata dall'art. 4([67]).

L'Autorità Garante si è espressa più volte sui sistemi di localizzazione installati sui veicoli aziendali che consentono di monitorare a distanza la posizione del mezzo e quindi indirettamente la posizione del lavoratore([68]).

È stata dichiarata l'illiceità, ad esempio, di dispositivi installati su veicoli in dotazione dei dipendenti di una società, in assenza della preventiva informativa e del rispetto dei precetti della norma statutaria, insistendo sul fatto che anche se i dispositivi fossero utili per esigenze di sicurezza e organizzazione del lavoro, fosse necessaria l'osservanza della disciplina in materia di trattamento dei dati personali e il rispetto dei diritti e delle libertà fondamentali degli interessati([69]).

Al contrario, il Garante ha riconosciuto la liceità del trattamento dei dati acquisiti dai sistemi di localizzazione di veicoli aziendali di una società erogatrice di servizi di fornitura d'acqua, tra le cui finalità perseguite vi era anche quella di tutela del patrimonio aziendale([70]), alla luce della quale ha rimarcato in ogni caso che il rispetto dell'art. 4, fosse condizione di legittimità del trattamento. Anche l'Ispettorato del lavoro, peraltro, con la circolare n. 2 del 7 novembre 2016, aveva chiarito relativamente all'installazione di sistemi di localizzazione sulle autovetture aziendali, che «in linea di massima e in termini generali […] i sistemi di geolocalizzazione rappresentano un elemento "aggiunto" agli strumenti di lavoro» e pertanto «le relative apparecchiature possono essere installate solo previo accordo con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione dell'Ispettorato nazionale del lavoro».

Sono stati numerosi gli interventi dell'Autorità anche in riferimento all'utilizzo di applicazioni informatiche che consentono di localizzare gli *smartphone* forniti ai dipendenti, che presentano ancor di più un rischio per le libertà, i diritti e la dignità dei lavoratori.

L'utilizzo di tali sistemi, diretto al perseguimento di finalità organizzative o di sicurezza del lavoro, deve essere subordinato all'adozione di misure volte ad impedire l'eventuale trattamento di informazioni presenti sul dispositivo di carattere strettamente personale e che siano estranee alla gestione del rapporto di lavoro, e rendere edotti i

([67]) Garante della Privacy, Provv. del 4 ottobre 2011, doc. web. 1850581.

([68]) Si v. a tal proposito A. Abbasciano, *Il controllo a distanza del datore di lavoro e il rispetto alla vita privata del lavoratore (ancora) sotto i riflettori della Corte Edu: il caso Gramaxo c. Portugal*, *LLI,* 2023, vol. 9, n. 1, 3 ss.

([69]) Garante della privacy, Provv. del 7 ottobre 2010, doc. web. 176307, si v. anche Provv. del 4 ottobre 2011, doc. web. 1850581, Provv. del 1° agosto 2012, doc. web. 1923293, Provv. del 7 marzo 2013, doc. web. 2471134, Provv. del 9 ottobre 2014, doc. web. 3505371, Provv. del 28 giugno 2018, doc. web. 9023246.

([70]) Garante della privacy, Provv. del 16 marzo 2017, doc. web. 6275314, nelle premesse par. 1.1.

lavoratori in tempo reale dell'attivazione della funzionalità di localizzazione, ma anche al rispetto della garanzia in materia di controlli a distanza([71]).

In una vicenda oggetto di un recente Provvedimento del giugno 2023, precedentemente citato, la società titolare ha effettuato un trattamento non conforme alla disciplina in materia di protezione dei dati personali, anche in riferimento al trattamento dei dati di geolocalizzazione, tramite un applicativo installato sugli *smartphone* dei lavoratori. Attraverso l'applicativo è risultata tracciata in modo continuativo la posizione del dispositivo e anche la posizione del lavoratore nello svolgimento della propria attività lavorativa. Questa condotta si pone in contrasto con la disciplina di settore in materia di controlli a distanza, con il principio di minimizzazione dei dati e sembra che non sia stato adempiuto neppure l'obbligo di un'adeguata informativa in merito al trattamento dei dati relativi alla posizione geografica([72]).

Altra interessante casistica è quella che riguarda la localizzazione geografica mediante dispositivi tecnologici indossabili([73]). Anche a tal proposito il Garante ha ribadito la necessaria sottoscrizione di un accordo di cui all'art. 4, come condizione di liceità del trattamento, unitamente all'individuazione di un dispositivo non lesivo della dignità del lavoratore e al rispetto della normativa sulla privacy([74]).

7. Rilevazione biometrica

L'attenzione del Garante si è focalizzata più di una volta anche sull'utilizzo di sistemi di riconoscimento biometrico([75]) ai fini della rilevazione degli accessi e delle presenze dei lavoratori.

A tal proposito, è bene ricordare che il secondo comma dell'art. 4 dello Statuto, così come riformato nel 2015, esclude dal regime autorizzatorio, oltre che gli strumenti utilizzati per rendere la prestazione lavorativa, anche quelli di registrazione degli accessi e delle presenze; denso il dibattito dottrinale sul tema([76]).

([71]) Garante della privacy, Provv. dell'11 settembre 2014, doc. web. 3474069, Provv. del 9 ottobre 2014, doc. web. 3505371, Provv. dell'8 gennaio 2015, doc. web. 3723437, Provv. del 18 maggio 2016, doc. web. 5217175, Provv. del 30 novembre 2017, doc. web. 7522639.

([72]) Garante della Privacy, Provv. del 1° giugno 2023, cit., cfr. Provv. del 14 settembre 2023, doc. web. 9936174.

([73]) Sul tema si v. R. Di Meo *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, *LLI*, 2018, vol. 4, n. 1, 3 ss., A. Ingrao, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, *DRI*, 2019, n. 3, 895 ss.

([74]) Nota del Segretario generale, 28 febbraio 2019, doc. web. 9094427.

([75]) Si v. Garante della privacy, Linee Guida biometria, 12 novembre 2014, doc. web. 3563006.

([76]) Si rinvia ad altra sede per approfondimenti sul tema, si v. I. Alvino, *I nuovi limiti al controllo a distanza*, *op. cit.*, 17; C. Zoli - E. Villa, *Gli strumenti di registrazione degli accessi e delle presenze,* in *Controlli a distanza e tutela dei dati personali del lavoratore*, *op. cit.*, 127 ss.; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. Lav., op. cit.*, 18; S. Ortis, *Biometria e videosorveglianza nella lotta all'assenteismo dei dipendenti pubblici: uno sguardo alla legge concretezza n. 56/2019, RIDL*, 2020, 3, 429 ss.; A. Ingrao, *Controllo a distanza e*

L'utilizzo di tecnologie biometriche nei luoghi di lavoro solleva profili di indiscutibile complessità, soprattutto in considerazione della disciplina dettata dal Regolamento 2016/679, che definisce i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»([77]), per questo ricondotti alla categoria di dati personali sensibili.

Lo stesso Garante ha evidenziato che «i dati biometrici sono, per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all' individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, richiedendo particolari cautele in caso di loro trattamento. L' adozione di sistemi biometrici, […] può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato»([78]).

Il trattamento di dati biometrici, di regola è vietato dal Gdpr([79]), ed è consentito unicamente in presenza di determinate condizioni, tra cui, in riferimento all'ambito lavorativo, quando è necessario «per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato»([80]).

Le finalità di rilevazione delle presenze e di verifica del rispetto dell'orario di lavoro rientrano nell'ambito di applicazione dell'art. 9, par. 2, lett. b del Gdpr, ma affinché il trattamento sia consentito, è necessario che sia autorizzato dal diritto dell'Unione o degli Stati membri.

Ad oggi l'ordinamento vigente però non consente il trattamento di dati biometrici dei dipendenti ai fini della rilevazione delle presenze e questo è stato ribadito più volte dal Garante, in quanto l'utilizzo dei suddetti dati nell'ordinaria gestione del rapporto di lavoro non è conforme ai principi di minimizzazione e proporzionalità([81]).

La casistica su cui l'Autorità ha fatto luce ha riguardato ipotesi di sistemi biometrici basati sul riconoscimento delle impronte digitali o sul riconoscimento facciale. Quest'ultimo, in particolare, ha costituito oggetto di recentissimi provvedimenti

privacy alla luce dei principi di finalità e proporzionalità della sorveglianza, cit., 114; V. Nuzzo, *Il controllo della prestazione di lavoro resa fuori dai confini dell'impresa*, *LLI*, 2023, vol. 9, n. 1, 74 ss.

([77]) Si v. art. 4, punto 14 del Reg. Ue 2016/679.

([78]) Garante della privacy, Provvedimento generale prescrittivo in tema di biometria, 12 novembre 2014, doc. web. 3556992, par. 4.

([79]) Si v. art. 9, par. 1 del Reg. Ue 2016/679.

([80]) Si v. art. 9, par. 2, lett. b del Reg. Ue 2016/679.

([81]) Sul punto si v. Garante della privacy, Provv. del 10 novembre 2022, doc. web. 9832838, Provv. del 14 gennaio 2021, doc. web. 9542071.

con cui è stata ribadita l'illiceità del trattamento in esame([82]). Il Garante ha sanzionato cinque società impegnate nello stesso sito di smaltimento di rifiuti per aver trattato illecitamente i dati biometrici di un numero elevato di lavoratori, tramite l'utilizzo di un sistema di rilevazione delle presenze basato sul riconoscimento facciale.

In sinergia con il Nucleo speciale privacy e frodi tecnologiche della Guardia di finanza, in seguito agli opportuni accertamenti ispettivi, il Garante ha accertato che tre delle cinque aziende avevano utilizzato lo stesso sistema di rilevazione biometrica per più di un anno senza aver adottato adeguate misure tecniche e di sicurezza. Le aziende non avevano neppure fornito ai lavoratori la dovuta informativa in merito alle caratteristiche del trattamento dei dati biometrici mediante riconoscimento facciale, né avevano provveduto ad effettuare una valutazione d'impatto dei trattamenti, configurando un'ulteriore violazione dei principi dettati dal Gdpr.

Sulla stessa scia si innesta un altro recente provvedimento avente ad oggetto un sistema di rilevazione delle presenze basato invece sulla lettura delle impronte digitali([83]).

La Società in questione affermava che il dispositivo risultasse conforme alla normativa in materia di tutela della privacy, poiché le impronte erano raccolte e memorizzate unicamente nella memoria interna del dispositivo stesso e rese inutilizzabili in altri ambiti, poiché criptate. Precisava altresì di aver reso edotti i dipendenti sul funzionamento del dispositivo che non avrebbe trattato dati generici o biometrici degli stessi.

L'Autorità garante, anche in questo caso, ha precisato che, sebbene la rilevazione delle presenze dei dipendenti e la verifica sull'osservanza dell'orario di lavoro possano rientrare nelle ipotesi di cui al par. 2, lett. b dell'art. 9 del Regolamento, oltre che nei casi di deroga previsti dal secondo comma della norma statutaria, il trattamento di dati biometrici è consentito solo se autorizzato dal diritto dell'Unione o degli Stati Membri. Considerata l'assenza di una normativa di questo tipo, il trattamento risulta illecito, anche in considerazione del fatto che all'esito dell'istruttoria si è rilevato che nell'informativa predisposta dalla Società non ci fosse alcun riferimento al trattamento dei dati biometrici per la rilevazione delle presenze, né fosse indicata la possibilità di utilizzare in alternativa, così come era stato dichiarato dalla Società, il sistema tradizionale basato sul badge.

([82]) Si v. Garante della privacy, Provv. del 22 febbraio 2024, doc. web. 9995808, doc. web. 9995785, doc. web. 9995762, doc. web. 9995741, doc. web. 9995701, doc. web. 9995680.

([83]) Garante della privacy, Provv. del 14 settembre 2023, doc. web. 9940565, cfr. Provv del 1° giugno 2023, doc.web. 9913830, cfr. Provv. del 15 dicembre 2022, doc. web. 9852776, cfr. Provv. del 14 gennaio 2021, doc. web. 9542071.

8. Conclusioni

Com'è possibile notare dalla rassegna di alcuni dei provvedimenti del Garante, spesso, oggetto di controversia sono stati i c.d. controlli difensivi, tema che più che mai mette in risalto il difficile equilibrio tra le due parti del rapporto di lavoro.

La tanto discussa categoria non sembra destare nel Garante molti dubbi. Il suo orientamento è stato costante nel corso degli anni, nonostante l'evoluzione normativa e l'incalzante progresso tecnologico.

"Esplorando" la sua produzione "giurisprudenziale" emerge a chiare lettere l'instabile equilibrio esistente tra la tutela dei diritti del lavoratore e le esigenze del datore di lavoro. Tuttavia, la teoria dei controlli difensivi sembrerebbe non trovare sostegno nelle elaborazioni del Garante, che tuttalpiù tende a ricondurre tutti gli strumenti di controllo nell'ambito di applicazione del dettato normativo. Infatti, risulta necessario il rispetto delle garanzie e delle tutele riconosciute dalla norma, che si pone anche in stretta connessione con la disciplina europea in materia di privacy.

Risulta evidente il contrasto con la giurisprudenza di legittimità, da sempre "promotrice" dei controlli difensivi e sostenitrice della loro legittimità al di fuori dell'ambito di applicazione della disciplina statutaria, incorrendo talvolta in contraddizioni, dando adito ad incertezze, e determinando un vero e proprio «labirinto concettuale»([84]).

In questo quadro, il Garante della privacy, con la sua "giurisprudenza", non lascia spazio ad incertezze e mostra quale priorità assoluta quella di realizzare un bilanciamento di interessi([85]) e assicurare un trattamento che sia volto a garantire il rispetto della libertà e dignità umana.

([84]) R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151 n. 151/2015), op. cit.*, 86, il quale ritiene che «la giurisprudenza si è inoltrata, e senza disporre del filo di Arianna, in un labirinto concettuale dal quale non è più riuscita ad uscire, con il risultato di ingenerare, al di là dell'apparente sicurezza delle formule utilizzate, una crescente incertezza».

([85]) Garante della privacy, Linee Guida del 1° marzo 2007, cit., par. 7 delle premesse.

Bibliografia

Abbasciano A., *Il controllo a distanza del datore di lavoro e il rispetto del diritto alla vita privata del lavoratore (ancora) sotto i riflettori della Corte Edu: il caso Gramaxo c. Portugal*, in *LLI*, 2023, 9, 1, 3 ss.

Alvino I., *I nuovi limiti al controllo a distanza, dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy,* in *LLI*, 2016, 2, 2, 3 ss.

Barbieri M., *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 183 ss.

Barraco E., *Controlli tecnologici*, in *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, a cura di E. Barraco - A. Sitzia, Ipsoa, 2016, 20 ss.

Bellavista A., *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, in *LDE*, 2023, 1, 2 ss.

Busia G., *Così vicini, così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente*, in *LDE*, 2020, 3, 2 ss.

Carinci M. T., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 45 ss.

Chieco P., *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*, Cacucci, 2000.

Colapietro C., Giubilei A., *Controlli difensivi e tutela dei dati del lavorato*re, in *LLI*, 2021, 7, 2, 189 ss.

Del Conte M., *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, in *Dir. Informatica*, 2007, 3, 497 ss.

Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151 n. 151/2015)*, in *RIDL*, 2016, I, 77 ss.

Di Meo R., *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *LLI*, 2018, 4, 1, 3 ss.

Fioriglio G., *Intelligenza artificiale, privacy e rapporto di lavoro: una prospettiva informatico-giuridica*, in *LDE*, 2022, 3, 2 ss.

Fratini R. - Maurelli R., *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e codice privacy*, in *LPO*, 2020, 11-12, 714 ss.

Fratini R., *Privacy ed efficienza nel pubblico impiego*, in *MGL*, 2021, 3, 607 ss.

Ingrao A., *I controlli difensivi tra passato e presente: privacy del lavoratore e inutilizzabilità dei dati*, in *NGCC*, 2019, 4, 652 ss.

Ingrao A., *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in *DRI*, 2019, 3, 895 ss.

Ingrao A., *La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritm*i, in *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, a cura di A. Bellavista - R. Santucci, Giappichelli, 2022, 127 ss.

Ingrao A., *Controllo a distanza e privacy alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *LLI*, 2023, 9, 1, 102 ss.

Lambertucci P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act*), in Biblioteca "20 maggio", 2015, 1, 521 ss.

Lorè F., *La tutela della privacy nell'esercizio del potere datoriale*, in *Amministrativamente*, 2020, 1, 32 ss.

Marazza M., *I controlli a distanza del lavoratore di natura «difensiva»*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 27 ss.

Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. Lav.*, in *Controlli a distanza e tutela dei dati personali del lavorator*e, a cura di P. Tullini, Giappichelli, 2017, 2 ss.

Nuzzo V., *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, 2018.

Nuzzo V., *Il controllo della prestazione di lavoro resa fuori dai confini dell'impresa*, in *LLI*, 2023, 9, 1, 61 ss.

Ogriseg C., *Il regolamento Ue n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in *LLI*, 2016, 2, 2, 29 ss.

Ortis S., *Biometria e videosorveglianza nella lotta all'assenteismo dei dipendenti pubblici: uno sguardo alla legge concretezza n. 56/2019,* in *RIDL*, 2020, 3, 429 ss.

Pinto V., *I controlli "difensivi" del datore di lavoro sulle attività informatiche e telematiche del lavoratore*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 139 ss.

Recchia G. A., *Controlli datoriali difensivi: note su una categoria in via di estinzione*, in *LG*, 2017, 348 ss.

Riccobono A., *Nuove tecnologie e controlli difensivi tra diritto positivo e creazionismo giudiziario*, in *RIDL,* 2023, 4, 506 ss.

Salimbeni M. T., *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *RIDL*, 2015, I, 589 ss.

Sitzia A., *Lavoro e privacy: adempimenti obbligatori e procedure*, in *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, a cura di E. Barraco - A. Sitzia, Ipsoa, 2016, 112 ss.

Sitzia A., *Il decreto legislativo di attuazione del Regolamento Privacy (n. 101 del 2018): profili giuslavoristici*, in *LDE*, 2018, 2, 2 ss.

Tufo M., *Potere di controllo datoriale vs. privacy del lavoratore: alla ricerca delle coordinate di ammissibilità dei controlli occulti*, in *Studium Iuris*, 2020, 7-8, 846 ss.

Tullini P., *Tecnologie informatiche in azienda: dalle linee-guida del Garante alle applicazioni concrete,* in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, a cura di P. Tullini, Cedam, 2010, 123 ss.

Tullini P., *I controlli aziendali per finalità difensive nella giurisprudenza*, in *RIDL*, 2022, I, 221 ss.

Tullini P., *Dati*, in *Lavoro digitale*, a cura di M. Novella - P. Tullini, Giappichelli, 2022, 105 ss.

Tursi A., *Note minime in tema di controlli difensivi del datore, onere della prova e utilizzabilità delle prove illecitamente acquisite nel processo*, in *LLI*, 2023, 9, 1, 85 ss.

Ziccardi G., *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *LLI*, 2016, 2, 1, 48 ss.

Zoli C. - Villa E., *Gli strumenti di registrazione degli accessi e delle presenze*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 127 ss.