



**LaBoUR & Law Issues**  
Rights | Identity | Rules | Equality

**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***

**ARIANNA ABBASCIANO**

Università degli Studi di Bari “Aldo Moro”

**vol. 9, no. 1, 2023**

ISSN: 2421-2695



# 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*

ARIANNA ABBASCIANO

Università di Bari

Dottoranda di ricerca in Diritto del Lavoro

arianna.abbasciano@uniba.it

---

## ABSTRACT

---

The balance between the workers' right to privacy and the employer's legitimate interest in exercising remote control by means of Gps tracking was submitted to the European Court of Human Rights in the case *Gramaxo c. Portugal*. Taking into account the Court's previous judicial decision as a starting point, this contribution will analyse the effects on domestic law of the rules on remote control and personal data protection, also with reference to geolocation data, with the aim of highlighting the changing nature of the limits imposed to the employers' interests by the European Court of Human Rights.

**Keywords:** privacy at workplace; remote control; geolocation mechanism; balancing test; respect for private life.

<https://doi.org/10.6092/issn.2421-2695/17457>

---

## **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***

SOMMARIO: 1. Qualche elemento di contesto. Alla ricerca del bilanciamento perduto. – 2. Il caso *Gramaxo c. Portugal*: il fatto, la Commissione nazionale per la protezione dei dati e la magistratura portoghese. – 2.1. I controlli a distanza e il rispetto del diritto alla vita privata al cospetto della Corte Edu: alcuni precedenti rilevanti. – 2.2. Decisione della Corte Edu e *dissenting opinion*. – 2.3. Prove di bilanciamento possibile. – 3. Riflessi sul diritto interno: i limiti al potere di controllo a distanza tra norme statutarie, Codice privacy e Gdpr. – 3.1. *Segue*. Il Gps tra norme statutarie e provvedimenti amministrativi del Garante privacy. – 4. Osservazioni conclusive.

### **1. Qualche elemento di contesto. Alla ricerca del bilanciamento perduto**

La tensione tra il diritto del lavoratore alla tutela della sua sfera privata nell'esecuzione della prestazione lavorativa e l'interesse datoriale alla verifica dell'esatto adempimento contrattuale continua a dominare la scena del contenzioso giurisprudenziale e, di conseguenza, ad alimentare il dibattito dottrinale. D'altronde, a fronte delle nuove sfide che la digitalizzazione impone al diritto del lavoro <sup>(1)</sup>, il conflitto tra potere di controllo (a distanza) e privacy è più che mai oggetto di attenzione <sup>(2)</sup>.

La sentenza della Corte Europea dei Diritti dell'Uomo (d'ora in poi, Corte Edu) in commento si inserisce, ancora una volta, nel solco del "bilanciamento possibile" tra il diritto alla vita privata, garantito anche nel rapporto di lavoro dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (d'ora in poi, Cedu), che si assume violato a seguito dell'installazione di uno strumento di geolocalizzazione Gps sull'auto aziendale a uso promiscuo, e la libertà di gestione e organizzazione della propria attività d'impresa.

La vicenda offre l'occasione per rileggere i confini del potere di controllo a distanza del datore di lavoro e le istanze di tutela di cui sono portatori i lavoratori alla luce della rivoluzione tecnologica e digitale che sta investendo gli attuali assetti produttivi e l'organizzazione stessa dell'attività di impresa.

---

<sup>(1)</sup> Si pensi ai nuovi spazi virtuali immersivi in cui potrebbe (potrà) "rendersi" la prestazione lavorativa, che ha spinto la dottrina a interrogarsi sulle prospettive, ma prima ancora, sull'adeguatezza degli strumenti giuridici conosciuti per tutelare la dignità di un lavoratore-*avatar* in un metaverso ancora in evoluzione. La riflessione conduce al percorso tematico presente sul vol. 8, n. 2 della rivista *Labour Law Issues* introdotto da A. Donini - M. Novella - M. L. Vallauri, *Prime riflessioni sul lavoro nel metaverso*, *LLI*, 2022, 8, 2.

<sup>(2)</sup> Il tema, infatti, è ancora centrale nel dibattito dottrinale. Si rinvia, più recentemente, a C. Pisani - G. Proia - A. Topo (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giappichelli, 2022.

È noto, infatti, come il potere di controllo costituisca il perno attorno al quale gravitano il potere direttivo, di cui rappresenta un corollario, e il potere disciplinare, rispetto al quale si colloca come presupposto logico e giuridico. Tuttavia, ove il controllo venga esercitato “a distanza” i rischi per la libertà e la dignità dei lavoratori si intensificano a tal punto da aver spinto l’ordinamento nazionale a predisporre un quadro regolatorio di stampo protettivo che ha trovato, negli articoli 4 e 8 dello Statuto dei lavoratori (d’ora in poi, St. lav.) una prima codificazione, successivamente integrata con il sistema normativo posto a protezione dei dati personali delle persone fisiche, oggi regolato a livello unionale dal Regolamento (Ue) 2016/679 (d’ora in poi Gdpr, secondo l’acronimo inglese).

D’altro canto, l’impatto delle nuove tecnologie (predittive ma anche algoritmiche<sup>(3)</sup>), così come la digitalizzazione applicata ai processi produttivi o ai sempre più diffusi *smart wearable devices* <sup>(4)</sup> hanno profondamente modificato le modalità di esecuzione della prestazione lavorativa rendendo più fumosi i confini – sui quali poggia la tutela apprestata dall’ordinamento interno – tra «strumenti di controllo», il cui utilizzo è proceduralizzato *ex lege*, e «strumenti di lavoro» sottratti al preventivo vaglio sindacale o amministrativo. La conseguenza è, inevitabilmente, l’esposizione del lavoratore a controlli anonimi sempre più invasivi e onniscienti <sup>(5)</sup>. Ma non solo. L’innovazione digitale ha modificato anche lo stesso esercizio dei poteri datoriali, in generale, e del potere di controllo a distanza, in particolare, che tende sempre più a mimetizzarsi nell’ambito dei processi produttivi automatizzati <sup>(6)</sup>, fondendosi in essi. In questo senso, l’evoluzione tecnologica e digitale presta il fianco anche a forme di controllo a distanza più subdole, in cui il controllo sulla prestazione è eventuale e

---

<sup>(3)</sup> Su cui si rinvia a A. Ingraio, *Il controllo a distanza sulla prestazione dei ciclofattorini tra Scoober App e GPS*, LLI, 2021, 7, 1, 165.

<sup>(4)</sup> R. Di Meo, *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, LLI, 2018, 4, 1, 1-19.; A. Ingraio, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, DRI, 2019, 3, 895. Si veda, inoltre, il provvedimento adottato dal Garante della Privacy il 28 febbraio 2019 in materia di trattamento di dati personali dei dipendenti mediante dispositivi indossabili consultabile al seguente link: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9094427>

<sup>(5)</sup> Come sottolinea L. Tebano, *Employees’ Privacy and employers’ control between the Italian and European system*, LLI, 2017, 3, 2, 3, «there are mechanisms of monitoring employees’ activity which are physically less cumbersome, but even more invasive», mutando, secondo G. Ziccardi, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, LLI, 2016, 2, 1, 49, l’ontologia del controllo che passa, da un «metodo orwelliano», pericoloso ma tutto sommato prevedibile, a un «controllo kafkiano, estremamente frammentato, complesso, labirintico, oscuro e burocratizzato, composto da dati che si incrociano – lavorativi e privati – e da problemi tecnici difficilmente comprensibili per il lavoratore, da catene di responsabilità [...] e da una separazione tra vita privata e vita lavorativa ormai inesistente».

<sup>(6)</sup> In simili contesti, «il controllo a distanza costituisce una parte integrante dell’ambiente digitale, non distinguibile dal processo produttivo e dall’organizzazione del lavoro», P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 119.

indiretto (c.d. per rifrazione) in quanto finalizzato al raggiungimento di obiettivi ultronei, come la rilevazione del comportamento e delle scelte d'acquisto dei consumatori, ma comunque idonei a trasmettere informazioni anche sulla prestazione lavorativa (7). È, dunque, di tutta evidenza come le istanze di tutela della libertà personale di cui è portatore il prestatore di lavoro si intreccino con le più ampie capacità tecniche in cui il controllo può avvenire, decretando la prevaricazione degli interessi – pur meritevoli di tutela – di una sola delle parti del contratto, non a caso la più forte.

Pertanto, in una realtà produttiva in cui il controllo a distanza indiretto coesiste con l'esercizio del relativo potere datoriale senza esaurirsi in esso, non è superata, quanto piuttosto acuita, l'attualità del dibattito sui limiti al potere di controllo a distanza (8). Per tali ragioni, ha senso soffermarsi ancora oggi sul tradizionale dibattito che vede l'installazione del Gps sul veicolo aziendale al centro della pronuncia in commento, con l'obiettivo di attrarre nel quadro regolativo anche ciò che nel prossimo futuro rischia di sfuggire al(l'esercizio del) "controllo".

## **2. Il caso *Gramaxo c. Portugal*: il fatto, la Commissione nazionale per la protezione dei dati e la magistratura portoghese**

Il caso in commento attiene al licenziamento di un «delegado de informação médica» sulla base dei dati raccolti da un sistema di geolocalizzazione installato sul veicolo messo a disposizione dal datore di lavoro per l'espletamento della prestazione lavorativa. L'uso del veicolo era autorizzato dall'azienda anche per gli spostamenti privati che avessero avuto luogo al di fuori dell'orario di lavoro, fermo restando che i chilometri percorsi per fini privati dovessero essere comunque rimborsati dal lavoratore all'azienda. A fronte di incongruenze nelle note spese di alcuni dipendenti e, in particolar modo, quelle concernenti i chilometri dichiarati a titolo professionale e quelli percorsi per esigenze della vita privata dei lavoratori, nel settembre 2011 la società aveva installato su tutti i veicoli aziendali un sistema satellitare di posizionamento globale (Gps), affidando la gestione dei dati a una società informatica esterna, e informando, il 24 novembre 2011 la Commissione nazionale per la protezione dei dati (d'ora in poi,

---

(7) Un meccanismo di tracciamento e analisi di dati secondo cui «i tempi di interazione [del consumatore], la sosta in certe zone del negozio, il flusso delle vendite possono fornire indicazioni sulla prestazione dell'addetto senza che sia necessario controllarne direttamente la prestazione stessa», così in M. Novella, *Poteri del datore di lavoro nell'impresa digitale: fenomenologia e limiti*, LD, 2021, 3-4, 466, che rinvia, in ordine alla "refractive surveillance" a K. Levy, S. Barocas, *Refractive surveillance: monitoring customers to manage workers*, in *Int. J. Commun.*, 2018, 12, 1166. Sul punto, si vedano anche le riflessioni di S. Laforgia, *I poteri del datore di lavoro, oggi. Opacità e rifrazioni sotto la lente del giurista*, in *Le conquiste legislative degli anni '70 e il ruolo del movimento sindacale in Puglia*, a cura di V. Leccese - V. Pinto, Edizione Radici Future, 2022, 239.

(8) Non a caso A. Pizzoferrato, *I limiti al potere di controllo datoriale nell'era digitale*, LDE, 2023, 1, 2, si domanda – retoricamente – se abbia ancora senso «parlare di limiti al potere di controllo datoriale in contesti organizzativi del lavoro pienamente digitalizzati».

Cnpd) e, il 5 gennaio 2012, il personale interessato. Sulla scorta dei dati raccolti tramite il Gps nel periodo novembre 2013 – maggio 2014, era stato avviato un procedimento disciplinare a carico del ricorrente addebitandogli di aver aumentato il numero di chilometri percorsi a titolo professionale rispetto a quelli percorsi a titolo personale; di aver manipolato il sistema Gps attraverso la rimozione della scheda Gsm; di non aver rispettato l'orario di lavoro. Il procedimento disciplinare era, poi, culminato nel licenziamento del dipendente.

Impugnato il licenziamento dinanzi al Tribunale di Vila Real, il giudice di prime cure aveva concluso per la legittimità del licenziamento con riferimento a tutte le contestazioni sollevate dall'azienda. In particolare, il Tribunale aveva ritenuto accertato che il ricorrente fosse stato informato sia sull'installazione del dispositivo Gps, sia della raccolta dei dati che del loro uso a fini disciplinari, e che la relativa installazione fosse stata correttamente comunicata anche alla Cnpd. Inoltre, tenuto conto delle finalità perseguite dalla società e della "assoluta indispensabilità" del veicolo per l'espletamento delle mansioni affidate al ricorrente, il Tribunale aveva considerato «comprensibile [*che la società volesse*] adottare misure per poter gestire razionalmente i mezzi che affida e per poter garantire che tali mezzi siano effettivamente utilizzati ai fini dell'esercizio delle funzioni professionali, e non per alcuna altro scopo» <sup>(9)</sup> (§ 42). Sicché, valutata non sproporzionata la sanzione disciplinare inflitta, il Tribunale aveva ritenuto il dispositivo Gps un mezzo di controllo legittimo che non rientrava nell'ambito del monitoraggio remoto e non violava la *privacy* o la dignità del lavoratore e che, pertanto, i dati raccolti da questo dispositivo fossero validi e giustificassero l'imputazione dei fatti contestati (§ 42).

Nelle more del giudizio di primo grado, adita da altro collega del ricorrente in merito a similari fatti di causa, la Cnpd aveva imposto un provvedimento conservativo con cui vietava – temporaneamente – alla società l'eventuale trattamento dei dati personali di geolocalizzazione fino a decisione definitiva del procedimento amministrativo, nonché l'utilizzo di eventuali dati personali precedentemente ottenuti nel corso del trattamento dei dati (§ 64), tra cui si dovevano annoverare anche quelli facenti capo al ricorrente. Il provvedimento era stato adottato sulla scorta della circostanza secondo cui, sebbene la società avesse informato la Cnpd dell'intenzione di utilizzare i dispositivi di geolocalizzazione, questa non aveva richiesto l'autorizzazione necessaria a tal fine, sicché, in assenza di tale autorizzazione, non avrebbe potuto avere inizio il trattamento dei dati dei dipendenti. Quanto, invece, al procedimento avviato dalla società a seguito della comunicazione alla Cnpd effettuata in data 24 novembre 2011, l'autorità amministrativa aveva emanato nell'ottobre 2015 la Delibera 1565/2015 con cui vietava alla società l'utilizzo dei sistemi Gps sui veicoli aziendali (§ 67). E tanto in quanto i dati di geolocalizzazione costituivano dati sensibili ai sensi della legge

---

<sup>(9)</sup> Traduzione a cura dell'A.

portoghese e, di conseguenza, il loro trattamento richiedeva l'autorizzazione della Cnpd. Il divieto è stato, poi, confermato da una successiva delibera adottata dalla Cnpd (§ 69) con cui l'autorità amministrativa aveva sì autorizzato l'utilizzo del sistema di geolocalizzazione, ma solo con riferimento ai mezzi di trasporto merci della società (§ 54), ribadendo che i dati di geolocalizzazione, in quanto dati personali, non potessero essere utilizzati per monitorare le prestazioni professionali di un dipendente. Altresì, specificava che quando il veicolo aziendale veniva utilizzato per scopi privati non dovessero essere trattati i dati di geolocalizzazione e che, quindi, l'azienda doveva trovare una soluzione per rendere la geolocalizzazione inaccessibile in quelle situazioni (§ 69).

Successivamente agli interventi dell'autorità amministrativa brevemente richiamati, il ricorrente impugnava la sentenza del Tribunale di Vila Real dinanzi alla Corte d'appello di Guimarães, adducendo la illegittimità delle prove acquisite nel procedimento disciplinare, in quanto il Gps costituiva un mezzo di sorveglianza vietato dal diritto portoghese <sup>(10)</sup> e, in ogni caso, il trattamento dei dati raccolti non solo non era stato autorizzato dalla Cnpd, ma era stato anche vietato con la Delibera 1565/2015, e lamentando, più in generale, la violazione del diritto al rispetto della sua vita privata. La Corte rigettava l'appello, confermando la cessazione del rapporto di lavoro, sulla scorta di un diverso *iter* argomentativo. In particolare, da un lato, riconosceva che l'utilizzo di un dispositivo Gps in un contesto professionale per controllare l'attività di un dipendente costituisse un mezzo di sorveglianza a distanza vietato *ex lege* potendo quest'ultimo, non solo rilevare la posizione approssimativa di una persona, ma anche l'ora di inizio e l'ora di fine di un viaggio, i luoghi di partenza e di arrivo, la distanza percorsa, la velocità, il tempo di circolazione e il tempo di sosta (§ 56). Pertanto, la Corte non confermava il *decisum* della sentenza di primo grado nella parte in cui giustificava il licenziamento anche con riferimento al mancato rispetto dell'orario di lavoro da parte del ricorrente. Dall'altro, ammettendo una gestione differenziata dei dati raccolti tramite Gps, riteneva che, diversamente dai dati relativi all'orario e al luogo di lavoro, quelli concernenti il chilometraggio non costituissero una sorveglianza a distanza e fossero, pertanto, leciti. Sulla base di queste premesse, la Corte considerava violato il dovere di lealtà in capo al ricorrente per aver impedito la corretta trasmissione dei dati di

---

<sup>(10)</sup> E, in particolare, dagli artt. 20 e 21 del *Código do Trabalho* che, rispettivamente, vietano l'utilizzo di mezzi di telesorveglianza nei luoghi di lavoro al fine di monitorare le prestazioni professionali del lavoratore (art. 20 co. 1), a meno che avesse come finalità la protezione e l'incolumità delle persone e dei beni, ovvero fosse giustificato da particolari esigenze inerenti alla natura dell'attività (art. 20 co. 2); subordinano l'utilizzo dei mezzi di telesorveglianza nei luoghi di lavoro all'autorizzazione del Garante nazionale per la protezione dei dati personali (art. 21 co. 1), fermo restando che il loro impiego dovesse essere necessario, adeguato e proporzionato alle finalità perseguite (art. 21 co. 2). Per un commento sulla disciplina portoghese si rinvia a T. Coelho Moreira, *The Electronic Control of the Employer in Portugal*, *LLI*, 2016, 2, 1, 4, e bibliografia ivi citata.

geolocalizzazione e per aver interferito con il funzionamento del dispositivo Gps, a tal punto da giustificare la risoluzione del rapporto di lavoro (§ 61).

Il rigetto dell'appello portava il ricorrente a presentare le proprie doglianze dinanzi alla Corte Edu deducendo, in particolar modo, la violazione del suo diritto al rispetto della vita privata sancito dall'art. 8 della Cedu, nonché, sotto il profilo processuale, la violazione del proprio diritto a un equo processo ex art. 6 Cedu, in quanto le Corti nazionali avevano fondato il loro convincimento su prove illegalmente assunte tramite il sistema Gps.

#### **a. I controlli a distanza e il rispetto al diritto alla vita privata al cospetto della Corte Edu: alcuni precedenti rilevanti**

Che il diritto al rispetto della “vita privata” sancito dall'art. 8 Cedu ricomprenda anche le attività professionali <sup>(11)</sup>, sia che abbiano luogo in un contesto privato che pubblico <sup>(12)</sup>, è un principio pacificamente accolto dalla Corte di Strasburgo. Invero, la Corte è a più riprese stata chiamata a verificare, nell'ambito degli obblighi negativi e positivi derivanti dall'art. 8 Cedu, se gli Stati membri non solo si siano astenuti dal porre in essere comportamenti potenzialmente lesivi della vita privata degli individui ma, soprattutto, se questi abbiano adottato misure idonee a garantire l'effettivo rispetto della loro vita privata o familiare, anche ove i comportamenti illegittimi siano stati perpetrati da soggetti privati <sup>(13)</sup>, come i datori di lavoro.

---

<sup>(11)</sup> Cfr. in tal senso Corte Edu, 16 dicembre 1992, *Niemietz c. Germany*, 13710/88, § 29 secondo cui «there appears, furthermore, to be no reason of principle why this understanding of the notion of “private life” should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world»; C. Edu, GC, 14 giugno 2014, *Fernández Martínez c. Spain*, 56030/07, § 110; C. Edu, GC, 5 settembre 2017, *Bărbulescu c. Romania*, 61496/08, § 71; C. Edu, GC, 17 ottobre 2019, *López Ribalda and others c. Spain*, 1874/13 – 8567/13, § 88.

<sup>(12)</sup> C. Edu, 28 gennaio 2003, *Peck c. Regno Unito*, 44647/98, § 58-59; principio ribadito, più recentemente, nella sentenza C. Edu, 28 Novembre 2017, *Antović and Mirković c. Montenegro*, 70838/13, § 42, in cui si afferma che «there is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life” [...], professional life being part of it». Il caso *Antović and Mirković c. Montenegro* attiene al ricorso presentato da due professori del polo universitario montenegrino a seguito dell'installazione di un sistema di videosorveglianza nelle aule universitarie in cui questi insegnavano, giustificato da motivi di tutela del patrimonio universitario e dell'incolumità personale, nonché dalla sorveglianza dell'insegnamento. La Corte Edu ha rilevato che una delle finalità per cui era stata introdotta la videosorveglianza e, in particolare, quella di controllare l'insegnamento, non era prevista dalla legge montenegrina come motivo di videosorveglianza (§ 59), sicché ha ritenuto violato l'art. 8 Cedu in quanto l'interferenza al diritto alla vita privata non era “conforme alla legge”.

<sup>(13)</sup> C. Edu, GC, 7 febbraio 2012, *Von Hannover c. Germany 2*, 40660/08 - 60641/08, § 98. Sugli obblighi negativi e positivi derivanti dall'applicazione dell'art. 8 Cedu si veda anche Consiglio d'Europa/Corte europea dei diritti dell'uomo, *Guida all'articolo 8 della Convenzione europea sui diritti dell'uomo*, aggiornata al 31 agosto 2021, disponibile al seguente link:

In generale, l'articolo 8 presenta una struttura bipartita<sup>(14)</sup>, in forza della quale nel primo comma viene enunciato il principio di diritto («ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza») e, nel secondo, le condizioni richieste affinché uno Stato possa ingerirsi nel godimento del diritto protetto. A tal proposito, le limitazioni sono considerate lecite ove siano “previste dalla legge” o “conformi alla legge” e siano “necessarie in una società democratica” per la tutela di “finalità legittime” specificate nell'articolo<sup>(15)</sup>.

Con particolare riferimento al diritto alla tutela della vita privata dei dipendenti nell'ambito del rapporto di lavoro, la Corte Edu si è più volte pronunciata sia in relazione all'utilizzo della videosorveglianza manifesta (Corte Edu, 28 novembre 2017, *Antović and Mirković c. Montenegro*, 70838/13) o occulta (più recentemente, Corte Edu, GC, 17 ottobre 2019, *López Ribalda and others c. Spain*, 1874/13 – 8567/13), che con riferimento all'accesso alle comunicazioni dei dipendenti (più recentemente, Corte Edu, GC, 5 settembre 2017, *Bărbulescu c. Romania*, 61496/08) nonché dei loro *file* informatici privati presenti all'interno del computer aziendale (Corte Edu, 2 luglio 2018, *Libert c. France*, 588/13).

Quanto al caso di specie, nonostante la causa *Gramaxo c. Portugal* differisca rispetto ai precedenti richiamati in ordine alla tipologia dei dati trattati, soffermarsi sulle decisioni più rilevanti della Corte di Strasburgo è significativo per almeno due ordini di ragioni. In primo luogo, questi stessi principi di diritto costituiscono – per espresso richiamo – la base giuridica del c.d. “test di proporzionalità”<sup>(16)</sup> che ha condotto alla decisione in commento. In secondo luogo, i precedenti consentono di cogliere un cambio di paradigma nell'interpretazione della Corte Edu nel bilanciamento possibile tra i contrapposti interessi, che oscilla tra la prevalenza attribuita, ora alla conoscibilità del controllo, ora ai vincoli derivanti dalle normative nazionali in tema di protezione di dati personali, con evidenti ripercussioni in tema di violazione, o meno, dell'art. 8 Cedu.

La legittimità del controllo a distanza sulle comunicazioni private dei lavoratori è già stata affrontata in numerose occasioni dalla Corte Edu che ha, tendenzialmente

---

[https://www.echr.coe.int/documents/guide\\_art\\_8\\_ita.pdf](https://www.echr.coe.int/documents/guide_art_8_ita.pdf); A. Stolfa, *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, LG, 2018, 5, 534.

<sup>(14)</sup> F. Perrone, *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Diritti dell'Uomo e giurisdizione nazionale dopo la sentenza Bărbulescu*, Labor, 2018, 3, 286.

<sup>(15)</sup> L'art. 8, co. 2, Cedu sancisce che «non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui».

<sup>(16)</sup> A. Sitzia - M. I. Ramos Quintana, *Sorveglianza difensiva “occulta” sui luoghi di lavoro e dignità nella prospettiva della Grande Camera della Corte EDU: la Sentenza López, LDE*, 2019, 3, 10.

(17), riscontrato la violazione dell'art. 8 Cedu. Si pensi al caso *Halford c. the United Kingdom* (18) in cui la ricorrente lamentava che le sue telefonate in ufficio e a casa fossero state intercettate dal datore di lavoro allo scopo di ottenere informazioni da utilizzare contro di lei nel procedimento da questa intentato per discriminazione di genere; o ancora al caso *Copland c. the United Kingdom* (19) avente a oggetto il monitoraggio, su iniziativa del superiore gerarchico, del telefono, della posta elettronica e dell'uso di internet da parte della ricorrente. In entrambi i casi, la C. Edu ha dichiarato la violazione dell'art. 8 Cedu ritenendo che la raccolta e l'archiviazione di informazioni personali relative all'uso del telefono, della posta elettronica e di internet da parte del lavoratore, e a sua insaputa, costituissero un'interferenza non "conforme alla legge" del suo diritto al rispetto della vita privata e della corrispondenza.

Alle medesime conclusioni, seppur seguendo un *iter* argomentativo differente, è giunta la *Grand Chambre* nella decisione *Bărbulescu c. Romania*. Il caso riguardava il licenziamento di un ingegnere romeno sulla base del controllo svolto dal datore di lavoro con riferimento alla *chat* dell'*account* aziendale *Yahoo Messenger* di cui era stato verificato l'utilizzo a fini privati in violazione del regolamento aziendale. Ribaltando la pronuncia della sezione semplice (20), la *Grand Chambre* ha accolto il ricorso del ricorrente (21), ritenendo non provato l'assolvimento dell'obbligo informativo in capo al datore di lavoro circa la possibilità che le comunicazioni che effettuava mediante l'*account* aziendale avrebbero potuto essere monitorate, né del carattere o della portata del monitoraggio o del livello di intrusività del controllo nella sua vita privata e nella sua corrispondenza (§ 140). Per quanto di maggiore interesse per la causa in oggetto, nel ritenere che le autorità interne dovessero garantire che «l'introduzione da parte del datore di lavoro di misure di monitoraggio della corrispondenza e delle altre

---

(17) Nel caso *Adomaitis v. Lithuania*, riguardante il monitoraggio e l'intercettazione delle telefonate del governatore di un carcere sospettato di aver assicurato, dietro compenso, migliori condizioni ai detenuti e di aver concesso loro degli incentivi, la Corte Edu non ha ritenuto violato l'art. 8 Cedu, ravvisando la necessità e la proporzionalità dell'interferenza nella vita privata del ricorrente e il fine legittimo perseguito (la prevenzione di disordini o crimini e la protezione dei diritti e delle libertà altrui § 84). Le intercettazioni erano state autorizzate nell'ambito di un'indagine penale aperta a carico del ricorrente e interrotta dopo un anno per mancanza di prove incriminanti. Tuttavia, l'uso delle informazioni raccolte è stato consentito nei procedimenti disciplinari che, alla fine, hanno portato al suo licenziamento (Corte Edu, 18 gennaio 2022, *Adomaitis v. Lithuania*, 14833/18).

(18) Corte Edu, 25 giugno 1997, *Halford c. the United Kingdom*, 20605/92.

(19) Corte Edu, 3 aprile 2007, *Copland c. the United Kingdom*, 62617/00.

(20) Per il cui commento critico si rinvia, *ex pluribus*, a A. Ingraio, *Il "cyberslacking" e i diritti del lavoratore "catturato nella rete informatica". Note critiche a margine della sentenza della Corte Europea dei diritti dell'uomo, sez. IV, 12 gennaio 2016, n. 61496, Bărbulescu vs. Romania, in attesa della pronuncia della Grande Camera, Osservatorio AIC, 2016, 3, 621; D. Pizzonia - A. Sitzia, Il controllo del datore di lavoro su Internet e posta elettronica: quale riservatezza sul luogo di lavoro?, NGCC, 2016, 6, 1, 901.*

(21) C. Carta, *Corte europea dei diritti dell'uomo: la Grande camera torna sul (e difende il) diritto alla privacy del lavoratore*, [www.rivistalabor.it](http://www.rivistalabor.it), 2017; F. Perrone, *La tutela della privacy sul luogo di lavoro*, cit.

comunicazioni, indipendentemente dalla portata e dalla durata di tali misure, [fosse] accompagnata da adeguate e sufficienti garanzie contro gli abusi» (§ 120), la *Grand Chambre* individua in *Bărbulescu c. Romania* un decalogo di principi generali che devono orientare l'interprete nella valutazione della fattispecie concreta. Si tratta di verificare se: (i) sia stato adempiuto, da parte datoriale, l'obbligo di una preventiva e chiara comunicazione circa l'eventuale controllo sulla corrispondenza e sulle altre comunicazioni del lavoratore; (ii) siano individuati limiti temporali e spaziali del monitoraggio, anche con riferimento ai dati trattati; (iii) siano stati forniti motivi legittimi a giustificazione del monitoraggio; (iv) vi fossero mezzi meno invasivi per il raggiungimento delle medesime finalità; (v) siano state comunicate le conseguenze in cui può incorrere il dipendente sottoposto a monitoraggio; (vi) siano state fornite al dipendente «adeguate garanzie» ove il monitoraggio possa risultare particolarmente invasivo. In ultimo, deve essere garantito al lavoratore l'accesso a un rimedio dinanzi a un organo giudiziario che possa verificare se le condizioni elencate siano o meno state soddisfatte.

I medesimi principi stabiliti dalla *Grand Chambre* in *Bărbulescu c. Romania* sono stati trasposti, *mutatis mutandis*, anche al caso *López Ribalda and others c. Spain* concernente la videosorveglianza occulta dei cassieri di un supermercato introdotta a fronte di alcune discrepanze riscontrate tra i guadagni giornalieri e il livello degli *stock* in magazzino <sup>(22)</sup>. Nel caso di specie, la *Grand Chambre*, ribaltando la pronuncia della sezione semplice e sviluppando un ragionamento che prende le mosse dall'analogo caso *Köpke c. Germany* <sup>(23)</sup>, ha ritenuto il controllo a distanza giustificato da legittime finalità, ovvero il sospetto di furto; la misura di controllo adottata proporzionata con riferimento alle aree sottoposte a sorveglianza e al personale monitorato; la durata della videosorveglianza – pari a 10 giorni – non eccedente rispetto a quanto necessario per confermare i sospetti di furto; la riservatezza tutelata da un limitato accesso da parte di soggetti autorizzati alle immagini registrate. Inoltre, enfatizzando non solo la disciplina nazionale in materia di protezione dei dati personali vigente all'epoca dei fatti <sup>(24)</sup>, ma anche il ruolo svolto

---

<sup>(22)</sup> Su cui si rinvia a A. Sitzia - M. I. Ramos Quintana, Sorveglianza difensiva “oculta” sui luoghi di lavoro, cit.; A. Ciriello, Videosorveglianza “oculta” sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo, LDE, 2019, 3; L. Tebano, I confini dei controlli difensivi e gli equilibrismi della Corte Edu, RIDL, 2020, II, 211; V. Nuzzo, Il ragionevole sospetto di illecito e la possibilità di controlli difensivi occulti all'esame della Grande Camera della Corte Europea dei diritti dell'uomo, Labor, 2020, 2, 208.

<sup>(23)</sup> Concernente un sistema di videosorveglianza occulto installato in un supermercato quale conseguenza del sospetto di ammanchi in uno dei reparti che ha portato al licenziamento di due dipendenti. La videosorveglianza, diretta verso due soli dipendenti, limitata nel tempo e nello spazio, limitata con riferimento ai soggetti aventi accesso ai dati trattati, ha condotto la Corte Edu a dichiarare inammissibile il ricorso sostenendo che le Corti nazionali avevano correttamente bilanciato i diversi interessi in gioco (Corte Edu, 5 ottobre 2010, *Köpke v. Germany*, 420/07).

<sup>(24)</sup> Il riferimento è alla *Ley Orgánica de protección de datos de carácter personal n. 15/1999* e la *Instrucción 1/2006* dell'8 novembre 2006 della Agencia Española de Protección de Datos «sobre el tratamiento de

dall'autorità garante spagnola – attraverso l'esplicito richiamo alla *Instrucción 1/2006* <sup>(25)</sup> – la Corte Edu ha sottolineato come nel caso di specie non esistevano altri mezzi per realizzare la finalità legittima perseguita dal datore di lavoro e che la misura doveva quindi essere considerata “necessaria”. Pertanto, conclude la *Grand Chambre*, i Tribunali nazionali hanno effettuato un corretto bilanciamento tra il diritto al rispetto della vita privata dei ricorrenti <sup>(26)</sup>, da un lato, e l'interesse del datore di lavoro a garantire la tutela dei suoi beni e il buon funzionamento dell'azienda, dall'altro, non riscontrando alcuna violazione dell'art. 8 Cedu.

Gli arresti della Corte Edu in materia di controlli a distanza nel luogo di lavoro e rispetto della vita privata dei lavoratori insistono, in particolar modo, su alcuni elementi rinvenibili nella legittimità dello scopo per cui il controllo è posto in essere e, soprattutto, nella consapevolezza del lavoratore <sup>(27)</sup>, ammettendo la legittimità del c.d. “controllo occulto” <sup>(28)</sup> solo se esercitato entro determinati limiti temporali e spaziali, sicché sia salvaguardata la dignità del sorvegliato. Inoltre, nel garantire la conformità alla legge richiesta dall'art. 8, co. 2 Cedu nella limitazione del diritto alla vita privata, la Corte di Strasburgo enfatizza il rispetto della normativa interna in materia di protezione dei dati personali, *ratione temporis* applicabile, e il ruolo dei Garanti nazionali per la protezione dei dati personali consolidando il binomio tra disciplina lavoristica e rispetto della privacy.

Date queste premesse, ci si soffermerà sull'applicazione di questi stessi principi al caso *Gramaxo c. Portugal* alla ricerca di una linea di (dis)continuità nel bilanciamento di interessi contrapposti.

## **b. Decisione della Corte Edu e *dissenting opinion***

Ritenuto applicabile l'art. 8 Cedu al caso di specie, nell'ambito degli obblighi positivi incombenti sullo Stato ai sensi del medesimo articolo, la Corte Edu ha rilevato l'esistenza, *ratione temporis*, di un quadro normativo inteso a tutelare la vita privata dei dipendenti nel luogo di lavoro rinvenibile nel combinato disposto delle garanzie in

---

datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras», entrambe richiamate in Corte Edu, GC, 17 ottobre 2019, *López Ribalda and others c. Spain*, cit., § 45-50; § 129.

<sup>(25)</sup> Si tratta della *Instrucción 1/2006*, cit., espressamente richiamata dalla Corte Edu, GC, anche al § 129.

<sup>(26)</sup> Pur limitato nella “*expectation of privacy*” in quanto le mansioni dei ricorrenti erano svolte in un luogo aperto al pubblico e comportavano il contatto permanente con i clienti (Corte Edu, GC, 17 ottobre 2019, *López Ribalda and others c. Spain*, cit., § 125).

<sup>(27)</sup> A. Sitzia - M. I. Ramos Quintana, *Sorveglianza difensiva “occulta” sui luoghi di lavoro*, cit., 11.

<sup>(28)</sup> Tanto da sollevare le critiche di coloro che ritengono la pronuncia idonea ad attribuire «nuova linfa» al dibattito – invero, mai sopito – sulla legittimità dei c.d. “controlli difensivi” nel contesto nazionale a fronte della modifica intervenuta sull'art. 4 St. lav. a opera dell'art. 23, co. 1, d.lgs. n. 151/2015, cfr. L. Tebano, *I confini dei controlli difensivi e gli equilibri della Corte Edu*, RIDL, 2020, II, 214-215; A. Bellavista, *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, LDE, 2023, 1, 5.

materia di protezione dei dati <sup>(29)</sup> contenute nella *Lei da Protecção de Dados Pessoais* n. 67/1998 (d'ora in poi, Lpdp) e gli artt. 20 e 21 del *Código do Trabalho*. Pertanto, la Corte Edu ha dovuto verificare se i giudici nazionali avessero o meno garantito, nella ponderazione degli interessi in gioco, una tutela sufficiente del diritto del ricorrente al rispetto della sua vita privata e se avessero applicato i criteri del “test della proporzionalità” elaborati in *Bărbulescu c. Romania*.

In primo luogo, la Corte rileva che il ricorrente era stato preventivamente informato non solo dell'installazione del dispositivo Gps, ma anche delle finalità (monitoraggio dei chilometri percorsi) e del possibile utilizzo di tali dati in un procedimento disciplinare. In secondo luogo, la Corte ritiene che, nell'operare una gestione differenziata dei dati Gps considerando solo quelli relativi al chilometraggio percorso, la Corte di Appello avesse «réduit l'ampleur de l'intrusion dans la vie privée du requérant» (§ 120) a quanto strettamente necessario allo scopo legittimo perseguito, ossia il controllo delle spese aziendali, e che tale scopo non potesse essere perseguito con mezzi meno intrusivi. In ultimo, constata che la diffusione delle informazioni era stata limitata a specifici soggetti.

Sulla base di queste considerazioni, la Corte di Strasburgo conclude per la non violazione dell'art. 8 Cedu.

Nell'analisi della pronuncia, un'attenzione particolare deve essere attribuita alla *dissenting opinion* espressa da tre dei sette giudici della sezione semplice. E tanto in quanto, al pari dei casi *Bărbulescu c. Romania* e *López Ribalda and others c. Spain*, questa avrebbe potuto rivelarsi foriera di un probabile, ma non più possibile <sup>(30)</sup>, *revirement* a opera della *Grand Chambre*. In particolare, i giudici dissenzienti non hanno ritenuto equilibrato il bilanciamento effettuato dalla maggioranza, essendo «l'ingérence de l'employeur dans la vie privée du salarié [...] très sérieuse» (§ 10). In effetti, il potere di controllo poteva essere esercitato in tempo reale e in maniera continuata 24 ore su 24, 7 giorni su 7, intaccando, inevitabilmente, anche i periodi di non lavoro. In più, i dipendenti non potevano disattivare in alcun modo il sistema di geolocalizzazione. I giudici dissenzienti hanno, inoltre, evidenziato come la Corte d'Appello avesse completamente ignorato «sans aucune justification raisonnable» (§ 14) le decisioni assunte dalla Cnpd nelle more del giudizio e, in ogni caso, prima della sentenza di secondo grado, nelle quali: veniva affermata l'illegittimità della geolocalizzazione quando l'auto aziendale veniva utilizzata in modo promiscuo <sup>(31)</sup>; veniva vietato alla società l'uso dei Gps sui veicoli aziendali dei dipendenti <sup>(32)</sup>; veniva autorizzato l'uso dei Gps ma solo con riferimento ai mezzi di

---

<sup>(29)</sup> Come il diritto all'informazione (art. 10), il diritto di opposizione (art. 12) esercitato anche dal ricorrente, nonché la predisposizione di un *iter* autorizzatorio per il trattamento lecito (artt. 23, 27, 28), il cui mancato rispetto poteva essere sanzionato dalla relativa autorità garante Cnpd (art. 43).

<sup>(30)</sup> Infatti, la sentenza è divenuta definitiva *ex art.* 44, co. 2, Cedu in data 3 aprile 2023.

<sup>(31)</sup> Cnpd, Delibera n. 7680/2014 del 28 ottobre 2014, per cui si rinvia al § 79 della sentenza.

<sup>(32)</sup> Cnpd, Delibera n. 1565/2015 del 6 ottobre 2015 (§ 67).

trasporto merci della società, ribadendo che non poteva esserci geolocalizzazione quando il veicolo aziendale veniva utilizzato per scopi privati e che, in ogni caso, l'azienda avrebbe dovuto trovare una soluzione per rendere inaccessibile la geolocalizzazione fuori dall'orario di lavoro <sup>(33)</sup>.

A ciò si aggiunga che il trattamento dei dati personali del ricorrente (relativi alla geolocalizzazione del veicolo) ha avuto inizio prima del rilascio dell'autorizzazione da parte della Cnpd richiesta *ex art.* 28, co. 1, Lpdp e, tra l'altro, concessa in un secondo momento ma limitatamente ai soli veicoli che trasportavano merci.

I giudici dissenzienti hanno anche contestato la circostanza di diritto posta alla base della sentenza della Corte d'Appello secondo cui il controllo sui chilometri percorsi *al di fuori* dell'orario di lavoro (corsivo dell'A.), e posti alla base del licenziamento del ricorrente (§ 8), fosse legittimo in quanto non rientrava nell'ambito del controllo delle sue prestazioni professionali <sup>(34)</sup>. La distinzione in merito al trattamento dei dati di geolocalizzazione, escluso solo durante l'orario di lavoro, è stata considerata arbitraria a tal punto da aver spinto i giudici dissenzienti a ritenere che «le manque de diligence de l'entreprise se trouve paradoxalement récompensé en fin de compte, sans que la vie privée du salarié ait été suffisamment protégée par les tribunaux internes» (§ 16). Infine, viene contestato ai Tribunali nazionali di non aver riconosciuto la possibilità di utilizzare, per il raggiungimento dello scopo di tutela del patrimonio aziendale, strumenti meno invasivi, come l'installazione di un interruttore per distinguere l'uso personale dell'auto aziendale da quello professionale, come anche richiesto dalla Cnpd.

### 2.3. Prove di bilanciamento possibile

Alla luce delle osservazioni sin qui condotte, la decisione a cui perviene la Corte Edu in *Gramaxo c. Portugal* non può che destare perplessità. L'impressione è che dinanzi al caso concreto, la Corte di Strasburgo abbia dato prevalenza alla conoscibilità del controllo da parte del lavoratore rispetto alla tutela della sua riservatezza, assicurata dalla normativa nazionale sulla protezione dei dati personali, sulla scorta della mera gestione differenziata del dato trattato (dato chilometrico).

Piuttosto, anche con riferimento ai propri precedenti, non è stato opportunamente preso in considerazione il principio di minimizzazione, volto a individuare se vi fossero mezzi meno invasivi per il raggiungimento delle medesime finalità, rinvenuti, poi, dalla stessa Autorità garante portoghese, nella possibilità di

---

<sup>(33)</sup> Cnpd, Delibera n. 11891/2015 del 3 dicembre 2015 (§ 69).

<sup>(34)</sup> Si riporta, per completezza, il passaggio della *dissenting opinion* § 12, secondo cui «dorsque la cour d'appel de Guimarães a confirmé le licenciement de l'employé, elle a estimé, notamment, que le comptage des kilomètres parcourus par lui en dehors de ses horaires de travail – pendant la période allant de novembre 2013 à mai 2014 – était légal, car ne relevant pas du contrôle de ses performances professionnelles» (corsivo dell'A.)

garantire il c.d. principio di esclusione e consentire, dunque, al lavoratore di poter disattivare il tracciamento della posizione durante l'utilizzo privato del veicolo. Di conseguenza, non sono stati individuati nel caso di specie dei limiti temporali e spaziali del monitoraggio, estendendosi questo, anche agli spostamenti privati e decretando una sproporzionata intrusione nella vita privata del ricorrente. Infatti, sebbene i dati utilizzati nel procedimento di impugnazione del licenziamento siano stati limitati, dalla Corte di Appello, ai soli dati chilometrici, è evidente che il sistema di geolocalizzazione, come anche riconosciuto dal Governo, consentisse a ogni modo di accedere anche altri dati, come l'ora di inizio e l'ora di fine del viaggio, i luoghi di partenza e arrivo, chilometri percorsi, velocità, tempo di sosta nel traffico e tempo di sosta (§ 40). Ma, per quanto più rilevante ai fini della presente trattazione, è indicativo il non aver tenuto conto delle delibere dell'Autorità garante portoghese emanate nelle more del giudizio dinanzi ai Tribunali nazionali, nonché la procedura autorizzatoria prescritta dal diritto interno per il caso di utilizzo di mezzi di monitoraggio a distanza <sup>(35)</sup>.

E tanto, infatti, è ancora più evidente ove si tenga conto delle indicazioni – benché non vincolanti – (come linee guida, raccomandazioni, buone pratiche) fornite dai documenti dell'organo consultivo indipendente dell'Unione Europea per la protezione dei dati e della privacy (Gruppo di lavoro articolo 29, d'ora in poi, WP29), oggi sostituito dal Comitato europeo per la protezione dei dati, istituito all'art. 68 del Gdpr, a cui le stesse autorità garanti nazionali si conformano. In particolare, il WP29, proprio con riferimento ai dati di geolocalizzazione di strumenti di lavoro autorizzati per uso promiscuo, aveva indicato già nell'*Opinion 13/2011* <sup>(36)</sup> e ribadito, successivamente, nell'*Opinion 2/2017* <sup>(37)</sup>, che il datore di lavoro dovesse assicurare al lavoratore «the option to temporarily turn off location tracking when special circumstances justify this turning off». Anche con riferimento a tali atti, la Corte Edu sembra discostarsi significativamente.

In virtù degli elementi evidenziati, è verosimile ritenere che, se vi fosse stato un giudizio dinanzi alla *Grand Chambre*, questa avrebbe potuto, ancora una volta, ribaltare la pronuncia della sezione semplice e considerare, di conseguenza, non superato il “test della proporzionalità”, avendo, piuttosto, la Corte Edu fatto prevalere la conoscenza del

---

<sup>(35)</sup> Il riferimento, lo si ricorda, è alla disciplina autorizzatoria prevista dal combinato disposto dell'art. 21 del *Código do Trabalho*, secondo cui «l'utilizzo di mezzi di tele sorveglianza nei luoghi di lavoro è subordinato all'autorizzazione del Garante nazionale per la protezione dei dati personali» e degli artt. 23 e 28 della Lpdp che individuano le competenze della Cnpd, tra cui quella autorizzatoria al trattamento dei dati personali.

<sup>(36)</sup> WP29, *Opinion 13/2011 on Geolocation services on smart mobile devices*, 16 maggio 2011, 14, la quale specifica che «an employee must be able to turn off any monitoring device outside of work hours and must be shown how to do so. Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle».

<sup>(37)</sup> WP29, *Opinion 2/2017 on data processing at work*, 8 giugno 2017, 20.

controllo da parte del lavoratore (pur necessaria, tanto che la prova non raggiunta aveva condotto la *Grand Chambre* nel caso *Bărbulescu c. Romania* a ribaltare la pronuncia della sezione semplice) al legittimo trattamento del dato personale secondo la normativa vigente all'epoca dei fatti e al ruolo della corrispondente autorità garante (enfaticizzato<sup>(38)</sup>, invece, in *López Ribalda and others c. Spain*).

### 3. Riflessi sul diritto interno: i limiti al potere di controllo a distanza tra norme statutarie, Codice privacy e Gdpr

La mancata attenzione della Corte di Strasburgo verso la procedimentalizzazione del potere datoriale prescritta *ex lege*, nonché il non aver considerato le posizioni dell'Autorità garante nazionale, costituisce un *vulnus* non irrilevante rispetto alla violazione del diritto alla privacy dei lavoratori. Infatti, è sempre più centrale il ruolo che le autorità di controllo rivestono negli ordinamenti nazionali, potenziato anche dalle normative unionali<sup>(39)</sup>, nella loro funzione di organismi amministrativi indipendenti deputati a controllare l'applicazione della disciplina in materia di privacy «al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione» (art. 51 Gdpr).

E tanto, è ancora più significativo ove si tenga conto del quadro normativo sovranazionale in materia di dati personali in costante evoluzione. Infatti, sebbene si assista a un cambio di paradigma delle politiche europee, che muovono dalla *Data Protection* alla *Data Governance*, le tutele apprestate con il Gdpr continuano pur sempre a prevalere<sup>(40)</sup>, soprattutto nel rapporto di lavoro «where the employer has significant powers with regard to employees and any abuse of those powers should be avoided»<sup>(41)</sup>.

A tal proposito, l'esercizio del potere di controllo a distanza del datore di lavoro costituisce un trattamento di dati personali del lavoratore ai sensi dell'art. 4, co. 1, n. 2),

---

<sup>(38)</sup> Si vedano, a tal proposito, le considerazioni di A. Sitzia - M. I. Ramos Quintana, *Sorveglianza difensiva "occulta" sui luoghi di lavoro*, cit., 11-14, sebbene con riferimento ai controlli occulti di carattere difensivo; nonché Corte Edu, GC, 17 ottobre 2019, *López Ribalda and others c. Spain*, cit., § 129.

<sup>(39)</sup> Il riferimento è all'art. 28 della Dir. 95/46/Ce che definiva poteri e compiti dell'autorità di controllo di cui ogni Stato membro doveva disporre, oggi abrogata dal Reg. (UE) 2016/679 il quale, agli artt. 51 ss., disciplina in maniera più articolata le competenze, i compiti e i poteri delle autorità di controllo nazionali, ivi ricomprendendovi gli obblighi in materia di cooperazione con le altre autorità di controllo nei casi stabiliti dallo stesso Gdpr.

<sup>(40)</sup> Il riferimento è alla «Strategia europea per i dati» avviata dalle Istituzioni europee per il periodo 2019-2024 nell'ambito del quale si inserisce il recente *Data Governance Act* (Dga) adottato con Regolamento (Ue) del 30 maggio 2022, n. 868 che, al considerando 4, sancisce la prevalenza del Gdpr e delle disposizioni nazionali adottate conformemente a tale disciplina. Per una prima lettura si rinvia a A. Trojsi, *Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, 2022, 4, 276; D. Poletti, *Gli intermediari dei dati*, *EJPLT*, 2022, 1.

<sup>(41)</sup> Corte Edu, GC, 17 ottobre 2019, *López Ribalda and others c. Spain*, cit., § 131.

Gdpr, e, guardando al nostro ordinamento interno, trova una esplicita delimitazione nella normativa in materia di protezione dei dati personali, secondo quanto espressamente stabilito dall'art. 4, co. 3, St. lav., così come novellato dall'art. 23, co. 1, d.lgs. n. 151/2015. Soffermarsi sulla disciplina interna è, quindi, di interesse al fine di apprezzare il ruolo chiave rivestito dalla disciplina privacy, così come elaborata dalla autorità garante nazionale, anche con riferimento alla installazione di geolocalizzatori sulle vetture aziendali.

L'articolo 4, invero, consente la «utilizzabilità a tutti i fini connessi al rapporto di lavoro» delle informazioni raccolte dagli strumenti dai quali possa derivare «anche la possibilità di controllo a distanza dell'attività dei lavoratori» sottoposti alla procedura codeterminativa sindacale o amministrativa per determinate finalità (art. 4, co. 1, St. lav.), nonché dagli «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze» (art. 4, co. 2, St. lav.), purché «sia data al lavoratore adeguata informazione» e sia rispettato «quanto disposto dal decreto legislativo 30 giugno 2003, n. 196» (art. 4, co. 3, St. lav.). La novella del 2015 ha, dunque, integrato la disciplina dei controlli a distanza con quella della tutela del diritto alla protezione dei dati personali rendendo lecito il controllo e, di conseguenza, utilizzabile il dato <sup>(42)</sup>, solo ove le informazioni siano state raccolte ai sensi – e nei limiti procedurali e finalistici – dei commi 1 e 2 e sia, contestualmente, stata garantita l'adeguata informazione e il rispetto del c.d. Codice della privacy <sup>(43)</sup>, così come integrato dal Gdpr. L'esplicito richiamo al Codice della privacy impone, ora, ai giudici del lavoro la diretta applicazione dei principi fissati non solo dal codice, ma anche dal Garante per la protezione dei dati personali (d'ora in poi, Garante privacy) <sup>(44)</sup>, il quale ha anche il potere di «adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento» <sup>(45)</sup>. Il riferimento è ai principi della *privacy by design* e *privacy by default* che impongono al titolare del trattamento-datore di lavoro di mettere in atto misure tecniche e organizzative adeguate, rispettivamente, a proteggere i dati già dalla fase della progettazione del trattamento stesso (art. 25, co. 1, Gdpr) e a garantire che siano trattati, «per impostazione predefinita», solo i dati personali

---

<sup>(42)</sup> Sull'utilizzabilità dei dati raccolti si veda 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; C. Gamba, *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, LLI, 2016, 2, 1, 122.

<sup>(43)</sup> D.lgs. n. 196/2003, come integrato dal d.lgs. n. 101/2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. (Ue) 2016/679.

<sup>(44)</sup> Considerate «il perno e il motore per la costruzione di un'efficace tutela della persona del lavoratore contro lo straripare del potere di controllo del datore di lavoro», così in M. T. Carinci, *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, 59.

<sup>(45)</sup> Art. 154-bis d.lgs. n. 196/2003, introdotto dall'art. 14, co. 1 lett. d) del d.lgs. n. 101/2018.

necessari per ogni specifica finalità del trattamento (art. 25, co. 2, Gdpr). L'introduzione di tali principi, connessi a quelli attinenti alla liceità del trattamento che può perseguire un legittimo interesse del datore purché non prevalgano gli interessi o i diritti o le libertà fondamentali dei lavoratori (art. 6, co. 1, lett. f), Gdpr), nonché ai principi generali del trattamento di cui all'art. 5 Gdpr <sup>(46)</sup>, concorrono a decretare il passaggio dal sistema autorizzatorio previsto dalla precedente Dir. 95/46/Ce al principio generale dell'*accountability* del titolare del trattamento <sup>(47)</sup> sancito all'art. 24 Gdpr. Il datore di lavoro, dunque, non è libero di scegliere gli strumenti attraverso cui esercitare il potere di controllo ma è vincolato, nell'organizzare la propria struttura, a individuare i dispositivi e le misure in grado di limitare a monte, e quanto più possibile, il trattamento dei dati personali del lavoratore <sup>(48)</sup>. Inoltre, in ossequio al principio di responsabilizzazione, il titolare del trattamento dovrà non solo valutare la conformità del trattamento che intende effettuare ma, qualora il trattamento, per la particolare tecnologia utilizzata, sia suscettibile di presentare un rischio elevato per i diritti e le libertà dei lavoratori, il datore dovrà effettuare una valutazione d'impatto sulla protezione dei dati (art. 35, co. 1, Gdpr) <sup>(49)</sup> ovvero attivare la consultazione preventiva dell'autorità di controllo ai sensi dell'art. 36 del Gdpr.

Questi principi concorrono a costruire l'impalcatura del trattamento lecito dei dati personali anche del prestatore di lavoro, non vietandolo *tout court*, ma limitandolo entro rigidi schemi di prevenzione e responsabilizzazione del titolare del trattamento-datore di lavoro, in un costante tentativo di contemperare gli interessi delle parti all'interno di un rapporto contrattuale, per sua natura, asimmetrico.

#### **a. *Segue.* Il Gps tra norme statutarie e provvedimenti amministrativi del Garante privacy**

Con specifico riferimento alla rilevazione della posizione del veicolo aziendale affidato al dipendente a mezzo del Gps ci si pone, preliminarmente, la questione se, in

---

<sup>(46)</sup> Riassumibili nei principi di correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; responsabilizzazione.

<sup>(47)</sup> Come evidenziato da A. Ingraio, Il potere di controllo a distanza sull'attività lavorativa e la nuova disciplina della privacy nella sfida delle nuove tecnologie, in *Nuove tecnologie e diritto del lavoro. Un'analisi comparata degli ordinamenti italiano, spagnolo e brasiliano*, a cura di G. Ludovico - F. Fita Ortega - T. Christina Nahas, Milano University Press, 2021, 130, la quale sottolinea come il Regolamento trasponga il modello preventivo già implementato in materia di salute e sicurezza dei lavoratori alla tutela della privacy.

<sup>(48)</sup> M. T. Carinci, Il controllo a distanza sull'adempimento della prestazione di lavoro, cit., 58.

<sup>(49)</sup> La quale deve essere effettuata, ad esempio, anche nel caso in cui sia introdotta una sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35, co. 3, lett. c), Gdpr), come avvenuto nel citato caso *Antović and Mirković c. Montenegro* giunto dinanzi alla Corte Edu, per cui si rinvia alla nt. (12).

base alla disciplina nazionale, il sistema di geolocalizzazione possa essere considerato uno strumento di controllo, ai sensi dell'art. 4 co. 1, o uno strumento di lavoro, ai sensi dell'art. 4 co. 2 e, in secondo luogo, in che modo ed entro quali limiti il trattamento dei dati di geolocalizzazione su veicolo aziendale intersechi la disciplina adottata in materia di protezione dei dati personali.

Quanto al primo aspetto, è evidente che, se il Gps fosse considerato uno strumento di controllo, allora potrebbe essere installato sugli strumenti utilizzati per rendere la prestazione lavorativa, come *tablet*, *smartphone*, *smartwatch*, auto aziendali, solo per specifiche finalità riscontrabili nelle esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e previo accordo collettivo stipulato dalla Rsu o Rsa o, in assenza di accordo, previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro <sup>(50)</sup>.

Ove, invece, il Gps fosse considerato uno strumento di lavoro <sup>(51)</sup>, sarebbe esente dalla procedura codeterminativa appena descritta. Il *discrimen* tra gli "strumenti" di cui al comma 1 e quelli di cui al comma 2 è riscontrabile nella indispensabilità, intesa come stretta correlazione funzionale, tra gli strumenti di cui il lavoratore viene dotato e quelli strettamente necessari per l'esecuzione in concreto delle mansioni affidate al lavoratore. Pertanto, non è possibile individuare una definizione univoca di strumenti di lavoro, essendo strettamente connessi alle circostanze di fatto, al grado di tecnologia che caratterizza l'organizzazione datoriale, nonché alle mansioni concretamente svolte dal prestatore di lavoro. In materia, è direttamente intervenuto l'Ispettorato nazionale del lavoro che, con la circolare n. 2 del 2016, ha specificato che «in linea di massima» i Gps rappresentano un elemento "aggiuntivo" allo strumento di lavoro (come l'autovettura) e, dunque, non utilizzato in via primaria ed essenziale per l'esecuzione dell'attività lavorativa quanto, piuttosto, per rispondere a esigenze ulteriori aventi carattere

---

<sup>(50)</sup> Così in M. T. Carinci, *op. cit.*, 52-53 secondo cui il Gps inserito nello *smartphone* dei fattorini addetti alla consegna di plichi funzionale a distribuire in modo più efficiente il lavoro costituisca uno strumento organizzativo e produttivo soggetto, pertanto, alle regole del comma 1; A. Ingraio, *Il controllo a distanza sulla prestazione dei ciclofattorini*, *cit.*, 168-169. In giurisprudenza, si veda più recentemente, A. Roma, 22 febbraio 2021, n. 641, (con nt. F. Aiello, *RGL Giurisprudenza Online*, 1, 2021) in cui viene specificato che, se il Gps viene installato sul veicolo aziendale per esigenze meramente produttive (nel caso di specie, per rispettare gli accordi con il committente) e, dunque, non indispensabili per l'esecuzione della prestazione lavorativa, si applicherà l'art. 4, co. 1, St. lav.

<sup>(51)</sup> I. Alvino, I nuovi limiti controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy, *LLI*, 2016, 2, 1, 25, sempre con riferimento agli addetti alla consegna di plichi, considera il Gps uno strumento di lavoro in quanto trattasi di un «meccanismo che consente di inserire la prestazione di lavoro nell'organizzazione del datore di lavoro, coordinandola con gli altri fattori produttivi che concorrono alla realizzazione del risultato produttivo dell'impresa»; dello stesso avviso, seppur con motivazioni parzialmente differenti, A. Maresca, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 16-17, secondo il quale il discrimine è dato dalla circostanza per cui la prestazione del lavoratore sia o meno caratterizzata dalla mobilità territoriale.

organizzativo, assicurativo, produttivo o per garantire la sicurezza sul lavoro. Pertanto, sarebbero *tendenzialmente* sottoposti alla procedura codeterminativa e alle finalità di cui al comma 1. Tuttavia, lo stesso Ispettorato evidenzia come, «solo in casi del tutto particolari»<sup>(52)</sup>, si possa ritenere il Gps un vero e proprio strumento di lavoro, sottratto ai vincoli procedurali e finalistici di cui al comma 1.

Con riferimento all'interazione tra il trattamento dei dati relativi all'ubicazione del veicolo e la disciplina in materia di protezione dei dati personali, è il Garante privacy a individuare le condizioni di liceità del trattamento effettuato per soddisfare esigenze produttive o organizzative del datore ovvero per la sicurezza sul lavoro o tutela del patrimonio aziendale, tenendo conto del diritto alla riservatezza di cui è titolare il lavoratore e dei maggiori rischi in cui questo incorre ove si tratti di mezzo affidato a uso promiscuo, come nel caso in commento *Gramaxo c. Portugal*. Invero, il Garante ha in più occasioni adottato prescrizioni relative alla installazione del Gps su flotte aziendali e al trattamento dei relativi dati stabilendo un decalogo di misure, anche organizzative, che devono essere adottate o implementate per la liceità del trattamento<sup>(53)</sup>. Tra queste, è richiesto il posizionamento di un'icona che indichi il funzionamento o meno del Gps; la possibilità di disattivare la funzionalità di localizzazione durante le pause lavorative o, nel caso di uso promiscuo, nell'utilizzo al di fuori dell'orario di lavoro; la pseudonimizzazione dei dati dei lavoratori che utilizzano il mezzo affinché questi siano identificabili non già direttamente, ma solo indirettamente; la presenza di una periodizzazione temporale del monitoraggio, onde evitare che questo sia continuo; la conformità ai principi di necessità e proporzionalità dei tempi di conservazione dei dati riferiti alla localizzazione geografica<sup>(54)</sup>, tenendo conto delle finalità perseguite. Inoltre, dovrà essere garantito un accesso limitato ai dati raccolti attraverso il Gps, autorizzando, se del caso, profili differenziati per la diversa tipologia di dati. Tra le misure organizzative disposte dal Garante privacy vi è anche la designazione del fornitore del *software* di localizzazione quale responsabile esterno del trattamento ai sensi dell'art. 28 Gdpr. In tal caso, l'assenza di un contratto scritto concernente la nomina da parte del titolare del trattamento (datore di lavoro) del responsabile del trattamento (fornitore del *software*) e la determinazione delle finalità e dei mezzi del trattamento comporta la illiceità dello

---

<sup>(52)</sup> La circolare n. 2 del 2016 fa espresso riferimento ai casi in cui la installazione sia richiesta *ex lege*, come per il trasporto di portavalori superiore a € 1.500.000,00, o sia richiesta da specifiche normative di carattere legislativo o regolamentare.

<sup>(53)</sup> Si vedano i provvedimenti n. 370 del 4 ottobre 2011 [*doc. web n. 1850581*]; n. 432 del 19 ottobre 2017 [*doc. web n. 7321142*]; n. 232 del 18 aprile 2018 [*doc. web n. 9358266*]; n. 396 del 28 giugno 2018 [*doc. web n. 9023246*]; adottati dal Garante della privacy nell'ambito della localizzazione di veicoli aziendali. A ogni modo, con riferimento al tema della geolocalizzazione, si rinvia alle relazioni annuali del Garante privacy disponibili al seguente link <https://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali>

<sup>(54)</sup> Successivamente ribaditi con provvedimento n. 138 del 16 marzo 2017 [*doc. web n. 6275314*] in relazione alla finalità del trattamento (se per il caso di sinistri, per finalità di tutela dei diritti in caso di contestazione di violazioni amministrative ecc.).

stesso <sup>(55)</sup>. Ma non solo. Infatti, con riferimento al ruolo rivestito dai fornitori dei servizi di geolocalizzazione, nonché alla necessità che la protezione dei dati personali venga garantita già in fase di progettazione di un prodotto o di un servizio, il Garante privacy ha ingiunto, per la prima volta, direttamente alla società fornitrice del servizio di localizzazione dei veicoli di configurare, secondo i principi di *privacy by design* e *privacy by default*, la versione *standard* dei servizi offerti «con modalità proporzionate rispetto al diritto alla riservatezza degli interessati, in particolare con riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati ed alla messa a disposizione delle mappe dei percorsi effettuati». Contestualmente, ha disposto che i fornitori dei servizi di geolocalizzazione debbano informare i clienti della possibilità di modificare il sistema rispetto alla impostazione *standard* (per esempio, attivando la funzione che consente la disattivazione del dispositivo) «senza eccessivi costi aggiuntivi» <sup>(56)</sup>.

#### 4. Osservazioni conclusive

In conclusione, a emergere è la considerazione secondo cui, sebbene la conoscibilità dell'atto, inteso come dovere di informazione, sia una pre-condizione sempre più richiesta a livello unionale per la liceità del trattamento, questa non può prevalere rispetto alla disciplina adottata dagli ordinamenti nazionali in tema di protezione dei dati personali e alle formalità ivi previste.

Quanto sostenuto, si può apprezzare anche con riferimento al recente intervento dell'Unione europea a mezzo della Dir. (Ue) 2019/1152 in materia di condizioni di lavoro trasparenti e prevedibili, recepita dall'ordinamento nazionale con il d.lgs. n. 104/2022, c.d. "decreto trasparenza". Esemplificativa, infatti, è l'implementazione a livello nazionale degli obblighi di trasparenza e prevedibilità in capo al datore di lavoro e al committente che, nell'intrattenere un rapporto di lavoro, organizzano la prestazione del lavoratore o del collaboratore attraverso l'utilizzo di sistemi decisionali o *di monitoraggio interamente automatizzati* (corsivo dell'A.) <sup>(57)</sup>, «deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della

---

<sup>(55)</sup> Tanto è stato disposto dai provvedimenti n. 427 [*doc. web n. 9856694*] e 428 [*doc. web n. 9861249*] del 15 dicembre 2022 alla luce delle Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del Gdpr adottate il 7 luglio 2021 che hanno comportato la irrogazione di una sanzione amministrativa di € 30.000,00 per la società titolare del trattamento che avrebbe dovuto designare il responsabile del trattamento con atto scritto e indicare, contestualmente, le caratteristiche dei trattamenti da effettuare.

<sup>(56)</sup> Si veda, in particolare, il provvedimento n. 396 del 28 giugno 2018, *cit.*

<sup>(57)</sup> Il riferimento è all'introduzione dell'art. 1-bis al d.lgs. n. 152/1997 a opera dell'art. 4, co. 1, lett. b), d.lgs. n. 104/2022 e successivamente modificato dall'art. 26, co. 2, lettera a) del d.l. n. 48/2023. Sul punto, si rinvia alle osservazioni di A. Bellavista, *Sorveglianza elettronica, protezione dei dati personali, cit.*, 8-12;

cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori», fermo restando quanto disposto dall'art. 4 St. lav. La disposizione, introdotta dall'art. 4, co. 1, lett. b), d.lgs. n.104/2022, è finalizzata a imporre al datore di lavoro-committente un ampio obbligo di informazione preventiva <sup>(58)</sup> diretta sia al lavoratore-collaboratore, che alle organizzazioni sindacali.

Sicché, alla luce del quadro normativo richiamato, sussistono in capo al datore di lavoro precisi obblighi informativi derivanti da diverse atti giuridici: il Codice privacy, così come integrato al Gdpr; l'art. 4, co. 3, St. lav. e, da ultimo, per il caso di sistemi di monitoraggio interamente automatizzati, l'art. 1-bis d.lgs. n. 152/1997, introdotto dal d.lgs. n. 104/2022. Sorge, allora, spontaneo interrogarsi sul rapporto esistente tra i vari obblighi informativi e, in particolare, se l'adempimento degli uni esoneri il datore dal fornire al lavoratore le informazioni richiamate dagli altri. Per rispondere al quesito è preliminare, dunque, indagare il (diverso) contenuto di tali obblighi informativi. Infatti, mentre l'informativa richiesta all'art. 4, co. 3, St. lav. riguarda specificamente le «modalità d'uso degli strumenti», siano essi strumenti di controllo o strumenti di lavoro, nonché l'«effettuazione dei controlli», quella prevista dal Codice privacy e, in particolar modo, dagli artt. 13 e 14 del Gdpr, è ben più ampia e solo parzialmente sovrapponibile con quella statutaria <sup>(59)</sup>. Invece, nel caso in cui si tratti di sistemi di monitoraggio interamente automatizzati, l'informativa da fornire al lavoratore contiene ulteriori e più specifici elementi <sup>(60)</sup> e risponde all'esigenza di rendere noto al lavoratore-collaboratore e, se del caso, ai soggetti collettivi, «il funzionamento e alla modalità di utilizzo di quei sistemi e strumenti tecnologici che realizzano un'integrale sostituzione del potere direttivo del datore di lavoro» <sup>(61)</sup>, facendo pur sempre salvo «quanto disposto

---

<sup>(58)</sup> Riguardante: «a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi di cui al comma 1; b) gli scopi e le finalità dei sistemi di cui al comma 1; c) la logica ed il funzionamento dei sistemi di cui al comma 1; d) le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi di cui al comma 1, inclusi i meccanismi di valutazione delle prestazioni; e) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità; f) il livello di accuratezza, robustezza e cybersicurezza dei sistemi di cui al comma 1 e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse» (art. 1-bis, co. 2, d.lgs. n. 152/1997).

<sup>(59)</sup> Quest'ultima, riguarda riguardando le finalità del trattamento, al base giuridica dello stesso, i destinatari dei dati personali, gli interessi legittimi perseguiti ai sensi dell'art. 6, par. 1, lett. f), Gdpr dal titolare del trattamento, il periodo di conservazione (ecc.). Infatti, come sottolinea A. Maresca, *Controlli tecnologici e tutele del lavoratore*, cit., 23, «il legislatore traccia il confine tra le materie disciplinate direttamente dall'art. 4 e quelle rimesse al d.lgs. n. 196/2003 che concorrono con le prime nel concretizzare la complessiva tutela del lavoratore in materia di controlli a distanza. Un concorso che si realizza attraverso l'integrazione delle due discipline, senza però sovrapposizioni». Dello stesso avviso M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE, It., n. 300/2016, 29.

<sup>(60)</sup> Già richiamati in nt. 58.

<sup>(61)</sup> B. Rossilli, *Gli obblighi informativi relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati indicati nel decreto "Trasparenza"*, federalismi.it, focus LPT, 5 ottobre 2022, 5.

dall'articolo 4 della legge 20 maggio 1970, n. 300» (art. 1-bis, co. 1, d.lgs. n.152/1997). Pertanto, appare evidente che il legislatore abbia voluto introdurre ulteriori adempimenti in capo al datore di lavoro-committente sommando gli obblighi di cui all'art. 1-bis d.lgs. n. 152/1997 a quelli di cui all'art. 4, co. 3, St. lav. i quali devono, a loro volta, essere integrati con i diritti e gli obblighi derivanti dal Codice della privacy e dal Gdpr, non trattandosi di obblighi di informazione fungibili tra di loro <sup>(62)</sup>.

Inoltre, come anche chiarito dalla Circolare n. 19 del 20 settembre 2022 adottata dal Ministero del Lavoro e delle Politiche Sociali, nel caso in cui siano adottati sistemi di monitoraggio automatizzati come «*tablet*, dispositivi digitali e *wearables*, gps e geolocalizzatori, sistemi per il riconoscimento facciale, sistemi di *rating* e *ranking*, etc.» l'obbligo informativo introdotto all'art. 1-bis trova applicazione anche in riferimento ai quei sistemi «integrati negli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, allorquando presentino le caratteristiche tecniche e le funzioni descritte» <sup>(63)</sup>. Contestualmente, viene richiesto al datore di lavoro o committente di integrare l'informativa «con le istruzioni per il lavoratore in merito alla sicurezza dei dati», fermo restando che, al fine di verificare la conformità degli strumenti utilizzati con il Gdpr, questi «effettuano un'analisi dei rischi e una valutazione d'impatto degli stessi trattamenti, procedendo a consultazione preventiva del Garante per la protezione dei dati personali ove sussistano i presupposti di cui all'articolo 36 del Regolamento medesimo» (art. 1-bis, co. 4, d.lgs. n. 152/1997).

È di tutta evidenza come, nel contesto dei profondi cambiamenti tecnologici e digitali in cui il potere direttivo si contamina sino a confondersi con il potere di controllo <sup>(64)</sup>, cercare un argine, sebbene mobile <sup>(65)</sup>, volto a demarcare un confine tra sfera lavorativa e sfera privata è quantomai necessario. D'altronde, che la prospettiva della tutela del lavoratore sia stata integrata, rispetto alla verifica di compatibilità del trattamento dei dati ai principi del Gdpr effettuata *ex ante*, dalla adeguata informativa e conoscibilità del controllo e del suo contenuto è palese, ma ciò non significa che la disciplina a tutela della protezione dei dati personali e, di conseguenza, il diritto alla riservatezza del lavoratore in costanza di esecuzione della prestazione lavorativa debbano arretrare, come pare emergere dalla decisione adottata dalla Corte Edu. Piuttosto, da una rilettura integrata e circolare delle norme lavoristiche e di quelle del

---

<sup>(62)</sup> Anche B. Rossilli, *op. cit.*, 5, sottolinea la non fungibilità dei diversi obblighi di informazione.

<sup>(63)</sup> Ministero del Lavoro e delle Politiche Sociali, Circolare n. 19 del 20 settembre 2022, 6. In dottrina si veda E. C. Schiavoni, *Gli obblighi informativi in caso di sistemi decisionali o di monitoraggio automatizzati* (art. 4, co. 1, lett. a, d.lgs. n. 104/2022) (art. 1, co. 1, lett. s, e art. 1-bis, d.lgs. n. 152/1997, inserito dall'art. 4, co. 1, lett. b, d.lgs. n. 104/2022), in *Trasparenza e attività di cura nei contratti di lavoro. Commentario ai decreti legislativi n. 104 e n. 105 del 2022*, a cura di D. Garofalo - M. Tiraboschi - V. Fili - A. Trojsi, ADAPT University Press, 2022, 221.

<sup>(64)</sup> Come evidenzia L. Tebano, *La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, Ianus, 2021, 24, 48.

<sup>(65)</sup> A. Pizzoferrato, *I limiti al potere di controllo datoriale nell'era digitale*, cit., 2.

Gdpr si dovrebbe ripartire per apprestare nuove tutele rese necessarie dall'adozione di futuri e, solo per ora, inediti sistemi tecnologici e digitali.

## Bibliografia

- Aiello F., *nt. a Corte Appello Roma, 22 febbraio 2021, n. 641*, in RGL *Giurisprudenza Online*, 1, 2021.
- Alvino I., *I nuovi limiti controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in LLI, 2016, 2, 1.
- 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.
- Bellavista A., *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, in LDE, 2023, 1, 1.
- 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.
- Carta C., *Corte europea dei diritti dell'uomo: la Grande camera torna sul (e difende il) diritto alla privacy del lavoratore*, in *www.rivistalabor.it*, 2017
- Ciriello A., *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in LDE, 2019, 3.
- Coelho Moreira T., *The Electronic Control of the Employer in Portugal*, in LLI, 2016, 2, 1.
- Di Meo R., *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in LLI, 2018, 4, 1.
- Donini A. - Novella M. - Vallauri M. L., *Prime riflessioni sul lavoro nel metaverso*, in LLI, 2022, 8, 2, 1.
- Gamba C., *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, in LLI, 2016, 2, 1, 122.
- Ingrao A., *Il "cyberslacking" e i diritti del lavoratore "catturato nella rete informatica". Note critiche a margine della sentenza della Corte Europea dei diritti dell'uomo, sez. IV, 12 gennaio 2016, n. 61496, Bărbulescu vs. Romania, in attesa della pronuncia della Grande Camera*, in Osservatorio AIC, 2016, 3, 621.
- Ingrao A., *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in DRI, 2019, 3, 895.
- Ingrao A., *Il controllo a distanza sulla prestazione dei ciclofattorini tra Scoober App e GPS*, in LLI, 2021, 7, 1, 165.
- Ingrao A., *Il potere di controllo a distanza sull'attività lavorativa e la nuova disciplina della privacy nella sfida delle nuove tecnologie*, in *Nuove tecnologie e diritto del lavoro. Un'analisi comparata degli ordinamenti italiano, spagnolo e brasiliano*, a cura di G. Ludovico - F. Fita Ortega - T. Christina Nahas, Milano University Press, 2021, 111.
- Laforgia S., *I poteri del datore di lavoro, oggi. Opacità e rifrazioni sotto la lente del giurista*, in *Le conquiste legislative degli anni '70 e il ruolo del movimento sindacale in Puglia*, a cura di V. Leccese - V. Pinto, Edizione Radici Future, 2022, 237.
- Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE, It., n. 300/2016.
- Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 1.
- Novella M., *Poteri del datore di lavoro nell'impresa digitale: fenomenologia e limiti*, in LD, 2021, 3-4, 451.
- Nuzzo V., *Il ragionevole sospetto di illecito e la possibilità di controlli difensivi occulti all'esame della Grande Camera della Corte Europea dei diritti dell'uomo*, in Labor, 2020, 2, 208.
- Perrone F., *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Diritti dell'Uomo e giurisdizione nazionale dopo la sentenza Bărbulescu 2*, in Labor, 2018, 3, 283.
- Pisani C. - Proia G. - Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giappichelli, 2022.
- Pizzoferrato A., *I limiti al potere di controllo datoriale nell'era digitale*, in LDE, 2023, 1, 2.
- Pizzonia D. - Sitzia A., *Il controllo del datore di lavoro su Internet e posta elettronica: quale riservatezza sul luogo di lavoro?*, in NGCC, 2016, 6, 1, 901.

- Poletti D., *Gli intermediari dei dati*, in *EJPLT*, 2022, 1.
- Rossilli B., *Gli obblighi informativi relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati indicati nel decreto "Trasparenza"*, in *federalismi.it, focus LPT*, 5 ottobre 2022
- Schiavoni E. C., *Gli obblighi informativi in caso di sistemi decisionali o di monitoraggio automatizzati (art. 4, co. 1, lett. a, d.lgs. n. 104/2022) (art. 1, co. 1, lett. s, e art. 1-bis, d.lgs. n. 152/1997, inserito dall'art. 4, co. 1, lett. b, d.lgs. n. 104/2022)*, in *Trasparenza e attività di cura nei contratti di lavoro. Commentario ai decreti legislativi n. 104 e n. 105 del 2022*, a cura di D. Garofalo - M. Tiraboschi - V. Fili - A. Trojsi, Adapt University Press, 2022, 211.
- Sitzia A. - Ramos Quintana M. I., *Sorveglianza difensiva "occulta" sui luoghi di lavoro e dignità nella prospettiva della Grande Camera della Corte EDU: la Sentenza López*, in *LDE*, 2019, 3.
- Stolfa A., *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, in *LG*, 2018, 5, 530.
- Tebano L., *Employees' Privacy and Employers' control between the Italian and European system*, in *LLI*, 2017, 3, 2, 3.
- Tebano L., *I confini dei controlli difensivi e gli equilibrismi della Corte Edu*, in *RIDL*, 2020, II, 211.
- Tebano L., *La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *Ianus*, 2021, 24, 43.
- Trojsi A., *Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, 2022, 4, 276.
- Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, Giappichelli, 2017, 97.
- Ziccardi G., *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *LLI*, 2016, 2, 1, 48.