SAPIENZA
UNIVERSITÀ DI ROMA

FACOLTÀ DI GIURISPRUDENZA
DIPARTIMENTO DI SCIENZE GIURIDICHE

Corso di Dottorato in Autonomia privata, impresa, lavoro e tutela dei diritti nella prospettiva europea ed internazionale

CURRICULUM DI DIRITTO DEL LAVORO
XXXII CICLO

ESERCIZIO DEL POTERE DI CONTROLLO E RISERVATEZZA DEL LAVORATORE

Tutor
Chiar.mo Prof. ARTURO MARESCA

Dottoranda
EMANUELA GUARELLA
Matr. 718519

Anno Accademico 2018-2019

C'è sempre un po' di follia nell'amore.
Ma c'è anche sempre un po' di ragione nella follia.
F. Nietzsche *Così parlò Zarathustra*

ESERCIZIO DEL POTERE DI CONTROLLO E RISERVATEZZA DEL LAVORATORE

Sommario

Introduzione

> *Se tutti gli altri contratti riguardano l'avere delle parti, il contratto di lavoro riguarda ancora l'avere per l'imprenditore, ma per il lavoratore riguarda e garantisce l'essere, il bene che è condizione dell'avere e di ogni altro bene.*
>
> F. Santoro Passarelli, *Spirito del diritto del lavoro*, in Annali del Seminario giuridico dell'Università di Catania, 1948.

Nella prospettiva civilistica il controllo da parte del creditore circa l'esatto adempimento dell'obbligazione non presenta particolari problematicità, mentre la specialità del vincolo contrattuale lavoristico che, pur se ricondotto allo schema del contratto di scambio, è connotato dall'inevitabile coinvolgimento psicofisico che caratterizza il comportamento solutorio, dall'implicazione della totalità della persona del lavoratore nell'adempimento dell'obbligazione di *facere* e dalla posizione asimmetrica delle parti nella relazione, con il lavoratore in posizione di soggezione e dipendenza rispetto alla preminenza economica dell'imprenditore, pone la necessità di individuare una "frontiera mobile" (D'Antona), nella quale il potere di controllo del creditore arretri di fronte all'esigenza di tutela della libertà e della dignità della persona del prestatore/debitore[1].

Il contratto di lavoro ha per oggetto non una *res* ma energie psicofisiche che sono tutt'uno con la persona del lavoratore e sebbene il lavoratore implicitamente accetti che dalla valutazione di attitudini e informazioni personali, funzionali all'attività da svolgere, e dalla comunanza stessa di vita aziendale, conseguano una naturale maggiore esposizione, questo non può significare che ogni spazio di libertà e di riservatezza sia sacrificato, a pena di compromettere la sua stessa dignità e personalità[2]. È inevitabile che alcuni dati personali

---

[1] *Tutto il diritto del lavoro è ordinato caratteristicamente a questo fine, alla tutela della libertà, anzi della stessa personalità umana del lavoratore, legato da un vincolo che, fra tutti i vincoli di contenuto patrimoniale, è il solo a porre giuridicamente un soggetto alle dipendenze di un altro soggetto. Quella tutela segna il limite del rispetto dell'interesse dell'imprenditore.* (F. Santoro Passarelli, *Nozioni di diritto del lavoro*, Jovene, Napoli, 1945, 12).

[2] Secondo E. Gragnoli il diritto alla riservatezza è un diritto disponibile, tanto che all'atto di stipulare il contratto di lavoro, il lavoratore rinuncia a una parte della propria riservatezza, però non è illimitatamente disponibile. *Da questo consegue che «in linea generale deve ritenersi che soggiacciano ai limiti inderogabili precisi posti dalla legge gli atti di disposizione del diritto di riservatezza aventi per oggetto l'acquisizione e il trattamento di dati personali in epoca successiva alla pattuizione, mentre la disponibilità del diritto individuale*

perdano il loro carattere riservato e che il diritto di riservatezza si ridimensioni quando è calato in un contesto lavorativo, affievolito dalle ragioni produttive e organizzative del datore che comportano il controllo sull'adempimento e pongono, in una certa misura, il lavoratore stesso sotto osservazione. Da questo devono discendere, però, un'attenzione specifica e specifiche tutele che tengano in debito conto le esigenze contrapposte e realizzino il necessario contemperamento fra le stesse, senza eliminare completamente quello spazio essenziale di libertà e riservatezza che ogni lavoratore ha diritto di vedere rispettato anche nella vita aziendale.

Una volta preso atto che il potere di controllo datoriale - le cui potenzialità risultano oggi dilatate dalla diffusione delle tecnologie informatiche - è caratteristica immanente alla prestazione subordinata, si tratta di stabilire dove si collochi il confine oltre il quale la riservatezza e la dignità della persona siano lese, in un bilanciamento tra interessi contrapposti, entrambi riconosciuti meritevoli di tutela.

In tema di controlli a distanza si manifesta con maggiore evidenza la doppia anima regolativa che caratterizza i controlli datoriali sul lavoratore: *la tutela della persona del lavoratore non può ragionevolmente esaurirsi in quella lavoristica, dovendosi dar voce anche all'altra fondamentale esigenza che viene in rilievo, consistente nella tutela della riservatezza*[3].

In questo ambito si intersecano due diversi piani regolativi, quello speciale statutario e quello della disciplina generale in materia di tutela dei dati personali, che evidenziano due angoli prospettici diversi, anche se entrambi focalizzati sulla tutela della dignità della persona. La norma lavoristica protegge la persona da forme di controllo ritenute "odiose" e contempera il diritto del lavoratore con la libertà d'impresa e con l'interesse alla sua efficiente organizzazione, la disciplina generale protegge la "riservatezza", l'"identità personale" e "i dati personali" (art. 2, comma 1 Codice privacy) e li contrappone all'interesse alla libera circolazione dei dati e a quello all'innovazione tecnologica e digitale[4]. Pur riconoscendo che

---

è illimitata per ciò che riguarda l'acquisizione e il trattamento attuati nell'immediatezza del consenso prestato, ovvero la singola e ben circoscritta "apertura" della propria sfera di riservatezza (così ad esempio, il lavoratore non può validamente autorizzare il datore di lavoro a svolgere in futuro indagini sulla sua vita privata, ma può fornire un'informazione in proposito autorizzando contestualmente il trattamento immediato del dato fornito). (E. Gragnoli, *Dalla tutela della libertà alla tutela della dignità e della riservatezza dei lavoratori*, in *Argomenti di diritto del lavoro*, n.1/2007, 1211 e ss.).

[3] A. Levi *Il controllo difensivo a distanza e l'inoperatività dell'art. 4 dello Statuto*, in *Il lavoro nella giurisprudenza* n. 5/2018, 478.

[4] G. Proia, *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza*, in *Rivista Italiana di Diritto del Lavoro*, fasc.4, 2016, 547. All'innovazione tecnologica e digitale è riconosciuto un ruolo centrale anche nelle strategie di Europa 2020: il programma dell'UE per la crescita e l'occupazione per il decennio che sta per concludersi prevede una crescita intelligente, sostenibile e inclusiva con l'obiettivo di realizzare un'economia di mercato sociale sostenibile.

i due corpi normativi costituiscono la risposta dell'ordinamento a vicende storiche e ad esigenze diverse, risulta comunque evidente che la vocazione e l'ambizione comune ad entrambi sia volta a dare attuazione ed effettività al valore costituzionalmente rilevante della dignità dell'individuo, sia nella qualità di lavoratore che, ancora prima e indipendentemente dal ruolo sociale rivestito, quale persona[5].

Si è progressivamente consolidata la consapevolezza che il lavoratore, come ogni persona fisica, ha diritto alla "protezione dei dati personali che lo riguardano" (art. 1, D.lgs. n. 196/2003 Codice privacy) ed evidentemente mantiene la titolarità di questo diritto anche durante lo svolgimento della prestazione lavorativa.

Il contratto di lavoro comporta, per sua stessa natura, il trattamento continuativo di dati personali del lavoratore ed il potere di controllo datoriale pone così una questione di disciplina della raccolta e poi dell'utilizzazione di dati personali, ossia di regolamentazione di tutti i comportamenti del datore che consistano nella acquisizione, consultazione, elaborazione, conservazione, utilizzo, cessione e distruzione di dati personali del lavoratore, operazioni che costituiscono trattamento di dati personali.

La definizione di trattamento di dato personale contenuta nel D.lgs. 196/2003 (art. 4, comma 1 lett. a) consente di considerare il controllo a distanza del lavoratore come una *species* del trattamento (automatizzato e non) di dati personali, che comincia con la raccolta e termina con la distruzione del dato, regolato dalla specifica disciplina dettata in materia[6]. Da questo momento in poi la tutela dei diritti della persona/lavoratore non si fonda più solo sulle previsioni statutarie, ma trova ulteriori garanzie nella disciplina di protezione dei dati personali, contenuta nel D.lgs. 30 giugno 2003, n. 196, come oggi modificato dal D.lgs. 101/2018, a seguito dell'entrata in vigore del Regolamento generale sulla protezione dei dati. Lo sintetizza efficacemente il Gruppo di lavoro ex art. 29 nel momento in cui afferma che "la legislazione sulla protezione dei dati non opera in modo isolato dal diritto e dalla prassi in materia di lavoro, né il diritto e la prassi in materia di lavoro operano in modo isolato dalla legislazione sulla protezione dei dati. Si tratta di un'interazione utile e necessaria, che dovrebbe facilitare la messa a punto di soluzioni in grado di tutelare adeguatamente gli interessi dei lavoratori"[7].

---

[5] R. Lattanzi, *Dallo statuto dei lavoratori alla disciplina di protezione dei dati personali,* in *Rivista italiana diritto del lavoro,* n. 1/2011, 151.

[6] A. Ingrao, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act,* in *Rivista Italiana di Diritto del Lavoro,* fasc.1, 2017, 49.

[7] Sulla base dell'art. 29 della direttiva 95/46 è stato creato un organo indipendente, il Gruppo di lavoro per la protezione dei dati (Data Protection Working Party), incaricato anche di analizzare il problema relativo ai limiti al potere di sorveglianza delle comunicazioni informatiche nei luoghi di lavoro. La citazione è tratta dal parere

In assenza di una normativa di settore che tipizzi, con riferimento al rapporto di lavoro, le regole generali in materia di protezione dei dati personali, si è imposta l'esigenza di integrare e coordinare le disposizioni e le tutele giuslavoristiche con le previsioni della normativa sulla protezione della persona rispetto al trattamento dei suoi dati personali: il potere di controllo del datore di lavoro dovrà essere contemperato non più solo con il diritto del lavoratore di salvaguardare la sua sfera privata dallo sguardo altrui e da profili eccessivamente invasivi, ma anche con quello di governare la conoscenza e la circolazione dei propri dati personali.

Considerato che tra la norma giuridica e la realtà sociale esistono una dialettica e una tensione continue, la tutela del diritto alla privacy, inteso nella sua versione più evoluta, come diritto della persona ad agire come padrone dei propri dati, deve fare i conti con la trasformazione delle modalità di svolgimento della prestazione e dell'organizzazione produttiva, con le implicazioni dell'utilizzo, spesso promiscuo, dei nuovi versatili strumenti di lavoro, con trasformazioni socio-economiche che aprono prospettive nuove e nuovi rischi di invasione nella sfera più intima dell'individuo.

Di fronte alla "invasione armata" di nuove tecnologie, soprattutto informatiche, e alla conseguente trasformazione dei modelli produttivi ed organizzativi tradizionali dell'impresa, il potere di controllo ha assunto nuovi contorni e confini sempre più sfumati: la normativa si dimostra al passo con gli sviluppi tecnologici e con la necessità di tutelare il moderno lavoratore, che è anche "cittadino tecnologico" (Faleri), riconoscendogli un ruolo attivo nel processo di elaborazione e gestione dei suoi dati personali?

Con maggiore evidenza nella *smart factory* l'implicazione della "persona tecnologica" nell'esecuzione della prestazione determina una crescente difficoltà di separare la vita professionale dalla vita privata del lavoratore. Questa continua sovrapposizione delle due sfere, privata e pubblica, rende maggiormente complesso il contemperamento tra la tutela dei legittimi interessi del datore di lavoro al corretto adempimento della prestazione e alla salvaguardia del patrimonio aziendale e la tutela della vita privata del lavoratore, del diritto di quest'ultimo di sviluppare la sua personalità e di instaurare rapporti personali e sociali sul luogo di lavoro. Per lavoratori divenuti "di vetro"[8], trasparenti e vulnerabili di fronte a

n. 8/2001, adottato il 13 settembre 2001, in materia di raccolta e trattamento dei dati personali nell'ambito del contesto lavorativo, dove tra l'altro il Gruppo indica i principi che governano la modalità di trattamento al fine di tutelare le persone: *finality, transparency, legitimacy, proportionality, accuracy and retention of the data, securuty, awareness of the staff.*

[8] *La formula "uomo di vetro" nasce nella Germania nazista ed è tipica di tutti i totalitarismi. Da qui nasce la giustificazione che consente allo Stato di impadronirsi della vita privata e della libertà di tutti. Se vuoi mantenere una sfera d'intimità, di riservatezza nelle relazioni personali e sociali, questo vuol dire che hai qualcosa da nascondere, diventi sospetto, e allora facciamo bene a mettere le mani sulle informazioni che ti*

chiunque voglia impadronirsi di informazioni personali, e spesso inconsapevoli di fornirle spontaneamente, rischiano di essere minacciati diritti fondamentali della persona, in particolare la dignità dell'individuo, di cui la riservatezza è un aspetto preminente.

In questo scenario ci ricorda Stefano Rodotà diventa fondamentale tutelare la privacy come una componente ineliminabile della "società della dignità": senza una resistenza continua alle microviolazioni, ai controlli continui, capillari, oppressivi o invisibili che invadono la stessa vita quotidiana, ci troviamo nudi e deboli di fronte a poteri pubblici e privati[9].

Di fronte a tecnologie, non solo capillarmente presenti nella vita quotidiana, ma anche "bifronti", che sono sviluppo ma anche soggezione, di fronte a persone/lavoratori, tanto assuefatti e dipendenti dalle tecnologie da essere spesso inconsapevoli che controllo e sorveglianza sono incorporati nella medesima architettura tecnologica, gli strumenti offerti dalla normativa si rivelano adeguati e sufficienti?

È legittimo chiedersi se oggi il bilanciamento tra l'interesse datoriale al controllo, finalizzato al buon andamento dell'impresa, e i diritti del lavoratore alla privacy e al governo dei propri dati personali, sia effettivo e se le tutele poste dalla normativa speciale, con il novellato articolo 4 dello Statuto dei lavoratori, e dalla normativa generale, con il Regolamento 2016/679 UE che ha modificato il Codice Privacy, siano coordinate e sistematicamente raccordate al fine di assicurare adeguata tutela alla persona del lavoratore.

Con grande lungimiranza, e forse un po' di ottimismo, già alla fine degli anni ottanta R. De Luca Tamajo individuava gli strumenti per neutralizzare le potenzialità intrusive delle nuove tecnologie e per garantire l'equilibrio fra le esigenze di tutela della persona e quelle di sviluppo economico, nella trasparenza, nella disciplina delle modalità di raccolta dei dati, nel riconoscimento del diritto di accesso da parte dell'interessato e nella non conoscibilità dei dati da parte di terzi[10].

---

riguardano perché probabilmente sei colpevole di chissà quale segreto peccato. S. Rodotà, *Intervista su privacy e libertà*, (a cura di P. Conti) Laterza, 2005, 29-30.

[9] S. Rodotà, *Intervista su privacy e libertà, op. cit.*, 149.

[10] *Una disciplina generale (per tutti i cittadini) o speciale (per i lavoratori subordinati) sulle modalità di raccolta delle informazioni e sulla sua trasparenza che fornisca garanzie circa l'esattezza e la non conoscibilità da parte di terzi dei dati, circa gli obiettivi perseguiti dalla raccolta e circa l'accesso da parte dell'interessato* [...] *potrebbe stemperare le preoccupazioni che oggi si appuntano nei confronti del controllo "tecnico" sulla prestazione reso possibile dagli elaboratori e sdrammatizzare – una volta garantiti adeguati livelli e valori di privacy individuale - la temibilità di apparecchiature pur così indispensabili per lo svolgimento del lavoro informatico, cioè a dire per una tipologia organizzativa che costituisce un aspetto determinante della competizione economica nell'attuale momento storico.* R. De Luca Tamajo, Presentazione della ricerca, in R. De Luca Tamajo-R. Imperiali d'Affitto-C. Pisani-R. Romei (a cura di), in *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Franco Angeli, 1988, 16-17.

A distanza di trenta anni dalle parole di De Luca Tamajo, è legittimo chiedersi se abbiamo maturato una cultura autentica della protezione dei dati, che non si riduca ad una logica di mercato e sia in grado di fronteggiare consapevolmente un processo di controllo rispetto al quale siamo non solo soggetti passivi, ma attori e complici collaboranti in un'evoluzione paradossale del *Panopticon* di J. Bentham[11]. Il modello panoptico assume forme nuove nella nostra quotidianità e fa sì che per la sola possibilità di essere sorvegliati ci trasformiamo in zelanti carcerieri di noi stessi, portatori dei nostri stessi dispositivi di lavoro e di controllo[12]. Come Z. Bauman ci ha ricordato: "Nel "mondo nuovo" liquido-moderno i lavoratori, come le lumache si portano dietro la casa, devono portare sul loro corpo i propri Panopticon personali. I subalterni sono talmente addestrati a svolgere il ruolo di sorveglianti di se stessi da rendere superflue le torrette di osservazione dello schema di Bentham e Foucault"[13]. Per dirla con altre parole, colui che è consapevole di essere esposto costantemente a visibilità, finisce per fare proprie spontaneamente le costrizioni del potere, inscrive in se stesso il rapporto di potere nel quale gioca simultaneamente i due ruoli, diviene il principio del proprio assoggettamento, così che la coscienza della propria visibilità diventa essa stessa limitazione della libertà[14].

---

[11] Il Panopticon, modello di struttura carceraria ideale, progettata da Jeremy Bentham, viene usato da Foucault per descrivere il funzionamento del potere. *Il Panopticon è un edificio a forma di anello, al centro del quale c'è un cortile, con una torre al centro. L'anello si divide in piccole celle che si affacciano tanto all'interno che all'esterno.* […] *Nella torre centrale c'è un sorvegliante. Dato che ogni cella dà tanto sull'interno che sull'esterno, lo sguardo del sorvegliante può attraversarla tutta; non c'è alcun punto in ombra, e di conseguenza tutto quello che fa l'individuo è esposto allo sguardo di un sorvegliante che osserva* […] *in modo da poter vedere tutto senza che nessuno lo veda* […] *il Panopticon è l'utopia di una società e di un tipo di potere che è in fondo la società e il tipo di potere che conosciamo oggi.* (M. Foucault, *La verità e le forme giuridiche*, Feltrinelli, Milano, 1997, 136-137).

[12] Si tratta dei cosiddetti BYOD: lo strumento denominato BYOD (Bring Your Own Device) consente di creare, sullo stesso dispositivo (di proprietà del dipendente), due ambienti diversi, contenenti rispettivamente dati personali e dati aziendali, che possono consentire all'utente anche di collegarsi alla intranet aziendale, utilizzandone dati ed applicazioni. In questa ipotesi, dunque, lo strumento è di proprietà del lavoratore, ma è da questi utilizzato, avvalendosi di un applicativo di proprietà del datore di lavoro, per accedere alle risorse informatiche dell'impresa al fine di eseguire la prestazione lavorativa, anche al di fuori dei locali aziendali e del normale orario di lavoro. (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*, in *Labour Law Issues*, n. 1/2016, 26).

[13] Z. Bauman-D. Lyon, *Sesto potere*. *La sorveglianza nella modernità liquida*, Laterza, Bari, 2013, 46-47.

[14] Vedi S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, 174 e anche A. Soro, *La protezione dei dati personali nell'era digitale*, in *Nuova Giurisprudenza Civile Commentata*, n. 2/2019, 345. È interessante il cambio di prospettiva rispetto alle parole di M. Dell'Olio che non poteva prefigurare uno scenario nel quale proprio a causa della consapevolezza di essere controllati, si diventa strumenti dell'esercizio del potere. *La mancanza di consapevolezza è la vera lesione della sfera di riservatezza. Gli americani usano l'immagine del "pesce rosso" per indicare l'essere continuamente sotto lo sguardo di qualcuno senza sapere di esserlo, senza poter controllare, nel momento in cui avviene, la stessa effettuazione del controllo: questa è la vera lesione della riservatezza, l'essere visto senza sapere di esserlo.* (Intervista a Matteo Dell'Olio, in R. De Luca Tamajo, R. Imperiali, C. Pisani, R. Romei, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Franco Angeli, Milano 1988, 226).

Data la posta in gioco, è essenziale che gli strumenti di tutela predisposti per la persona/lavoratore si dimostrino alla prova dei fatti efficaci.

Capitolo 1 Le fonti

L'occhio del Grande Fratello (Grande Padre?) Fiat arrivava lo stesso lontano, registrava impietosamente orgoglio ideologico e miserie familiari, senza bisogno di sofisticate attrezzature elettroniche.

B. Guidetti Serra, *Le schedature Fiat.*

Quanto spesso e con quali principi la Psicopolizia veniva ad interferire sui cavi che vi riguardavano, era pura materia per congetture. E sarebbe stato anche possibile che guardasse tutti, e continuamente. Ad ogni modo avrebbe potuto cogliervi sul vostro cavo in qualsiasi momento avesse voluto. Si doveva vivere (o meglio si viveva, per un'abitudine che era diventata, infine, istinto) tenendo presente che qualsiasi suono prodotto sarebbe stato udito, e che, a meno di essere al buio, ogni movimento sarebbe stato visto.
G. Orwell, *1984.*

1.1 Le origini del diritto alla riservatezza: il diritto "ad essere lasciato solo"

Furono due giovani avvocati di Boston, Samuel D. Warren e Louis D. Brandeis, quest'ultimo destinato a diventare un giudice della Corte Suprema, a coniare nel 1890 l'espressione *the right to privacy* in un saggio pubblicato sull'Harvard Law Review. Il diritto alla privacy, presupposto indispensabile per la protezione della persona, prende inizialmente la forma del diritto ad essere lasciato solo, espressione moderna dello "ius solitudinis": *the right to be let alone*, il diritto ad essere lasciati soli per godere in pace della propria vita.

Preoccupati dalle rivelazioni della stampa popolare sulla vita privata e familiare delle persone, Warren e Brandeis sostanzialmente equipararono l'inviolabilità della sfera privata immateriale a quella della proprietà privata, intesa come diritto di escludere l'altro, ed estesero all'inviolabilità della sfera personale le tutele poste a garanzia del possesso indisturbato dei propri beni materiali. Pur risentendo della logica proprietaria borghese, riconobbero la specificità del diritto alla privacy e nel lontano 1890 arrivarono alla conclusione che "solo una parte del piacere, del dolore, della soddisfazione della vita deriva, per gli uomini, dai beni materiali e che pensieri, sentimenti ed emozioni richiedono un

riconoscimento ed una protezione giuridica"[15]. Quindi quasi si trattasse di un prolungamento del diritto alla tutela della proprietà privata, distinto ma meritevole di altrettanta protezione, prefigurarono un'azione di tutela che consentisse ai singoli individui di difendersi da indebite intrusioni nella propria vita privata. Inevitabilmente in questa fase, la vita privata era assimilata alla proprietà privata e tutelata secondo la logica del recinto, del divieto di accesso nello spazio privato altrui, sia esso fisico o interiore.

Da questo momento in poi *the right to privacy* si è venuto definendo ed affermando come un diritto costituzionalmente riconosciuto, anche attraverso successive fondamentali pronunce della Corte Suprema (Griswald v. Connecticut 1965 sulla contraccezione[16] e Lawrence and Garner v. Texas 2003 sul diritto alle unioni omosessuali[17]), e ricondotto al XIV emendamento della Costituzione degli Stati Uniti. Si è così esplicitato il principio di inviolabilità della sfera intima dell'individuo, non solo rispetto ai poteri pubblici ma anche nelle relazioni tra privati, il diritto ad essere lasciato solo diventa il presupposto per fare liberamente le proprie scelte, dandosi pieno riconoscimento giuridico al diritto secondo il quale ciascuno può utilizzare la propria libertà in base all'indirizzo che assegna alla propria vita privata.

Il diritto al rispetto della vita privata fa il suo ingresso nel novero dei diritti fondamentali della persona con la Dichiarazione Universale dei Diritti dell'Uomo, proclamata

---

[15] *The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.* […] *Now the right to life has come to mean the right to enjoy life, - the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession - intangible, as well as tangible*. […] *The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested, the right to privacy, as a part of the more general right to the immunity of the person, - the right to one's personality* (Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4, No. 5, Dec. 15, 1890, 195).

[16] Nel 1879 lo Stato del Connecticut approvò una legge che metteva al bando i metodi contraccettivi: un ginecologo, C. Lee Buxton, e Ms Estelle Griswold aprirono una clinica per il controllo delle nascite a New Haven, appellandosi alla Corte Suprema e al 14° emendamento in difesa del diritto di libertà e determinazione della propria vita. Nella sentenza si legge: *We deal with a right of privacy older than the Bill of Rights - older than our political parties, older than our school system. […] the principles laid down in this opinion affect the very essence of constitutional liberty and security. […] they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life*. (Griswold c. Connecticut 381, US 476 1965)

[17] Analogamente si legge nella sentenza Lawrence c. Texas 539 US 558 2003 in difesa della libertà e del diritto alla tutela della propria vita privata: *First, among the fundamental rights that are implicit in our concept of order of liberty, must be the right of all adult couples, whether same-sex or not, to be free from unwarranted State intrusion into their personal decisions about their preferred forms of sexual expression. […] free as adults to engage in the private conduct in the exercise of their liberty under the Due Process Clause of the Fourteenth Amendment to the Constitution.*

all'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948. L'articolo 12 stabilisce che "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".

Anche il Patto internazionale relativo ai diritti civili e politici, approvato dall'assemblea dell'ONU con risoluzione n. 2200 del 16 dicembre 1966, vieta qualsiasi interferenza arbitraria nella vita privata dell'individuo: la riservatezza si configura quale presupposto per l'esercizio di altri diritti di libertà.

In Europa *the right to privacy* si afferma come diritto umano fondamentale nel novembre 1950 quando viene firmata dagli allora dodici Stati membri del Consiglio d'Europa, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), ratificata dall'Italia con legge 4 agosto 1955 n. 848, che riconosce il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza (articolo 8)[18]. Al fine di assicurare l'osservanza e l'applicazione dei diritti enunciati nella Convenzione viene istituita nel 1959 la Corte europea dei diritti dell'uomo, la Corte EDU, con funzione giurisdizionale sussidiaria rispetto agli organi giudiziari nazionali: ad essa possono adire sia individui che Stati, una volta esaurite le vie di ricorso interne. La giurisprudenza della Corte EDU ha svolto nel tempo un ruolo fondamentale nel tracciare i confini del diritto alla riservatezza e nel determinare l'evoluzione dell'oggetto, dell'ambito di applicazione e delle relative tutele.

Nella cultura occidentale emergono in origine due concezioni della privacy, destinate ad evolversi e a sovrapporsi: quello europeo, sostanzialmente fondato sull'idea di dignità e l'altro, tipico soprattutto degli Stati Uniti, fondato invece sull'idea di libertà. Tuttavia, come osserva Stefano Rodotà, le dinamiche legislative e culturali di questi anni dimostrano che, proprio nella materia della protezione dei dati, quella contrapposizione frontale non è più proponibile. Soprattutto non è proponibile una estraneità della dimensione della libertà al modello europeo di privacy. Questo, anzi, si è progressivamente evoluto, affiancando alla tutela dell'intimità e della segretezza l'obiettivo di contrastare possibili discriminazioni, di

[18] L'articolo 8 della Convenzione europea dei diritti dell'uomo stabilisce il Diritto al rispetto della vita privata e familiare: 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

rendere effettiva l'eguaglianza. Così cambia profondamente la funzione socio-politica della privacy, che si proietta ben al di là della sfera privata, divenendo elemento costitutivo della cittadinanza del nuovo millennio[19].

L'esigenza di integrale tutela della persona per garantire il libero svolgimento della sua personalità e la centralità dei diritti della persona, della sua dignità e libertà, sono state da ultimo esplicitamente affermate nel preambolo della Carta di Nizza[20] dove si afferma l'inviolabilità della dignità della persona (art. 1) e si legge che "L'Unione pone la persona al centro della sua azione". La tutela dei diritti della persona si configura quale indirizzo irrinunciabile della politica degli Stati membri e suo principio cardine.

La Carta di Nizza ha inoltre rappresentato la prima formalizzazione in una dichiarazione dei diritti dell'uomo del diritto alla protezione del dato personale: l'articolo 8, rubricato "Protezione dei dati di carattere personale", delinea un diritto nuovo e autonomo alla protezione dei dati personali, distinto dal diritto al rispetto della vita privata e familiare (art. 7). Ad esso corrisponde una tutela dinamica che segue i dati nella loro circolazione, non più solo una tutela negativa che si sostanzia nell'esclusione delle altrui interferenze dal proprio ambito privato.

Anche dopo l'entrata in vigore del Regolamento 2016/679 UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati), rimane aperta la questione del coordinamento della disciplina generale sul trattamento dei dati con le molteplici discipline speciali, relative sia al trattamento che all'utilizzo dei dati, tra le quali anche quella della protezione dei dati nell'ambito dei rapporti di lavoro. In assenza di una specifica normativa di settore che raccordi le regole generali in materia di protezione dei dati personali alla specificità dei rischi connessi al rapporto di lavoro, il sistema delle fonti normative a tutela della riservatezza della persona nel momento dello svolgimento della propria attività lavorativa si configura come una disciplina multilivello e plurisettoriale, con fonti che si richiamano, si intersecano e si integrano reciprocamente: il coordinamento fra le discipline

[19] S. Rodotà, *Privacy libertà e dignità*. *Discorso conclusivo della Conferenza internazionale sulla protezione dei dati.* 26° Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali, Wroclaw (PL), 14, 15, 16 settembre 2004.

[20] La Carta dei diritti fondamentali dell'Unione europea è stata proclamata a Nizza il 7 dicembre 2000. Con l'entrata in vigore del Trattato di Lisbona la Carta ha assunto il medesimo valore giuridico dei Trattati al fine di definire diritti fondamentali e libertà di eccezionale rilevanza che fossero garantiti a tutti i cittadini dell'Unione.

resta affidato agli interpreti e a soluzioni individuate caso per caso, talvolta a discapito della coerenza[21].

1.2 Il fondamento di un autonomo diritto alla riservatezza: gli articoli 2 e 41 della Costituzione.

Il riconoscimento di un autonomo diritto alla riservatezza nel nostro ordinamento giuridico è stato frutto di dibattito e riflessioni dottrinali e giurisprudenziali.

Adottando una prospettiva dialogica del diritto, non calato dall'alto nella realtà materiale, ma espressione e orientamento dei processi reali, capace di registrare e in alcuni casi di guidare i mutamenti in atto, si può comprendere la genesi di due diritti soggettivi autonomi, quali il diritto di riservatezza ed il diritto all'identità personale, rispetto ai quali i giuristi si pongono come interpreti di avvertite e condivise esigenze a tutela della persona.

Come ci rivelano sia la risalente vicenda dei due avvocati di Boston, che l'esperienza dottrinale e giurisprudenziale italiana degli anni cinquanta e sessanta, il diritto alla riservatezza, così come il diritto all'identità personale[22], entrambi espressione della centralità riconosciuta alla persona, soggetto ed oggetto del diritto, si affermarono inizialmente in contrapposizione con l'esercizio del diritto di cronaca e di informazione, esercitato attraverso stampa, televisione e radio, che nel nostro ordinamento beneficia di tutela costituzionale (art. 21 Cost.), ma incontra un limite nel rispetto della dignità delle persone.

Il riconoscimento del diritto alla riservatezza ha contato in una primissima fase sull'applicazione analogica di disposizioni dettate a tutela dell'immagine (art. 10 c.c. e artt. 93-97 legge n. 633/1941): un diritto alla riservatezza che si sostanziava nel divieto di ingerenze e indiscrezioni da parte di terzi nella sfera privata della persona. In contrapposizione all'esercizio del diritto di cronaca si è affermato il diritto della persona all'integrità e all'inviolabilità della propria vita privata, al riserbo delle informazioni

[21] Così scrive G. Proia: *Il legislatore italiano, nel recepire la direttiva comunitaria, ha scelto di operare una semplice sommatoria tra la disciplina generale e quella lavoristica. In tal modo, non solo non ha realizzato l'opportuno adeguamento della protezione dei dati personali alle esigenze del rapporto di lavoro e del complessivo apparato giuridico che lo regola, ma ha determinato una parziale sovrapposizione tra le due discipline, causando interferenze e difetti di coordinamento* (G. Proia, *op. cit.*, 547).

[22] Diritto che la Corte Costituzionale ha incluso tra i diritti che formano il patrimonio irretrattabile della persona umana ai sensi dell'art. 2 Cost. Cfr. sentenza 3 febbraio 1994, n. 13 nella quale i giudici costituzionali definiscono il diritto all'identità personale come il diritto "ad essere se stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo".

personali, che non hanno ragione di essere divulgate nel "villaggio globale"[23] o che offrono una rappresentazione parziale o in grado di falsare l'immagine della persona. Nella prospettiva iniziale le informazioni riguardanti la persona, raccolte e diffuse dai mass media, erano prese in considerazione in un'ottica di esclusione dei terzi dalla sfera privata. L'esigenza di tutela veniva garantita inibendo la circolazione delle notizie, se lesive del diritto di riserbo della persona o imponendo la rettifica di quelle distorte, con un'attenzione circoscritta all'intimità domestica. Solo in un secondo momento si è estesa a tutte le manifestazioni della vita personale che *anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile* (Cass. civ. Sez. I, 27 maggio 1975, n. 2129).

La disciplina in materia di protezione della sfera personale si fonda inizialmente su disposizioni costituzionali orientate alla preminenza della dignità dell'uomo, intesa come bene supremo, che si declina anche attraverso la tutela della riservatezza della persona, della libertà morale e del libero sviluppo della sua personalità: con la Costituzione repubblicana la persona in sé diviene il valore primario attorno al quale ruota l'ordinamento giuridico.

Grazie alle riflessioni della dottrina civilistica, si viene individuando il fondamento normativo della riservatezza o, per dirla con F. Carnelutti, della privatezza[24], quale diritto della personalità, strettamente connesso alla dignità della persona, in una lettura sistematica e integrata di tutte quelle disposizioni costituzionali che individuano nello sviluppo della personalità umana uno dei principali obiettivi che deve essere perseguito dallo Stato e nel rispetto della dignità uno dei valori fondamentali e dei confini invalicabili all'azione pubblica e privata.

Il legislatore costituzionale pone la persona al centro dell'ordinamento giuridico: la dignità dell'uomo evoca la sfera più intima e preziosa dell'individuo, rappresenta il fondamento dell'intera costruzione giuridica dei diritti umani ed è motivo ispiratore della nostra carta costituzionale. Il suo rilievo in Costituzione prescinde dalle citazioni testuali e risalta dal testo costituzionale se oggetto di una lettura "in filigrana"[25]: attraverso un approccio ermeneutico che sia volto ad individuare i valori sottesi alle disposizioni stesse, si individua

[23] L'espressione è stata usata per la prima volta da Herbert Marshall McLuhan (1911-1980) nel suo saggio *Understanding Media: The Extensions of Man* (nella traduzione italiana "Gli strumenti del comunicare") nel 1964.

[24] F. Carnelutti, *Diritto alla vita privata – contributo alla teoria della libertà di stampa*, in *Riv. Trim. dir. pubbl*., 1955, 3. Cfr. anche S. Niger: *L'interesse della privatezza attiene all'aspetto della individualità: perché riflette unicamente l'aspirazione del soggetto a conservare quella tranquillità di spirito, quella pace interiore, che al suo modo d'essere privato si ricollega e che una pubblicità indesiderata turberebbe.* (S. Niger, *op. cit.*, 41).

[25] A. D'Atena, *In tema di principi e valori costituzionali,* in *Giurisprudenza Costituzionale*, n. 5/1997, 3065.

nella dignità dell'uomo un autentico valore giuridico e la dignità umana non può prescindere dalla riservatezza, ne costituisce uno degli elementi fondativi, ne rappresenta un aspetto e un presupposto, così che la tutela della dignità implica la tutela della riservatezza[26].

È ancora Stefano Rodotà ad offrirci un'acuta sintesi: *Nel quadro della privacy, la dignità si precisa come un concetto riassuntivo dei principi di riconoscimento della personalità e di non riduzione a merce della persona, di eguaglianza, di rispetto degli altri, di solidarietà, di non interferenza nelle scelte di vita, di possibilità di agire liberamente nella sfera pubblica.*

Questo vuol dire che i poteri pubblici non hanno solo un dovere negativo di astensione, di non interferenza nelle sfere individuali. Devono anche agire perché vi siano le condizioni positive che permettano a ciascuno di vivere in condizioni di dignità. Il diritto alla privacy rappresenta proprio una di queste essenziali condizioni[27].

Il riconoscimento di un autonomo diritto alla riservatezza si configura inizialmente quale *species* del *genus* diritti della personalità, che appartengono all'uomo in base ad una prospettiva giusnaturalistica, e, pur in assenza di un esplicito riconoscimento del diritto positivo, si configurano come diritti inviolabili. Attraverso un'interpretazione dell'articolo 2 della Carta Costituzionale non quale formula riassuntiva dei diritti della persona costituzionalmente riconosciuti, ma come clausola a fattispecie aperta, verrebbero immessi nell'ordinamento altri diritti dell'uomo, di cui si assicura il pieno riconoscimento e l'inviolabilità, in quanto garantiscono il rispetto e lo sviluppo della sua personalità. Grazie all'intermediazione della clausola generale contenuta nell'art. 2 Cost., che non si esaurisce nei diritti tipizzati, è possibile ricondurre le radici del diritto alla riservatezza al catalogo costituzionale.

Alla dottrina civilistica va il merito di aver riconosciuto ed individuato il fondamento normativo di un autonomo diritto alla riservatezza, quale diritto fondamentale della persona, in una prima fase circoscritto al diritto di escludere ingerenze esterne dalla propria sfera personale. La riservatezza assume inizialmente la natura di diritto a contenuto negativo, lo *ius excludendi alios,* basato sull'esigenza di non subire intrusioni nella propria sfera privata,

---

[26] *Una delle clausole generali più adoperata dalla giurisprudenza per delimitare l'area degli interessi apprezzabili soprattutto in relazione alla riservatezza e all'identità personale è proprio la clausola della dignità; contenuta non solo nei manifesti dei diritti fondamentali ma anche nei testi costituzionali di molti paesi dell'Unione europea.* (S. Niger, *op. cit.*, 47).

[27] S. Rodotà, *Privacy, libertà, dignità. Discorso conclusivo della 26° Conferenza internazionale sulla protezione dei dati.* Wroclaw, 14, 15, 16 settembre 2004.

espressione del diritto ad essere lasciato solo, tutela la dimensione intima e privata del singolo, fondata sull'isolamento della persona, collocata quasi in *a vacuum*.

Il merito della dottrina lavoristica è di aver riconosciuto ed imposto la dimensione sociale del diritto alla riservatezza, sviluppando una particolare attenzione alla vita di relazione, a partire dallo stesso articolo 2 Cost.: la Repubblica tutela i diritti inviolabili dell'uomo, non solo nella sfera individuale ma anche nelle relazioni sociali. La tutela dei diritti inviolabili dell'uomo avviene sia in quanto singola individualità, sia nelle formazioni sociali in cui si esplica la sua personalità e l'impresa si configura esattamente come una di quelle formazioni sociali.

Nel commentario alla Costituzione, a proposito dell'art. 2 C., Augusto Barbera scrive, citando K. Marx: La "persona" per non scadere ad "individuo" va considerata non solo nella sua "immanenza" e nel suo isolamento ma anche nella sua "apertura sociale", non solo "nell'isolamento dell'uomo dall'uomo" ma anche "nel legame dell'uomo con l'uomo"[28].

Nel percorso di definizione di un autonomo diritto alla riservatezza, vale menzionare una fondamentale sentenza della Corte di Cassazione, 27 maggio 1975, n. 2129[29], passata alla storia come "caso Soraya", che arriva al termine di circa un ventennio di oscillanti orientamenti giurisprudenziali e dottrinali e nella quale il diritto alla riservatezza ha trovato

---

[28] La suggestiva affermazione riportata da A. Barbera, in *Commentario della Costituzione, Principi fondamentali,* a cura di Giuseppe Branca, Zanichelli, 1975, 106 è di K. Marx, *La questione ebraica,* in Marx e Engels, Opere scelte, 93.

[29] Cass. civ., sez. I, 27 maggio 1975, n. 2129 Anche questo caso si origina da una controversia instaurata contro alcuni giornali che avevano pubblicato delle fotografie ritraenti l'ex imperatrice, Soraya Esfandiari, in atteggiamenti intimi con un uomo fra le mura della sua abitazione. *Deve ritenersi esistente nel nostro ordinamento un generale diritto della persona alla riservatezza, inteso alla tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti* (dalla massima). La Corte individua tre ambiti di riferimento del diritto alla riservatezza: *Con l'espressione "diritto alla riservatezza", una delle prime e più usate formulazioni del fenomeno, che non può essere più abbandonata, sono indicate diverse ipotesi, che implicano un problema, non solo di formula, ma anche di sostanza. Esse possono sintetizzarsi almeno in tre aspetti. Da una parte si tende a restringere rigorosamente l'ambito di questo diritto al riserbo della "intimità domestica", collegandola al concetto ed alla tutela del domicilio. A questa concezione corrisponde forse il "the right to be alone" degli anglosassoni. All'opposto vi sono formulazioni molto generiche, il riserbo della "vita privata" da qualsiasi ingerenza, o la c.d. "privatezza" (privacy), cui corrisponderebbe un sostanziale ambito troppo vasto o indeterminato della sfera tutelabile.*

Una concezione intermedia, che riporta in limiti ragionevoli la portata di questo diritto, può identificarsi nelle formule che fanno riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza). Fondamentale per il riconoscimento di un autonomo diritto alla riservatezza anche Corte Costituzionale sent. 12 aprile 1973 n. 38.

Nel senso dell'inesistenza di un autonomo diritto alla riservatezza si vedano anche Cass. civ. sez. I 22 dicembre 1956, n. 4487 e Cass. civ. 7 dicembre 1960, n. 3199.

un primo esplicito riconoscimento quale autonomo diritto soggettivo, ancora una volta in contrapposizione al diritto di cronaca. Anche la Suprema Corte ha fondato l'autonomia del diritto alla riservatezza attraverso il riferimento a principi costituzionali (articoli 2, 13, 14, 15, 29 C.) e all'espresso riconoscimento in deliberazioni di carattere internazionale, la Dichiarazione Universale sui diritti dell'uomo, 1948 e la Convenzione europea diritti dell'uomo, 1950. La Corte affronta preliminarmente la questione relativa alla tesi della configurabilità di un autonomo diritto alla riservatezza delle proprie vicende personali ed individua tre ambiti di riferimento della nozione di riservatezza: da quello ristretto all'intimità domestica collegata alla tutela del domicilio, si passa ad una concezione intermedia che fa riferimento alla intimità personale in una certa sfera della vita personale e familiare, includendovi alcune manifestazioni della vita di relazione in un domicilio ideale, anche non legato al tradizionale concetto di domicilio, fino ad una concezione ampia della privacy e del riserbo della vita privata, cui corrisponderebbe un ambito indeterminato della sfera tutelabile da qualsiasi ingerenza.

È significativa la conclusione della Suprema Corte: superando le vie della *analogia iuris* o del ricorso ai principi generali dell'ordinamento, i giudici ritengono possibile individuare un fondamento normativo e una tutela diretta del diritto soggettivo alla riservatezza non soltanto nella prima ristretta accezione, ma anche per l'ambito indicato dalla terza concezione, ritenendo che una tutela del diritto alla riservatezza più ampia di quella circoscritta all'intimità domestica, non solo non contrasti con i principi costituzionali, ma trovi in essi vari motivi di convalida (Cass. Civ. sez. I, 27 maggio 1975, n. 2129)[30].

Espressione di una aspirazione, poi di una pretesa, la privacy è stata affidata inizialmente all'elaborazione giurisprudenziale e dottrinale, a giudici e giuristi particolarmente sensibili ai valori della persona, che l'hanno ricondotta ad una lettura delle norme costituzionali che delineasse un diritto radicato nel più generale diritto della personalità e che non si esaurisse nella pretesa ad essere lasciati soli.

In tema di rapporti economici l'articolo 41 C. costituzionalizza il principio di bilanciamento tra *esigenze produttive* ed *istanze protettive*[31], tra la sfera dell'avere e quella dell'essere, tra le ragioni organizzative e di buon andamento dell'impresa, il riconoscimento della libertà di

[30] Questa sentenza era stata preceduta da una sentenza della Corte Costituzionale, 12 aprile 1973, n. 38 nella quale già si affermava che tra i diritti inviolabili sanciti dall'art. 2 Cost. oltre al diritto all'onore, al decoro e alla reputazione, rientrasse anche il diritto all'intimità e alla riservatezza. Onore, decoro, reputazione, riservatezza, identità personale non costituiscono autonomi oggetti di tutela ma distinte manifestazioni della persona umana nella sua interezza, che è il vero bene tutelato.

[31] A. Trojsi, *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli, Torino 2103, 105.

iniziativa economica privata da una parte e la tutela della libertà e della dignità del lavoratore dall'altra. Il secondo comma dell'articolo 41 *"esplicita un "ordine" assiologico tra gli interessi eventualmente in conflitto: esso traccia, cioè, uno schema di bilanciamento tra la libertà di impresa e la tutela della persona implicata nel processo produttivo, in cui la prima cede al rispetto della sicurezza, della libertà e della dignità umana, in diretta applicazione del combinato disposto degli articoli 2 e 3 co. 2, Cost., ovvero della necessità di garantire il pieno sviluppo del lavoratore nella formazione sociale ove (più che altrove) si svolge la sua personalità"*[32]. Lo stesso secondo comma art. 41 C. segna il limite che la libertà di impresa economica non può valicare, impone all'imprenditore di non esercitare la sua libertà di iniziativa economica facendo valere la sua posizione dominante in modo da ledere la sicurezza, la libertà e la dignità umana del lavoratore. Sancisce il primato della dignità umana sulla libertà di impresa e afferma il principio fondamentale secondo cui dovrà ricercarsi un modello che pone la produzione al servizio dell'uomo e dei suoi valori e mai il contrario[33].
In questo senso già nella sentenza della Corte Cost. 30 dicembre 1958 n. 78 si affermava che la dignità figura tra i limiti di ordine negativo alla libera iniziativa economica privata, e si declinava la nozione di dignità includendovi sia l'incolumità che l'assenza di umiliazione o di sfruttamento del lavoratore[34].Le esigenze della produzione non possono in nessun caso pregiudicare, oltre che l'integrità psicofisica, la personalità morale del lavoratore: il rispetto e la tutela di quest'ultima si pongono come espresso limite alla libertà di iniziativa economica privata e come obbligo a carico del datore di lavoro[35].
Attraverso la valorizzazione della dignità umana e l'elaborazione del concetto di riservatezza, la dottrina civilistica ha il merito di aver posto le fondamenta del moderno diritto alla protezione dei dati personali. Tuttavia, accreditare una concezione della riservatezza basata sull'isolamento della persona avrebbe condotto a vietare qualsiasi forma

[32] V. Nuzzo, *La protezione del lavoratore dai controlli impersonali,* Editoriale Scientifica, Napoli, 2018, 28.
[33] A. Ingrao, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy*: *una lettura integrata,* Cacucci Editore, Bari, 2018, 15-18.
[34] Cfr. Corte Cost. 78/1958 Nel dichiarare l'illegittimità costituzionale del decreto legislativo del Capo Provvisorio dello Stato 16 settembre 1947, n. 929, ratificato con legge 17 maggio 1952, n. 621, in riferimento agli articoli 38, 41, 42, 44 della Costituzione, contenente norme circa il massimo impiego di lavoratori agricoli (con assunzioni di manodopera imposte dal Prefetto) rileva che: *Nel secondo comma dell'art. 41 C. sono posti limiti di ordine negativo alla libera iniziativa privata: essa non può svolgersi in contrasto con l'utilità sociale in senso collettivo, essa non può comunque recar danno alla sicurezza, alla libertà, alla dignità umana (attività nocive alla salute e incolumità dei cittadini o che importino umiliazione o sfruttamento dei lavoratori).*
[35] La tutela della dignità della persona entra a pieno titolo, per effetto dell'art. 2087 c.c., nella relazione contrattuale lavoristica come obbligazione del datore di lavoro. Le norme del codice civile stabiliscono infatti il dovere dell'imprenditore di tutelare anche la personalità morale del lavoratore: "L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro".

di controllo sull'operato del lavoratore, una concezione incompatibile con la funzionalità stessa dell'organizzazione aziendale. Il controllo è un elemento essenziale anche ai fini della qualificazione del rapporto di lavoro come subordinato: la conclusione di un contratto di lavoro e il concetto stesso di lavoratore subordinato sono di per sé incompatibili con il divieto di qualsiasi ingerenza nella sfera privata del lavoratore[36].

La dottrina lavoristica, rispetto alla concezione privatista che intendeva la riservatezza come esclusione di qualsiasi apertura della sfera privata del singolo lavoratore all'interazione con terzi, ha necessariamente modificato l'ambito del diritto alla riservatezza ponendo però una serie di limiti al potere di controllo per rendere effettiva la tutela dei diritti del lavoratore. L'oggetto dell'originario diritto alla riservatezza si differenzia notevolmente dal contenuto del moderno diritto alla protezione dei dati personali: la visione statica del diritto alla riservatezza, inizialmente sovrapponibile al diritto ad essere lasciati soli, mero interesse all'isolamento, è stata progressivamente sostituita da una visione dinamica del diritto alla privacy, presupposto per lo sviluppo di altri diritti individuali, e quindi dal diritto di mantenere il controllo sulla circolazione delle proprie informazioni personali - che spesso l'individuo stesso fornisce per usufruire di servizi - e di determinare liberamente le modalità della costruzione della propria sfera privata. La privacy diventa parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può svilupparsi in armonia con i postulati della dignità umana[37].

Si sono rivelate profetiche le riflessioni di uno Stefano Rodotà che nei primi anni '70 già ci indicava la direzione: Dovrebbe essere ormai chiaro che una tutela della riservatezza, adeguata all'ambiente in cui viviamo, richiede soprattutto la possibilità di controllare la stessa attività di raccolta delle informazioni, il modo del loro trattamento, le sedi in cui le informazioni sono raccolte. Nella definizione della riservatezza, quindi, entra come parte integrante non solo il diritto di respingere le invasioni della sfera privata, ma soprattutto il diritto di controllare il flusso di informazioni riguardanti un determinato soggetto[38].

Nel 1997 Rodotà individuava nella riservatezza e nella trasparenza, nella protezione della sfera privata da indebite ingerenze esterne e nel controllo dei propri dati, veri e propri strumenti di progresso sociale. L'affermazione della privacy con la redistribuzione del potere informativo che comporta, ha, almeno in parte, corretto le asimmetrie che hanno

[36] A. Ingrao, *op. cit.*, 19.
[37] C. Cost. 23 luglio 1991, n. 366.
[38] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 130.

caratterizzato il rapporto tra dignità umana e iniziativa economica, per tornare al binomio contenuto nell'art. 41 della Costituzione[39].

1.3 Il diritto alla riservatezza del lavoratore subordinato: lo Statuto dei lavoratori

Mentre voci autorevoli del diritto civile elaboravano teorie a fondamento dell'esistenza e della necessità di tutela del diritto alla riservatezza, nella più nota ed importante fabbrica italiana si andavano accumulando fascicoli informativi sui lavoratori: 354.077 schede sono state raccolte tra il 1949 e il 1971 dall'ufficio servizi generali della FIAT, un vero e proprio dettagliato archivio di informazioni personali e di notizie riservate sulla vita privata e non, dei dipendenti o aspiranti tali. L'ufficio era impegnato nella acquisizione di informazioni e nell'effettuazione di investigazioni private di ogni genere e con ogni mezzo, nei confronti di lavoratori da assumere, da promuovere o che in qualsiasi modo fossero entrati o stessero per entrare in contatto con l'azienda[40]. C. Jemolo, citato nella prefazione al libro della Guidetti Serra sulle schedature Fiat, constatava amaramente che l'ideale liberale dello Stato, casa comune aperta a tutti, ove gli uomini dabbene erano tutti di pari dignità, in cui non si chiedeva a nessuno se avesse una fede religiosa e quale, è nella pratica completamente abbandonato[41].

La lettura delle schede ci racconta di un'altra costituzione nella Fiat: dalle schede emerge un'attività spionistica, connotata da un'inequivocabile discriminazione politica, sindacale e religiosa, che vede i poteri pubblici complici e asserviti all'interesse privato. Il pregiudizio anticomunista e antisindacale imperversa, così come un'attenzione esasperata per una religiosità apparente e una rispettabilità familiare di facciata, comportamenti ritenuti moralmente riprovevoli vengono stigmatizzati[42]. La Fiat, attraverso quelle schedature, tentava di controllare ogni forma di dissenso politico interno, di azione sindacale, di

[39] A. Soro, *Persone in rete*, Fazi editore, Roma, 2018, 6.

[40] Malgrado siano trascorsi molti anni dalle schedature Fiat, è molto più recente (2006) la notizia dello scandalo Telecom Italia: la schedatura di centinaia di dipendenti o aspiranti tali di Telecom e Pirelli, migliaia di fascicoli illegali raccolti all'insaputa dei lavoratori dalla security aziendale. I vertici Telecom, a margine del processo avviato anche per questi fatti, hanno deciso di patteggiare, offrendo ad ogni dipendente spiato un risarcimento che ammonterebbe a circa 3.000 euro ciascuno. Il caso è citato da M. Paissan, *E-mail e navigazione in Internet: le linee del Garante,* in P. Tullini, *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro,* Cedam, 2010.

[41] B. Guidetti Serra, *Le schedature Fiat, Cronaca di un processo e altre cronache*, Rosenberg&Sellier, Torino, 1984, 10.

[42] *A comprova della sua tendenza verso il partito comunista tutti gli anni quando passa il sacerdote per la benedizione delle case, gli viene vietata l'entrata", "l'essere nenniano non è considerato un elemento di favore ma motivo di sospetto, mentre un'inclinazione saragattiana redime*. (B. Guidetti Serra, *op. cit.*).

comportamento sociale non conforme alla "normalità". Dobbiamo a questo clamoroso episodio la consapevolezza che il problema della privacy non era la tutela di un egoismo del singolo, non era semplicemente il diritto a essere lasciati soli. Era in gioco una fetta consistente della libertà, a cominciare da quella di associazione politica, e del diritto al lavoro uguale per tutti. Da lì, proprio dal nesso fra privacy e schedature FIAT, è nata una nuova consapevolezza politica del problema[43].

Simili violazioni alla libertà e alla dignità del lavoratore, oggetto di puntuale e circostanziata denuncia nel testo della Guidetti Serra, sono documentate anche da altre fonti dell'epoca: dagli atti del Convegno nazionale della Società Umanitaria sulle condizioni del lavoratore nell'impresa industriale[44], dalla relazione della Commissione parlamentare d'inchiesta sulle condizioni dei lavoratori in Italia, istituita dalla legge n. 96/55, che impegna il Parlamento in un'indagine conoscitiva sulla situazione dei lavoratori nelle aziende[45] e da alcune decisioni giurisprudenziali dalla cui lettura emergono violazioni odiose dei diritti della persona diffusamente perpetrate nei luoghi di lavoro[46].

È significativa l'ordinanza del pretore di Monopoli, 27 ottobre 1970, nella quale, accertata l'esistenza di un clima di dura avversione ad ogni attività sindacale dei lavoratori, vietava le aperture a vetro alle porte dei "gabinetti di decenza" che consentivano l'osservazione da fuori, ordinando che agli stessi fossero apposte chiusure dall'interno. Si legge nella motivazione dell'ordinanza che "l'apertura delle finestrelle aveva il preciso scopo di creare all'interno della fabbrica un clima oppressivo che valesse a scoraggiare gli operai da iniziative sindacali: il lavoratore che sa d'essere controllato dalla direzione perfino nel suo atto più innocuo e normale, qual è il bisogno fisiologico, è verosimilmente portato a ritenere che egualmente egli sarà sotto controllo in ogni altro discorso o atteggiamento specie se di tipo sindacale. Ecco quindi che l'introduzione degli spioncini alle porte dei gabinetti di

[43] S. Rodotà, *Intervista su privacy e libertà*, Laterza, Bari, 2005, 26-28.

[44] Al Convegno di studio tenutosi a Milano nei giorni 4, 5 e 6 giugno 1954 viene invitato il Segretario della CGIL, Giuseppe Di Vittorio e in questa occasione l'Umanitaria sarà coinvolta nella stesura dello Statuto dei lavoratori.

[45] Nel Resoconto stenografico dell'audizione dei vertici delle principali aziende italiane presso la X Commissione permanente del Senato, seconda seduta del 26 marzo 1969, si legge: il Senatore Brambilla rivolge al direttore del personale e per le relazioni sociali della società Fiat, Sig. Garino, una domanda riguardo la sorveglianza che si effettua quando gli operai si ritirano nei *luoghi di decenza* e sul tempo che vi si trattengono. Il sig. Garino elusivamente replica*:* Il sorvegliante, se in un suo giro normale trova un operaio addormentato in un magazzino, secondo le disposizioni molto chiare che gli abbiamo dato, non ha il potere di prendere un provvedimento e, ad eccezione di quello che è un semplice richiamo di carattere personale, deve soltanto segnalare l'infrazione al suo capo diretto.

[46] Pretura di Torino 25 luglio 1955, in *Riv. giur. lav*. 1955, II, 384. Il pretore di Torino nell'ordinanza del 25 luglio 1955 interveniva per condannare l'operato dei responsabili Fiat che "infiltravano" fra gli operai una guardia giurata, sotto mentite spoglie, mimetizzata da "falso lavoratore" ed in realtà adibita a "spiare" gli altri operai e a riferire al datore di lavoro chi fossero i promotori di uno sciopero in preparazione.

decenza finisce per esprimere plasticamente agli occhi dello sprovveduto e già mal fermo operaio - ex contadino della ceramica l'apparato di controllo potenzialmente repressivo, cui egli soggiace in seno alla fabbrica"[47].

In questo clima di scarsa considerazione e rispetto per la dimensione privata dei prestatori di lavoro si approva lo Statuto dei Lavoratori con il quale, come titolò l'Avanti, la Costituzione entra in fabbrica e si realizza la prima formalizzazione del diritto alla riservatezza, quale valore da garantire e tutelare nell'ordinamento giuridico, restando per un certo tempo questa l'unica norma di diritto positivo di riferimento per la tutela della riservatezza, quale diritto della persona[48]. Paradossalmente un diritto ritenuto tipico della borghesia trova il suo primo riconoscimento legislativo nella carta dei diritti dei lavoratori: nasce come reazione all'uso delle informazioni personali quale strumento di discriminazione politica e sindacale dei lavoratori e contro i crescenti rischi per la dignità dei lavoratori legati ai controlli a distanza e alla possibilità di trattare le informazioni attraverso gli elaboratori elettronici[49].

Nel titolo I dello Statuto dei lavoratori, intitolato "Della libertà e dignità del lavoratore", il legislatore ha per la prima volta previsto e disciplinato, limitandone i modi di esercizio, il potere di controllo del datore di lavoro, mai nominato espressamente nel codice civile, ma riconosciuto quale corollario del potere direttivo e presupposto di quello disciplinare[50]. A proposito del termine dignità Antonino Cataudella ha osservato che: *Il termine dignità, quando adoperato senza particolari specificazioni, è atto ad assumere il significato più comprensivo. Nello Statuto dei lavoratori, la dignità comprende tutte le qualità tali da individuare un soggetto umano e abbraccia una sfera assai estesa di interessi; e di essa la difesa della riservatezza è un aspetto preminente*[51].

---

[47] Pretura di Monopoli, 27 ottobre 1970, F.i.l.c.e.a.-C.g.i.l. c. Soc. ceramiche Puglie, in *Foro It.,* 1971, I, 1060.

[48] Gragnoli afferma efficacemente che il diritto alla riservatezza in Italia ha "fatto ingresso nell'ordinamento attraverso il portone dello Statuto" (E. Gragnoli, *Dalla tutela della libertà alla tutela della dignità e della riservatezza dei lavoratori*, in ADL, 1/2007, 1211).

[49] S. Niger, *op. cit*., 52-53.

[50] È significativa la collocazione delle norme sul controllo dei lavoratori nel Titolo I dello Statuto dedicato alla tutela della dignità e della libertà del lavoratore.

[51] A. Cataudella, *La "dignità" del lavoratore. Considerazioni sul titolo I dello Statuto dei lavoratori*, in *Diritto del lavoro,* 1973, I, 5 e ss. V. anche R. Romei: *accogliendo un'interpretazione molto ampia del termine "dignità" che finisce per assolvere la funzione di un contenente in grado di recepire tutti i valori richiamati dal titolo primo dello Statuto dei lavoratori o dalle norme costituzionali. E quindi "dignità" come tutela della personalità del lavoratore; come libertà di manifestazione delle proprie opinioni e del proprio pensiero; come pudore e come riservatezza, intesa quest'ultima non solamente nell'accezione più ristretta di interesse ad impedire le altrui intrusioni nella propria vita privata, ma anche in quella, più ampia e comprensiva, di "interesse ad impedire la cognizione delle proprie vicende (sia interne che esterne alla propria sfera privata) da parte degli estranei.* (R. De Luca Tamajo, R. Imperiali, C. Pisani, R. Romei, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Franco Angeli, Milano, 1988, 125).

In risposta al clima vessatorio esistente nelle aziende, il legislatore del 1970 ha voluto escludere la legittimità di forme di controllo che eccedano i limiti della cosiddetta subordinazione tecnica: il potere di controllo dell'imprenditore è funzionalizzato all'interesse oggettivo dell'impresa che rappresenta il limite interno di quel potere.

Lo Statuto stabilisce così il divieto di indagini sulle opinioni politiche, religiose o sindacali del lavoratore: l'art. 8 St. lav. pone un divieto di indagine sull'orientamento ideologico del lavoratore e su fatti ritenuti ininfluenti rispetto alla valutazione dell'attitudine professionale e della prestazione lavorativa, individuando delle "zone di riserbo" del lavoratore. In questo modo "l'art. 8 tutelava, quando ancora non si parlava di privacy, la riservatezza del lavoratore subordinato dai possibili rischi derivanti da illegittime intromissioni del datore nella sua vita privata[52] circoscrivendo "il rilievo della persona del lavoratore in relazione a quanto è funzionalmente collegato con la soddisfazione dell'interesse del creditore di lavoro"[53].

Il legislatore del 1970 mostra una nuova sensibilità per i rischi connessi alle schedature ed evidenzia il percorso di trasformazione della domanda di riservatezza, che non ha più solo una connotazione individualistica, ma è espressione della richiesta di protezione da parte della classe dei lavoratori, costantemente sottoposti al rischio di controlli occulti che restringono e condizionano la sfera intangibile della persona. Al tempo stesso è espressione di un'esigenza di tutela estesa ad un contesto relazionale, dove sia consentita al singolo la libera estrinsecazione della sua personalità nell'interazione con gli altri e dove devono essere contemperate le opposte legittime esigenze del datore e del lavoratore[54].

Nell'ambito del rapporto di lavoro esiste un'inscindibile relazione tra esercizio del potere di controllo e libertà della persona, tra vigilanza e rispetto della riservatezza ed il legislatore dello Statuto si preoccupa di contenere le ingerenze del datore di lavoro, attraverso un processo di costruzione di limiti ai poteri datoriali, rispetto al rischio di una totale espropriazione dello spazio di libertà e di riservatezza del lavoratore. Furono ritenuti illeciti tutti quei controlli in grado di ledere la dignità della persona e la sua libertà morale per le modalità disumane con cui venivano esercitati, in quanto occulti, spionistici e polizieschi: questo vale tanto per i controlli effettuati tramite personale di vigilanza (art. 3 St. lav.) quanto

[52] A. Levi, *Il controllo difensivo a distanza e l'inoperatività dell'art. 4 dello Statuto*, in *Il lavoro nella giurisprudenza*, 5/2018, 478.
[53] O. Mazzotta, *Diritto del Lavoro*, IV ed., Giuffrè, Milano, 2011, 536.
[54] C. Colapietro, *Digitalizzazione del lavoro e tutela della riservatezza della persona*, in P. Tullini, (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Torino, 2017, 27.

a maggior ragione per i controlli a distanza effettuati tramite strumenti tecnologici (art. 4 St. lav.).

Il legislatore del 1970, con gli articoli 2 e 3 St. lav., non intende impedire o contrastare il controllo sull'esatto adempimento degli obblighi derivanti dal contratto di lavoro, che è e resta legittimo, ma, al fine di tutelare il valore della persona partecipe dell'attività produttiva, intende precluderne quelle modalità poliziesche, potenzialmente lesive della dignità umana, basate sul controllo occulto del lavoratore, oggetto inconsapevole di sorveglianza da parte di personale non identificato e identificabile, così che il lavoratore non fosse sottoposto ad una continua pressione psicologica, alimentata dal costante timore di essere colto in fallo e quindi di subire sanzioni disciplinari. La *ratio* delle disposizioni statutarie è proprio quella di mantenere il controllo in una dimensione umana, vietando i controlli occulti e consentendo al lavoratore di sapere che è controllato, nel momento in cui lo è[55]. Il legislatore ha per la prima volta inteso realizzare un tentativo di mediazione tra le esigenze organizzative e produttive dell'impresa e la tutela della libertà e dignità dei lavoratori, secondo l'idea madre dello Statuto per cui l'organizzazione deve modellarsi sull'uomo, e non viceversa[56]. Il datore può certamente vigilare sul comportamento solutorio ma entro i limiti del controllo uomo-uomo, che è l'unico capace di rendere possibile un confronto immediato tra due intelligenze umane, senza alimentare nel soggetto vigilato preoccupazioni di un eventuale esercizio del potere disciplinare soggettivamente percepito come incombente[57].

Più complesso è il caso dei controlli a distanza effettuati attraverso impianti audiovisivi, controlli potenzialmente continui e anelastici, in grado di eliminare ogni zona di riservatezza e di autonomia nello svolgimento della prestazione e più difficili da conciliare con il principio di trasparenza. Gli impianti audiovisivi e le altre apparecchiature dalle quali può derivare un controllo a distanza dell'attività dei lavoratori sono in grado di effettuare il controllo continuo, automatizzato ed impersonale della macchina sull'uomo, che non ha nulla di umano e non consente al lavoratore di sapere se, quando e per quanto tempo i suoi comportamenti nel luogo di lavoro siano monitorati. L'art. 4 St. lav., pensato per le telecamere a circuito chiuso e riferito poi anche ad altre apparecchiature e strumenti, racchiude al suo interno l'instabile equilibrio tra il diritto alla salvaguardia della dignità e

[55] Così come è stabilito dall'art. 3 St. lav. Personale di vigilanza. I nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa debbono essere comunicati ai lavoratori interessati.
[56] L. Mengoni, *Le modificazioni del rapporto di lavoro alla luce dello Statuto dei lavoratori*, in Aa.Vv., *L'applicazione dello Statuto dei lavoratori*, Milano, 1973, 23.
[57] A. Ingrao, *op. cit.*, 27.

della personalità del lavoratore nei luoghi di lavoro, in attuazione dei richiamati principi costituzionali, e l'interesse del datore di lavoro all'esercizio dell'attività di impresa.

Come ribadito recentemente dalla Cassazione, Sez. lav., 8 novembre 2016, n. 22662, "L'art. 4 fa parte di quella complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore, sul presupposto - espressamente precisato nella Relazione ministeriale - che la vigilanza sul lavoro, ancorché necessaria all'organizzazione produttiva vada mantenuta in una dimensione umana e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua ed anelastica, eleminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro (Cass. 17 luglio 2007 n. 15982; conforme Cass. 23 febbraio 2012 n. 621115)".

Come vedremo con la riscrittura dell'art. 4 St. lav. del 2015, tale distinzione appare meno limpida e il controllo tecnologico, soprattutto se esercitato attraverso gli strumenti di lavoro, risulta ora associato anche all'area dell'adempimento e dell'attività dei lavoratori[58].

A differenza di quanto previsto negli artt. 2 e 3 St. lav. che fanno riferimento alla vigilanza sull'"attività lavorativa", l'art. 4 St. lav., nella sua originaria formulazione, esordiva con un'affermazione di principio, un perentorio divieto di controllo sull'"attività dei lavoratori"[59], espressione che racchiude in sé sia i comportamenti solutori che altri comportamenti non funzionali all'adempimento della prestazione ed inerenti alla sfera personale. Con il divieto di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dell'"attività dei lavoratori" non solo si intendeva stigmatizzare il controllo sulla prestazione attraverso tali impianti, ma si intendeva porre un divieto più ampio che include tutti i comportamenti, anche le attività che esulano dall'adempimento della prestazione, pur se svolte in occasione dell'esecuzione della stessa, comprese le cosiddette licenze comportamentali, proprio in considerazione dell'anelasticità e pervasività degli strumenti di controllo, in grado di registrare senza distinzione sia l'esecuzione della prestazione che ogni altra attività che il lavoratore compia sul luogo di lavoro[60].

---

[58]P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in P. Tullini, (a cura di) *Web e lavoro*, *op.cit.*, 9.

[59] Il termine "distanza" ricomprende sia la distanza in senso spaziale che la distanza in senso temporale (Cass.civ. sez. lav. n. 1236 del 18 febbraio 1983), mentre la locuzione "attività dei lavoratori" ricomprende non solo lo svolgimento della prestazione lavorativa, ma ogni comportamento posto in essere durante l'orario di lavoro.

[60] Si tratta di gesti e comportamenti di carattere personale di cui è inevitabilmente costellata la giornata lavorativa. L'uso per fini non lavorativi delle risorse telematiche aziendali nella scienza economica dell'organizzazione, è denominato cyberslacking o cyberloafing e annovera al suo interno una gamma di

Si stabiliva una netta distinzione concettuale tra la verifica del corretto adempimento della prestazione e la vigilanza diretta a soddisfare esigenze organizzative ed interessi esterni al rapporto di lavoro.

L'art. 4 St. lav. vietava esplicitamente un controllo che si riteneva eliminasse ogni spazio di riservatezza e sottoponesse il lavoratore ad un controllo automatizzato ed "inumano" proprio per la sua estensione spazio temporale. Il controllo esercitato "a distanza" nello spazio rendeva il lavoratore controllabile da un luogo diverso e distante da quello nel quale si stava svolgendo la prestazione e un controllo differito nel tempo lo rendeva controllabile in un momento diverso, successivo rispetto all'esecuzione della prestazione, esponendolo ad un potenziale controllo ininterrotto. Si configurava pertanto come anelastico, continuativo e inumano e per questo lesivo del bene della dignità del lavoratore, alla cui protezione la disciplina statutaria era espressamente dedicata, come si legge nella relazione di accompagnamento del Ministro del Lavoro Brodolini[61].

Al comma 2 la norma specificava per quali esigenze e a quali condizioni l'utilizzo degli impianti audiovisivi o delle altre apparecchiature di controllo poteva essere legittimo, pur potendo dar luogo al controllo sull'attività dei lavoratori. I poteri datoriali risultavano limitati attraverso la tecnica del "giustificato motivo", nonché attraverso la previsione di una procedura autorizzativa: la possibilità del controllo a distanza indiretto dell'attività dei lavoratori era consentita qualora fosse motivata da esigenze aziendali qualificate e previo accordo con i sindacati o autorizzazione amministrativa[62].

In presenza di esigenze organizzative e produttive o per garantire la sicurezza del lavoro, e a fronte di un preventivo accordo con le rappresentanze sindacali aziendali o di un provvedimento autorizzativo dell'Ispettorato del lavoro (oggi Direzione Territoriale del Lavoro), che dettavano le modalità per l'uso degli impianti e verificavano le esigenze

---

attività online, che spaziano dall'utilizzo della connessione per socializzare, per svolgere commissioni personali e, talvolta, anche per realizzare comportamenti indecenti. I lavoratori "catturati nella rete informatica" attuano condotte che oltre a costituire forme di devianza produttiva, perché distraggono tempo ed efficienza al lavoro, comportano dei costi per l'impresa imputabili all'attività illecita svolta in rete, che può compromettere la sicurezza dei sistemi informatici e la funzionalità della banda". (A. Ingrao, *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 Costituzionale AIC*, 3/2016, 2).

[61] Il disegno di legge n. 738, presentato nel giugno 1969, con relazione di accompagnamento del Ministro del Lavoro Brodolini, contenente *Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro* è destinato a diventare lo Statuto dei lavoratori. Nella Relazione si legge: "Il proposito del disegno di legge è di contribuire a creare un clima di rispetto della dignità e libertà umana nei luoghi di lavoro, riconducendo l'esercizio dei poteri direttivo e disciplinare dell'imprenditore nel giusto alveo e cioè in una stretta finalizzazione allo svolgimento delle attività produttive".

[62] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D.lgs. n. 151/2015)*, in *Rivista Italiana di Diritto del Lavoro*, n. 1/2016, 77.

organizzative e produttive o di sicurezza del lavoro, potevano installarsi impianti e apparecchiature da cui potesse derivare un controllo a distanza. Queste apparecchiature avrebbero potuto determinare "incidentalmente" un controllo dell'attività dei lavoratori: si trattava di un "effetto collaterale", di un controllo cosiddetto "preterintenzionale" sull'attività dei lavoratori, in quanto la loro finalità principale era un'altra[63]. L'accordo o la procedura autorizzativa avrebbero dovuto realizzare il contemperamento tra il generale divieto di utilizzo dei mezzi di controllo a distanza dell'attività dei lavoratori (comma 1) e le esigenze organizzative, produttive ovvero di sicurezza del lavoro.

L'articolo 4 St. lav. proseguiva poi con un comma dedicato ad aspetti di diritto transitorio, sul trattamento degli impianti già esistenti al momento dell'entrata in vigore della norma[64], e con la disciplina del regime delle impugnazioni nei confronti dei provvedimenti emessi dalle Sezioni territoriali delle Direzioni regionali e provinciali del lavoro da presentare entro 30 giorni al Ministero per il Lavoro e la Previdenza Sociale.

1.4 La normativa statutaria alla prova dell'evoluzione del contesto socio economico

Per un certo tempo l'interpretazione integrativo-evolutiva della giurisprudenza era riuscita ad adeguare le disposizioni dello Statuto ai mutamenti socio-economici in atto: con una

[63] *In applicazione di tali principi è stata ritenuta inammissibile l'installazione unilaterale di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori, benché non destinati all'attività lavorativa, quali bagni, spogliatoi, docce, armadietti e luoghi ricreativi. Lo stesso vale per le telecamere collocate nei luoghi di lavoro, anche se non destinate a riprendere i posti di lavoro dei dipendenti. Pertanto le garanzie previste dall'art. 4, secondo comma, St. lav. vanno osservate sia all'interno degli edifici sia in altri luoghi in cui si svolge la prestazione di lavoro, così come rilevato dal Garante per la protezione dei dati personali a proposito delle telecamere installate sugli autobus, le quali non devono riprendere in modo stabile la postazione di guida e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti.* (C. Zoli, *Il controllo a distanza del datore di lavoro: l'art. 4, L. N. 300/1970 tra attualità ed esigenze di riforma,* in *Rivista Italiana di Diritto del Lavoro,* n. 1/2009, 488).
Sulla preterintenzionalità dei controlli vedi in senso critico R. Del Punta: *Anche a trattenersi dal sorridere di fronte all'evocazione di un datore di lavoro che controlla i lavoratori al di là delle proprie intenzioni, affermare che il controllo è lecito soltanto quando è "preterintenzionale" dovrebbe implicare, per coerenza, un'indagine sull'elemento soggettivo del datore di lavoro. Ma di una tale indagine non si è mai materializzata neppure l'ombra nelle aule giudiziarie, anche perché essa non avrebbe alcun senso.* E in senso contrario si veda M. Barbieri: *Quando si parlava di "controlli preterintenzionali" […] lo si faceva per metafora, non intendendosi affatto indagare sull'elemento soggettivo della decisione datoriale, bensì sugli effetti di un controllo che avesse altre finalità da quella, allora vietata dal co. 1 dell'art. 4 St. lav., di controllo sulle prestazioni lavorative*. (*L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in P. Tullini (a cura di), *op. cit.*, 185).

[64] Il legislatore del Jobs Act ha omesso d'inserire nella norma indicazioni sul regime applicabile agli strumenti installati prima della riforma, cosa che aveva fatto invece il legislatore del 1970, prevedendo espressamente (art. 4, comma 3, St. lav.) che il datore di lavoro avesse a diposizione un anno dall'entrata in vigore dello Statuto dei lavoratori per mettere a norma le apparecchiature già installate.

nozione aperta di "impianti audiovisivi e altre apparecchiature" per limitare gli effetti potenzialmente invasivi dei nuovi strumenti tecnologici utilizzati nell'impresa, con la categoria dei controlli difensivi per garantire adeguata tutela al patrimonio aziendale e con un tentativo di coordinamento tra la disciplina a tutela dei dati personali di derivazione comunitaria e quella di settore.

Nel corso degli anni, però, l'art. 4 St. lav. ha mostrato con sempre più evidenza i segni del tempo e l'equilibrio complessivo della disciplina statutaria si è andato progressivamente incrinando, tra l'altro in un clima di diffusa elusione della norma: i dispositivi da cui derivava il controllo finivano per essere utilizzati in assenza di qualunque procedura sindacale o amministrativa.

Due elementi in particolare hanno messo in luce la progressiva inadeguatezza del quadro giuridico esistente, probabilmente due aspetti del medesimo processo evolutivo. In primo luogo, l'evoluzione tecnologica ed informatica che ha investito tanto le modalità esecutive della prestazione di lavoro quanto l'organizzazione del lavoro, con la diffusione di dispositivi necessari allo svolgimento della prestazione lavorativa, ma idonei anche a registrare una pluralità di informazioni sull'attività svolta dal lavoratore e sul lavoratore stesso[65]. In secondo luogo, l'ambito stesso della riservatezza, alla cui protezione era volta la norma statutaria, si è arricchito ed ampliato, evolvendosi dal diritto ad essere lasciato solo, verso il diritto al governo dei propri dati personali. Lo riconosceva la Corte Costituzionale tedesca nel 1983, nella sentenza n. 15: la nozione di privacy si evolve come "diritto all'autodeterminazione informativa" come protezione delle scelte di vita contro ogni forma di controllo pubblico e di stigmatizzazione sociale, attribuendo ad ogni persona il diritto di prendere autonomamente le decisioni relative ai propri dati.

L'originaria disciplina statutaria aveva esclusivamente considerato, vietandole, le apparecchiature preordinate al controllo dell'attività dei lavoratori, ma la diffusione di

[65] Il fenomeno è descritto da A. Trojsi con particolare attenzione verso il cambiamento culturale in atto: *non si può non tener conto dell'evoluzione dell'atteggiamento degli stessi fruitori (e/o utenti) delle tecnologie (in generale, ed anche in ambito lavorativo), oggi significativamente mutato rispetto ai primi anni di utilizzo di tali strumenti, dovuta proprio alla consuetudine (ovvero, all'abitudine e all'assuefazione) a queste, che ha prodotto una naturale ed inevitabile accettazione della nuova realtà tecnologica, non percepita più, a differenza di una volta, come causa di possibili continui attentati alla propria sfera personale e di un'intrusione così intollerabile e molesta. Per non parlare, poi, dei casi, sempre più diffusi, in cui l'utilizzo del computer è incorporato nella prestazione lavorativa stessa, per cui diventa difficile, se non impossibile, attuare il controllo su questa se non attraverso lo strumento informatico, non permettendo di distinguere "strumento di lavoro" e "strumento di controllo".* (A. Trojsi, *Il comma 7, lettera f) della legge delega n. 183/2014. Tra costruzione del Diritto del lavoro dell'era tecnologica e liberalizzazione dei controlli a distanza sui lavoratori*, in M. Rusciano et al., *Jobs Act e contratti di lavoro dopo la legge delega 10 dicembre 2014, n. 183*, W.P. C.S.D.L.E. "Massimo D'Antona", Collective Volumes, n. 3/2014, 122).

computers, posta elettronica, reti internet aziendali, tablet e smartphone, che ha rivoluzionato il modo di lavorare e produrre, ha costretto gli operatori a misurarsi con le notevoli potenzialità di controllo, anche occulto, insite nell'utilizzo di dispositivi, funzionali all'esecuzione della prestazione, capaci di verificarne la correttezza, ma anche di acquisire ed "immagazzinare" dati personali. Tanto più che l'uso di questi dispositivi nella quotidianità lavorativa da parte di un numero crescente di lavoratori, spesso si sovrappone all'uso degli stessi nella vita privata e per finalità personali. Le potenzialità lesive della personalità del lavoratore, sotto il profilo dell'"asservimento" alla macchina e dei controlli che essa comporta, si presentano molto più ampie che in passato. Questo ha significato l'emergere di nuovi fattori di rischio per la riservatezza e la dignità del lavoratore, sconosciuti al legislatore del 1970. Il datore di lavoro può utilizzare lo sviluppo tecnologico e le sue potenzialità per migliorare l'efficienza e la produttività, ma al tempo stesso acquista nuove possibilità di controllo occulto del lavoratore attraverso gli strumenti tecnologici: potrebbe raccogliere informazioni sui tempi di connessione e disconnessione, sulle pagine web visitate, sull'uso e l'eventuale abuso degli strumenti in dotazione, sui numeri telefonici chiamati e la durata delle telefonate, sui destinatari e il contenuto delle mail inviate e ricevute, realizzando di fatto quel controllo a distanza, continuativo e occulto, vietato dallo Statuto.

Si diffondono strumenti di sorveglianza apparentemente meno visibili e ingombranti, ma sostanzialmente più invasivi, meno solidi e più liquidi direbbe Bauman, attraverso i quali è possibile registrare integralmente il comportamento del lavoratore, acquisendo anche dati sensibili.

Si devono prendere in considerazione un universo sconosciuto al momento dell'entrata in vigore dello Statuto di sistemi di controllo che riguardano il luogo e il tempo di lavoro come pure il ritmo dello stesso. In poco più di un ventennio siamo passati dall'occhio onniveggente del Grande Fratello aziendale in grado di spiare in ogni momento il lavoratore, anche attraverso le famigerate aperture a vetro delle porte dei luoghi di decenza, per "rubarne" i comportamenti fisici e gli atteggiamenti psicologici, all'attuale "società della sorveglianza", nella quale si verifica un monitoraggio permanente che non si preoccupa di fare distinzioni fra vita privata e vita lavorativa e nella quale l'acquisizione dei dati non passa attraverso strumenti di controllo *ad hoc* "occhiuti ed asfissianti", ma piuttosto attraverso forme di "dataveglianza". Si tratta di una sorveglianza basata sulla ricostruzione delle tracce lasciate

nei vari ambienti virtuali da un lavoratore non sempre consapevole delle informazioni che dissemina e che vengono raccolte dal datore di lavoro[66].

Lo scenario nelle imprese è completamente mutato. Le schedature Fiat e le guardie giurate infiltrate tra gli operai hanno lasciato il posto ai sensori di rilevamento della presenza dei lavoratori alla scrivania[67], alle etichette intelligenti, al polsino Motorola, utilizzato nei supermercati Tesco per registrare elettronicamente le consegne, stabilire il tempo necessario per completarle ed assegnare un punteggio positivo o negativo in base alla rapidità, fino ai braccialetti di Amazon[68], ai badge che incorporano microchip RFID (Radio-Frequency IDentification) in grado di trasmettere ad un server non solo l'entrata e l'uscita del lavoratore ma anche le sospensioni, gli spostamenti, le pause, e alle *app* installate sullo *smartphone* che consentono la geolocalizzazione del dipendente, e da ultimo ai rilevatori di dati biometrici. E il legislatore del 1970 non poteva certo immaginare che si arrivasse all'applicazione sui caschi dei lavoratori di sensori intelligenti che analizzano gli impulsi nervosi emessi dal soggetto e ne desumono lo stato emotivo e, quindi, l'eventuale inidoneità a svolgere certe mansioni: *il neuro-cap rievoca l'orwelliana psicopolizia, la polizia del pensiero, in una post-modernità che ripropone l'uomo-automa, rappresentando una minaccia quando invece aveva promesso speranza*[69].

L'irrompere delle nuove tecnologie, in particolare del computer, ha indotto a riconsiderare il bene protetto dall'art. 4 St. lav.: le nuove tecnologie applicate alla vita quotidiana e lavorativa fanno riaffiorare le necessità più elementari di tutela e contribuiscono a trasformare ed arricchire nella coscienza sociale e in quella degli operatori il concetto di dignità e quindi di riservatezza, non solo come tutela della personalità ma anche come necessità di non rendere l'uomo alienato e oggetto della macchina. Il diritto alla riservatezza protetto dall'ordinamento viene ad assumere nel tempo una complessità molto maggiore di quella che gli era attribuita ai tempi dell'entrata in vigore dello Statuto dei lavoratori. Da un

---

[66] L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *Rivista italiana diritto del lavoro* n. 3/2016, 345. La sociologia contemporanea definisce la sorveglianza come quel mondo di monitoraggio, tracciamento, pedinamento, selezione, controllo e sistematica osservazione degli individui, a fini di controllo sociale.

[67] È il caso della scatoletta nera con il nome emblematico *OccupEye*, installata sotto ogni scrivania dei dipendenti del Daily Telegraph, e più recentemente di quelli della banca Barclays, con sensori in grado di rilevare attraverso il movimento e la temperatura, la presenza del lavoratore alla sua postazione. (www.independent.co.uk).

[68] Il braccialetto consentirebbe un'ottimizzazione dei tempi dell'attività dei *picker* all'interno dei magazzini Amazon attraverso l'incrocio dei dati relativi al posizionamento del lavoratore e dei pacchi da ritirare, ma al tempo stesso offrirebbe la possibilità di un controllo continuo dei lavoratori, della loro attività e dei loro spostamenti.

[69] A. Soro, *La protezione dei dati personali nell'era digitale*, in *Nuova Giurisprudenza Civile Commentata*, n. 2/2019, 344.

primordiale diritto all'isolamento, proiezione dell'interesse ad essere lasciato solo, che prevedeva una tutela statica e negativa, limitata all'esclusione delle altrui interferenze dal proprio ambito privato, si è sviluppata una nozione dinamica di privacy, dal diritto "ad essere lasciati soli" al diritto "di poter sviluppare la propria personalità secondo i tratti individuali caratteristici che le sono propri" fino al diritto "di seguire le proprie informazioni ovunque si trovino e di opporsi alle interferenze". L'attenzione si sposta sulla centralità acquisita dal trattamento di dati personali e sul loro valore anche economico, rispetto al controllo fisico della persona: ciò che resta immutato, anzi si accentua, è la necessità di tutela dell'intimità e dell'identità del soggetto, sempre più fragile ed esposto nella relazione contrattuale.

La situazione giuridica soggettiva indicata con il termine *privacy* viene ad assumere una diversa connotazione semantica e acquista una diversa connotazione nel momento in cui deve confrontarsi con una nuova realtà tecnologica che consente non solo la raccolta ma anche l'organizzazione e la conservazione di una quantità enorme di dati personali. Dal punto di vista soggettivo non rilevano più solo le intrusioni nella sfera privata, quanto l'utilizzazione che di quei dati viene fatta dagli operatori economici del mercato[70].

Questa trasformazione è confermata anche da un'evoluzione lessicale che vede sempre più frequentemente sostituire al temine *privacy* quello di *data protection*, proprio per sottolineare che non si tratta di restare chiusi nel proprio mondo privato, al riparo da sguardi indiscreti, ma anche di potersi proiettare liberamente nel mondo attraverso le proprie informazioni, mantenendo però sempre il controllo sul modo in cui queste circolano e vengono da altri utilizzate[71]. Prende consistenza il diritto di mantenere il controllo sulla conoscenza (e sulla conoscibilità) da parte di terzi delle proprie informazioni. Il diritto alla protezione dei dati personali viene inteso come diritto all'autodeterminazione informativa, riferito alla scelta di ogni soggetto di autodefinirsi e determinarsi.

Evidenti sono le ricadute di questa evoluzione sulle dinamiche dei rapporti di lavoro e sull'applicazione della disciplina contenuta nell'articolo 4 St. lav.: i limiti sanciti dallo

---

[70] *Sul piano oggettivo la privacy, ormai metabolizzata come diritto alla riservatezza o ancora come diritto all'identità personale, muta significato ed acquista una diversa connotazione al termine del XX secolo, quando deve confrontarsi con una diversa realtà tecnologica che, vorticosamente sviluppata nell'arco di pochi anni, non soltanto consente la raccolta massiva di un più vasto novero di informazioni ricavabili dall'esperienza quotidiana di ciascun individuo, ma soprattutto permette di organizzare le informazioni raccolte così da ricostruire la vita privata come sommatoria di dati personali che divengono appetibili da parte degli operatori economici del mercato*.[…] *Sul piano soggettivo, non vengono più (solo) in considerazione le intrusioni nella vita privata poste in essere dai mezzi di informazione, cui si contrappone l'interesse al riserbo del singolo fatto oggetto di notizia, quanto le utilizzazioni dei dati da parte degli operatori, economici e non, presenti sul mercato, cui si contrappone l'interesse di ciascuno a conoscere l'uso che vien fatto dei propri dati.* (V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, n. 3/2018, 1101).

[71] S. Rodotà, *Intervista su privacy e libertà*, Laterza, Roma-Bari, 2005, 19.

Statuto miravano a precludere le ingerenze nelle "vite degli altri", a proteggere i confini della sfera di intimità del lavoratore minacciata da strumenti di controllo, non a salvaguardare il diritto a disporre dei propri dati e a controllarne la circolazione.

Come acutamente osserva Laura Tebano, la partita dei diritti del lavoratore non si giocherà tanto sul confronto fra riservatezza e controllo, quanto sulla pervasività, spesso impercettibile, del controllo e sul contenimento ed auto-contenimento dei nuovi strumenti di controllo[72] che, come dimostra il caso dei social network, vedono gli stessi controllati assumere un ruolo attivo. Per *privacy* si arriva così ad intendere proprio il "diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata"[73].

1.5 Le fonti comunitarie: dalla Carta europea dei diritti dell'uomo alle Raccomandazioni

Anche a livello europeo è maturata la consapevolezza dei cambiamenti indotti dalle grandi innovazioni tecnologiche nell'organizzazione del lavoro e delle implicazioni sulle relazioni di lavoro, dell'importanza del dato personale quale *frammento minimo dell'identità umana*[74] e della dimensione sovranazionale del rapporto di lavoro. Le istituzioni europee hanno quindi avvertito la necessità di integrare ed approfondire l'art. 8 della Carta europea dei diritti dell'uomo e di adeguare le tutele ai mutamenti del contesto socio economico.

Il Consiglio Europeo è intervenuto inizialmente con la Convenzione n. 108, adottata a Strasburgo il 28 gennaio 1981, al fine di garantire ad ogni persona fisica, il rispetto dei diritti e delle libertà fondamentali, in particolare il diritto alla vita privata in relazione

[72] *Si spazia così da sistemi di controllo "attivi" come badges, geolocalizzatori, meccanismi di riconoscimento biometrico, o appunto programmi di sorveglianza di cellulari o tablet a sistemi "passivi" che si fondano sull'acquisizione ed intercettazione di informazioni fornite spontaneamente dagli stessi lavoratori-utenti della rete che permettono di offrire un quadro completo ed esaustivo della personalità e delle attitudini dei soggetti (opinioni espresse su noti network sociali come Facebook o Twitter, esperienze professionali indicate su Linkedin, siti internet visitati, email inviate, visualizzazioni di giornali online o di negozi virtuali ecc.). Proprio le informazioni collezionate, aggregate e confrontate sono in grado di tradursi in una forma di "dossieraggio" suscettibile di testare costantemente la sussistenza del rapporto fiduciario con i dipendenti. Al riguardo basti ricordare il caso del dipendente della Cassa nazionale di previdenza dei commercialisti i cui "like" espressi su Facebook — fuori dall'orario di lavoro e tramite il cellulare personale — erano stati annotati, registrati, archiviati sì da giustificare il licenziamento. O ancora alla vicenda, sempre di fonte giornalistica, della bancaria trevigiana che, dopo aver espresso su Facebook il proprio disappunto per l'utilizzo di criteri prevalentemente estetici nelle procedure di selezione del personale, si è vista recapitare una lettera di contestazione, poi una sanzione disciplinare e infine, accusata di diffamazione, ha rassegnato le dimissioni*. (L. Tebano, *op. cit*., 345).

[73] S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, 122.

[74] L'espressione è di A. Ingrao.

all'elaborazione automatica dei dati a carattere personale. Pur attribuendo alla privacy status di diritto umano fondamentale, l'oggetto della Convenzione risultava generico, focalizzato sulle modalità di contemperamento del valore della vita privata con il valore altrettanto fondamentale della libertà di circolazione delle informazioni.

Successivamente il Consiglio è intervenuto con maggiore specificità attraverso nove Raccomandazioni di carattere settoriale, dirette a regolamentare l'utilizzo dei dati personali in specifici settori. La Raccomandazione del Consiglio d'Europa (89)2 del 18 gennaio 1989 relativa alla protezione dei dati a carattere personale utilizzati ai fini dell'occupazione, è poi stata sostituita dalla Raccomandazione sul trattamento dei dati personali sul posto di lavoro, pubblicata in data 1 aprile 2015, rispondente all'esigenza di tutela dei dati personali in riferimento ai rapporti di lavoro e ai rischi che i metodi di elaborazione informatica dei dati, a disposizione dei datori di lavoro, potrebbero rappresentare per i diritti e le libertà fondamentali dei lavoratori. La Raccomandazione riprende quanto già affermato nel 1989: il principio del diritto al rispetto della vita privata e della dignità umana dei lavoratori dovrebbe essere garantito con particolare riferimento alle relazioni sociali ed individuali sul luogo di lavoro, e al momento della raccolta e dell'utilizzazione di dati a carattere personale a fini di occupazione (par. 2)[75].

Il punto fondamentale (par. 3) è la previsione del principio di informazione e consultazione dei lavoratori, con garanzie preventive di natura collettiva, non solo con riferimento al controllo a distanza dell'attività dei lavoratori ma anche rispetto all'introduzione di un sistema automatizzato per la raccolta e l'utilizzazione dei dati personali dei lavoratori[76].

Rispetto all'art. 4 St. lav., il controllo collettivo auspicato dalla Raccomandazione non opera solo limitatamente alle apparecchiature di controllo a distanza dell'attività dei lavoratori, ma rispetto ad ogni sistema automatizzato per la raccolta e l'utilizzazione dei dati personali concernenti i lavoratori. Il ruolo delle rappresentanze sindacali e l'autodeterminazione dei lavoratori in materia risultavano valorizzati dall'indicazione di ricercare l'accordo dei dipendenti o dei loro rappresentanti prima dell'introduzione o della modificazione di tutti i sistemi che prevedessero la raccolta e l'uso di dati personali (par. 3.2).

[75] Il rispetto della vita privata e della dignità umana dei dipendenti, in particolare la possibilità di relazioni sociali e individuali sul luogo di lavoro, dovrebbe essere garantito all'atto della raccolta e dell'utilizzazione di dati personali per scopi di lavoro.

[76] *Informazione e consultazione dei dipendenti*. Conformemente alle legislazioni e prassi nazionali e, all'occorrenza, ai contratti collettivi, i datori di lavoro dovrebbero informare o consultare i propri dipendenti o i rappresentanti di questi ultimi precedentemente all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione di dati personali riguardanti i dipendenti.

La Raccomandazione del 2015/5 aggiorna la precedente del 1989 sul tema specifico delle nuove tecnologie e dei mezzi di comunicazione elettronica, divenuti di uso comune nelle relazioni di lavoro, e della dimensione internazionale del lavoro. Conferma e rafforza le previsioni basilari del 1989: la garanzia del rispetto della vita privata e la protezione dei dati personali, presupposto per consentire il libero sviluppo della personalità del dipendente e l'opportunità di rapporti personali e sociali sul luogo di lavoro. In particolare, auspica la minimizzazione dei controlli difensivi o comunque la residualità dei controlli sull'attività e sul comportamento dei lavoratori in quanto tale ed il tendenziale divieto di accesso alle comunicazioni elettroniche del dipendente.

Nella prima parte (artt. 1-13) la Raccomandazione richiama i principi generali in materia di protezione dei dati personali dei lavoratori nel momento dell'acquisizione e conservazione dei dati, prevedendo che i datori di lavoro adottino *policies* aziendali o regolamenti interni in materia di trattamento di dati personali dei lavoratori che siano coerenti con i principi indicati, con particolari tutele per i dati sensibili e genetici, prescrivendo norme volte a ridurre al minimo la circolazione dei dati e a garantire la maggior trasparenza possibile nel loro utilizzo, il diritto di accesso, rettificazione e opposizione, la sicurezza e conservazione dei dati. Già si definisce un impianto di tutele basato sui principi di trasparenza, necessità e proporzionalità.

Nella seconda parte (artt. 14-21) si fa specifico riferimento alle possibili forme di controllo derivanti dall'utilizzo delle nuove tecnologie, ponendo diverse garanzie a favore dei lavoratori, soprattutto in materia di trasparenza e giustificazione del trattamento dei dati personali connessi all'uso di Internet, alla posta elettronica, alla videosorveglianza e alla geolocalizzazione. L'estrazione di dati relativi alle connessioni internet, l'accesso allo scambio di comunicazioni elettroniche, l'analisi delle informazioni di geolocalizzazione da parte del datore di lavoro sono assimilabili a un trattamento dei dati personali del dipendente. Anticipando quanto poi introdotto anche nel nostro ordinamento dalla novella dell'art. 4 St. lav., la normativa europea distingue tra strumenti di lavoro, concepiti per finalità diverse da quelle del controllo, ma che pure si prestano alla registrazione di informazioni personali, e strumenti di controllo che hanno come scopo diretto quello di realizzare operazioni di verifica e monitoraggio. Se il controllo si realizza indirettamente tramite strumenti di lavoro, la Raccomandazione invita a ricorrere a misure preventive (filtri volti a precludere determinate operazioni, controlli a scalare, casuali e su dati anonimi) in luogo dell'accesso diretto alle comunicazioni elettroniche, possibili soltanto quando strettamente necessario ed in presenza di ragioni legittime, per minimizzare l'ingerenza nella sfera personale del

lavoratore. Si afferma il divieto di introdurre e utilizzare sistemi informativi e tecnologie con lo specifico e diretto scopo di monitorare l'attività dei lavoratori e, se introdotti per altro legittimo scopo, sono previste forme collettive di protezione sindacale, consistenti nella consultazione e autorizzazione delle rappresentanze sindacali: nella prospettiva delle Raccomandazioni, il diritto alla privacy del lavoratore è legato alla valorizzazione del ruolo delle rappresentanze sindacali, con l'accordo sindacale, la consultazione delle parti sociali e, quale ulteriore salvaguardia, la consultazione delle autorità nazionali di controllo per il trattamento dei dati personali, in un'ottica di procedimentalizzazione dei poteri datoriali. Le legittime finalità che consentono i controlli indiretti non sono determinate a priori, come avviene nell'art. 4 St. lav., ma la loro individuazione è lasciata alla dialettica delle parti sociali.

Queste Raccomandazioni, strumento di *soft law*, per essere la loro attuazione affidata alla volontà e alla scelta degli Stati destinatari, hanno svolto un'importante funzione programmatica, di ispirazione e monito per la legislazione degli Stati membri, tuttavia l'utilizzo di uno strumento normativo privo di efficacia giuridica vincolante nei confronti dei paesi dell'Unione Europea, quale è la Raccomandazione, ha impedito che tale intervento potesse incidere efficacemente nelle discipline nazionali interne. Per questo si è ritenuto opportuno ricorrere ad uno strumento dotato di maggiore efficacia e incisività ed in data 24 ottobre 1995, è stata adottata la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché della libera circolazione di tali dati.

Pur non prevedendo nulla di specifico rispetto al settore dei rapporti di lavoro, con essa viene offerta la prima disciplina di carattere organico e generale sulla protezione dei dati personali, anche con riferimento al trattamento automatizzato: una disciplina non calibrata sul lavoratore e sui rapporti nei luoghi di lavoro, ma comunque punto di svolta per il passaggio dal diritto ad essere lasciato solo al diritto alla protezione dei propri dati personali.

Anche se la Direttiva prendeva in considerazione la circolazione delle informazioni personali attraverso i canali tecnologici utilizzati quotidianamente dai singoli in ogni ambito della propria attività, rifletteva ancora uno *"small data" world*, dove i trattamenti massivi dei dati erano cosa rara perché ancora molto costosa: *era l'alba della cosiddetta dot-com era*[77]. Ad essa faranno seguito la Direttiva 97/66/CE sul trattamento dei dati personali e sulla

[77] La citazione è in Dagnino, E. *People Analytics: lavoro e tutele al tempo del management tramite big data*, in *Labour&Law Issues*, v. 3, n. 1/2017, 10.

tutela della vita privata nel settore delle telecomunicazioni, integrata dalla Direttiva n. 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, e da ultimo il recente Regolamento 2016/679/UE che abroga la Direttiva 95/46/CE.

Nel contesto europeo è importante menzionare il contributo fornito dal Gruppo di lavoro Articolo 29 (WP29)[78], istituito ai sensi dell'art. 29 della Direttiva 95/46 (e per questo così denominato) al fine di garantire una corretta implementazione della normativa sulla *privacy* dell'Unione. Il Gruppo che riuniva le Autorità di protezione dei dati degli Stati membri della UE, ha elaborato importanti pareri e linee guida: il Parere sul trattamento di dati personali nell'ambito dei rapporti di lavoro, n. 8 del 2001, il Documento sulla sorveglianza delle comunicazioni elettroniche sul luogo di lavoro del 29 maggio 2002 e ancora il parere dell'8 giugno 2017 sull'evoluzione delle nuove procedure informatiche, sui sistemi per il controllo del lavoro da remoto, la geolocalizzazione, e *Data Loss Prevention*.

In tema di sorveglianza nel luogo di lavoro, il Gruppo ha contribuito ad estrapolare i principi fondamentali della trasparenza, necessità, equità e proporzionalità, quali parametri da rispettare nel trattamento dei dati personali.

Dal 25 maggio 2018 il Gruppo di lavoro Articolo 29 ha cessato la sua attività ed è stato sostituito dal Comitato Europeo per la Protezione dei Dati (European Data Protection Board – EDPB), che è composto dai vertici di ciascuna Autorità di controllo per ciascuno Stato membro e dal Garante Europeo per la protezione dei dati (artt. 68 e ss., Reg. 2016/679 UE).

[78] Organo indipendente creato sulla base dell'art. 29 della direttiva 95/46, il Gruppo di lavoro per la protezione dei dati (Data Protection Working Party) è stato incaricato anche di analizzare il problema relativo ai limiti al potere di sorveglianza delle comunicazioni informatiche nei luoghi di lavoro. Tale organo, nel parere n. 8/2001, adottato il 13 settembre 2001, in materia di raccolta e trattamento dei dati personali nell'ambito del contesto lavorativo, ha estrapolato i principi base per la tutela dei dati del lavoratore: *finality, transparency, legitimacy, proportionality, accuracy and retention of the data, securuty, awareness of the staff*. Lo stesso organismo, ha elaborato un documento ufficiale relativo alla sorveglianza ed al monitoraggio delle comunicazioni elettroniche sul luogo di lavoro (adottato il 29 maggio 2002), nel quale ha stabilito inequivocabilmente che l'interesse del datore di lavoro al controllo sull'attività svolta dai propri dipendenti non può giustificare un'indebita intrusione nella privacy dei medesimi, ed ha altresì ribadito che ogni forma di controllo deve rispondere a canoni di trasparenza, necessità, equità e proporzionalità, sostenendo che "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace".
Il WP29, dopo aver suggerito ai datori di lavoro specifiche misure di sicurezza idonee a prevenire eventuali violazioni della riservatezza degli interessati, ha anche individuato possibili scenari di rischio per i diritti e le libertà fondamentali dei lavoratori che possono derivare dal trattamento di dati personali: dalla selezione del personale allo screening dei dipendenti attraverso i social media, fino allo sviluppo del lavoro da remoto e alle politiche BYOD e al trasferimento internazionale dei dati delle risorse umane o di altri dati dei dipendenti derivanti dall'utilizzo di applicazioni e servizi cloud-based.

1.6 Il Codice privacy: dal diritto alla riservatezza al diritto alla protezione dei dati personali

Dobbiamo attendere la metà degli anni novanta per avere un primo approccio sistematico alle disposizioni in materia di tutela dei dati personali con la L. n. 675 del 31 dicembre 1996[79], che recepisce la Direttiva europea 95/46/CE, e successivamente con il D.lgs. 30 giugno 2003, n. 196, il Codice per la protezione dei dati personali, contenente una disciplina organica e generale per la tutela della privacy nel trattamento automatizzato e non, dei dati personali. Si tratta di un vero e proprio compendio organico della normativa in materia, che raccoglie in un testo unico sia la legge 675/96 che le altre fonti legislative, regolamentari e i codici deontologici succedutesi negli anni in materia di tutela delle persone fisiche rispetto al trattamento dei dati personali. Il Codice Privacy "rappresenta il primo tentativo, su scala internazionale, di riordino generale di una materia complessa e, soprattutto, straordinariamente mobile"[80], un compendio organico della disciplina vigente che porta anche innovazioni rilevanti in materia. Il Codice rappresenta il momento conclusivo di un percorso che ha avuto inizio con il riconoscimento giurisprudenziale dei diritti alla riservatezza e all'identità personale, è poi proseguito con l'emanazione della legge n. 675/1996, fino ad aprire un nuovo capitolo per la teoria e la prassi dei diritti fondamentali nell'esperienza italiana[81].

Tra le situazioni soggettive tutelate dalla norma, l'articolo 2 del Codice privacy cita accanto al diritto alla riservatezza e all'identità personale, anche il diritto alla protezione dei dati personali ed è "difficile degradare il diritto alla protezione dei propri dati al mero rango ancillare nei confronti della riservatezza, dell'identità personale e così via"[82]. Trova dunque la sua formalizzazione un nuovo diritto della persona, il diritto alla protezione dei propri dati personali, che supera il criterio dell'esclusione dell'altro dalla propria vita privata ed è inteso come "diritto di mantenere il controllo sulla circolazione delle proprie informazioni e di determinare liberamente le modalità della costruzione della propria sfera privata"[83].

---

[79] L'articolo 1 comma 1 della legge 675/1996 nello specificare le sue finalità precisa che *il diritto alla riservatezza è solo uno dei diritti che possono risultare tutelati dalle sue disposizioni (la legge fa, infatti, un riferimento esplicito a tale diritto, insieme al diritto all'identità personale e alla dignità della persona, nell'ambito dei diritti e delle libertà fondamentali che la legge stessa garantisce) e che il suo oggetto è invece la tutela del "trattamento dei dati personali".*

[80] S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, in *Europa e diritto privato*, 2004, 2.

[81] G. Resta, *Il diritto alla protezione dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno Zencovich, *Il Codice dei dati personali. Temi e problemi*, Milano, 2004, 11-64.

[82] S. Sica, *La nuova disciplina della privacy*, *Commentario* dir. da S. Sica e P. Stanzione, Torino, 2004.

[83] G. Resta, *op. cit.*

Nella società tecnologica per avere accesso a molti beni e servizi ognuno di noi è chiamato a cedere nelle forme più disparate informazioni personali, senza rilasciare le quali sarebbe escluso, tagliato fuori anche da processi sociali: da qui nasce il diritto alla protezione del dato, inteso come diritto ad esserci e come diritto di non esserci.

Non solo i confini della riservatezza sono caratterizzati da estrema dinamicità e cambiano in relazione al soggetto interessato, al tempo, al tipo di dato, alle modalità di raccolta e ai possibili destinatari, per cui alcune informazioni perdono o acquistano carattere di riservatezza, ma diventa essenziale tutelare la possibilità del soggetto di conoscere, controllare, interrompere il flusso di informazioni che lo riguardano, le modalità di circolazione e di impiego dei suoi dati personali[84]. Ci si è progressivamente resi conto che non era sufficiente tutelare dalle possibili ingerenze di terzi le sole informazioni personali riservate, attraverso un diritto alla riservatezza come diritto a contenuto negativo, ma era necessario garantire e tutelare, tutti i dati personali, indipendentemente dal loro carattere riservato, in modo da offrire al soggetto il potere di controllarne la circolazione, tanto da concludere che "privato" significa "personale" e non necessariamente "riservato" o "segreto"[85].

Pur avendo entrambi ad oggetto le informazioni personali, il bene tutelato dai due diritti non coincide: oggetto del diritto alla protezione del dato personale non sono solo le informazioni riservate ma qualsiasi informazione personale, anche conosciuta o conoscibile o persino ceduta spontaneamente all'esterno.

Il diritto alla protezione dei dati personali, precursore di un vero e proprio diritto all'identità personale digitale, rispetto ai dati che potrebbero circolare sui sistemi informatici, si è dunque affiancato, e in parte sovrapposto al diritto alla riservatezza.

Con il Codice privacy l'espressione diritto alla privacy diventa un vero e proprio diritto ad autodeterminare gli ambiti e le modalità di circolazione dei dati che riguardano ciascuna persona. La privacy si configura come un elemento costitutivo della cittadinanza, come diritto a determinare le modalità di costruzione della propria sfera privata e come precondizione della cittadinanza elettronica[86], si presenta come una dimensione della libertà esistenziale, costitutiva non solo della sfera privata, ma pure di quella pubblica[87].

[84] A. Trojsi, *Il diritto del lavoratore alla protezione dei dati personali*, *op. cit*., 21, 23, 24.
[85] A. Trojsi, *op. cit.*, 27.
[86] S. Niger, *op. cit*., 70.
[87] A. Trojsi, *op. cit.*, 27.

L'evoluzione del diritto alla riservatezza è ben visibile nella Carta dei diritti fondamentali dell'Unione Europea, firmata a Nizza nel dicembre 2000, alla quale, con l'entrata in vigore del Trattato di Lisbona del 2007, è riconosciuto lo stesso valore giuridico dei Trattati: in essa si distinguono in due disposizioni consecutive ma distinte, gli articoli 7 e 8, il tradizionale diritto "al rispetto della propria vita privata e familiare" (art. 7) e il "diritto alla protezione dei dati personali" (art. 8)[88], che si configura come un diritto fondamentale autonomo. Nel diritto al rispetto alla vita privata e familiare si manifesta soprattutto il momento individualistico, la tutela è statica, negativa, si esaurisce sostanzialmente nell'escludere interferenze altrui. La protezione dei dati, invece, disciplina le modalità del trattamento dei dati, prevede una tutela dinamica che segue i dati nella loro circolazione[89].

L'art. 1 del Codice Privacy riproduce l'art. 8 della Carta di Nizza per cui ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Nell'ordinamento europeo il diritto alla protezione dei dati personali si afferma come un diritto nuovo e autonomo dell'individuo[90], direttamente azionabile dinanzi al giudice europeo o nazionale, soggetto al bilanciamento con altri "diritti e libertà fondamentali delle persone fisiche", che può essere compresso solo in casi espressamente previsti dalla legge ed in circostanze ben definite, come anche la giurisprudenza della Corte di giustizia è esplicita nel ritenere[91].

---

[88] L'art. 7 della Carta di Nizza, rubricato "Rispetto della vita privata e della vita familiare", recita "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni. L'art. 8, rubricato "Protezione dei dati di carattere personale", al paragrafo 1 stabilisce che: «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano» e al paragrafo 2 specifica che «Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenere la rettifica».

[89] *Si coglie qui il punto d'arrivo di una lunga evoluzione del concetto di privacy, dall'originaria sua definizione come diritto ad essere lasciato solo fino al diritto di mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata. Si contribuisce in maniera determinante al processo di "costituzionalizzazione della persona*" . (Rodotà, *op.cit*., 3).

[90] Analogamente la nostra Cassazione accanto al diritto alla riservatezza ha individuato uno spazio autonomo al diritto alla tutela dei propri dati personali (Cass. sez. un., n. 318/1999 e Cass. civ. sez. II, n. 186 del 4 gennaio 2011). La Corte ha affermato che nel nostro ordinamento giuridico tutti i soggetti hanno diritto alla propria integrità morale: un diritto, tutelato con le norme penali in tema di ingiuria e di diffamazione, che trova la sua consacrazione costituzionale nell'art. 2 della Costituzione. Proprio in base a una interpretazione estensiva ed evolutiva di questa norma costituzionale la giurisprudenza e la dottrina hanno riconosciuto i più moderni diritti alla riservatezza e alla identità personale e il legislatore, in adempimento anche di un dovere comunitario, con la legge 675 del 1996 ha disciplinato il diverso, anche se connesso, diritto alla tutela dei propri dati personali. In Cass. civ. II sez., 186/2011 si afferma che: Ha assunto rango di diritto fondamentale il diritto alla protezione dei dati personali, tutelato dall'articolo 2 della Costituzione italiana e dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea: un diritto a mantenere il controllo sulle proprie informazioni che, spettando non solo alle persone in vista ma a "chiunque" (articolo 1 del codice) e ad "ogni persona" (articolo 8 della Carta) nei diversi contesti ed ambienti di vita, concorre a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza.

[91] Un contemperamento equilibrato dei differenti interessi in causa avrebbe richiesto che le istituzioni interessate, prima dell'adozione delle disposizioni di cui si contesta la validità, verificassero se la pubblicazione

Il legislatore comunitario e quello del Codice privacy dettano regole volte a tutelare il diritto di ciascuno alla protezione dei propri dati personali, diritto di cui la persona rimane sicuramente titolare anche durante lo svolgimento della prestazione lavorativa. Tuttavia, nella direttiva n. 95/46/CE non si prevedeva alcuna disciplina peculiare per il trattamento dei dati personali dei lavoratori: la tutela era riservata a chiunque fosse titolare di dati personali utilizzati da altri per scopi soprattutto commerciali e si promuoveva l'elaborazione di codici di condotta per assicurare l'adeguamento delle disposizioni generali alle specificità settoriali.

La disciplina in materia di protezione dei dati personali è strutturata in termini generali, senza una considerazione specifica per le caratteristiche del rapporto di lavoro e per le peculiarità del controllo a distanza da parte del datore di lavoro: è attraverso rimandi alla norma speciale che gli articoli 113 e 114 del Codice della privacy (rimasti sostanzialmente invariati anche dopo l'entrata in vigore del D.lgs. 101/2018[92]) intendono regolare i rapporti tra le due normative, facendo espressamente salvo quanto previsto dagli articoli 8 e 4 St. lav. In particolare, l'art. 114, oggi rubricato "Garanzie in materia di controllo a distanza", riconduce nell'ambito delle regole dettate dallo Statuto dei lavoratori il problema della definizione dei limiti all'impiego degli strumenti di controllo. La successiva individuazione di una sintesi fra l'impianto tradizionale della disciplina lavoristica e le disposizioni in tema di privacy è lasciata all'iniziativa degli interpreti.

La definizione di "trattamento" di dato personale stabilita dal Codice privacy consente di considerare anche il controllo a distanza di cui all'art. 4 St. lav. come una *species* di trattamento automatizzato di dati personali: molte attività o provvedimenti concernenti il lavoratore costituiscono un trattamento di dati personali da parte del datore di lavoro e pongono la necessità di disciplinare la possibilità del datore di lavoro di acquisire e trattare dati personali del lavoratore (sia attraverso le apparecchiature dalle quali può derivare il controllo a distanza dell'attività lavorativa, che attraverso gli strumenti di lavoro) e di garantire al lavoratore sia la tutela della dignità che la possibilità di governare la circolazione

attraverso un sito Internet unico per ogni Stato membro e liberamente consultabile dei dati nominativi relativi a tutti i beneficiari interessati e agli importi precisi provenienti dal FEAGA e dal FEASR percepiti da ciascuno di essi — e senza distinguere in base alla durata, alla frequenza, o al tipo e all'entità dei finanziamenti percepiti — non andasse oltre quanto era necessario per la realizzazione degli obiettivi legittimi perseguiti, alla luce in particolare della lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta conseguente ad una simile pubblicazione. Sentenza della Corte di Giustizia del 9 novembre 2010, Causa C-92/09.

[92] Art. 113 Raccolta di dati e pertinenza 1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300 nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276.
Art. 114 Garanzie in materia di controllo a distanza 1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

e la conoscibilità dei propri dati personali. Non si tratta più soltanto del divieto di sottoporre il lavoratore ad un controllo continuativo ed impersonale, ma di evitare che il datore possa venire in possesso di dati personali del dipendente, acquisiti attraverso gli stessi strumenti di lavoro o raccolti attraverso le tracce disseminate in rete dallo stesso lavoratore. La possibilità per il datore di acquisire informazioni sulle opinioni e sulle preferenze del singolo dipendente e di raccogliere dati sensibili combinando le numerose tracce lasciate navigando sul *web* o sui *social network*, oltrepassa i confini del controllo a distanza fino a delineare un vero e proprio pericolo di "profilazione"[93], tanto che rischia di non essere più sufficiente vietare le indagini sulle opinioni politiche, religiose, sindacali dei lavoratori come fa l'art. 8 St. lav.[94].

La normativa privacy è riuscita a ricavarsi uno spazio di influenza nell'ambito del rapporto di lavoro fino ad incidere nella prassi operativa delle aziende con ulteriori tutele per il lavoratore. Nonostante la preminenza sistematica riservata dagli operatori alla disciplina statutaria ne abbia ridimensionato l'impatto, la disciplina sulla protezione dei dati ha apportato alla disciplina lavoristica un *quid pluris* in termini garantistici, integrando i limiti al potere di controllo del datore di lavoro con l'ulteriore rispetto di principi (di finalità, non eccedenza, pertinenza, necessità e trasparenza) che orientano le modalità di trattamento di tutti i dati personali ed il cui rispetto è presidiato da sanzioni civili, penali e amministrative[95]. Oltre che dei principi che regolano il trattamento dei dati personali e dell'informativa, entrambi mutuati dalla normativa sulla privacy, la dottrina giuslavoristica risulta debitrice alla normativa generale anche della procedimentalizzazione del trattamento dei dati del lavoratore: il processo di trattamento delle informazioni personali rappresenta un procedimento articolato e scomporlo in momenti procedurali successivi consente la verifica della correttezza in ogni fase del trattamento.

[93] La profilazione rappresenta una forma particolarmente invasiva di trattamento automatizzato dei dati della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

[94] Devono prendersi in considerazione anche le nuove forme di dossieraggio condotte su fonti e dati volontariamente forniti dagli stessi interessati, il cosiddetto *web scraping* o *opinion mining*, ossia la raccolta massiva di informazioni sul web e l'estrazione di informazioni dalla congerie di dati raccolti. (A. Soro, *op. cit.*, 95).

[95] Il potere datoriale di controllo deve superare quindi un test di legittimità relativo prioritariamente al rispetto dei limiti dell'art. 4 St. lav., in secondo luogo, all'osservanza della normativa sulla raccolta delle informazioni relative ai lavoratori, che si fonda sul principio per cui i sistemi informativi e informatici sono configurati in modo da ridurre al minimo l'utilizzazione dei dati personali e l'invasività del controllo deve essere graduata in funzione del principio di pertinenza e non eccedenza. (M. T. Salimbeni, L*a riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Riv.it. Dir. Lav.* n. 1/2015, 598).

Tuttavia l'integrazione fra le due normative è risultata poco riuscita, anche perché la disciplina generale non può tenere conto del caso specifico in cui l'acquisizione del dato personale avvenga nell'ambito di una relazione continuativa tra le parti, caratterizzata dall'esistenza del potere di controllo di una di esse sui comportamenti solutori dell'altra. I due apparati normativi hanno continuato a gravitare nelle rispettive sfere, senza sviluppare interazioni e si è definito un patto di reciproca non belligeranza, più che di complementarietà, che affidava alla norma statutaria il governo sostanzialmente esclusivo della materia[96].

Anche dopo l'emanazione del Codice privacy, l'art. 4 St. lav. è restato la principale norma di riferimento per verificare la legittimità dell'uso di strumenti tecnologici dai quali potesse derivare il controllo e l'acquisizione di dati personali, attività potenzialmente lesive della dignità e della personalità del lavoratore. Ci fa notare Maria Teresa Carinci che la stessa giurisprudenza si è limitata a fare riferimento al solo art. 4 St. lav. e non risulta abbia chiamato in causa i vincoli imposti dalla normativa privacy per decretare l'inutilizzabilità dei dati raccolti, come peraltro esplicitamente previsto all'art. 11 del Codice Privacy[97].

Resta l'impressione che le due normative abbiano continuato a procedere in parallelo[98], almeno fino alla novella del 2015, quando l'esplicito rinvio al Codice della privacy contenuto nel terzo comma dell'art. 4 St. lav. ha imposto di riconsiderare e raccordare la normativa generale con quella speciale. L'esplicito richiamo alla disciplina in materia di privacy impone ai giudici del lavoro la diretta applicazione di principi sulle modalità di trattamento dei dati e di regole fissate dal Codice, incluse le determinazioni del Garante, e

---

[96] Come osserva criticamente Del Punta: *che ciò sia avvenuto per la sfasatura originaria tra le due prospettive regolative, o per la preoccupazione diplomatica di non interferire con una normativa già vigente, e per giunta dotata di un crisma autorevole come quello statutario, il legislatore del Codice non ha neppure tentato di pervenire ad una sintesi delle due discipline, badando semplicemente a precisare (nell'art. 114) che le nuove garanzie introdotte dal Codice si aggiungevano a quelle già vigenti in tema di controlli a distanza, che restavano disciplinate dall'art. 4 della legge n. 300/1970.* (R. Del Punta, *op. cit.*, 77).

[97] Così M. T. Carinci: *Tuttavia il fatto che l'art. 114 D.Lgs. 196/2003 facesse salvo l'art. 4 St. lav., ha sì fugato ogni dubbio sul fatto che fosse quest'ultima norma a fissare i limiti al potere di controllo del datore di lavoro, ma ha contribuito a far rimanere in ombra i vincoli generali al trattamento dei dati previsti dal Codice della Privacy. Non si registrano, infatti, fino ad oggi significative pronunce giurisprudenziali che abbiano utilizzato le regole del Codice della Privacy per decretare l'inutilizzabilità dei dati raccolti, come peraltro da esso esplicitamente previsto all'art. 11.* (M. T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito*, in *Labour Law Issues* n. 1/2016, 6).

Nello stesso senso M. P. Aimo: *I giudici - benché l'attività di controllo sull'uso individuale dei mezzi informatici costituisca un trattamento di dati personali, come ha espressamente affermato il garante nelle linee guida del marzo 2007 – raramente valutano se le modalità concrete con cui il controllo si è svolto in azienda rispettano i principi fondamentali che regolano i trattamenti di dati*. (M. P. Aimo, *La c.d. cybersurveillance sui luoghi di lavoro,* in P. Tullini, (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, 148).

[98] G. Proia parla di reciproca indifferenza fra la disciplina generale e la tutela lavoristica.

dunque il superamento di quell'atteggiamento di *self restraint* che ne ha, invece, fino alla novella determinato la scarsa considerazione in sede di definizione delle controversie[99].

1.7 Il Garante per la protezione dei dati personali

Gli strumenti di tutela predisposti nel Codice privacy arricchiscono il corredo di garanzie a tutela della sfera identitaria e della riservatezza del lavoratore anche grazie alle interpretazioni, agli orientamenti e alle linee guida formulate dall'Autorità Garante per la protezione dei dati personali.

In attuazione della direttiva 95/46/CE, la legge 675 del 1996 ha istituito un'autorità amministrativa indipendente con il compito di vigilare sul rispetto della disciplina in materia di trattamento di dati personali, il Garante per la protezione dei dati personali. Si tratta di un organo collegiale con due componenti eletti dalla Camera dei deputati e due dal Senato, i quali eleggono nel loro ambito un Presidente, il cui voto prevale in caso di parità, ed un vicepresidente che lo sostituisce in caso di impedimento[100].

La funzione primaria dell'Autorità è quella di vigilare sul rispetto della disciplina in materia di trattamento dei dati personali e per questo è dotata del potere di controllo sulla conformità del trattamento dei dati alla normativa, del potere di rilasciare autorizzazioni al trattamento dei dati sensibili, giudiziari e genetici, o al trasferimento dei dati all'estero, nonché autorizzazioni generali per determinate categorie di titolari o di trattamenti. L'Autorità ha anche il compito di garantire una tutela amministrativa a favore di chi lamenti una lesione del diritto alla protezione dei dati, prescrivendo le misure idonee a rendere il trattamento conforme alle disposizioni, imponendone l'interruzione e stabilendo il divieto del trattamento illecito.

Il Garante esercita una funzione para-giurisdizionale a seguito di ricorso, con il quale l'interessato fa valere i propri diritti (art. 7 del D.lgs. 196/2003), secondo un procedimento scandito dalla legge che specifica modalità, contenuto, e procedura per la presentazione del ricorso. L'inosservanza dei provvedimenti del Garante, adottati ai sensi dell'art. 150 commi 1 e 2, e 143, comma 1 lett. c, è sanzionata penalmente. Avverso le pronunce del Garante,

[99] M.T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in P. Tullini, (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017, 57.

[100] Il Presidente rappresenta l'Autorità, cura i rapporti con il Parlamento e con gli altri organi costituzionali, con le pubbliche amministrazioni, con le Authority degli altri paesi, con le istituzioni dell'Unione Europea e con gli altri organismi internazionali. I componenti, scelti tra affermati esperti in materia di diritto e di informatica, durano in carica 4 anni e non possono essere confermati per più di una volta.

che possono essere di rigetto tacito, di non luogo a provvedere, di manifesta infondatezza, di inammissibilità, o di accoglimento, l'interessato può poi proporre opposizione mediante ricorso al tribunale[101].

Dal nuovo Regolamento europeo sulla protezione dei dati vengono potenziati ambiti di intervento, poteri di indagine, poteri correttivi e consultivi delle Autorità Garanti Nazionali e specificati i requisiti di indipendenza. Per il controllo dell'effettivo rispetto delle norme sono riconosciuti poteri di intervento ed un potere correttivo di avvertimento o ammonimento al titolare o al responsabile del trattamento (artt. 51 e ss., Reg. UE 2016/679). Di particolare interesse è il potere del Garante di emanare provvedimenti generali riferiti a categorie di titolari o di trattamenti, che sostanziano un potere di fatto normativo, anche se formalmente amministrativo. Attraverso le autorizzazioni generali[102], la cui funzione è quella di autorizzare automaticamente il trattamento dei dati, se effettuato nel rispetto dei criteri indicati, per una specifica tipologia di dati o per una specifica categoria di titolari, il Garante ha spesso realizzato efficaci aggiustamenti, integrazioni e specificazioni della disciplina, svolgendo sostanzialmente una funzione para legislativa. Nei provvedimenti generali il Garante prescrive, anche d'ufficio, oltre che sulla base di istanze, reclami, segnalazioni e richieste, le regole applicabili e le misure necessarie al fine di rendere il trattamento conforme alle disposizioni vigenti, spesso con funzioni di supplenza del legislatore.

Il D.lgs. 196/2003, nonostante l'opera di razionalizzazione della materia, ha lasciato irrisolta la questione relativa al rapporto fra la disciplina generale sul trattamento dei dati e le numerose discipline speciali relative all'utilizzo di dati nei vari settori: il Codice ha optato per l'autoregolamentazione demandando proprio al Garante la promozione di codici di deontologia e buona condotta.

---

[101] Si segnala un caso arrivato fino alla pronuncia in Cassazione, avente ad oggetto l'installazione, da parte del datore di lavoro di un sistema di raccolta dei dati biometrici della mano per la rilevazione delle presenze dei dipendenti. La società datrice di lavoro aveva fatto ricorso al Tribunale di Catania avverso ordinanza-ingiunzione n. 345/2012 con la quale il Garante per la protezione dei dati personali aveva irrogato la sanzione pecuniaria di Euro 66.000,00, previa contestazione della violazione degli artt. 13, 17, 23, 33, 37, 38, 161, 162, comma *2- bis,* 162 del d.lgs. n. 196 del 2003. Successivamente il Garante aveva proposto ricorso in Cassazione avverso sentenza del Tribunale di Catania 2164/2015 del 15/5/2015, recentemente deciso con sentenza favorevole al Garante, Cass. Civ. sez. II 25686, 15 ottobre 2018.

[102] Il Garante ha esercitato pienamente il suo potere "normativo", emanando sei autorizzazioni generali (rinnovate periodicamente per adeguarle alle sopraggiunte eventuali nuove esigenze) al trattamento dei dati sensibili, nei confronti di diverse categorie di soggetti che per ragioni di lavoro utilizzano questi dati, una settima autorizzazione per il trattamento dei dati giudiziari e un'ultima al trattamento dei dati genetici, (è del 22 febbraio 2007 la prima versione) che ha colmato un vuoto legislativo rappresentando l'unica fonte di disciplina del trattamento dei dati genetici in Italia. Attraverso questi provvedimenti il Garante pone una serie di regole per rafforzare la protezione dei dati sensibili, giudiziari, genetici cercando di ridurre al minimo i rischi di danni che i trattamenti potrebbero comportare.

Il contributo del Garante è stato fondamentale nell'offrire un'interpretazione sistematica e di ricostruzione del composito quadro di regole da applicare alla specificità di ciascun settore e nel caso dei rapporti di lavoro gli interventi del Garante hanno riempito di contenuti quel sistema di rimandi reciproci di cui agli articoli 113 e 114 del Codice Privacy e 4 e 8 dello Statuto. Si è realizzato così il primo importante avvicinamento fra la tematica della privacy e quella dei controlli a distanza del lavoratore e si sono concretizzati i principi regolatori del trattamento dei dati personali, posti dalla normativa privacy, rispetto al contesto specifico delle relazioni di lavoro.

Come abbiamo visto l'integrazione fra i due sistemi normativi e l'adeguamento delle regole di principio dettate a protezione dei dati alla specialità del rapporto di lavoro ha fatto fatica ad affermarsi e la sede in cui la complessa opera di raccordo ha cominciato a "germogliare" è quella dei provvedimenti del Garante[103].

I provvedimenti, in accordo con le indicazioni comunitarie, si sono orientati su tre direttrici fondamentali: trasparenza, prevenzione e proporzionalità.

Il Garante ha correttamente tratto dalla normativa privacy una generale istanza di trasparenza nella gestione dei dati, estendendola anche al contesto dei rapporti di lavoro: un'istanza di pubblicizzazione preventiva ai lavoratori delle modalità di raccolta e trattamento dei dati. Da qui si è affermata la prassi di un'informativa che ha preso la forma di disciplinari interni, da redigere "in modo chiaro e senza formule generiche", nonché "da pubblicizzare adeguatamente verso i singoli lavoratori e da sottoporre ad aggiornamento periodico". In sintonia con la linea regolativa europea, il Garante prescrive la predisposizione, da parte delle imprese, di policy aziendali che chiariscano in anticipo ai lavoratori l'uso consentito degli strumenti assegnati e se sia consentito anche un uso a fini personali, nonché le modalità con cui essi possono essere controllati. L'assenza di una esplicita policy aziendale avrebbe potuto ingenerare una legittima aspettativa di "confidenzialità" da parte del lavoratore[104] rispetto ad alcune forme di comunicazione.

Con alcuni provvedimenti generali, adottati sotto forma di linee guida[105], il Garante riepiloga la disciplina applicabile, sintetizza gli adempimenti, le garanzie e le tutele richieste in base

[103] A. Ingrao, *op. cit.*, 64.

[104] Vedi in proposito la giurisprudenza della Corte EDU sul caso Copland c. Regno Unito, n. 62617/00.

[105] Tra le numerose linee guida vanno annoverate: le Linee guida in materia di trattamento dei dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati n. 53 del 23 novembre 2006, Linee guida per l'utilizzo della posta elettronica e il collegamento a internet nell'ambito del rapporto di lavoro n. 13 dell'1 marzo 2007, le linee guida in materia di trattamento dei dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro in ambito pubblico, n. 23 del 14 giugno 2007, Provvedimento del 5 giugno 2008 sull'utilizzo di un sistema satellitare di localizzazione da parte di una società che gestisce linee di trasporto pubblico, Provvedimento in materia di

alle norme vigenti e rispetto alla varietà delle situazioni concrete, facilitandone l'osservanza da parte degli operatori ma anche esprimendo contenuti innovativi, prescrizioni nuove e discipline *ad hoc* per le singole materie trattate. Il Garante fornisce con le Linee Guida indicazioni operative per prevenire il rischio di utilizzi impropri e per ridurre al minimo l'impiego di dati riferibili ai lavoratori, valorizzando i principi codicistici di necessità, minimizzazione e proporzionalità rispetto alle finalità per le quali sono stati raccolti.

Ed in questo senso si esprime Maria Teresa Carinci che ravvisa nel Garante il perno ed il motore per la costruzione di un'efficace tutela della persona del lavoratore contro lo straripare del potere di controllo del datore di lavoro e nella giurisprudenza del Garante il luogo per definire compiutamente il bilanciamento d'interessi prefigurato dal nuovo art. 4 St. lav.[106].

Il delicato compito cui è chiamata l'Autorità Garante è sintetizzato nelle parole del suo primo presidente, Stefano Rodotà, nel discorso pronunciato in occasione della 26° Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali: *Le autorità per la protezione dei dati personali lavorano sulla sottile frontiera che separa gli interventi corretti di bilanciamento tra la privacy e gli altri valori dalle limitazioni che possono snaturare i caratteri della democrazia.* (Wroclaw - PL, 14, 15, 16 settembre 2004).

1.8 La giurisprudenza della Corte europea dei diritti dell'uomo

In diverse occasioni la giurisprudenza della Corte europea dei diritti dell'uomo è stata chiamata a confrontarsi con la difficile sfida del contemperamento tra tutela del diritto del lavoratore alla riservatezza ed esercizio del potere organizzativo, di gestione efficiente delle risorse e dell'attività produttiva da parte del datore di lavoro, anche attraverso l'uso di strumenti tecnologici. Nell'argomentare le sue decisioni la Corte ha tracciato un percorso verso la definizione del contenuto e dei limiti della sorveglianza elettronica rispetto alla tutela della dignità e liberta del lavoratore, ha stabilito alcuni principi chiave ed individuato le modalità che consentano di bilanciare i contrapposti interessi, integrando di fatto la disciplina generale sulla protezione dei dati personali con quella speciale relativa al rapporto di lavoro.

---

videosorveglianza dell'8 aprile 2010, Linee guida in materia di trattamento di dati per lo svolgimento di indagini di *customer satisfaction* in ambito sanitario, n. 182 del 5 maggio 2011.

[106] M.T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in P. Tullini, (a cura di) *op. cit.*, 59-60.

La giurisprudenza europea ha contribuito ad ampliare la nozione di vita privata, che ha lasciato lo spazio angusto delle mura domestiche e la dimensione individuale, per estendersi anche ai luoghi di lavoro nei quali si svolge la vita dell'individuo e alle relazioni sociali attraverso le quali si esplica la sua personalità. Secondo l'interpretazione ampia fornita dalla Corte di Strasburgo, l'art. 8 della Convenzione europea dei diritti dell'uomo include nel diritto al rispetto "della vita privata" anche il diritto alla "tutela della vita professionale". La nozione di vita privata non può essere circoscritta alla ristretta sfera domestica, a quell'*inner circle* all'interno del quale i singoli soggetti vivono la loro vita personale e dal quale decidono di escludere il mondo esterno, ma deve essere comprensiva anche della *private social life*, la dimensione sociale nella quale si manifesta e si definisce l'identità e si sviluppa la personalità dell'individuo.

Un punto di svolta si ha nel 1992 con la sentenza Niemietz v. Germania[107]: la Corte EDU nel motivare l'accoglimento del ricorso presentato dal signor Niemietz, un avvocato tedesco il cui ufficio era stato oggetto di perquisizione, interpreta estensivamente il concetto di vita privata, includendovi il luogo di lavoro, dove in misura maggiore si ha l'occasione di stabilire e sviluppare relazioni sociali ed esprimere la propria personalità, ed estendendo l'ambito di applicazione delle tutele ad ogni aspetto della vita della persona. Conseguentemente, secondo i giudici di Strasburgo, la tutela del diritto alla vita privata, di cui all'art. 8 CEDU, si arricchisce di contenuti, tutelandosi il pieno e libero sviluppo della personalità anche nell'ambito delle relazioni sociali che si sviluppano nell'ambiente lavorativo o che hanno luogo in un contesto pubblico. Punto di criticità, afferma la Corte europea, è che la linea di confine tra l'attività lavorativa e la sfera personale di lavoratori e di terzi, può essere tracciata, spesso, solo con difficoltà.

Il problematico contemperamento tra l'esigenza del datore di lavoro di garantire la sicurezza e il corretto utilizzo delle risorse aziendali e il diritto alla vita privata di coloro che prestano

[107] Cfr. Corte EDU 16 December 1992, Niemietz v. Germania, n. 13710/88: […] *The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. 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. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not*. […] *More generally, to interpret the words "private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 (art. 8), namely to protect the individual against arbitrary interference by the public authorities*.

lavoro a suo favore, torna ad interessare la Corte nelle sentenze *Halford v. Regno Unito*[108] e *Copland v. Regno Unito*[109]. In queste ultime vengono ricondotte nell'ambito di applicazione dell'art. 8 CEDU anche le telefonate private fatte sul luogo di lavoro, le comunicazioni avvenute attraverso la posta elettronica e la navigazione in Internet: si equipara alla corrispondenza tradizionale quella elettronica, alla quale si estende il principio di segretezza della corrispondenza, e si riconosce e tutela il diritto ad uno spazio di riservatezza per le comunicazioni private anche se effettuate sul posto di lavoro.

Nel caso Copland la Corte ha ritenuto che la raccolta di informazioni avvenuta attraverso il monitoraggio di telefonate, e-mails e navigazione in internet, protratto per un lungo periodo e senza preventiva informazione circa la possibilità di essere sottoposti a controllo, sia avvenuta in violazione del diritto alla riservatezza del lavoratore, dell'art. 8 CEDU.

Pur affermando che la privacy non si configura come diritto assoluto[110], che non ammette restrizioni, ma come interesse che può recedere di fronte a legittimi interessi datoriali, ed il diritto del lavoratore deve essere contemperato con il legittimo interesse datoriale alla verifica dell'esatto adempimento della prestazione e del corretto utilizzo delle risorse aziendali, sussiste in capo al lavoratore una aspettativa di riservatezza per la corrispondenza e le comunicazioni nel luogo di lavoro in assenza di un regolamento interno o di una policy

---

[108] Cfr. Corte EDU 25 giugno 2007, Halford c. Regno Unito, n. 20605/92 *In the Court's view, it is clear from its case-law that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 para. 1 (art. 8-1) […] There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls […] The Court holds unanimously that Article 8 of the Convention (art. 8) is applicable to the complaints concerning both the office and the home telephones; Holds unanimously that there has been a violation of Article 8 (art. 8) in relation to calls made on the applicant's office telephones*.

[109] Cfr. Corte EDU 3 aprile 2007, Copland c. Regno Unito, n. 62617/00. Nel caso di specie, Ms Copland, impiegata di un College gallese, ricorre alla Corte di Strasburgo dopo aver scoperto che per un lungo periodo di tempo il telefono, le mail e la sua navigazione in Internet erano stati monitorati per verificare se vi fosse un uso eccessivo e scorretto delle risorse del College per scopi personali. Secondo la Corte il caso rientra nell'ambito di applicazione dell'art. 8 che è stato violato: in assenza di informativa al lavoratore sul possibile monitoraggio di mail, telefono ed Internet, la lavoratrice aveva una ragionevole aspettativa di privacy. *the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8. It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage. The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see Halford). The same expectation should apply in relation to the applicant's e-mail and Internet usage*. […] *There has therefore been a violation of Article 8 of the Convention in this regard.*

[110] Il diritto alla vita privata non è un diritto assoluto e può essere limitato quando ricorrano le condizioni di cui all'art. 8, par. 2. In sostanza, la Convenzione europea lascia alle autorità nazionali il "margine di apprezzamento", ossia la facoltà di adottare misure restrittive del diritto purché esse "trovino fondamento in una legge" o siano ad essa conformi e risultino necessarie a conseguire talune finalità tipicamente descritte dalla stessa Convenzione.

aziendale che preveda la possibilità di monitoraggio e ne determini modalità e limiti. In questo modo prende forma il concetto di *reasonable expectation of privacy*: i lavoratori hanno una legittima e ragionevole aspettativa di privacy sul posto di lavoro che non si annulla per il solo fatto che usino strumenti del datore di lavoro.

Altre pronunce della Corte EDU, susseguitesi negli ultimi mesi del 2017 e nei primi del 2018 e aventi ad oggetto il controllo a distanza del lavoratore attraverso strumenti tecnologi, hanno stabilito che il controllo deve essere preceduto da un'adeguata informazione concernente le modalità di realizzazione dello stesso, deve essere compiuto per finalità legittime e con modalità proporzionate (Bărbulescu v. Romania), sia in relazione al numero di lavoratori coinvolti nel monitoraggio e alla sua durata (López Ribalda e altri v. Spagna), che con riferimento al grado d'intrusività dello stesso (Antovič e Mirkovič v. Montenegro).

Dopo 9 anni dal caso Copland, la Corte europea torna sul tema del monitoraggio delle mail inviate dal luogo di lavoro con la sentenza *Bărbulescu v. Romania*[111] e svolge nell'occasione un ruolo fondamentale di orientamento interpretativo, offrendoci una panoramica sistematica sul tema del monitoraggio delle strumentazioni informatiche utilizzate dai lavoratori, individuando i criteri per valutare la legittimità della sorveglianza informatica datoriale.

A seguito di *referral* avverso quanto deciso in prima istanza dalla IV Sezione, che aveva respinto il ricorso del lavoratore, ritenendo legittimo il comportamento del datore di lavoro[112], la Grande Camera ribalta quanto deciso e valorizza le opinioni dissenzienti allegate alla prima decisione.

Dalla *dissenting opinion* del giudice Pinto de Albuquerque si traggono diversi interessanti profili partendo dal presupposto che *Internet surveillance in the workplace is not at the employer's discretionary power*[113]. In primo luogo, la comunicazione via Internet è

---

[111] Corte EDU, *Bărbulescu v. Romania 5 settembre 2017*, n. 61496/08. Il caso si origina dal licenziamento di un ingegnere rumeno, Bogdang Mihai Bărbulescu, motivato dall'utilizzo dell'account di messaggistica Yahoo Messenger, aperto su indicazione dell'azienda per la gestione dei rapporti con i clienti, per lo scambio di messaggi a carattere personale, in particolare con il fratello e con la fidanzata. Il signor Bărbulescu ha adito la Corte europea lamentando la violazione dell'art. 8 della CEDU per essere stato leso il suo diritto alla vita privata e alla riservatezza della corrispondenza.

[112] La IV sezione (12/1/2016) aveva ritenuto che l'interesse dei lavoratori alla protezione della privacy, inteso nella prospettiva di una *reasonable expectation*, rispetto all'interesse datoriale al controllo, dovesse soccombere poiché *non è irragionevole per un datore di lavoro voler controllare che i lavoratori adempiano i propri obblighi durante l'orario di lavoro*.

[113] Si legge nella *dissenting opinion* del giudice Pinto de Albuquerque: "States have a positive obligation to promote and facilitate universal Internet access, including the creation of the infrastructure necessary for Internet connectivity. In the case of private communications on the Internet, the obligation to promote freedom of expression is coupled with the obligation to protect the right to respect for private life.

[…] In a time when technology has blurred the diving line between work life and private life, and some employers allow the use of company-owned equipment for employees' personal purposes, others allow

considerata una forma privilegiata di espressione e l'accesso ad Internet si configura come un diritto umano - *Access to the Internet as a human right.* Accanto ai tradizionali interessi contrapposti, si dovrà tenere conto anche di diritti emergenti, quali il diritto del lavoratore di comunicare e di avere accesso all'informazione attraverso Internet. Internet fornisce una straordinaria piattaforma per l'esercizio della libertà di espressione, uno strumento di promozione dei diritti umani e può essere considerato una sorta di livellatore sociale, veicolo di non mercificazione del lavoratore[114].

Inoltre dato che un divieto assoluto di utilizzo delle comunicazioni elettroniche nel luogo di lavoro per scopi privati non appare né realistico né ragionevole, e considerato che attraverso Internet vengono veicolate informazioni private, rispetto alle quali possono svilupparsi forme di controllo sia rispetto all'uso di Internet che sul contenuto delle comunicazioni trasmesse, è auspicabile che vengano specificate le regole di comportamento che il lavoratore è tenuto ad osservare, con limiti e condizioni d'uso della rete: *employees must be aware of the purposes, scope, technical means and time schedule of such monitoring*.

Ne consegue la necessità di adottare in materia una politica aziendale di trasparenza delle regole, con regolamenti interni che specifichino quali comportamenti siano ammessi e quali modalità di controllo siano messe in atto, senza escludere irrealisticamente l'uso personale delle risorse informatiche e senza che la sola presenza di disciplinari interni sia sufficiente ad allontare possibili violazioni delle disposizioni a tutela della privacy[115]. I regolamenti interni o le istruzioni di un datore di lavoro non possano azzerare la vita privata sul luogo di lavoro: "an employer's instructions cannot reduce privacy social life in the workplace to

---

employees to use their own equipment for work-related matters and still other employers permit both, the employer's right to maintain a compliant workplace and the employee's obligation to complete his or her professional tasks adequately does not justify unfettered control of the employee's expression on the Internet. Even where there exist suspicions of cyberslacking, diversion of the employer's IT resources for personal purposes, damage to the employer's IT systems, involvement in illicit activities or disclosure of the employer's trade secrets, the employer's right to interfere with the employee's communications is not unrestricted. Given that in modern societies Internet communication is a privileged form of expression, including of private information, strict limits apply to an employer's surveillance of Internet usage by employees during their worktime and, even more strictly, outside their working hours, be that communication conducted through their own computer facilities or those provided by the employer".

[114] Analoga intuizione è espressa dal Presidente Soro che scrive: *Internet, da strumento di comunicazione, si è trasformato nella principale piattaforma su cui si svolgono le relazioni interpersonali, il lavoro, l'erogazione di servizi, e in cui vengono diffusi i contenuti.* (A. Soro, *Persone in rete, op. cit.,* 26). Lo stesso Autore osserva che *la rete come ogni sistema relazionale, rischia di determinare in forme nuove quelle asimmetrie – anzitutto di potere – da cui aveva promesso di liberarci.* (A. Soro, *La protezione dei dati personali nell'era digitale*, in NGCC 2/2019, 343).

[115] Cfr. Cassazione civ. sez. I n. 18302, 19/9/2016 in cui la Corte contrasta una lettura del sistema normativo che ritenga sufficiente, per ammettere il rispetto dei diritti fondamentali in ambito lavoristico, la semplice adozione di un regolamento aziendale. La Cassazione esplicita che "il fatto di aver fornito informazioni ai propri dipendenti non è elemento decisivo per escludere la violazione del disposto di cui all'art. 4, secondo comma, dello Statuto dei lavoratori".

zero. Respect for private life and for the privacy of correspondence continue to exist, even if these may be restricted in so far as necessary"[116]. Nelle parole del giudice sono sostanzialmente riprodotti i principi di trasparenza, finalità, necessità e proporzionalità.

Il giudice Albuquerque ha anche richiamato l'attenzione della Corte sulla mancanza di linee guida in ordine agli interessi che il datore di lavoro può invocare per giustificare le interferenze nella privacy dei lavoratori: in assenza di criteri per valutare la legittimità del contro-interesse datoriale, la soluzione è lasciata al criterio del caso per caso, con risultati non sempre coerenti.

Accogliendo molti dei rilievi del giudice Albuquerque, nel riesame del caso Bărbulescu, la Grande Camera verifica che nulla si diceva nel regolamento interno, che pure vietava l'utilizzo a scopo personale degli strumenti aziendali, in merito alla possibilità di effettuare controlli o monitorare la corrispondenza, e soprattutto che non vi era stata specifica informativa circa la possibilità di monitorare i messaggi scambiati dal lavoratore[117].

Il contributo fondamentale della Grande Camera consiste nell'aver delineato una sorta di *vademecum* per verificare la legittimità e la "proporzionalità" tra le misure di controllo poste in essere e la tutela dell'interesse datoriale rispetto all'adeguatezza delle garanzie offerte al lavoratore. È una sorta di "test di verifica" che specifica le caratteristiche di un'informazione trasparente e le modalità di un controllo legittimo, necessario e proporzionale. Al riguardo già uno studio del 2009 proponeva una lista di "indicatori obiettivi" sostanzialmente analoga per verificare l'intrusività delle tecnologie di sorveglianza[118].

La Corte europea propone una lista di indicatori volti ad accertare i seguenti profili: se il lavoratore sia stato informato della possibilità del monitoraggio e dell'adozione di misure di controllo e se l'informazione sia stata fornita preventivamente e risulti chiara in ordine alle caratteristiche del monitoraggio, l'estensione e il grado di intrusione, distinguendo il monitoraggio del solo flusso di comunicazioni e quello del loro contenuto, (la cosiddetta granularità della sorveglianza, estesa o meno anche al contenuto della corrispondenza), il

---

[116] Sulla stessa linea anche il nostro Garante ha sottolineato l'importanza dell'adozione di un disciplinare interno, soprattutto in caso di aziende di medie o grandi dimensioni, cui sia data adeguata pubblicità in azienda, che elenchi i comportamenti non tollerati rispetto alla navigazione in Internet e chiarisca l'eventuale possibilità di utilizzare posta elettronica e Internet per scopi personali oltre che professionali, suggerendo anche misure tecnologiche di tipo preventivo (black lists di siti o altri filtri all'accesso).

[117] Il datore aveva allegato alla contestazione 45 pagine di trascrizione di messaggi personali, monitorati per una settimana, anche tratti dall'account personale e aventi ad oggetto dati sensibili del lavoratore come la salute sessuale, senza aver informato il lavoratore del monitoraggio.

[118] Si tratta dello studio di Jacob Thommesen and Henning Boje Andersen, *Privacy Implications of Surveillance Systems*, in http://orbit.dtu.dk/fedora/objects/orbit:56150/datastreams/file_4010841/content, Technical University of Denmark, 2009.

numero di persone che vi possono avere accesso, la sua durata; se non vi siano altre misure a disposizione del datore di lavoro, meno invasive di quelle adottate per raggiungere il medesimo scopo, ad esempio limitandosi ai metadati[119]; se siano previste misure di salvaguardia adeguate per il dipendente e il suo livello di identificazione personale; il carattere più o meno "sensibile" delle informazioni estratte; il luogo dove la sorveglianza è realizzata; quali siano le conseguenze del monitoraggio e qual è l'uso che il datore di lavoro intende fare delle informazioni[120].

Con riferimento a forme di sorveglianza più complesse, sotto il profilo della tecnologia utilizzata, altra dottrina individua un altro indicatore: la valutazione dello scopo originario per il quale la tecnologia in uso sia stata disegnata[121].

Applicato dalla Corte al caso Bărbulescu, questo test induce la Grande Camera a concludere nel senso di una violazione dell'art. 8 CEDU: il regolamento interno risultava generico, il lavoratore non era stato informato preventivamente della possibilità di essere oggetto di misure di controllo, dello scopo, della durata e della natura di tali misure, né era stata identificata una specifica motivazione capace di giustificare un monitoraggio così stringente come quello operato. Nel caso le autorità nazionali non hanno garantito l'attuazione del fondamentale principio di trasparenza, richiamato già dalla Raccomandazione del Consiglio d'Europa (2015)5, e pilastro fondante del sistema di tutela della vita privata e familiare nel rapporto tra datore di lavoro e lavoratore.

La Corte europea in sintesi ci dice che il potere di controllo è esercitato legittimamente nella misura in cui non ecceda la finalità di verifica dell'adempimento, o eventualmente la verifica della commissione di atti illeciti da parte del lavoratore, e risulti proporzionato e ragionevole nelle modalità di esercizio, modalità di cui il lavoratore è reso consapevole attraverso un disciplinare interno o adeguata informativa.

---

[119] I "metadati", in telematica, sono informazioni che accompagnano i dati in transito, "definendone ed individuandone le coordinate fondamentali (data e ora del "passaggio", indicazioni quali-quantitative su provenienza, destinazione, "peso" e velocità, tipologia, natura, formato, se aperto o chiuso/proprietario, e contenuto: tutti oggetto di possibile aggregazione/disaggregazione, elaborazione e, di conseguenza, controllo. Si tratta di masse di dati che circolano in rete (cd. big data) suscettibili di utilizzo a fini commerciali (data mining e data analysis), di controllo politico e anche di difesa dell'ordine pubblico" (I. Sigismondi, Telematica [Dir. cost.], in http://www.treccani.it/enciclopedia).

[120] Cfr. punto 121 della sentenza della Grande Camera sul caso Bărbulescu v. Romania.

[121] È evidente che vi sono grandi differenze in termini di rischi per la dignità e la riservatezza delle persone a seconda che il software o il sistema informatico siano stati originariamente progettati per finalità di controllo o siano utilizzati con effetti di controllo, implementando altre funzioni rispetto a quelle per le quali il programma sia stato ideato. La questione attiene alla verifica dell'assetto "architetturale" del sistema informatico: dovrà tenersi in debito conto il contesto tecnologico e le finalità per le quali l'algoritmo che costituisce la base di funzionamento del programma è stato disegnato.

La Corte di Strasburgo si sofferma sul rispetto del principio di proporzionalità in un'altra recente sentenza, *López Ribalda et al. v. Spagna*[122]. La videosorveglianza di un lavoratore sul luogo di lavoro deve essere considerata una significativa intrusione nella sua vita privata e anche nel caso di sospetto di atti illeciti il controllo deve essere proporzionato e limitato nel tempo, nello spazio, nei target selezionati rispetto alle finalità perseguite. Nel caso di specie la mancanza di proporzione tra le modalità del controllo e il pur legittimo fine perseguito è alla base del giudizio espresso dalla Corte: il monitoraggio è stato prolungato nel tempo, non circoscritto nello spazio e nei soggetti destinatari del controllo, oltre che non preceduto da adeguata informativa. La misura risultava sproporzionata rispetto al fine di tutela del patrimonio aziendale, in quanto destinata a colpire indiscriminatamente e indistintamente tutti i lavoratori e per questo lesiva dell'art. 8 CEDU, non essendovi stato, secondo i giudici, un corretto bilanciamento tra il diritto alla salvaguardia della vita privata del lavoratore e le esigenze del datore di lavoro.

Il ruolo dell'informativa e l'importanza del regolamento aziendale sono evidenziati nel caso *Libert v. Francia*[123]*:* in questo non solo si formalizza l'equiparazione fra diritto alla riservatezza della corrispondenza elettronica e diritto alla riservatezza del contenuto di documenti salvati sul pc aziendale, ma si fonda la decisione, favorevole al datore di lavoro, sull'esaustività delle disposizioni interne aziendali che prevedevano di utilizzare una specifica opzione su *outlook* per l'inserimento dei *files* privati. Il regolamento aziendale è giudicato dalla Corte sufficientemente chiaro nell'indicare le modalità in base alle quali certi *files* potessero essere esentati dai controlli della direzione: si intendevano salvaguardare le attività private svolte durante il lavoro e rientranti nella nozione di vita privata e al tempo stesso consentire al datore di lavoro di verificare il contenuto dei documenti di lavoro per

[122] Corte EDU, Sez. III, 9 gennaio 2018, López Ribalda et al. v. Spagna, n. 1874/13 e n. 8567/13: si tratta di una fattispecie piuttosto tipica di videosorveglianza occulta funzionale all'esigenza di individuare i responsabili di una serie di ammanchi verificatisi all'interno di un supermercato. A differenza del caso simile *Köpke v. Germania*, 5 ottobre 2010, n. 420/2007 nel quale il monitoraggio aveva riguardato due specifici lavoratori e solamente costoro, per un tempo limitato di due settimane e nello spazio circoscritto delle casse in modo da non estendersi all'intero ambiente di lavoro, e l'accesso alle informazioni registrate era stato limitato ad un ristretto numero di operatori dell'agenzia investigativa ed al personale incaricato dell'impresa, nel caso Lopez la videosorveglianza occulta era si era protratta per un periodo prolungato di tempo e per tutto l'orario di lavoro, senza un target specifico, coinvolgendo tutti i lavoratori addetti alle casse, e senza nessuna informazione ai dipendenti circa l'installazione di telecamere. Per questo l'esito dei due casi è diverso e nel caso Lòpez si ravvisa una violazione dell'art. 8 CEDU.

[123] Corte EDU, Sez. V, 22 febbraio 2018, Libert v. Francia, n. 533/2013. Dal controllo effettuato sui file denominati "personali" sul computer in uso al dipendente era emersa la presenza di diversi filmati di natura pornografica ed alcune false attestazioni a favore di terzi, e da questo era scaturito il licenziamento del lavoratore.

accertare che gli strumenti messi a disposizione fossero utilizzati per l'attività professionale[124].

In tema di videosorveglianza, nel caso *Antovic e Mirkovic v. Montenegro*[125] la Corte ha motivato l'accoglimento del ricorso presentato dai professori montenegrini, escludendo che il solo fatto che la prestazione lavorativa si svolga in un luogo pubblico possa comportare la deroga dell'art. 8, in quanto ciò comporterebbe un'ingiustificata restrizione del diritto al rispetto della vita privata del lavoratore. I giudici richiamano nell'occasione uno degli elementi del "test" di bilanciamento: la verifica dell'esistenza di altre possibili modalità, meno invasive di quelle adottate, che consentano di perseguire la medesima finalità. Pur ritenendo in linea di principio legittime le finalità perseguite, la tutela del patrimonio aziendale e dell'organizzazione produttiva e la sicurezza del personale, la Corte ha ritenuto illegittimo il bilanciamento operato tra i due opposti interessi: si sarebbero potute perseguire le medesime finalità con modalità che avessero un minor grado di intrusività e consentissero il contemperamento fra il diritto alla tutela della vita privata nei luoghi di lavoro e il contrapposto interesse del datore di lavoro.

Anche i principi e i criteri estrapolati dai giudici di Strasburgo contribuiscono a consolidare il corredo di tutele per il lavoratore, a partire dell'innesto regolativo tra disciplina lavoristica e normativa generale in materia di protezione dei dati personali.

[124] Secondo i giudici il signor Libert, dipendente della società, aveva violato il regolamento aziendale salvando sul pc in uso i file come "personali", mentre avrebbe dovuto denominarli "privati", non "personali", come specificato dal regolamento interno. La diversa denominazione aveva indotto l'azienda, la società nazionale delle ferrovie francesi, a ritenere che potesse trattarsi di *files* di lavoro personalmente trattati dal dipendente.

[125] Corte EDU, Sez. II, 28 novembre 2017, Antovic e Mirkovic v. Montenegro, n. 70838/13. Nel caso si discute della legittimità dell'installazione di un sistema di videosorveglianza nelle aule dell'Università montenegrina: il Preside della Facoltà di matematica aveva informato il Consiglio di Facoltà dell'avvenuta installazione di un sistema di videosorveglianza. Qualche giorno dopo il Preside aveva deciso di estendere la videosorveglianza a sette anfiteatri e all'area antistante l'ufficio di presidenza, il tutto al fine di proteggere la sicurezza della proprietà e delle persone, inclusi gli studenti. L'accesso alle informazioni registrate era protetto da un codice in possesso del solo Preside e i dati sarebbero stati conservati per un anno. Il contenzioso domestico, in questo caso, riguardava una pretesa risarcitoria avanzata da alcuni professori per asserita violazione del diritto alla privacy. Il tribunale montenegrino, pur avendo rilevato che l'aspettativa alla protezione della privacy non viene meno per il solo fatto che il luogo di lavoro è pubblico o aperto al pubblico, aveva comunque concluso nel senso che i ricorrenti non avessero dimostrato che il loro diritto fosse stato violato. Diversamente, la Corte di Strasburgo ha ritenuto che, pur dovendo ritenersi legittimi gli scopi perseguiti dall'Università, non risultava, nel caso di specie, che fosse stato garantito un equo bilanciamento tra contrapposti interessi, in ragione del fatto che non risultava dimostrata l'impossibilità di fare ricorso a strumenti meno invasivi ma comunque idonei a perseguire le finalità prefissate, e tutto ciò nonostante il fatto che in questo caso l'informativa fosse stata fornita in modo adeguato.

1.9 L'autoregolamentazione: dai codici di deontologia e buona condotta alle regole deontologiche

Nel rapporto tra disciplina generale e discipline speciali e al fine di adattare i principi generali della legge a tutela della privacy alle peculiari esigenze del rapporto di lavoro, nelle intenzioni del legislatore i codici di deontologia e buona condotta occupano un posto di rilievo.

I codici di condotta sono stati introdotti per la prima volta nell'ambito della protezione dei dati personali dalla legge 675/96, in sede di recepimento dell'articolo 27, paragrafo 3, della direttiva 95/46/CE. Successivamente l'art. 12 del D.lgs. 196/2003, oggi abrogato, ha conferito al Garante il potere di promuovere la sottoscrizione di codici di deontologia e buona condotta, nell'ambito delle categorie interessate, di verificarne la conformità e di contribuire a garantirne la diffusione e il rispetto con il compito di curare la pubblicazione dei codici nella Gazzetta Ufficiale della Repubblica[126]. L'intento era di dotare questi codici di autodisciplina di una specifica forza prescrittiva e poter garantire la trasparenza, la riservatezza, il corretto uso dei dati che viaggiano nella rete, ricorrendo a degli strumenti elastici, in grado di adeguarsi rapidamente alle nuove esigenze dell'epoca attuale. Questi codici, elaborati direttamente dalle parti interessate, dalle associazioni e dagli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento, possono rappresentare strumento idoneo a precisare e dettagliare l'applicazione delle disposizioni normative rispetto a specifici settori. Il rispetto dei codici di deontologia e di buona condotta rappresenta una condizione per la liceità e la correttezza del trattamento dei dati personali effettuato da soggetti pubblici e privati.

Il momento di maggior rilevanza di tali codici è legato al D.lgs. 467/2001 che all'art. 20 li ha previsti allo scopo di disciplinare il trattamento dei dati personali in determinati settori

[126] Si veda in proposito anche l'articolo di E. Del Prato: *Un caso emblematico è nell'art.12 del d. legisl. 30 giugno 2003, n.196 (codice in materia di protezione dei dati personali), di cui sono esplicazione ulteriori disposizioni contenute nello stesso decreto legislativo. Esso, sotto il controllo del Garante (e cioè di una autorità amministrativa indipendente), rinvia ai codici di deontologia e buona condotta per stabilire i criteri di valutazione del trattamento dei dati personali: "liceità" e "correttezza" sono, con qualche sovrabbondanza, i termini adoperati. Mediante tale norma i codici in questione sono diventati regola circa l'impiego dei dati personali: rilevanti, quindi, a pieno titolo nella giuridicità. Veicolo di ciò è l'iniziativa del Garante, a cui si chiede di favorire la partecipazione di soggetti interessati. Un esempio di rilievo è nel codice deontologico dei giornalisti (art. 139 d. legisl. cit.), che detta le regole in base a cui valutare il rispetto dei doveri che incombono al giornalista nel divulgare notizie, concretizzando i criteri della verità, della continenza e dell'interesse sociale che rendono legittima l'ingerenza nella riservatezza. L'art. 139 cit. demanda al Consiglio nazionale dell'ordine dei giornalisti la formazione del codice, sotto la supervisione del Garante, che ha il potere di prescrivere "eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire".* (E. Del Prato, *Regole deontologiche delle professioni e principio di sussidiarietà: l'esperienza italiana*, in *Riv. Dir. civ*. 4/2014, 769).

quali internet, il marketing, il settore previdenziale, i sistemi informativi, adottando un modello già sperimentato in altri campi, come quello giornalistico.

Questi codici non sono più ascrivibili alla sfera del *soft law*, e non possono essere semplicisticamente fatti ricadere in quella dell*'hard law*: dal punto di vista del processo di produzione, questi codici sono promossi dal Garante "nell'ambito delle categorie interessate", che tuttavia non hanno la disponibilità del prodotto finale, sottoposto ad un controllo di conformità a leggi e regolamenti da parte del Garante. In questo modo si cerca di tenere insieme una presenza "autonoma" delle categorie interessate ed una garanzia pubblica, in coerenza con una legislazione per principi che deve mantenersi al passo con una realtà in continuo movimento. Legislazione per principi e codici di deontologia sarebbero accomunati dalla finalità di realizzare una disciplina omeostatica rispetto al cambiamento sociale[127].

Il D.lgs. 101/2018 ha abrogato l'articolo 12 del Codice privacy eliminando il riferimento ai codici di deontologia e buona condotta e li ha ribattezzati regole deontologiche, in attuazione dell'art. 40 del Regolamento 679/2016[128]. L'art. 111 del Codice, come modificato dal D.lgs. 101/2018, oggi rubricato *Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro*[129], prevede la promozione, da parte del Garante, di regole deontologiche per le finalità di cui all'art. 88 del Regolamento, nonché l'individuazione di specifiche modalità per le informazioni da rendere all'interessato.

---

[127] S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy,* in *Europa e diritto privato*, 1/2004, 8-9.

[128] Art. 40: 1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

2. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati; b) i legittimi interessi perseguiti dai titolari del trattamento in contesti specifici; c)la raccolta dei dati personali; d) la pseudonimizzazione dei dati personali; e)l'informazione fornita al pubblico e agli interessati; f)l'esercizio dei diritti degli interessati; g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore; h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32; i)la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato; j)il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; k)le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

[129] Art. 111 Codice privacy, novellato dal d.lgs. 101/2018: *Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro* Il Garante promuove, ai sensi dell'articolo 2-*quater*, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

È dunque rivisitata la materia dei codici di condotta, a cavallo fra l'autoregolamentazione dei privati e la regolazione pubblica: si stabilisce che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggino l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, funzionali alla definizione di un modello di bilanciamento ispirato ai criteri di equità, correttezza e trasparenza in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese. I codici riempiono di contenuti i principi di liceità e correttezza del trattamento, contenendo previsioni esplicative di tale principio ed offrendo un parametro per la loro valutazione.

Nell'ambito dei settori indicati dal legislatore, in assenza di disposizioni del Regolamento, sono stati finora adottati sette codici di deontologia relativi a specifici trattamenti di dati, pubblicati in Gazzetta Ufficiale conformemente alle previsioni dell'art. 2 quater del D.lgs. 196/2003, come modificato dal decreto legislativo 101/2018[130].

È prevista una specifica sanzione (art. 83, par. 5 Reg. 2016/679UE) per non aver osservato le regole deontologiche per trattamenti nell'ambito dei rapporti di lavoro.

I codici di condotta assumeranno nel nuovo sistema di protezione dei dati un ruolo importante: il Regolamento prevede in capo al titolare e al responsabile del trattamento, l'onere di provare di aver attuato le misure organizzative e di sicurezza adeguate alla particolare tipologia di dati ed in questo senso *best practices*, certificazioni, codici di condotta possono essere utilizzati come elementi di prova per dimostrare la conformità del trattamento da parte del titolare del trattamento o del responsabile.

In futuro le regole deontologiche potrebbero essere valorizzate quali validi strumenti sia per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura e gravità, che l'individuazione delle migliori prassi o di opportune misure per attenuare il rischio.

[130] Si tratta, in particolare delle Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica (G.U. del 4 gennaio 2019, n. 3); Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica G.U. del 15 gennaio 2019, n. 12); Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (G.U. del 14 gennaio 2019, n. 11); Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (G.U. del 14 gennaio 2019, n. 11); Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (G.U. del 15 gennaio 2019, n. 12). I codici relativi ai sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti e quello riguardante il trattamento dei dati personali effettuato ai fini di informazione commerciale restano in vigore fino a che non subentrino i nuovi codici approvati a norma dell'art. 40 Regolamento.

1.10 Il Regolamento 2016/679 UE

Presa coscienza dell'evoluzione dei modelli produttivi, delle trasformazioni socio economiche, dell'esistenza di nuovi rischi e potenziali *vulnus* per la sfera privata delle persone, del valore assunto dal dato personale, le istituzioni europee hanno ritenuto di codificare le precedenti produzioni normative, l'elaborazione giurisprudenziale della Corte di Giustizia Europea e gli approfondimenti del Gruppo di lavoro articolo 29, intervenendo con lo strumento più vincolante per gli Stati membri, il Regolamento. Il legislatore europeo non ha ritenuto più sufficiente il perseguimento di obiettivi comuni da parte degli Stati membri, reputando indispensabile vincolare tutti gli operatori ad un regime giuridico uniforme attraverso l'adozione del Regolamento.

Il Regolamento del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE, pur essendo un atto *self-executing*, ossia una disciplina immediatamente esecutiva nell'ordinamento degli Stati membri (art. 288 TFUE), per sua espressa previsione, si è sostituito alla disciplina previgente solo a partire dal 25 maggio 2018, quando è divenuto esecutivo in tutti gli Stati membri. Il legislatore comunitario, considerate le difficoltà di transizione dalle previgenti norme nazionali alle nuove norme europee, aveva previsto di sospenderne l'applicazione nei primi due anni dall'approvazione per dare tempo agli Stati membri di adeguare le norme interne, cosa che il nostro paese ha fatto con il D.lgs. 101 del 10 agosto 2018 *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*. Oggi dunque il Codice Privacy, come modificato dal D.lgs. 101/2018, risulta integrato ed armonizzato rispetto alle prescrizioni del Regolamento UE 2016/679[131].

La precedente direttiva 95/46/CE non aveva impedito la frammentazione nell'applicazione della disciplina di protezione dei dati personali nel territorio dell'Unione, né eliminato

[131] Il D.lgs. 101/2018, con i suoi 27 articoli, interviene sui 191 articoli del previgente D.lgs. n. 196/2003, abrogando 110 articoli, sostituendone 35, modificandone 29 ed aggiungendone altri 29 limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili del GDPR.

l'incertezza giuridica: le divergenze nell'attuazione e nell'applicazione della direttiva nei singoli Stati membri avevano fatto nascere l'esigenza di una normativa vincolante.

L'obiettivo principale perseguito dal Regolamento Generale sulla Protezione dei Dati (denominato GDPR, acronimo derivante dalla denominazione inglese General Data Protection Regulation) è quello di ovviare alla frammentazione della protezione dei dati personali nel territorio dell'Unione, alla compresenza di diversi livelli di protezione dei dati personali, con tanto di ricaduta sulla libera circolazione dei dati personali all'interno dell'Unione e conseguente freno all'esercizio delle attività economiche dell'Unione (considerando 9).

Data la necessità di "assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità di trattamento che possono ostacolare la libera circolazione dei dati personali nel mercato interno", la scelta dello strumento regolamentare, direttamente applicabile e senza necessità di essere recepito dall'ordinamento di ogni Paese, è apparsa particolarmente appropriata.

Come si legge nella rubrica, oggetto di tutela sono unicamente i dati personali nella misura in cui riguardino le persone fisiche: non sembra più essere consentito introdurre una disciplina nazionale che estenda la tutela della riservatezza anche alle persone giuridiche, come accadeva sotto la vigenza della Direttiva n. 95/46/CE.

L'ambito di applicazione territoriale della disciplina sulla protezione dei dati personali si estende significativamente alla protezione dei dati personali di tutti coloro che si trovano nell'Unione, indipendentemente dal luogo in cui sia effettuato il trattamento dei dati personali: la tutela riguarderà anche trattamenti effettuati da titolari non stabiliti nell'Unione Europea se avrà ad oggetto dati personali di interessati che si trovano (anche virtualmente) nell'Unione e riguarderà l'offerta di beni o servizi e/o con monitoraggio dei loro comportamenti all'interno dell'Unione (art. 3 Reg. 2016/679). Ci sarà una sostanziale "extraterritorialità" dell'efficacia delle norme Regolamento: il principio del *locus stabilimenti*[132] del titolare o del responsabile sarà integrato nel senso che il Regolamento si applicherà sia se il titolare o il responsabile del trattamento siano stabiliti nell'Unione, anche se il trattamento venga effettuato all'esterno dell'Unione stessa, sia nel caso in cui il soggetto a cui si riferiscono i dati si trovi, realmente o virtualmente, nel territorio europeo e ancora nel caso di un datore con sede fuori dall'Unione che però conservi i dati raccolti attraverso

[132] Il diritto di stabilimento consiste nel diritto di svolgere attività autonome e di creare e gestire imprese al fine di esercitare un'attività permanente su base stabile e continuativa, alle stesse condizioni che la legislazione dello Stato membro di stabilimento definisce per i propri cittadini.

il controllo a distanza in un *service provider* di *cloud* situato all'interno dei confini dell'Unione, scongiurando così il rischio di possibili aggiramenti della normativa da parte di Internet Service provider esteri.

Il GDPR, pur non stravolgendo l'impianto complessivo del sistema della protezione dei dati personali, segna il passaggio da un regime autorizzatorio ad uno improntato sulla responsabilizzazione del titolare del trattamento: una tutela della riservatezza ideata secondo un sistema di responsabilità intra-aziendale in cui il principio dell'*accountability* o responsabilizzazione del titolare del trattamento si sostituisce al precedente approccio autorizzatorio. Il mutato approccio alla protezione dei dati personali, codificato nel Regolamento, si sostanzia in un sistema capace di garantire l'adozione di adeguate misure di protezione, grazie ad analisi e valutazioni del rischio preliminari, a Codici di condotta, a Linee Guida e modelli organizzativi previsti da sistemi di certificazione volontaria. Le norme a tutela della riservatezza proceduralizzano gli obblighi a carico del titolare, promuovendo la diffusione nelle aziende di un sistema organizzativo complesso volto alla protezione del dato personale.

Il titolare deve essere in grado di dimostrare l'adozione e l'attuazione di un modello organizzativo che preveda misure giuridiche, organizzative, tecniche, adeguate a garantire l'efficace attuazione delle regole poste dal Regolamento, avendo riguardo alle peculiarità e ai bisogni della singola organizzazione[133].

Il Regolamento richiede di incorporare il rispetto del diritto alla tutela nel trattamento dei dati personali nelle piattaforme tecnologiche e nei processi organizzativi in modo che l'attività produttiva - la fornitura di beni e servizi o di prestazioni professionali – incorpori, *by design* e *by default*, le garanzie per il trattamento dei dati personali.

In materia di trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, l'art. 88 del Regolamento europeo non impone l'armonizzazione dei sistemi giuridici dei Paesi membri dell'UE e questo secondo Andrea Sitzia dimostra il fallimento di un tentativo, che pure era stato fatto, di condividere, a livello europeo, una precisa linea di indirizzo in materia [134]. L'art. 88 si limita a prevedere che gli Stati membri possano introdurre, per legge o attraverso la contrattazione collettiva norme più specifiche per assicurare la protezione dei diritti e delle libertà in relazione al trattamento dei dati personali dei lavoratori nell'ambito del rapporto di lavoro, quest'ultimo inteso in senso ampio, dalla fase pre-assuntiva sino alla

[133] A. Ingrao, *op. cit*., 76.

[134] A. Sitzia, *I limiti del controllo della posta elettronica del lavoratore: una chiara presa di posizione della Grande Camera della Corte eur. dir. uomo*, in *NGCC* 12/2017, 1659.

cessazione del rapporto di lavoro e per finalità altrettanto diversificate[135]. Prevede poi "misure appropriate e specifiche" a protezione "della dignità umana, degli interessi legittimi e dei diritti fondamentali" nell'ipotesi particolarmente delicata di trattamento di dati personali, quale la sorveglianza dei dipendenti.

Sono nel segno della continuità molti dei principi declinati nel Regolamento 2016/679, già presenti nella previgente normativa europea: il Capo II è dedicato ai principi applicabili al trattamento dei dati personali, dalla trasparenza alla proporzionalità, dalla minimizzazione alla finalità, mentre il Capo III è dedicato ai diritti dell'interessato dall'informazione all'accesso ai dati personali, dalla rettifica e cancellazione, al diritto alla portabilità dei dati e al diritto di opposizione.

L'obiettivo finale di tutela delle persone fisiche rispetto al trattamento dei dati personali, anche nel contesto occupazionale, dovrebbe risultare rafforzato dalla conferma e dallo sviluppo dei principi già contenuti nella previgente disciplina, come ampliati e sviluppati nel Regolamento.

[135] Reg. 2016/679/UE Articolo 88 Trattamento dei dati nell'ambito dei rapporti di lavoro (C155):
1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.
2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.
3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Capitolo 2 Il Regolamento UE 2016/679

Personal data is the new oil of the internet and the new currency of the digital world.
Meglena Kuneva, Commissario europeo per la tutela dei consumatori (2009).

Com'è definita l'identità?
In passato si diceva: "Io sono quello che dico di essere".
Oggi, siamo quello che Google dice che siamo. Siamo sempre meno persone, sempre più profili.
Stefano Rodotà

2.1 Il dato personale

Nella puntualizzazione e nell'aggiornamento delle definizioni già presenti nella Direttiva n. 95/46/CE, il Regolamento 2016/679 amplia lo spettro semantico della nozione di "dato personale"[136] (e poi di "trattamento"), prevedendo categorie ulteriori e particolari di dati e casi particolari di trattamento.

[136] Sulla qualifica del dato personale come bene giuridico si vedano le riflessioni di A. Iuliani, *Note minime in materia di trattamento dei dati personali*, in *Europa e Diritto Privato*, fasc.1, marzo 2018, 293.
La normativa sul trattamento dei dati personali non disciplina il fenomeno della cessione di informazioni personali, né a titolo gratuito, né a titolo oneroso, non parla mai di scambio, ma soltanto di consenso al trattamento quale condizione di ammissibilità del trattamento, non sembra sostenere la tesi che assimila l'informazione al bene giuridico, ma sarà opportuno sviluppare qualche riflessione sulla qualifica del dato personale come bene, soprattutto in relazione ai *big data* e alla loro commercializzazione. Tanto più che il Regolamento europeo si preoccupa di definire una strategia funzionale alla creazione di un "Mercato Unico Digitale" per promuovere un'"economia europea dei dati" ritenuto fattore determinante nell'incremento del Prodotto Interno Lordo dell'UE: questo pone con maggiore urgenza all'attenzione degli studiosi la questione della possibile qualificazione delle informazioni, personali e non, come bene giuridico, dunque oggetto di appropriazione e della compatibilità con gli strumenti giuridici tradizionali delle nuove forme del capitalismo cognitivo. La rilevanza giuridica dell'informazione ha messo alla prova le diverse teorie sul bene giuridico che si sono confrontate sul controverso rapporto tra bene e cosa a partire dalla definizione formulata dall'art. 810 c.c. che definisce il bene come quella cosa oggetto di diritto. Svincolare dalla materialità la qualifica di bene giuridico nella consapevolezza che non tutte le cose sono beni, ma soltanto quelle oggetto di situazioni giuridiche soggettive, e non tutti i beni sono cose, poiché lo sono anche le entità immateriali, e infine non tutti i beni sono oggetto dei diritti che si appuntano sulle cose materiali, ci invita a riflettere sulla tutela giuridica assegnata dall'ordinamento nella forma del diritto soggettivo ad entità materiali o immateriali.
L'ordinamento non è arbitro libero della scelta ma recepisce e consolida un nesso di corrispondenza con il mercato, in virtù del quale si considera bene qualunque entità che presenta l'attitudine ad essere oggetto di valore di scambio. La qualifica di bene, perciò, al di là del riferimento contenuto nell'art. 810 c.c. ai beni materiali, si desume indirettamente per il tramite del principio di patrimonialità che attribuisce la qualifica di bene a qualsiasi entità, incluso il fare, suscettibile di valore di scambio, che cioè abbia assunto la qualità di merce e per la quale l'ordinamento non ne abbia escluso la circolazione. Da qui le argomentazioni a favore del

Ai sensi dell'art. 4, p. 1, n. 1 Reg. costituisce dato personale qualsiasi informazione, di tipo oggettivo, come un dato biometrico, o di tipo soggettivo come una opinione, una tendenza, una valutazione, attinente a una persona fisica identificata o identificabile, direttamente o indirettamente. Il dato personale contiene l'informazione ma l'informazione non è l'unico elemento costitutivo del dato personale: è necessario un collegamento tra informazione e persona fisica, il cosiddetto interessato, che consenta la riconducibilità del dato alla persona, e quindi la sua identificazione o identificabilità.

Si considerano identificativi della persona il nome, dati relativi all'ubicazione, un identificativo *on line*, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. La previsione anche di un identificativo *online*, quale l'indirizzo IP del computer, rappresenta una significativa novità e rinvia ad una più attenta considerazione dell'identità digitale.

Non sono da considerare dati personali quelli resi anonimi per effetto della "pseudominizzazione", di cui all'art. 4, n. 5 del Reg.[137], così come restano esclusi dalla tutela quelli che appartengono alle persone giuridiche.

Nella prospettiva giuslavoristica si evidenzia come qualunque dato e/o informazione attinente a un lavoratore o collaboratore, identificabile direttamente o indirettamente, nonché qualunque valutazione riferibile al suo comportamento in costanza di rapporto lavorativo, risulterà compresa nella nozione di dato personale e sarà meritevole di tutela in base al Regolamento. La protezione non riguarda solo le informazioni raccolte in occasione dell'assunzione e poi della gestione del rapporto lavorativo ma anche le informazioni "seminate" dal lavoratore durante la navigazione in internet tramite strumenti elettronici forniti dall'azienda o personali, quelle salvate dal dipendente nei profili personali dei social network (Facebook, Twitter, Istagram), quelle tratte dalle mail, che il datore potrà raccogliere, conservare e utilizzare con il consenso dell'interessato e nel rispetto dei principi enumerati nella normativa europea.

Il Regolamento supera la già nota distinzione fra dati comuni e dati sensibili[138], prevedendo categorie particolari di dati, idonei a rivelare l'origine razziale o etnica, le opinioni politiche,

riconoscimento del valore di bene all'informazione, e di conseguenza sulla sua possibilità di essere oggetto di diritti reali.

[137] Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Deve risultare impossibile e non soltanto complessa l'identificazione dell'interessato.

[138] L'espressione "dati sensibili" non è più utilizzata nel regolamento, i dati sensibili risultano inclusi nelle "categorie particolari di dati personali" di cui all'articolo 9 del Regolamento.

le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, nonché i dati genetici, relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute e che risultano in particolare dall'analisi di un campione biologico, e i dati biometrici, 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. Il Regolamento riserva inoltre particolari tutele ai dati personali relativi a condanne penali e reati (art. 10 Reg.), che sostituiscono l'espressione dati giudiziari, non più utilizzata.

Il Regolamento non pone un divieto inderogabile di raccogliere e utilizzare dati appartenenti a particolari categorie, ma posto che il loro trattamento comporta un rischio elevato per i diritti e le libertà della persona, precisa che il trattamento sarà consentito in casi individuati, obbligando nel nostro caso il datore di lavoro a valutare la necessità rispetto all'obiettivo perseguito. Ai sensi dell'art. 9, comma 2, lett. b), GDPR) il trattamento di particolari categorie di dati è consentito qualora sia "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 dagli 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".

2.2 Il trattamento dei dati personali

La nozione di trattamento include "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la memorizzazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, ma anche la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" (art. 4, n. 3 Reg. 2016/679). Le disposizioni del Regolamento relative al trattamento dei dati sono riferite anche ai lavoratori quali soggetti interessati ed il trattamento include le operazioni che comportino la comunicazione, diffusione o qualunque altra messa

a disposizione dei dati personali rilevanti nei casi di distacco o di somministrazione del personale.

Costituiscono casi particolari di trattamento, i trattamenti automatizzati e la profilazione, che non è altro che una forma particolarmente invasiva di trattamento automatizzato, consistente nell'utilizzo di dati personali per valutare determinati aspetti concernenti una persona fisica, al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti. La profilazione consiste, dunque, in un'analisi dei più disparati comportamenti umani, rispetto ad una popolazione di riferimento, al fine di ricavarne dati, analizzarli tramite algoritmi e categorizzarli nei cosiddetti *cluster* predefiniti dal titolare del trattamento, sulla base di parametri che quest'ultimo considera necessari allo scopo del trattamento stesso. Ai sensi dell'articolo 22 p.1 del Regolamento, l'interessato ha il diritto di non essere sottoposto a decisioni basate unicamente su tecniche automatizzate, compresa la profilazione e nei casi in cui ciò avviene, ad esempio, in quanto necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, il Regolamento prevede misure di tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato[139]. I trattamenti decisionali automatizzati devono essere oggetto di specifica informativa (art. 13, comma 2, lett. h, art. 14, comma 2, lett. g, art. 15, comma 1, lett h), che deve estendersi anche alla logica sottesa all'algoritmo. Inoltre, le decisioni assunte non possono essere affidate all'operare esclusivo dell'algoritmo, ma sono obbligatori meccanismi tecnici che assicurino l'umanizzazione del giudizio finale e il diritto di contestazione.

Nel caso in cui il trattamento automatizzato sia necessario per la conclusione o lo svolgimento di un contratto di lavoro tra il titolare e l'interessato e si trattino in modo

[139] Art. 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

automatizzato dati riferibili al lavoratore al fine di analizzarne o prevederne aspetti riguardanti il rendimento professionale, l'affidabilità nello svolgimento delle mansioni, o al fine di porre in essere forme di recesso automatico dal contratto o sospensioni collegate al *rating* raggiunto, sono previsti, a tutela dell'interessato, il diritto di richiedere l'intervento umano e di esprimere la propria opinione o contestare le decisioni (art. 22 p. 2 Reg.)[140].

Le tutele previste con riferimento alla profilazione e alle decisioni automatizzate si applicano anche ai *gig workers*, coloro che prestano lavoro nella cosiddetta economia dei lavoretti, che in quanto soggetti interessati del trattamento, sono anch'essi destinatari delle disposizioni del Regolamento[141].

La stessa cancellazione o distruzione del dato personale rientra nella nozione di trattamento: ne conseguono obblighi a carico dell'azienda in occasione della conclusione del rapporto e della distruzione dei dati personali contenuti sui personal computers e sui devices aziendali concessi in dotazione al lavoratore.

Ulteriore novità introdotta dal Regolamento è la definizione di "pseudonimizzazione" (art. 4 Reg.): il trattamento dei dati effettuato in modo tale che i dati personali non possano più essere attribuiti a uno specifico interessato senza l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano immediatamente attribuiti a una persona fisica identificata o identificabile.

Il Regolamento subordina il trattamento dei dati personali ad una serie di presupposti di liceità, al verificarsi di almeno una delle condizioni indicate nell'articolo 6, tra le quali il consenso al trattamento dei propri dati personali per una o più specifiche finalità o la necessità del trattamento per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. Tra le condizioni di liceità del trattamento, è opportuno richiamare l'attenzione sul "perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che

---

[140] Critica A. Donini: *in relazione al contratto di lavoro, che rientra nella deroga, l'efficacia protettiva ricavabile dalla conoscenza dei criteri per il trattamento sia inadeguata rispetto alle possibili conseguenze sulla posizione del prestatore* (A. Donini, *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali*, n. 1/2018, 222).

[141] Degli effetti della profilazione nel rapporto di lavoro abbiamo un'esperienza concreta nella *Gig economy*: algoritmi includono giudizi e valutazioni della clientela sulle prestazioni dei lavoratori, le elaborano e ne estraggono un punteggio che rappresenta il valore della prestazione del singolo. Qualora il punteggio scenda sotto una soglia decisa dalla piattaforma, questa è in grado di assumere decisioni automatizzate, disattivando, per esempio, automaticamente il profilo del prestatore, ed esercitando un vero e proprio diritto di recesso automatizzato dal rapporto di lavoro con i rischi che si possono facilmente immaginare.

richiedono la protezione dei dati personali" (art. 6, par. 1, lett. f), che non è altro che la riformulazione dell'equo bilanciamento tra interessi contrapposti[142].

2.3 Accountability: il titolare del trattamento e il responsabile della protezione dei dati

Un vero e proprio mutamento di prospettiva si rinviene nell'assetto delle responsabilità delineato nel Regolamento europeo: vengono fortemente responsabilizzate due figure, il titolare del trattamento e il responsabile della protezione dei dati (Data Protection Officer DPO), al quale è affidato un inedito ruolo di consulenza e di garanzia. Il Regolamento riformula gli obblighi a carico del titolare, quanto alle modalità di trattamento ed alle informazioni da fornire all'interessato, e prescrive nuovi adempimenti quanto all'adozione di misura tecniche e organizzative per la sicurezza dei dati ed alla preventiva valutazione del rischio inerente il trattamento.

Nel nuovo assetto stabilito dal Regolamento uno dei principi cardine è l'*accountability*: il principio di responsabilizzazione ispira tutto il Regolamento e condiziona le scelte organizzative sin dalla loro genesi. La libertà imprenditoriale di decidere come organizzare l'attività economica è vincolata alla verifica che gli impianti e/o gli strumenti produttivi prescelti non determinino un controllo più penetrante di quello necessario, imponendo una verifica preliminare dei rischi per la dignità e la riservatezza dell'individuo.

Il titolare del trattamento (Controller), al vertice della gerarchia, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4, n.7 Reg.). Il titolare è il principale obbligato a mettere in atto misure che garantiscano la conformità del trattamento alla normativa europea: grava interamente sul titolare l'onere probatorio della dimostrazione della liceità dei trattamenti svolti. Deve essere in grado di dimostrare di avere adottato misure adeguate ed efficaci a proteggere i dati personali, elaborando uno specifico "modello organizzativo" che, tenuto conto del contesto e delle finalità di trattamento, minimizzi i rischi per le libertà degli interessati. Al titolare è richiesto di assumere un atteggiamento proattivo che consenta di perseguire le sue legittime finalità, ad esempio di

[142] Da leggere in correlazione con i considerando 47, 48 e 49 a proposito dei legittimi interessi del titolare del trattamento: I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

tutela del patrimonio informatico, adottando al contempo tutte le misure necessarie a prevenire comportamenti rischiosi del lavoratore e controlli invasivi dello stesso.

Nell'ambito del rapporto di lavoro, il titolare coincide con il "centro effettivo di imputazione" del rapporto di lavoro[143]: nel caso in cui siano ammessi più datori di lavoro (codatorialità) la titolarità del trattamento deve essere congiunta.

Al titolare si affianca il responsabile della protezione dei dati (DPO) (artt. 37-39 Reg.), designato dal titolare stesso, tramite nomina documentata per iscritto e comunicata all'Autorità Nazionale Garante per la protezione dei dati personali, al fine di collaborare nella gestione della protezione dei dati personali, soprattutto in presenza di trattamenti più a rischio. Può trattarsi di un consulente esterno o di un lavoratore subordinato (che non potrà essere penalizzato o licenziato a causa dell'adempimento dei propri compiti) che in ragione delle sue elevate competenze tecnico giuridiche dovrà garantire la conformità dei trattamenti al Regolamento, una sorta di sostituto del Garante all'interno dell'azienda, coinvolto "tempestivamente" ed "adeguatamente" in tutte le questioni riguardanti la protezione dei dati personali. Il DPO sorveglia sull'osservanza del Regolamento inclusa la sensibilizzazione e la formazione del personale, verifica l'esercizio dei diritti da parte dei lavoratori interessati dal trattamento e fornisce pareri sulla valutazione d'impatto delle misure adottate. Inoltre, coopera con l'Autorità di controllo anche fungendo da contatto con la stessa per questioni attinenti al trattamento di dati particolari o di trattamenti che presentino un rischio elevato per l'interessato. La nomina è obbligatoria per tutte le autorità o organismi pubblici e per le imprese private nel caso in cui le loro attività principali consistano in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o comunque trattamenti su larga scala di dati particolari o penali. Nel caso la nomina non sia obbligatoria il Gruppo dei Garanti europei ne auspica la nomina volontaria.

Il Regolamento prescrive nuovi ed ulteriori adempimenti riferiti all'adozione di misura tecniche e organizzative per la sicurezza dei dati ed alla preventiva valutazione del rischio inerente il trattamento. Si configura una procedura obbligatoria e indispensabile per processi di trattamento dei dati considerati "pericolosi" dal Regolamento, dalle Autorità Garanti o dal

[143] Il richiamo all'effettività da parte del Gruppo ex art. 29 si riferisce all'effettiva capacità di un soggetto all'interno dell'organizzazione di decidere in ordine alle finalità e ai mezzi di trattamento, in base alle circostanze del caso concreto (parere n.1/2010 sui concetti di responsabile ed incaricato del trattamento). V. conformemente Linee guida per il trattamento dei dati dei dipendenti privati del 23.11.2006.

Comitato Europeo, che prevede l'analisi e la valutazione dei rischi, unitamente a una valutazione d'impatto sulla protezione della riservatezza (Privacy Impact Assessment).
L'analisi e la valutazione dei rischi determinano il conseguente obbligo del titolare di adottare misure di sicurezza tecniche e organizzative "adeguate" al rischio e alla pericolosità del trattamento per i diritti e la libertà delle persone (artt. 5 e 32 Reg.), non più "minime" come nella precedente disciplina. La valutazione d'impatto sulla protezione dei dati, che sostituisce il previgente istituto della verifica preliminare da parte del Garante per la protezione dei dati, impone di valutare in anticipo le conseguenze negative sui diritti e sulle libertà delle persone fisiche interessate al trattamento rispetto allo sviluppo di un prodotto/servizio/processo e tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento e della sua definizione, impone una mappatura periodica in relazione allo stato di applicazione del sistema di privacy ai processi aziendali. L'iter di trattamento dei dati personali è procedimentalizzato al fine non solo di valutare preliminarmente l'impatto sulla privacy rispetto alle soluzioni tecnico-organizzative adottate nell'azienda ma anche di effettuare le opportune verifiche e apportare i necessari correttivi.
Tra i nuovi adempimenti ai quali sono sottoposti il titolare e il responsabile del trattamento vi è anche quello di tenere il registro delle attività di trattamento (art. 30 Reg.), redatto a cura del titolare, nel quale vengono annotati i trattamenti effettuati con l'obbligo di conservazione della documentazione, l'indicazione di una serie dettagliata di informazioni (riferimenti dei responsabili interni/esterni; finalità e ambiti di comunicazione e diffusione; misure di sicurezza adottate) e l'obbligo di esibirlo al Garante su sua richiesta. Il registro dei trattamenti rappresenta una rigorosa formalizzazione dei doveri di documentazione degli adempimenti e delle procedure di trattamento e impone di comunicare eventuali violazioni nel trattamento dei dati e/o incidenti informatici (*personal data breach*) entro termini molto brevi (dalle 48 alle 72 ore) agli interessati e alle Autorità Garanti (artt. 33-34 Reg.). Tale registro sarà obbligatorio per imprese o organizzazioni con più di 250 dipendenti ovvero per imprese di dimensioni inferiori qualora il trattamento effettuato dalle stesse possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di dati che nella precedente regolamentazione erano definiti come sensibili o giudiziari (art. 30, co. 5, Reg.).
A carico di titolari e responsabili sono previsti obblighi informativi e formativi del personale volti alla promozione della consapevolezza rispetto a tutti i temi della privacy nei diversi livelli aziendali. La condivisione della nuova normativa e l'acquisizione da parte dei

dipendenti di maggiore consapevolezza dovrebbero garantire una maggiore tutela della *privacy* anche a livello di *policies* e di prassi aziendali.

2.4 Privacy by design e privacy by default

In un'evoluzione concettuale del principio di minimizzazione del dato e del principio di necessità, per cui il trattamento dei dati personali deve avvenire nella misura minore possibile, in quella strettamente necessaria per la specifica finalità perseguita, il Regolamento introduce i principi di *privacy by default* e di *privacy by design*[144].

Con l'espressione *privacy by default* (art. 25 Reg.) si intende la predisposizione di determinate impostazioni automatiche, predefinite, chiuse e non aperte, da parte di chi elabora il sistema informatico, per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità, automaticamente esclusi i dati che eccedono quanto necessario, e per assicurare che non siano resi accessibili se non a un numero definito di persone.

La finalità è quella di rispettare pienamente il principio di minimizzazione nell'utilizzo dei dati che devono essere detenuti e trattati solo nella misura in cui sono necessari allo scopo per cui vengono raccolti, e solo per il periodo di tempo necessario al raggiungimento di tale scopo. Si dovranno adottare accorgimenti tecnici che siano in grado di realizzare una protezione dei dati "per impostazione predefinita", *by default* appunto, senza lasciare alcuna discrezionalità nel momento successivo del trattamento dei dati[145].

La tutela della *privacy* attraverso il *design* dei sistemi informatici comporta che chi sviluppa il sistema deve, sin dall'inizio, valutare i possibili rischi per la riservatezza dei dati e l'autodeterminazione informativa del soggetto e prevedere i possibili rimedi. Compiuta tale analisi preliminare d'impatto, si dovranno inserire nel *design* del sistema i necessari correttivi, con un intervento *ex ante* (quando vi è un maggior numero di soluzioni possibili) invece che *ex post*. La *privacy by design* è dunque contraddistinta dal prevalere del momento

[144] *Il principio di necessità che impone al datore di lavoro di strutturare la propria organizzazione in modo da minimizzare il trattamento dei dati personali* […] *trova ora più puntale e specifica conferma nel Reg. UE 2016/679* […] *che impone al titolare di proteggere i dati fin dalla progettazione della propria organizzazione (c.d. privacy by design cfr. art. 25, co.1) sia di adottare tutte le misure tecniche per limitare il trattamento, nei casi in cui è ammesso dalla legge, solo ai dati strettamente necessari rispetto alle sue specifiche finalità (c.d. privacy by default, cfr. art. 25, co.2.* M. T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro,* in P. Tullini, (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, 58.

[145] È sempre salva la possibilità di cambiamento da parte dell'utente dell'opzione predefinita (Considerando 78 e art. 25, Reg.).

preventivo ed onnicomprensivo: il dato personale va protetto sin dal momento della progettazione dei sistemi aziendali, la protezione dei dati deve essere integrata sin dalla progettazione nell'intero ciclo di vita di una data tecnologia o servizio o processo. Qualsiasi progetto deve essere realizzato avendo cura di tutelare sin dal principio la riservatezza dell'utente finale e la protezione dei suoi dati personali, con tutte le necessarie applicazioni di supporto, al fine di incorporare le regole di protezione dei dati dei lavoratori all'interno della strumentazione aziendale e a mantenerle per tutto il ciclo di vita dei sistemi.

Il concetto di privacy *by design* opera in modo diverso a seconda che si tratti dei modi di conservazione e trattamento dei dati già acquisiti (momento *back-end*) o di ciò che avviene nel momento in cui l'utente si interfaccia con lo strumento/servizio e si acquisiscono i suoi dati personali (momento *front-end*). Nel momento *front-end* lo scopo deve essere quello di fornire all'utente le necessarie informazioni sui dati che verranno acquisiti e di accrescere il controllo dell'utente stesso su di esse. Nella fase di back-end il *design* deve assicurare una corretta fruizione dei dati sia da parte di chi tratta i dati direttamente sia di parti terze.

Lo stesso Regolamento dà alcuni esempi di misure di *privacy by design*, quali la pseudonimizzazione e la cifratura: metodi tecnici di oscuramento di dati personali da implementare per evitare che i dati sulla prestazione siano associabili al singolo lavoratore.

Questi principi si collegano all'approccio proattivo e alla responsabilizzazione del titolare rispetto alla tutela dei dati personali cui si ispira il Regolamento: sarà responsabile il titolare del trattamento dell'adozione di sistemi e servizi strutturati fin dal momento della progettazione nel senso della minimizzazione dei dati trattati e dell'integrazione delle garanzie necessarie, con verifiche periodiche sull'adeguatezza ed effettività delle misure predisposte.

2.5 L'informativa

Altro principio cardine volto ad assicurare la tutela delle persone rispetto al trattamento dei dati personali è il principio di trasparenza: la funzione essenziale dell'informativa, già riconosciuta pacificamente fin dalla Raccomandazione del 1989(2) e poi nel quadro complessivo del sistema generale di tutele predisposto dalla Direttiva n. 95/46 e quindi dal nostro Codice della Privacy art. 13, d.lgs. n. 196/2003, è ora valorizzata e potenziata nel Regolamento (artt. 12-14).

I contenuti dell'informativa vengono distinti a seconda che i dati siano raccolti presso l'interessato oppure no, con la previsione di informazioni aggiuntive in questo secondo caso

(artt.13 e 14, Reg.). L'interessato dovrà essere informato dell'esistenza del trattamento dei dati personali, dell'identità e dei dati di contatto del titolare del trattamento e del responsabile della protezione dei dati, delle finalità del trattamento nonché della base giuridica del trattamento, delle categorie di dati personali in questione e degli eventuali destinatari o categorie di destinatari, dell'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o ad un'organizzazione internazionale, dell'esistenza del diritto alla portabilità dei dati, del diritto a revocare il consenso in ogni momento e di proporre reclamo al Garante e del periodo di conservazione dei dati. In caso sia posto in essere un processo decisionale automatizzato, compresa la profilazione, con conseguente valutazione della persona in termini di rendimento, dovranno essere fornite all'interessato informazioni aggiuntive sulla logica utilizzata, sull'importanza e sulle conseguenze di tale trattamento per l'interessato.

I criteri da rispettare per la compilazione delle informative, soprattutto laddove siano finalizzate a ottenere un valido consenso "informato" e "consapevole", prevedono la redazione in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, trasmessa per iscritto o con altri mezzi, anche elettronici.

Efficacia, puntualità ed intellegibilità delle informazioni fornite sulle modalità di trattamento dei dati sono requisiti fondamentali al fine di perseguire la correttezza dei trattamenti da parte dei responsabili.

Le disposizioni che prescrivono precisi contenuti di "adeguatezza" delle informative avranno un impatto nel contesto delle relazioni giuslavoristiche: le aziende saranno indotte a riformulare le informative da consegnare ai lavoratori sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli.

La corretta e trasparente informazione in merito ai controlli e alla tipologia dei dati personali raccolti e detenuti dal datore di lavoro, potrà consentire al dipendente un pieno esercizio dei propri diritti.

2.6 Il lavoratore come soggetto interessato: diritto di accesso, rettifica, di portabilità e diritto all'oblio

Il lavoratore, in qualità di soggetto interessato al trattamento dei dati, è titolare di una serie di diritti che il Regolamento riconosce all'interessato: avrà così un ruolo attivo di intervento nel trattamento dei propri dati personali e di controllo sulla circolazione delle informazioni. Sono espressamente enunciati il diritto di accesso (art. 15 Reg.), il diritto di rettifica (art. 16), il diritto all'oblio (art. 17), il diritto di limitazione del trattamento (art. 18), il diritto alla

portabilità dei dati (art. 20), il diritto di opposizione (art. 21) ed il diritto a non essere sottoposto a decisioni automatizzate (art. 22).

Il diritto di accesso consiste, essenzialmente, nel consentire al lavoratore di poter conoscere dal titolare, non tanto l'esistenza di un trattamento, ma più concretamente cosa viene trattato e, ad esempio, quali i destinatari dei dati e quanto lungo il periodo di conservazione degli stessi o se è in corso un trattamento automatizzato che comporti la profilazione. Era già previsto nella Direttiva n. 95/46/CE e nell'art. 7 d.lgs. n. 196/2003 ma ora è declinato con maggior puntualità nell'art. 15, Reg. UE n. 2016/679 che lo estende esplicitamente ai cosiddetti dati valutativi: "tutte le valutazioni che contribuiscono a formare il giudizio annuale sul rendimento di un dipendente" e prevede il diritto di ottenere copia dei dati personali oggetto di trattamento.

Già l'Autorità Garante si era espressa ripetutamente sul diritto di accesso dell'interessato: in più occasioni aveva ribadito l'obbligo per le aziende di consentire e facilitare l'accesso del dipendente al complesso di tutti i dati personali presenti negli archivi aziendali e contenuti in altri atti rispetto alle schede identificative o anagrafiche del dipendente. Il diritto di accedere al proprio fascicolo personale è stato solo recentemente considerato dalla Suprema Corte come vero e proprio diritto soggettivo del dipendente già radicato nel contratto di lavoro[146]. Nelle nuove norme, qualora l'interessato eserciti il diritto di accesso al proprio fascicolo, il Titolare sarà tenuto a informare l'interessato entro un mese dal ricevimento della richiesta e in caso di ritardo il Titolare sarà obbligato a darne giustificazione precisandone i motivi e la facoltà di proporre reclamo all'Autorità Garante e/o ricorso all'autorità giudiziaria (art. 12 e art.15 Reg. UE n. 2016/679).

Il diritto di rettifica e d'integrazione dei dati (art. 16 Reg.) prevede per l'interessato il diritto di ottenere, senza ingiustificato ritardo, dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano. Inoltre, tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, fornendo una dichiarazione integrativa. È da segnalare, invece, che è venuto meno il vecchio limite alla rettifica (di cui all'art. 8 del vecchio testo del Codice) da parte dell'interessato in ordine ai propri dati valutativi soggettivi: nel nuovo regime normativo, pure tali dati sono integrabili da parte del lavoratore, non nel senso che il lavoratore può sostituirsi al valutatore (o

[146] Cass. civ. sez. Lav. 7 aprile 2016 n. 6775 sul diritto soggettivo del lavoratore di accedere al proprio fascicolo personale, tutelabile in quanto si tratta di una posizione giuridica soggettiva che trae la sua fonte dal rapporto di lavoro.

all'eventuale nucleo di valutazione), ma nel senso che può avanzare pretese di rettifica, qualora le valutazioni presentino profili d'incompletezza e si rivelino "ingiuste e sleali".

Il diritto alla cancellazione (art. 17 Reg.) prevede il diritto del lavoratore/interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo. Enfaticamente rinominato diritto all'oblio, viene identificato nella possibilità di riappropriarsi delle informazioni di carattere personale, da esercitare non soltanto in seguito all'opposizione al trattamento, che consente la qualificazione della cancellazione come rimedio, ma anche nel caso in cui l'interessato abbia revocato il consenso. Il diritto alla cancellazione si qualifica dunque come espressione del potere sostanziale di autodeterminazione informativa: il Regolamento tutela il diritto dell'interessato di chiedere la cancellazione dei propri dati personali qualora non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, o abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano o infine il trattamento dei suoi dati non sia conforme al Regolamento, ossia il diritto di veder cancellati o deindicizzati (eliminati dai motori di ricerca) dati personali dopo un determinato periodo di tempo, fatta salva l'esistenza di motivi legittimi di conservazione (ad esempio per rispettare obblighi di legge, per garantire diritto di cronaca o per finalità documentaristiche) (art. 17 Reg.).

Malgrado l'interessato abbia fatto valere tale diritto e sussista l'obbligo di cancellazione per il titolare, se la tecnologia disponibile o i costi di attuazione siano tali da rappresentare un ostacolo alla cancellazione, è previsto che il titolare del trattamento adotti le misure ragionevoli, anche tecniche, per informare coloro che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Tali misure potrebbero consistere, tra l'altro, nel trasferire i dati selezionati verso un altro sistema di trattamento o nel rendere i dati selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

In caso di esercizio del diritto di opposizione (art. 21 Reg.) da parte dell'interessato al trattamento dei dati, il titolare del trattamento dopo aver cercato di dimostrare l'esistenza della necessità e delle finalità in base alle quali procedere al trattamento, può proseguire il trattamento, non dando corso all'opposizione, solo quando abbia motivi legittimi che prevalgono sugli interessi, sui diritti e le libertà dell'interessato: quegli interessi posti alla base del trattamento potrebbero valere come causa di rigetto dell'opposizione.

Il diritto di limitazione di trattamento (art. 18 Reg.) è un diritto di natura cautelare consente al lavoratore di ottenere che sia limitato il trattamento dei propri dati, sottoposto a vincolo

d'inutilizzabilità o d'indisponibilità, nel caso in cui sia necessario verificare l'esattezza e liceità dei dati o l'illiceità del trattamento, o procedere alla conservazione probatoria delle informazioni. Il lavoratore-interessato ha diritto alla limitazione del trattamento durante la fase di verifica.

Il diritto alla portabilità del dato (art. 20 Reg.) consente un più semplice trasferimento dei propri dati personali, il che potrà avere rilevanza per i lavoratori impiegati in gruppi societari multinazionali che risulteranno maggiormente protetti grazie al più esteso campo di applicazione territoriale, al rafforzamento degli obblighi di informativa e dei diritti di accesso ai dati inseriti nel fascicolo personale e agli obblighi di notifica in caso di rettifica, cancellazione o limitazioni del trattamento codificati con maggiore attenzione nel Regolamento europeo.

Attraverso il conferimento in capo all'interessato della possibilità di esercitare il diritto al trasferimento presso un altro operatore dei propri dati personali, si attribuisce alla scelta dell'interessato il ruolo di strumento per l'instaurazione, anche in tale settore, di un mercato altamente concorrenziale quale quello delle informazioni personali.

2.7 Le sanzioni

Nel Regolamento la materia sanzionatoria è regolata nel Capo VIII ove trova conferma il principio della responsabilità risarcitoria per il "danno da trattamento", ma con una codificazione più puntuale e delle sanzioni pecuniarie con soglie massime estremamente elevate. Il sistema sanzionatorio appare notevolmente inasprito, secondo una strategia di deterrenza fatta propria dal Regolamento, per cui le sanzioni debbono essere in ogni singolo caso effettive, proporzionate e dissuasive.

L'art. 82 Reg. stabilisce che chiunque subisca un danno patrimoniale o non patrimoniale ricollegato ad una violazione delle disposizioni del Regolamento ha diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento, salvo che questi dimostrino che il danno non gli sia in alcun modo imputabile, perché il trattamento è stato compiuto in conformità agli obblighi previsti nel Regolamento. Risulta risarcibile civilmente solo il danno patrimoniale ricollegabile all'inadempimento delle prescrizioni contenute nel Regolamento da parte del titolare e non più da chiunque lo abbia cagionato.

Il Regolamento lascia comunque irrisolto il problema della natura giuridica della responsabilità per violazione della disciplina sulla protezione dei dati personali restando

divisi gli interpreti tra quanti la ascrivono all'alveo extracontrattuale e quanti, invece, ne hanno tentato una collocazione in ambito contrattuale.

Si riconosce il diritto di proporre reclamo all'autorità di controllo e/o ricorso all'autorità giudiziaria nello Stato membro in cui si risiede abitualmente oppure del luogo in cui si è verificata la presunta violazione e le sanzioni si aggiungono alle misure sanzionatorie che l'Autorità di controllo può emettere (artt. 77 e 79 Reg.).

Per le infrazioni meno gravi, quali quelle riferite alla designazione e al ruolo del responsabile per la protezione dei dati, sono previste sanzioni fino a 10.000.000 di euro o commisurate a percentuali del fatturato lordo dell'impresa (fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente se superiore all'importo fissato in valore assoluto), mentre per le infrazioni più gravi, quali quelle riguardanti la violazione dei principi fondamentali per il trattamento e dei diritti degli interessati, sono indicate sanzioni pecuniarie il cui massimo edittale è pari a 20.000.000 euro o il 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Quanto alle sanzioni penali, il Regolamento affida a ciascuno Stato membro l'individuazione delle "altre" sanzioni per le violazioni al testo del Regolamento che in ogni caso dovranno essere effettive, proporzionate e dissuasive, nonché l'adozione dei provvedimenti necessari per assicurarne l'applicazione (art. 84 Reg.).

Capitolo 3 Il controllo a distanza del lavoratore: l'acquisizione dei dati

L'ideale del potente è sempre stato quello di vedere ogni gesto e di ascoltare ogni parola dei suoi soggetti (possibilmente senza essere visto né ascoltato): questo ideale oggi è raggiungibile. Nessun despota dell'antichità, nessun monarca assoluto dell'età moderna, pur circondato da mille spie, è mai riuscito ad avere sui suoi sudditi tutte quelle informazioni che il più democratico dei governi può attingere dall'uso di cervelli elettronici.

N. Bobbio *Il futuro della democrazia*

3.1 Il nuovo art. 4 St. lav.: limiti procedurali e finalistici all'acquisizione del dato.

Sono già state ricordate le ragioni per le quali l'art. 4 della L. n. 300/1970 mostrava i segni del tempo ed era diffusamente avvertita la necessità di un intervento di modifica e di adeguamento del dato normativo: l'art. 4 St. lav. è stato novellato dall'art. 23 del D.lgs. n. 151 del 14 settembre 2015, secondo le indicazioni contenute nella legge delega. I criteri direttivi, indicati nell'art. 1 comma 7, lett. f, della legge 183/2014 (Jobs Act) che delega il Governo a procedere alla revisione della disciplina sui controlli a distanza sugli impianti e sugli strumenti di lavoro, ribadiscono l'esigenza di un bilanciamento dei valori in conflitto, "tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore".

Come abbiamo visto, la precedente formulazione dell'articolo 4 non poteva prendere in considerazione l'ipotesi che il datore di lavoro potesse organizzare la prestazione lavorativa attraverso strumenti tecnologici, in grado di ricostruire totalmente e a posteriori l'attività svolta dal prestatore di lavoro, accedendo anche a dati personali del lavoratore.

Il legislatore del 1970 non poteva indicare i limiti entro i quali il datore di lavoro potesse gestire le informazioni rilevate attraverso computer, posta elettronica, cronologia delle pagine visitate durante la navigazione in internet o attraverso le applicazioni installate su smartphone e tablet, strumenti ancora pressoché sconosciuti, non poteva prevedere che da

questi potesse derivare un controllo a distanza continuativo, pervasivo e avente ad oggetto non solo l'attività lavorativa ma l'intera sfera personale del lavoratore[147].

Nei fatti si era determinata una "fuga dall'art. 4 St. Lav."[148], in un clima di diffusa elusione della norma e con uno scarso ricorso all'accordo sindacale o all'autorizzazione amministrativa. A. Maresca individua le cause del (mal)funzionamento dell'art. 4 (vecchio testo) e della manifesta inidoneità della norma a realizzare una effettiva tutela della riservatezza del lavoratore, nella sostanziale inerzia di sindacati e imprese che non avviavano le trattative ed evitavano negoziati sindacalmente poco interessanti. Si determinava così una situazione "ipocrita" nella quale i controlli a distanza sull'attività dei dipendenti si moltiplicavano in assenza del preventivo accordo sindacale e, quindi, delle garanzie previste dal legislatore, ma si produceva anche una sorta di impunità del singolo lavoratore, eventualmente responsabile di un'infrazione disciplinare dimostrabile soltanto attraverso controlli che, in mancanza dell'accordo sindacale o dell'autorizzazione amministrativa, si consideravano illeciti[149].

La disciplina prevista dall'art. 4 St. lav. era in uno stato di indubbia sofferenza (Carinci): si dimostrava non solo sempre più incapace di tenere il passo con i processi di trasformazione dei modelli produttivi e di informatizzazione e digitalizzazione del lavoro, ma anche di rispondere al problema dell'utilizzabilità a fini disciplinari delle risultanze del controllo indiretto legittimamente effettuato. Il tasso di inosservanza della norma aumentava considerevolmente, determinando anche incertezze sui corretti comportamenti da tenere.

La diffusa istanza riformatrice è stata accolta dal legislatore del *Jobs Act* che ha inteso adeguare le previsioni normative sia alle innovazioni tecnologiche, che hanno investito le modalità di svolgimento della prestazione e determinato nuove possibilità di controllo occulto, insite negli stessi strumenti di lavoro, che all'evoluzione del concetto stesso di riservatezza. Per ovviare al rilevato malfunzionamento della norma e arginare i nuovi rischi di pregiudizio per la riservatezza e la dignità del lavoratore, il legislatore del 2015 ha ridefinito quel delicato "punto di equilibrio tra le ragioni dell'economia capitalistica e

---

[147] *È difficile immaginare un'invasione della privacy maggiore di quella derivante dall'ispezione di un computer personale. I computer spesso contengono le nostre comunicazioni più intime. Contengono dettagli delle nostre situazioni finanziarie, mediche e personali. Essi rivelano perfino nello specifico i nostri interessi, preferenze e propensioni*. Così la Corte Suprema canadese citata da A. Ricci, *Il controllo informatico a distanza sul lavoratore fra giurisprudenza e Jobs Act. La web sorveglianza nella modernità liquida*, in *Studium iuris* 3/2016, 306.

[148] A. Ricci, *op. cit*., 309.

[149] A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori*, in *Rivista Italiana di Diritto del Lavoro,* 4/2016, 512.

l'esigenza di garanzia dei soggetti implicati nel processo produttivo"[150], ridisegnando i confini tra la tutela della riservatezza del lavoratore e il controllo effettuato dal datore di lavoro, con particolare attenzione ai controlli tecnologici e agli strumenti utilizzati dal lavoratore per rendere la prestazione. Tuttavia, secondo V. Nuzzo proprio sugli aspetti su cui il legislatore voleva far "chiarezza", emergono i principali problemi interpretativi[151].

La nuova formulazione non contiene più un espresso divieto di utilizzo di impianti audiovisivi e altre apparecchiature finalizzate al controllo a distanza dell'attività dei lavoratori: il divieto è ritenuto, tuttavia, dagli interpreti quasi unanimemente presupposto, in forza dell'impostazione statutaria e della preminenza della dignità del lavoratore nell'assetto costituzionale, di quel richiamo contenuto nell'art. 41 comma 2 Cost. che non si ha ragione di ritenere superato[152].

Non è mancato chi ha considerato l'eliminazione dell'enunciato come il segno di una sorta di assuefazione generalizzata al controllo, che sposta pericolosamente in avanti il confine della lesione alla dignità e alla privacy e ha denunciato un progressivo pericoloso passaggio verso una forma liquida di controllo, cosiddetta postpanottica, molto più strisciante e insidiosa, poiché si avvale della collaborazione attiva del controllato e risponde ad interessi privati non pubblici[153].

Nel senso della persistenza di un divieto di controllo a distanza della prestazione di lavoro che sopravvivrebbe nella formulazione e nella ratio del nuovo primo comma dell'art. 4 nonostante la cancellazione dell'enunciazione esplicita, si esprime Valeria Nuzzo. E a conferma della tesi, viene citata Cass. Pen., Sez. III, 8 settembre 2016, n. 51897: *è solo apparentemente venuto meno il divieto esplicito di controlli a distanza, nel senso che il superamento del divieto generale di detto controllo non può essere predicato sulla base della mancanza, nel nuovo art. 4, di una indicazione espressa [...] di un divieto generale di controllo a distanza sull'attività del lavoratore, avendo la nuova formulazione solamente*

---

[150] M. D'Antona, *La reintegrazione nel posto di lavoro*, Cedam, Padova, 1979.

[151] V. Nuzzo, *La protezione del lavoratore dai controlli impersonali*, *op. cit.*, 97. E in senso critico vedi anche Cosattini: *molte sono ancora le questioni irrisolte ed altre ancora, addirittura, sorgono per effetto della modifica normativa*. (L.A. Cosattini, *op. cit.*, 985).

[152] Si veda in senso critico F. Liso, *Jobs Act e controlli a distanza dei lavoratori: qualche considerazione*, in http:// www.nelmerito.com, 6 luglio 2015, il quale deduce *dalla "perfida" eliminazione del divieto generale di utilizzo di apparecchiature mirate a controllare l'attività dei lavoratori l'apertura della strada a pervasivi controlli della prestazione lavorativa fatti attraverso gli strumenti di lavoro*.

[153] V. Maio fa osservare che *la delega pretendeva che la revisione della disciplina dei controlli intervenisse in coerenza con la regolazione dell'Unione europea e le convenzioni internazionali. Ed è quantomeno dubitabile che una totale ed incondizionata liberalizzazione dei controlli intenzionali possa essere ritenuta coerente con quanto dispongono, non solo la Direttiva n. 95/46/CE, ma soprattutto gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea.* (V. Maio, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in ADL n. 6/2015, 1192).

adeguato l'impianto normativo alle sopravvenute innovazioni tecnologiche e, quindi, mantenuto fermo il divieto di controllare la sola prestazione lavorativa dei dipendenti, posto che l'uso di impianti audiovisivi e di altri strumenti di controllo può essere giustificato "esclusivamente" a determinati fini, che sono numerus clausus, e alle condizioni normativamente indicate[154].

Il controllo sulla prestazione realizzato attraverso gli strumenti tecnologici per sua stessa natura enfatizzerebbe i profili di asimmetria e pervasività, di onniveggenza e onnipresenza, e metterebbe maggiormente a rischio la dignità del lavoratore: ragion per cui è maggiormente necessario mantenere il divieto di controllo a distanza sulla prestazione[155].

Nella nuova formulazione risultano distinti il momento dell'installazione dell'apparecchiatura, dalla quale può derivare anche il controllo dell'attività lavorativa, che viene sottoposto a condizione procedurale legittimante ("possono essere installati previo accordo collettivo o provvedimento autorizzativo da parte dell'autorità amministrativa"), il momento in cui lo strumento è "impiegato", per il quale sono previsti limiti finalistici, ("possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale") e infine il momento eventuale dell'utilizzazione dei dati raccolti, a sua volta subordinato ad altre condizioni, l'adeguata informazione al lavoratore e il rispetto del Codice privacy.

---

[154] V. Nuzzo, *op. cit.*, 96. V. anche M. Verzaro sul rilievo dell'avverbio "esclusivamente": *il legislatore, sebbene abbia cancellato il divieto assoluto di controllo a distanza (che figurava nel primo comma del vecchio testo), ha introdotto nel nuovo comma 1, l'avverbio "esclusivamente" che, a mio sommesso avviso, non può non avere rilevanza. A fronte del chiaro tenore letterale della norma – secondo cui gli impianti e gli strumenti possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale – risulta, infatti, evidente che la ratio sottesa alla norma è proprio quella di evitare l'utilizzo degli strumenti elettronici per finalità diverse da quelle esplicitamente indicate* (M. Verzaro, *Controlli tecnologici e utilizzabilità dei dati acquisiti tra finalità del trattamento e diritto alla protezione dei dati personali*, in *Riv. Giur. Lav.* 4/2018, 566).

[155] In questo senso anche V. Maio: *Se così è, un divieto, per quanto non più espresso, di installare ed utilizzare strumenti od apparecchiature con funzioni di controllo esclusivo e diretto dell'attività dei lavoratori continuerebbe ad essere implicitamente riaffermato, a ragione della speciale potenzialità lesiva della libertà e dignità del lavoratore tipica di tali forme di controllo, come noto, odiose proprio perché tendenzialmente continue e pervasive, capaci di sottrarre al lavoratore, nello svolgimento delle sue mansioni, uno spazio e un tempo nel quale potersi ritenere ragionevolmente certo di non essere osservato, ascoltato o comunque "seguito" nei propri movimenti. Del resto, notoriamente, il richiamo alla tutela della dignità del lavoratore ha consentito storicamente alla dottrina ed alla giurisprudenza di ancorare il divieto in questione al presidio costituzionale contenuto all'art. 41, co. 2, Cost. Ancoraggio che, di per sé, non v'è motivo di ritenere venuto meno nel caso del nuovo comma 1 dell'art. 4 cit.* (V. Maio, *op. cit.*, 1191).

In senso contrario M. T. Carinci: *non ha dunque solo portata simbolica ma riveste invece un pregnante significato il fatto che nell'attuale testo normativo non sia stata riprodotta la previsione già contenuta nel primo comma della precedente versione della norma, che disponeva appunto il divieto assoluto di qualunque controllo – diretto o indiretto – sull'attività dei lavoratori, comprensiva dell'attività di esecuzione del lavoro. Oggi, infatti, non solo il controllo indiretto sull'attività dei lavoratori complessivamente intesa è ammesso, pur nel rispetto dei limiti finalistici individuati dai commi 1 e 2 dell'art. 4 St. lav. ma trova anche esplicita legittimazione il controllo diretto sull'adempimento della prestazione effettuato tramite gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"*. M.T. Carinci, in P. Tullini, (a cura di) *op. cit.*, 55.

La condizione legittimante per l'installazione degli strumenti di controllo è costituita dall'accordo con le rappresentanze sindacali o dal provvedimento autorizzativo da parte dell'autorità amministrativa, mentre l'impiego degli stessi, sebbene siano stati legittimamente installati, resta subordinato anche al fatto che lo richiedano esigenze organizzative e produttive, la sicurezza del lavoro e la tutela del patrimonio aziendale.
Si stabilisce così una procedimentalizzazione, che rappresenta di per sé una forma di garanzia, nella quale sono prese in considerazione distintamente e sottoposte a limiti diversi sia le fasi che precedono che quelle che seguono la captazione del dato personale.
Il cambio di impostazione rispetto alla previgente impostazione della norma, che difettava di una proceduralizzazione del potere diretta a renderlo trasparente per il lavoratore e a limitarne le modalità di esercizio, sembra essere il risultato di una più intensa commistione tra norme lavoristiche e normativa *privacy*. Quest'ultima appare fondata sulla procedimentalizzazione e maggiormente orientata alle finalità del trattamento.
Come vedremo meglio affrontando il tema dell'utilizzabilità dei dati, il cambiamento di prospettiva non ha una rilevanza meramente formale: il momento della verifica dell'esistenza di una ragione aziendale qualificata si sposta dall'installazione all'utilizzo dell'impianto e quindi alle finalità del controllo.
Tenendo conto dell'evoluzione del contesto aziendale-produttivo, il novellato art. 4 St. lav. introduce un altro elemento di novità: consente nel caso di imprese plurilocalizzate, con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni o dislocate negli ambiti di competenza di più DTL, che l'istallazione degli strumenti avvenga previo accordo stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale e in mancanza di accordo, previa autorizzazione del Ministero del lavoro e delle politiche sociali. Per esigenze di semplificazione si tende a favorire l'impresa territorialmente articolata e multilocalizzata e ad evitare che vi siano trattamenti difformi tra lavoratori di una medesima impresa a seconda dell'ubicazione dell'unità produttiva nella quale sono occupati. Il confronto avverrebbe una sola volta con le associazioni sindacali comparativamente più rappresentative a livello nazionale, invece che con le rappresentanze sindacali di ciascuna unità produttiva, al fine di concludere un solo accordo a valere per tutte le unità dislocate sul territorio. Analogamente in mancanza di accordo sindacale, l'impresa con unità produttive situate negli ambiti di competenza di più sedi territoriali, può ricorrere direttamente al Ministero del lavoro e delle politiche sociali, senza dover rivolgersi a ciascuna DTL.

È infine stabilita la definitività dei provvedimenti autorizzatori adottati dall'Ispettorato: non sarà possibile avanzare ricorso gerarchico contro tali provvedimenti, ferma restando la possibilità di impugnarli dinanzi al TAR.

3.2 I controlli difensivi: gli orientamenti della giurisprudenza.

Nel contesto del precedente quadro normativo, la giurisprudenza aveva elaborato la categoria dei cosiddetti controlli difensivi, sostanzialmente occulti, posti in essere in assenza del preventivo accordo sindacale (o autorizzazione amministrativa) di cui all'art. 4 St. lav., al fine di tutelare il datore di lavoro dagli atti illeciti commessi dai lavoratori contro il patrimonio aziendale, inteso in un'accezione ampia, comprensiva tanto del complesso dei beni materiali, quanto di quelli immateriali, dell'immagine pubblica dell'azienda, del know-how, nonché del complesso dei rapporti che sono essenziali per lo svolgimento dell'attività produttiva. La giurisprudenza aveva trovato questo *escamotage* per giustificare l'utilizzo delle informazioni raccolte dal datore, senza il rispetto delle condizioni di cui al secondo comma dell'art. 4 St. lav. (testo previgente), nell'ipotesi in cui ciò fosse necessario per tutelare il patrimonio aziendale rispetto a comportamenti illeciti dei dipendenti. L'elaborazione giurisprudenziale legittimava il controllo difensivo argomentandone l'estraneità alla fattispecie prevista dall'art. 4 St. lav. in quanto effettuato per la tutela di beni estranei al rapporto di lavoro: oggetto dello stesso non erano inadempimenti contrattuali, che continuavano a rimanere soggetti alle garanzie procedurali dell'art. 4 St. lav., ma comportamenti del lavoratore qualificabili come illeciti extracontrattuali, anche se commessi in occasione della prestazione lavorativa[156].

L'orientamento della Suprema Corte in tema di controlli difensivi non è tuttavia sempre stato univoco, come dimostrano le argomentazioni addotte dai giudici e ripercorse in alcune sentenze.

Sentenza capofila in materia di controlli difensivi è stata la pronuncia della Suprema Corte del 3 aprile 2002, n. 4746, nella quale i giudici hanno sostenuto che se la norma statutaria

[156] Secondo l'orientamento che negli ultimi anni si era andato consolidando, ove l'installazione degli strumenti di controllo non fosse finalizzata alla verifica del regolare adempimento della prestazione lavorativa da parte del dipendente ma fosse imposta dalla necessità di tutelare il patrimonio aziendale contro gli atti illeciti di quest'ultimo o di terzi, allora si era al di fuori dell'ambito applicativo dell'art. 4 Stat. lav. ritenuto del tutto inapplicabile. Ancora recentemente la Suprema Corte, Sez. lav., nella sentenza 27 maggio 2015, n. 10955, ha ribadito che "ove il controllo sia diretto non già a verificare l'esatto adempimento delle obbligazioni direttamente scaturenti dal rapporto di lavoro, ma a tutelare beni del patrimonio aziendale ovvero ad impedire la perpetrazione di comportamenti illeciti, si è fuori dallo schema normativo della L. n. 300 del 1970, art. 4".

vieta il controllo a distanza dell'attività lavorativa, ciò non esclude che il datore di lavoro possa effettuare controlli difensivi finalizzati alla tutela del patrimonio aziendale e, in particolare, alla repressione degli eventuali illeciti commessi dai lavoratori, oltre che dai terzi. In questo caso, ad essere oggetto di controllo era esclusivamente l'accertamento di condotte illecite, lesive di beni estranei alla prestazione lavorativa, non il corretto adempimento della prestazione lavorativa, per cui non sarebbe stato necessario attivare la procedura di controllo sindacale (o eventualmente amministrativo), prevista dall'art. 4, comma 2[157].

La giurisprudenza successiva della Cassazione ha corretto il tiro e rispetto all'impostazione iniziale, che riteneva legittimi i controlli difensivi a prescindere dal loro grado di invasività, ha chiarito che anche la possibilità di tali controlli si ferma dinanzi al diritto alla riservatezza del dipendente, in quanto *neanche l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore* (Cass. 17 luglio 2007, n. 15892)[158].

Emergono già da qui due orientamenti della Corte: l'uno volto a consentire il ricorso a controlli per finalità difensive, al di fuori delle garanzie statutarie, al fine di prevenire reati o accertare condotte illecite estranee all'esatto adempimento della prestazione lavorativa, l'altro, ritenendo di non poter sacrificare la garanzia della dignità e della riservatezza del prestatore di lavoro, propenso a ricondurre nell'ambito della disciplina dell'art. 4 Stat. lav.

---

[157] La Suprema Corte sosteneva che *devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate.* (Cass. civ. 4746/2002).

[158] Nel 2007 la Suprema Corte ha riconosciuto che *anche l'esigenza di evitare condotte illecite dei dipendenti non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino, come nel caso l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso, ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro*. Il caso verteva su un licenziamento in tronco basato sulle risultanze incrociate dei dati raccolti attraverso un badge, utilizzato per l'accesso ad un garage aziendale, che attraverso un meccanismo elettronico registrava anche l'identità di chi passava, l'orario del passaggio e consentiva così di controllare la presenza dei dipendenti. Il meccanismo elettronico era stato installato senza previa autorizzazione/accordo. In questo caso la Corte ha stabilito una differenza tra i dati registrati senza autorizzazione e quelli raccolti sulla base di una regolare procedura autorizzativa: i dati sono utilizzabili anche ai fini disciplinari, a condizione che l'installazione degli strumenti fosse stata autorizzata. Dunque, la possibilità di utilizzare le informazioni risultanti da tale strumento era condizionata alla previa autorizzazione, sindacale o amministrativa, dello stesso, affinché i dipendenti ne potessero avere piena conoscenza ed eventualmente essere stabilite in maniera trasparente misure di tutela della loro dignità e riservatezza. In mancanza di accordo/autorizzazione la prova acquisita a distanza relativa ad un inadempimento contrattuale non era utilizzabile al fine di sanzionare disciplinarmente il lavoratore. (Cass. 27 maggio 2015, n. 10955; Cass. 23 febbraio 2012, n. 2722; Cass. 23 febbraio 2010 n. 4375).

anche i controlli diretti ad accertare illeciti commessi dai lavoratori, concludeva nel senso che in mancanza di accordo/autorizzazione la prova acquisita a distanza relativa ad un inadempimento contrattuale non era utilizzabile al fine di sanzionare disciplinarmente il lavoratore[159].

Seguendo il primo orientamento, la giurisprudenza sia di legittimità che di merito aveva aperto il varco ad un'ampia "zona franca" di inapplicabilità dell'art. 4, ravvisabile ogni qual volta il controllo a distanza avesse come obiettivo la tutela del patrimonio aziendale nei confronti di comportamenti illeciti, pur consentendo, più o meno al di là delle intenzioni del datore, anche il controllo sull'attività lavorativa dei dipendenti. La Suprema Corte ha precisato che solo i controlli diretti ad accertare comportamenti estranei al rapporto di lavoro, illeciti o lesivi del patrimonio aziendale, inclusivo anche dell'immagine esterna dell'azienda, e non volti ad accertare l'inadempimento delle ordinarie obbligazioni contrattuali, restavano esclusi dall'ambito di applicazione dell'art. 4 St. Lav. e i dati raccolti dovevano ritenersi in ogni caso utilizzabili ai fini disciplinari in ragione della finalità di tutela del patrimonio aziendale (Cass. sez. lav. 23 febbraio 2012, n. 2722)[160].

---

[159] Vedi nel primo senso Cass. 4746/2002, 2722/2012, 10955/2015, 20440/2015, 10636/2017 e in linea con il secondo orientamento Cass. 15892/2007, 16622/2012, 9904/2016.

[160] Nel caso di specie, la Banca aveva licenziato per giusta causa un proprio dipendente accusato di aver divulgato a mezzo di messaggi di posta elettronica indirizzati ad estranei, notizie riservate concernenti un cliente della banca e di aver posto in essere, grazie alle notizie in questione, operazioni finanziarie da cui aveva tratto vantaggio personale. La Banca aveva acquisito in un secondo momento il testo dei messaggi di posta elettronica scambiati dal dipendente con soggetti esterni, nel momento in cui erano emersi elementi di fatto tali da raccomandare l'avvio di un'indagine "retrospettiva". La Corte di Cassazione ha precisato che il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il c.d. controllo difensivo, in altre parole, non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'Istituto bancario presso i terzi. In questo caso entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale" (Cass. sez. lav. 23 febbraio 2012, n. 2722). Il controllo è stato ritenuto legittimo ed estraneo al campo di applicazione dell'art. 4 dello statuto dei lavoratori in quanto il comportamento del lavoratore poneva in pericolo l'immagine dell'Istituto bancario presso il pubblico e sussistevano motivi di sospetto nei suoi confronti. Il c.d. controllo difensivo non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'Istituto bancario presso i terzi. In questo caso entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale.

V. in questo senso anche Cass. civ. 22662/2016 che ha escluso la sussunzione nell'ambito dell'art. 4 del controllo difensivo non attinente all'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma destinato ad accertare un comportamento che ponga in pericolo la sicurezza dei lavoratori, oltre al patrimonio aziendale; Cass. civ. 10 novembre 2017, n. 26682 e Cass. civ. 2 maggio 2017, n. 10636 dove si riconosce *una tendenziale ammissibilità dei controlli difensivi "occulti", anche ad opera di personale estraneo*

Si può ricondurre al primo orientamento, anche la sentenza Cass. sez. lav. 27 maggio 2015, n. 10955 che ha legittimato un controllo occulto attraverso la creazione di un falso profilo femminile su un social network per indurre il lavoratore, già sospettato, ad una conversazione virtuale in orario e in luogo di lavoro ed accertarne il comportamento illecito. La pronuncia ha adottato in motivazione una nozione ampia di controllo difensivo, sottratto alle garanzie di cui all'art. 4: i giudici ritengono che la verifica "non ha avuto ad oggetto l'attività lavorativa più propriamente detta ed il suo esatto adempimento", ma, piuttosto, la verifica di eventuali comportamenti illeciti da parte del dipendente, pure successivamente riscontrati, "idonei a ledere il patrimonio aziendale, sotto il profilo del regolare funzionamento della sicurezza degli impianti". Ad avviso del Collegio, la fattispecie si pone al di fuori del campo di applicazione dell'art. 4 dello Statuto[161].

In altra sentenza sempre espressione del primo orientamento, la Corte, pur esprimendosi nel senso della tendenziale ammissibilità dei controlli difensivi occulti anche ad opera di personale estraneo all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sottolinea però che le attività di accertamento debbono svolgersi con modalità non

all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo, ferma comunque restando la necessaria esplicazione delle attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali l'interesse del datore di lavoro al controllo ed alla difesa della organizzazione produttiva aziendale deve contemperarsi, e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale (vedi in tali sensi, Cass. n. 10955 del 2015). Inoltre si legge *non corrisponderebbe ad alcun criterio logico-sistematico garantire al lavoratore, in presenza di condotte illecite sanzionabili penalmente o con sanzione espulsiva, una tutela alla sua "persona" maggiore di quella riconosciuta ai terzi estranei all'impresa*. V. da ultimo la recente Cass. civ. ord. n. 13266/2018 in base alla quale le garanzie procedimentali previste dall'art. 4 non si applicano quando i comportamenti illeciti dei lavoratori non riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma piuttosto la tutela di beni estranei al rapporto stesso.

[161] In senso critico rispetto alle argomentazioni dei giudici si veda F. Olivelli: *In realtà, è indubbio che quel controllo è stato, o perlomeno si è rilevato essere un'attività che, attraverso "altre apparecchiature", ha anche monitorato a distanza l'attività del lavoratore, addirittura in tempo reale, proprio per verificare l'esatto adempimento della prestazione lavorativa (verificare se il dipendente chattasse durante l'orario di lavoro nello svolgimento delle sue mansioni). In fondo il datore di lavoro ha utilizzato un'apparecchiatura, Facebook, per controllare a distanza sul luogo di lavoro e durante l'orario di impiego proprio l'attività del lavoratore, fattispecie questa esplicitamente vietata dall'originaria versione del primo comma dell'art. 4 Stat. Lav*. Interessante annotare che sul caso ci si è interrogati se chattare con il proprio dipendente via social network non configuri, in ultimo, una forma di acquisizione illegittima dei suoi dati personali e se predisporre uno stratagemma per verificare l'esatto adempimento della prestazione sia, o meno, un uso "lecito e secondo correttezza" di quel dato. Inoltre, si dovrebbe pure valutare se un comportamento come quello del datore non integri la fattispecie di cui all'art. 8 Stat. Lav. e violi il divieto di effettuare indagini, anche a mezzo di terzi, "su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore" (F. Olivelli, *Lo "stratagemma" di Facebook come controllo difensivo occulto: provocazione o tutela del patrimonio aziendale*, in ADL 6/2015, 1313, 1315-1316).

eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, e nel rispetto dei canoni generali della correttezza e buona fede contrattuale[162].

In linea con il secondo orientamento della Cassazione che tende a ricondurre nell'alveo dell'art. 4 anche i controlli difensivi, si è posta Cass. 23 febbraio 2010, n. 4375 che ha ritenuto inutilizzabili, per difetto di accordo/autorizzazione, le informazioni relative a inadempimenti del lavoratore, consistiti in ingiustificati accessi ad internet durante l'orario di lavoro, registrati da un apposito programma informatico, denominato "Super Scout". Pur affermando l'insopprimibile esigenza di evitare condotte illecite, la Suprema Corte ha negato l'utilizzabilità a fini disciplinari dei dati acquisiti mediante programmi informatici atti a monitorare la posta elettronica e gli accessi internet dei dipendenti, sul presupposto che quei programmi consentissero al datore di lavoro un controllo a distanza continuativo sul corretto adempimento della prestazione di lavoro, e perciò fossero necessarie per la loro installazione le garanzie procedurali previste dall'art. 4 St. lav.[163].

In continuità con la sentenza 4375/2010, si pone Cass. Sez. Lav. 1 ottobre 2012, n. 16622: la Cassazione afferma esplicitamente che dal divieto di controlli a distanza ex art. 4 consegue che i controlli difensivi (posti in essere nel caso in esame con il sistema informatico Bluès 2002) ricadono nell'ambito dell'art. 4, comma 2, e, fermo il rispetto delle garanzie procedurali previste, non possono investire la sfera della prestazione lavorativa dei singoli lavoratori. Questa sentenza è rilevante perché è uno dei pochi casi in cui ai fini della valutazione di legittimità sono analizzate le modalità con le quali il controllo è posto in essere. La Corte menziona accorgimenti preventivi, consistenti in sistemi di filtraggio delle telefonate, per non consentire di risalire all'identità del lavoratore, avvertendo che in caso contrario i relativi dati non potranno essere utilizzati per provare l'inadempimento contrattuale del lavoratore[164].

---

[162] Cass. sez. lav. 2 maggio 2017, n. 10636.

[163] *I programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento* (Cass. sez. lav. 23 febbraio 2010, n. 4375).

[164] La Sezione lavoro, invero, intervenendo in ultima istanza sulla vicenda del controllo sugli accessi ad Internet realizzato attraverso apposito programma informatico (nel caso di specie denominato "Blue's 2002", del tutto analogo ad altri programmi quali "Super Scout" o "Squid"), ritiene che i programmi che consentono il monitoraggio della posta elettronica e degli accessi ad Internet sono strumenti di controllo allorquando consentono al datore di lavoro di controllare a distanza e in via continuativa l'attività lavorativa. In tal caso, la loro installazione è soggetta alla disciplina di cui all'art. 4 l. n. 300 del 1970, la cui violazione rende inutilizzabili i dati acquisiti per eventuali sanzioni disciplinari. (Cass. Sez. Lav, n. 16622 del 2012). Si colloca nell'ambito del secondo orientamento anche Cass. Sez. lav., 8 novembre 2016, n. 22662 dove si afferma: *la tutela del diritto alla riservatezza non consente di escludere che rientrino nella fattispecie di cui al citato art. 4 i controlli diretti ad accertare comportamenti illeciti dei lavoratori nel caso in cui la sorveglianza riguardi*

Anche il Tribunale di Roma, in una recente ordinanza del 13 giugno 2018 pone l'accento su "come si fa il controllo": secondo questo giudice dal momento che non è più presente il divieto in termini assoluti di effettuare controlli a distanza sui lavoratori, non è più necessario appellarsi a finalità difensive per superare un divieto di controllo a distanza che non esiste più, ma è fondamentale osservare i limiti chiari e rigorosi che il legislatore del 2015 ha posto alle modalità del controllo[165].

Rispetto all'iniziale impostazione che riteneva in ogni caso legittimi i controlli difensivi, a prescindere dal loro grado di invasività (Cass. n. 4746 3 aprile 2002), la posizione dei giudici sul punto sembra tenere in maggior conto il rispetto della libertà e dignità dei lavoratori, e nelle modalità del controllo il rispetto dei principi di correttezza, pertinenza e non eccedenza.

Da notare infine che sulla ammissibilità dei controlli difensivi si è riscontrata la maggiore distanza fra Sezione penale e Sezione lavoro della Cassazione: i giudici penali hanno da tempo sostenuto la legittimità dei controlli difensivi quando questi ultimi siano finalizzati a prevenire o accertare il compimento di atti illeciti poiché la riservatezza del dipendente è

---

l'espletamento dell'attività lavorativa e venga attuata mediante strumenti potenzialmente lesivi della sfera personale, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro nel caso in cui dai controlli difensivi derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.

[165] Si legge nell'ordinanza: *Il legislatore, con il nuovo testo dell'art. 4 della l. n. 300 del 1970, sembra ormai aver superato la discutibile ed estremistica logica per cui il lavoratore non possa essere controllato a distanza salvo che non si dimostri che ci si è dovuti difendere perché è un delinquente, affermando l'opposto principio, che realizza normativamente il contemperamento tra interesse al controllo e protezione della dignità e riservatezza dei lavoratori, per cui il lavoratore può ben essere controllato con mezzi a distanza, ma alle seguenti condizioni cumulative: a) l'impianto deve essere stato previamente autorizzato con accordo sindacale o dall'INL; b) l'impianto deve avere una o più delle finalità (diverse da quelle di controllare i lavoratori) previste dal primo comma dell'art. 4; c) il datore deve aver previamente informato il lavoratore che l'impianto è stato installato e che vi si potranno esperire controlli; d) il controllo deve essere esperito in conformità al Codice della Privacy, il che comporta essenzialmente che esso va fatto secondo i princìpi di trasparenza, scopo legittimo e determinato, non invasività, ricavabili dall'art. 11 del D.lgs. 196/2003 e s.m.. Le regole sub a) e b), che dettano, rimodulandolo, il regime procedurale autorizzatorio, non valgono per gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", quali, evidentemente, il software PRS e la email aziendale. Le regole sub c) e d) valgono invece sempre, alla sola condizione che si tratti di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori".*

Vedi in senso contrario A. Sitzia, che, a conferma della persistente legittimità dei controlli difensivi occulti anche dopo la riforma dell'art. 4 l. n. 300 del 1970, cita una ordinanza del Tribunale di La Spezia. Il Tribunale afferma che "l'interpretazione della norma non può spingersi sino al punto di ritenere l'applicabilità della stessa e, dunque, la necessità dell'informativa, anche nel caso in cui il controllo sia finalizzato all'accertamento di illeciti completamente avulsi dalla prestazione lavorativa. Milita in questo senso la stessa formulazione letterale della nuova disposizione: l'art. 4 novellato, infatti, richiama le esigenze organizzative e produttive, la sicurezza del lavoro e la tutela del patrimonio come esclusive finalità in funzione delle quali possono essere installati strumenti che consentano il controllo a distanza dell'attività dei lavoratori. Pertanto, l'informativa che va data è relativa alla possibilità che sia controllata l'attività lavorativa, per ragioni, tra le altre, di tutela del patrimonio aziendale. Non si ritiene invece necessario dover informare il lavoratore che lo strumento dal quale derivi la possibilità di controllo, se verrà utilizzato al di fuori dell'orario di lavoro o comunque per finalità estranee allo svolgimento della prestazione, potrà essere utilizzato per contestare illeciti che, per l'appunto, non hanno alcuna connessione, neppure indiretta, con l'attività lavorativa" (cfr. Trib. La Spezia 25 novembre 2016, est. Romano, in A. Sitzia, *Videosorveglianza occulta, privacy e diritto di proprietà: la Corte EDU torna sul criterio di bilanciamento, nota a Corte EDU, Sez. III, 9 gennaio 2018*, in ADL n. 2/2018, 520).

destinata a recedere di fronte ad esigenze di ordine pubblico, di prevenzione o repressione di reati. Secondo un consolidato orientamento della giurisprudenza penale, il controllo difensivo, volto a proteggere il patrimonio aziendale da azioni delittuose da chiunque commesse, resta estraneo alla disciplina statutaria, con possibilità di utilizzo delle prove nel processo penale[166]. Così la V sez. pen., Cass. sentenza 13 settembre 2017, n. 46428, allineandosi al proprio consolidato orientamento, ha confermato che *le garanzie procedurali previste dall'art. 4 St. lav. non trovano applicazione quando si procede all'accertamento di fatti che costituiscono reato*. *Tali garanzie, infatti, riguardano solo l'utilizzabilità delle risultanze delle apparecchiature di controllo nei rapporti interni, di diritto privato, fra datore di lavoro e lavoratore; la loro eventuale inosservanza non assume pertanto alcun rilievo nell'attività di repressione di fatti costituenti reato, al cui accertamento corrisponde sempre l'interesse pubblico alla tutela del bene penalmente protetto, anche qualora sia possibile identificare la persona offesa nel datore di lavoro.*
Sul tema il dibattito non pare essere ancora essersi sopito.

3.3 I controlli difensivi: una categoria ancora dibattuta

La previsione di controlli effettuati al di fuori delle procedure statutarie, per finalità difensive, ha sollevato in dottrina serie perplessità per il circolo vizioso nel quale sembrava scivolare il ragionamento. Si obiettava in primo luogo che per quanto il controllo fosse finalizzato ad accertare condotte illecite dei lavoratori, era potenzialmente idoneo anche a rilevare informazioni relative all'attività svolta dal lavoratore, perché ad essere oggetto di controllo era il comportamento del lavoratore in occasione dell'esecuzione della prestazione. Il controllo su condotte potenzialmente illecite inevitabilmente comporterebbe anche il controllo sull'adempimento della prestazione lavorativa, finendo per violare il divieto che il legislatore aveva stabilito.
La legittimità del controllo difensivo presupponeva la netta separazione tra condotte illecite e attività lavorativa, non tenendo conto, secondo alcuni Autori, che separare l'attività lavorativa dal comportamento illecito tenuto in occasione di quella non è sempre agevole, così che spesso l'accertamento della condotta illecita comporta necessariamente l'osservazione del comportamento complessivo del dipendente e perciò assoggetta a controllo anche l'esecuzione della prestazione lavorativa[167]. Ancor di più questo è vero

[166] Cass. pen., sez. II, n. 8687/1985 e Cass. pen., 15/12/2006 n. 8042, Cass. pen.,14/12/2009, n. 47429.
[167] Fortemente critico A. Bellavista: la Cassazione pensa di separare con l'accetta due aree: da un lato, l'attività lavorativa, che rientrerebbe nel campo di applicazione della disposizione, dall'altro, le condotte illecite del

laddove sono utilizzati strumenti e dispositivi in grado di registrare informazioni qualitativamente e quantitativamente tali da permettere la ricostruzione dell'intero comportamento del lavoratore, senza alcuna possibilità di circoscrivere la memorizzazione dei dati all'ambito dell'illecito. Il controllo difensivo di fatto renderebbe possibile, seppure indirettamente, un monitoraggio continuo dell'attività lavorativa, mentre anche la sola potenzialità del controllo avrebbe richiesto l'osservanza delle garanzie statutarie. Inoltre, il comportamento illecito (civile e/o penale) costituisce spesso anche inadempimento dell'obbligazione di lavoro, rilevante ai sensi degli artt. 2104 e 2105 cod. civ.

Alla ricostruzione dei controlli difensivi si obiettava anche che la legittimità del controllo si poteva stabilire solo *ex post*, qualora si fosse dimostrata esistere effettivamente una condotta fraudolenta del dipendente, senza poter giustificare *ex ante* un'area di esenzione rispetto all'applicazione dello Statuto. La legittimità dell'esercizio del potere di controllo risulterebbe subordinata all'accertamento giudiziale della fondatezza dei sospetti datoriali nei confronti del lavoratore per la commissione di un fatto illecito valutabile solo *ex post*, in contrasto con lo spirito della disposizione statutaria che al contrario avrebbe richiesto una verifica *ex ante*. La conseguenza ultima è che se dopo il controllo occulto non risulteranno commessi inadempimenti/illeciti, i controlli rimarranno presumibilmente sconosciuti, se, invece, emergeranno degli illeciti, le prove di essi potranno essere utilizzate contro il lavoratore e giustificheranno, a posteriori, il controllo occulto.

Da ultimo, essendo il controllo a distanza difensivo svolto all'insaputa del lavoratore, che evidentemente non è informato della possibilità di essere controllato, della frequenza e del grado d'intrusività che il monitoraggio può assumere, si prospetterebbe un contrasto sul piano sistematico con la normativa sul trattamento dei dati personali, e l'obbligo d'informare l'interessato delle modalità e finalità di acquisizione dei suoi dati personali: norma già applicabile al potere di controllo a distanza in virtù del sistema di "innesti regolativi" tra D. lgs. 196/2003 e Statuto dei lavoratori che presupponeva che il datore di lavoro dovesse assicurare il rispetto di entrambe le normative.

---

medesimo lavoratore, le quali invece sarebbero al di fuori del suddetto campo di applicazione e sulle quali pertanto il controllo tecnologico potrebbe svolgersi senza alcun limite. Ma nella realtà effettuale le cose non stanno proprio così. Ciò perché i controlli diretti ad accertare condotte illecite del lavoratore molto spesso sono anche controlli sull'attività lavorativa. (A. Bellavista, *La Cassazione e i controlli a distanza sui lavoratori*, in *Riv. giur. lav*., 2010, II, 465). V. anche G. A. Recchia, *Controlli datoriali difensivi: note su una categoria in via di estinzi*one, in Il lavoro nella giurisprudenza, 4/2017, 346.

V. anche P. Lambertucci a parere del quale l'accertamento della condotta "illecita" del dipendente spesso può essere rilevata solo controllando l'esecuzione della prestazione lavorativa.

Per queste ragioni la categoria dei controlli difensivi sarebbe affetta *da un'aporia logica di non poco momento*[168]. Il sospetto dell'esistenza di un comportamento illecito verificabile a posteriori non può legittimare preventivamente un controllo vietato dallo Statuto o la disapplicazione di limiti e condizioni poste all'esercizio del potere datoriale, a rischio di trasformare paradossalmente proprio l'art. 4 nello strumento per cancellare limiti posti all'esercizio di quel potere e per giustificare una condotta illecita del datore sulla base del timore di una condotta illecita del lavoratore[169].

L'interpretazione proposta da Arturo Maresca prevede la distinzione fra il controllo "realmente" difensivo, posto in essere, ad esempio, quando il sistema informatico o una sua applicazione vengano predisposti per accertare esclusivamente condotte illecite del singolo dipendente e non l'attività lavorativa nel suo complesso, e quello illegittimamente effettuato al di fuori delle garanzie previste dall'art. 4 St. lav. Il controllo tecnologico che registra tutti i dati relativi all'attività lavorativa svolta indistintamente dalla generalità dei dipendenti, senza alcuna selettività né soggettiva né oggettiva, focalizzato non sull'attività illecita ma sulla prestazione lavorativa complessivamente resa da tutto il personale dipendente, non può configurare un controllo difensivo. Allo stesso modo non si potrà legittimare, con effetto retroattivo, il controllo già effettuato, qualificandolo a posteriori come difensivo, quando una condotta illecita emerga dall'analisi dei dati relativi all'ordinaria attività lavorativa svolta dalla generalità del personale dipendente. A tale controllo si dovrà sicuramente applicare l'art. 4 e la sua violazione rende illegittimo il controllo effettuato[170].

---

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

[169] *Il controllo volto a palesare eventuali condotte illecite ha a oggetto proprio "l'attività dei lavoratori" che l'art. 4 St. Lav. espressamente considera, in tale ampia eccezione, per ricomprendere nel suo campo di applicazione i controlli volti, pur involontariamente, su di essa. Pertanto il controllo a distanza sui dipendenti, se specificamente diretto a verificare la loro attività, resta vietato anche se volto a palesare un illecito e l'impiego di un dispositivo avente tal fine, determinando l'effetto che la norma statutaria considera e per il quale appresta le sue garanzie, va sottoposto al vincolo procedimentale ivi previsto.* […] *Il sospetto di un comportamento illecito non è assolutamente idoneo a legittimare un controllo che lo Statuto vieta.* […] *Se fosse possibile disapplicare limiti e condizioni imposti all'esercizio del potere datoriale a fronte del mero sospetto di un comportamento illecito del lavoratore (per quanto fondato e plausibile), questo diventerebbe l'arma per la cancellazione di quegli stessi limiti. Con il paradosso che proprio nella disciplina dell'art. 4 il (solo) timore di una condotta penalmente illecita (del lavoratore) finirebbe per giustificare una condotta penalmente illecita del datore! […] Se la legittimità dell'esercizio del potere di controllo viene ancorata a un fatto (l'illecito o l'inadempimento) che è accertabile solo ex post, non vi è alcuna possibilità di stabilire se esso sia o meno legittimo prima del suo esercizio in concreto.* Nuzzo, prosegue citando a sostegno della propria tesi sia Cass. civ. 15892 17 luglio 2007, n. 4375, 23 febbraio 2010 e n. 2722, 23 febbraio 2012, che la Corte EDU ricorso n. 1874/13 del 9 gennaio 2018 sul caso Lòpez. *Il controllo effettuato con continuità, generalizzato a tutta l'attività svolta in azienda e senza aver informato i lavoratori, quand'anche per fini difensivi, è una forma di ingerenza illecita nella loro vita privata.* (V. Nuzzo, *op. cit.*, 52-53).

[170] A. Maresca, *op. cit.*, 512.

Le esigenze di tutela del patrimonio aziendale sono state recepite dal legislatore del 2015 che nella novella dell'art. 4 St. lav. ha introdotto tra le esigenze aziendali che legittimano l'impiego di strumenti dai quali possa derivare il controllo a distanza, la tutela del patrimonio aziendale, in aggiunta alle finalità organizzative e produttive e di sicurezza del lavoro.

Dopo l'intervento riformatore sull'art. 4 St. lav., con il quale il legislatore ha davvero rimescolato le carte (Cosattini), si contrappongono due orientamenti dottrinali. Il primo legge il riconoscimento di questa ulteriore finalità come un recepimento normativo della categoria dei controlli difensivi, ricondotti così nell'ambito dell'art. 4 St. lav. Il legislatore avrebbe "normativizzato" nella nuova disposizione la categoria del controllo difensivo, volto ad accertare comportamenti illeciti dei lavoratori, estranei al rapporto di lavoro ma idonei a pregiudicare beni aziendali, materiali o immateriali, e, in questo modo, l'avrebbe superata. La conseguenza è che l'attivazione di controlli difensivi potrebbe oggi avvenire soltanto previo accordo sindacale o autorizzazione amministrativa.

Il secondo orientamento dottrinale individua uno spazio di autonoma sopravvivenza per i controlli difensivi: al di fuori delle previsioni e delle garanzie dell'art. 4 St. lav. permane un ambito di applicazione per quei controlli diretti all'accertamento di illeciti estranei al rapporto di lavoro, in un'accezione selettivamente rigorosa dell'illecito che escluda il controllo sulla prestazione lavorativa[171].

Molti autori si esprimono nel senso del superamento della categoria dei controlli difensivi dopo la novella del 2015. Secondo Riccardo Del Punta la norma con l'aggiunta delle esigenze di "tutela del patrimonio aziendale" dimostra di voler superare il concetto di controllo difensivo che trovava nella protezione del patrimonio aziendale una delle sue basi di appoggio[172].

È esplicita Elena Gramano, secondo la quale il legislatore ha inteso, togliere ogni spazio ai controlli che, in quanto difensivi, potessero in qualche modo essere posti in essere eludendo

---

[171] Dalla giurisprudenza della Corte di Strasburgo si può trarre ulteriore argomento per confermare la persistente legittimità dei controlli difensivi occulti, anche alla luce del nuovo sistema normativo, purché superino il "test" di bilanciamento. Non si può omettere di considerare, infatti, che un'interpretazione dell'art. 4 l. n. 300 del 1970 che neghi un qualsiasi spazio per una effettiva tutela del diritto di proprietà (oltre che del diritto all'esercizio libero dell'iniziativa economica privata tutelata dall'art. 41 Cost. e dall'art. 16 della Carta dei diritti fondamentali dell'Unione Europea), si porrebbe in chiaro contrasto con una lettura costituzionalmente e convenzionalmente orientata del sistema.

Ne risulterebbe un modello ingiustificatamente sbilanciato verso una tutela sproporzionata della privacy a fronte di una compressione degli interessi contrapposti che non trova alcun fondamento nel sistema delle fonti nazionali e sovranazionali. Avremmo, inoltre, un effetto di sbilanciamento anche in relazione al contemperamento del diritto alla riservatezza del lavoratore rispetto al diritto alla difesa del datore di lavoro, garantito dall'art. 24 Cost. Cosi A. Sitzia, *Videosorveglianza occulta, privacy e diritto di proprietà: la Corte EDU torna sul criterio di bilanciamento*, in ADL, n.2/2018, 520-521.

[172] R. Del Punta, *op. cit.*, 77.

i limiti legali, internalizzando proprio nel comma 1 la stessa finalità che, secondo i precedenti orientamenti giurisprudenziali, giustificava la mancata applicazione dell'art.4[173].

Anche Maurizio Ricci si esprime nel senso del superamento della categoria dei controlli difensivi volti ad accertare comportamenti illeciti dei lavoratori idonei a pregiudicare beni estranei al rapporto di lavoro: con l'introduzione di questa nuova causa giustificatrice, il legislatore sembra cristallizzare nella nuova disposizione la soluzione elaborata in giurisprudenza e superare la ragion d'essere dei controlli difensivi[174]. Con il nuovo art. 4 Stat. lav. anche i controlli difensivi saranno sottoposti al regime autorizzatorio e l'utilizzo dei dati registrati dovrà avvenire nel rispetto delle regole dettate dal Codice della privacy.

Si è anche sostenuto in dottrina che con l'inclusione delle esigenze di tutela del patrimonio aziendale tra le finalità considerate dal primo comma dell'art. 4, sarebbe ammissibile anche il controllo sulla prestazione in quanto il puntuale adempimento dell'obbligazione lavorativa concorre alla valorizzazione del patrimonio aziendale, dovendosi intendere il patrimonio dell'azienda come comprensivo anche del corretto adempimento della prestazione[175]. Interpretazione questa accolta anche da Maria Teresa Carinci che fa discendere dall'esplicita inclusione anche dei controlli difensivi nell'ambito dei controlli indiretti legittimamente esperibili dal datore di lavoro previa autorizzazione, il superamento del divieto assoluto al potere datoriale di controllare in via indiretta la prestazione di lavoro. Non sussisterebbe più un limite esterno al potere organizzativo e di controllo del datore sulla prestazione di lavoro tramite strumenti organizzativi e di lavoro*:* tanto più che, rileva Carinci, la medesima

---

[173] E. Gramano, *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi*, in *Diritto delle Relazioni Industriali*, 1/2018, 265.

[174] M. Ricci, *I controlli a distanza dei lavoratori tra istanze di revisione e flessibilità "nel" lavoro*, in *ADL* 4-5/2016, 748. E si veda anche Cosattini: *Con la modifica normativa recentemente introdotta, il Legislatore ha espressamente ricondotto i controlli finalizzati alla tutela del patrimonio aziendale fra quelli disciplinati dall'art. 4: in particolare ha stabilito che anche l'impiego degli strumenti di controllo per finalità di tutela del patrimonio aziendale richiede e presuppone il previo esperimento della procedura autorizzativa disciplinata dal comma 2, con ciò ineludibilmente escludendo che la finalità di tutela del patrimonio aziendale consenta, di per sé, di dar corso all'instaurazione delle apparecchiature necessarie ed all'esecuzione dei controlli senza il rispetto della procedura autorizzativa prevista dal (nuovo) comma 1 dell'art. 4.* (L. A. Cosattini, *Le modifiche all'art. 4 Stat. lav. sui controlli a distanza, tanto rumore; per nulla?* In *Il lavoro nella giurisprudenza*, n. 11/2015, 988). Alla medesima conclusione giunge Ilario Alvino che con l'espresso riferimento alla tutela del patrimonio aziendale considera superata l'artificiosa categoria dei controlli difensivi. (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*, in *Labour Law Issues* n. 1/2016, 18).

[175] M. Marazza, *op. cit.*, 16. Per una nozione dinamica di patrimonio aziendale comprensiva delle proprietà immateriali, quali l'efficienza aziendale e la produttività dell'impresa vedi M. Lanotte, *La ridefinizione dei limiti al potere di controllo a distanza*, in A. Levi (a cura di), *op. cit*., 41. In senso contrario vedi V. Nuzzo, *op. cit.*, 49.

condotta del dipendente, in una molteplicità se non nella totalità dei casi, infatti, riveste al contempo rilievo di illecito extracontrattuale e di inadempimento contrattuale[176].

Alla luce del nuovo testo dell'art. 4 St. Lav. possono dunque ancora dirsi possibili controlli di carattere difensivo oppure la norma li ha definitivamente assorbiti, riconducendoli nell'ambito dell'art. 4?

A parere di Arturo Maresca se ne può sostenere la sopravvivenza solo delimitando una sottocategoria di controlli difensivi in senso stretto, ossia di controlli mirati a contrastare un illecito extracontrattuale o penale o, comunque, un comportamento non riconducibile, direttamente o indirettamente, all'inadempimento delle obbligazioni tipiche discendenti dal contratto di lavoro. La distinzione da operare è dunque fra controlli a difesa del patrimonio aziendale, in senso materiale ed immateriale, che riguardino la generalità dei dipendenti nello svolgimento della loro normale attività lavorativa e controlli difensivi in senso stretto, mirati ad accertare selettivamente condotte illecite, anche di aggressione al patrimonio aziendale, di cui si presume, in base ad indizi concreti, siano autori specifici dipendenti, anche se ciò avviene in occasione dello svolgimento della prestazione lavorativa. I primi dovranno avvenire nel rispetto delle previsioni del comma 1 dell'art. 4 (e poi del comma 3), mentre i secondi si collocano al di fuori dell'ambito applicativo dell'art. 4, non avendo ad oggetto l'attività del lavoratore ma un comportamento del lavoratore, posto in essere in occasione dello svolgimento del rapporto, che ha un'autonoma rilevanza penale. In questo caso il controllo difensivo sopravvivrebbe alla novella perché ha ad oggetto una condotta antigiuridica e non l'attività del lavoratore[177].

Per la validità di questa tesi è necessario che il controllo difensivo si configuri come un controllo tecnico molto puntuale e mirato, non continuo, anelastico o diretto ad un target indefinito, riducendo al minimo la compressione della libertà e dignità del lavoratore.

Analogamente Marco Marazza fonda l'esistenza di una più circoscritta tipologia di controlli a distanza difensivi sul fatto che il controllo riguardi comportamenti penalmente rilevanti, (più che l'esigenza di tutela del patrimonio) con una rilevanza antigiuridica autonoma e indipendente rispetto all'obbligazione di lavoro, lesivi di un bene del datore, diverso dal mero diritto di credito alla prestazione lavorativa e il controllo sia poi selettivamente dedicato all'accertamento dell'illecito. Pur potendo quel comportamento rappresentare contemporaneamente, anche un inesatto adempimento dell'obbligazione di lavoro, i

[176] M. T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro,* in P. Tullini, (a cura di), *op. cit.*, 54.
[177] A. Maresca, *op. cit.*, 512.

controlli difensivi risulterebbero giustificati dalla rilevanza penale della condotta già posta in essere dal dipendente e suscettibile di reiterazione, e dalla natura potenzialmente continuativa della condotta illecita che si intende accertare[178].

In questo dibattito a più voci non manca chi invoca a sostegno della sopravvivenza di un'autonoma categoria dei controlli difensivi, la nozione di legittima difesa nei rapporti interprivati. Valerio Maio propone una rilettura dei controlli difensivi ricollocati nell'ambito della nozione civilistica di legittima difesa a fronte di atti di aggressione altrui, fondata sul combinato disposto degli artt. 2044 c.c. e 52 cod. pen.[179]. Resterebbe estranea al campo di applicazione del novellato comma 1 dell'art. 4 la categoria degli atti di aggressione contro l'altrui diritto: la presenza di un'aggressione in atto, di concreta e attuale situazione di pericolo, produrrebbe un'esigenza defensionale non dilazionabile nel tempo e legittimerebbe, nel rispetto della proporzionalità tra l'offesa e lo strumento di difesa, il controllo difensivo. Secondo questa interpretazione sarebbe contrario al buon senso imporre le condizioni procedurali del previo accordo sindacale o del nulla osta amministrativo richieste dall'art. 4 anche ai controlli disposti per realizzare esigenze indilazionabili, ossia per impedire condotte illecite in atto o di imminente realizzazione[180].

---

[178] M. Marazza, *I controlli a distanza del lavoratore di natura "difensiva",* in P. Tullini, (a cura di) *op. cit.*, 40-41.

[179] V. Maio, *Il regime delle autorizzazioni del potere di controllo del datore di lavoro*, in P. Tullini, (a cura di) *op. cit.*, 68.

[180] *Anche il datore di lavoro potrebbe invocare legittime esigenze defensionali a sostegno della deroga agli adempimenti procedurali di cui all'art. 4 cit., dimostrando la sussistenza della necessità di difendere un diritto proprio o altrui contro il pericolo attuale di un'offesa ingiusta. Il controllo difensivo per poter essere considerato legittimo in deroga al nuovo testo dell'art. 4 St. lav. dovrebbe essere motivato dalla necessità eccezionale, non dilazionabile nel tempo e non realizzabile altrimenti, di fronteggiare "atti di aggressione contro l'altrui diritto" da parte del lavoratore, al di là dell'interesse al corretto adempimento della prestazione, che pure può concretamente coesistere con l'esigenza defensionale.*[…] *Tutto questo si potrebbe ottenere attingendo fino in fondo allo strumentario di diritto comune, ed in particolare alla nozione civilistica di legittima difesa nei rapporti interprivati, da sempre intesa come facoltà di respingere l'attacco altrui e ritenuta compatibile con la "predisposizione di uomini e strumenti, onde evitare che il pericolo preventivato dell'altrui aggressione possa realizzarsi".* […] *Dunque, appartiene anche al datore di lavoro che volesse invocare legittime esigenze defensionali a sostegno della deroga agli adempimenti procedurali di cui all'art. 4 cit., dimostrando la sussistenza della "necessità di difendere un diritto proprio o altrui contro il pericolo attuale di un'offesa ingiusta"* (V. Maio, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. Dir. Lav.*, n.6/2015, 1199 e ss.). Sul punto si veda anche Pettinelli che propone un aggiornamento della nozione di controllo difensivo, che varrebbe a legittimare sul piano disciplinare un utilizzo delle informazioni relative all'inadempimento acquisite in assenza dei requisiti previsti dall'art. 4, commi 1 – 3, quando sia comunque "occasionato dalla necessità eccezionale, non dilazionabile nel tempo e non realizzabile altrimenti, di fronteggiare comportamenti del lavoratore che sono qualificabili come illecito in quanto [...] integrano atti di aggressione contro l'altrui diritto" in virtù del principio di legittima difesa ex artt. 2044 Cod. Civ. e 52 Cod. Pen. ovvero, secondo altra prospettiva, sia "proporzionalmente orientato a scongiurare il rischio concreto di comportamenti del lavoratore di rilevanza penale posti in essere in occasione dello svolgimento della prestazione lavorativa" (R. Pettinelli, *Controlli difensivi: storia di un anacronismo,* in *Argomenti di diritto del lavoro*, 6/2018, 1591 e ss. Nota a Tribunale di Roma, ord. 13 giugno 2018).

3.4 Strumenti di lavoro o strumenti di controllo?

Uno degli aspetti "caldi" delle nuove disposizioni sui controlli tecnologici attiene alla diversa disciplina applicabile agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e a quelli di registrazione degli accessi e delle presenze, esentati dai vincoli dettati dal comma 1 del novellato art. 4 St. lav. per tutti gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.

La *ratio* del legislatore sembra essere chiara: si è inteso sottrarre a vincoli procedimentali quegli strumenti, ormai di uso comune, utilizzati per rendere la prestazione o per accedere al luogo di lavoro, liberalizzandone l'installazione da parte del datore di lavoro, in quanto valutati *ex ante* legittimi. Si tratta di strumenti che per la loro natura e funzione non possono essere assoggettati ad una causale che ne giustifichi l'utilizzo né sarebbe ipotizzabile una preventiva autorizzazione sindacale o amministrativa, senza stravolgere il potere organizzativo del datore di lavoro che si esplica anche nella scelta degli strumenti di cui il dipendente si avvale per svolgere la propria attività[181].

Si è inteso sollevare il datore di lavoro dal notevole aggravio che avrebbe comportato l'attivazione della preliminare valutazione sindacale o amministrativa, per l'assegnazione di ogni computer o telefono, di ogni singolo indirizzo di posta elettronica o di ogni badge. Secondo M.T. Carinci si è inteso anche evitare di esporlo a possibili prescrizioni limitative, contenute negli accordi sindacali o nelle autorizzazioni amministrative, rispetto alle modalità di utilizzo di quegli strumenti[182].

Il concetto di "strumenti utilizzati dal lavoratore per rendere la prestazione di lavoro" pone una serie complessa e delicata di questioni interpretative, la prima delle quali è di tipo qualificatorio: consiste nell'identificare gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa. Una volta identificati, si dovrà stabilire in che misura vadano esenti

---

Mentre si veda in senso contrario A. Ingrao: *Non si condivide, infatti, la tesi di chi considera il controllo occulto come una manifestazione della legittima difesa civilistica: l'operare della scriminante postula l'esistenza di un pericolo attuale di un'offesa ingiusta ad un bene di natura personale. Sembra quasi pleonastico rilevare che a un controllo occulto su un illecito già realizzato mancherebbe il requisito sia dell'attualità del pericolo che della natura non patrimoniale dell'interesse leso*. (A. Ingrao, *I controlli difensivi tra passato e presente: privacy del lavoratore e inutilizzabilità dei dati,* in *Nuova giurisprudenza civile commentata*, 4/2019, 656).

[181] A. Maresca, *op. cit.*, 512.

[182] *Si pensi per es. ad una autorizzazione che ammetta sì l'uso dello smartphone, ma escluda l'utilizzo del gps per localizzare la posizione del lavoratore*. M.T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. Lgs. 151/2015): spunti per un dibattito*, in *Labour Law Issues* 1/2016, 5.

dai vincoli di cui al comma 1, se l'esonero copra solamente le funzionalità strettamente necessarie allo strumento di lavoro o anche qualsiasi software o applicativo installabile sullo stesso strumento e se vadano esenti oltre che dai vincoli procedurali, anche dai vincoli finalistici, sottratti ad ogni vincolo di scopo.

La precisazione delle sole caratteristiche funzionali come elemento di distinzione induce a ritenere che tra i dispositivi del primo e quelli del secondo comma non vi sia una differenza basata sulle caratteristiche morfologiche, ma solo sulle finalità del loro impiego, tanto che gli strumenti di lavoro non possono essere oggetto di una catalogazione tassativa da parte della legge o dell'autonomia privata. Presupponendo una nozione di strumento di lavoro opportunamente elastica e non sussistendo una differenza ontologica tra gli strumenti, la riconduzione degli stessi alla disciplina generale o a quella in deroga dipende dal nesso funzionale esistente tra questi e lo svolgimento delle mansioni assegnate al lavoratore, e pertanto non sarà determinabile a priori, ma di volta in volta, in relazione alla prestazione stessa, alle specifiche mansioni o alle modalità con cui devono essere rese[183]. Come scrive Patrizia Tullini la separazione a priori fra le tecnologie di controllo e quelle di lavoro sconta un vizio di astrattezza, mentre si dovrà valutare la reale funzionalità dello strumento rispetto al lavoro svolto e verificare caso per caso che gli strumenti siano "programmati" per minimizzare i dati rispetto alla finalità perseguita[184].

La dottrina appare divisa però sul livello di essenzialità dello strumento rispetto allo svolgimento delle mansioni, sulla misura in cui lo strumento debba essere necessario rispetto all'attività lavorativa prestata.

In quanto norma eccezionale, derogatoria di limiti posti al potere di controllo, la disposizione sembra dover essere oggetto di interpretazione restrittiva, a meno di ampliare oltremisura la sfera "liberalizzata" del potere datoriale (Trojsi): lo strumento deve essere necessario e indispensabile rispetto alla prestazione da svolgere.

---

[183] La sintesi è di M. Marazza: *Egli è tenuto ad eseguire la prestazione utilizzando gli strumenti individuati e forniti dal datore e che, pertanto, non esiste - né può esistere - una nozione ontologica di strumento di lavoro. In altri termini, appare del tutto inutile ogni tentativo di catalogare in via astratta gli strumenti riconducibili ad un certo tipo di lavoro. Piuttosto, per ciascun lavoro occorrerà verificare in concreto, e quindi nella specifica organizzazione che lo ospita, ciò che il potere direttivo dell'imprenditore consente di qualificare, caso per caso, alla stregua di uno strumento di lavoro.* M. Marazza *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in WP C.S.D.L.E. "Massimo D'Antona", 10.

[184] *Il sol fatto che una piattaforma software sia utilizzata al fine di rendere la prestazione lavorativa non può indurre a concludere che essa sia strumento di lavoro: è necessario, piuttosto, verificare sia la sua reale funzionalità al lavoro (comma 2, art. 4 St. lav.) sia la minimizzazione dei dati rispetto alla finalità perseguita (art. 3 d.lgs. n. 192/2003 e art. 5 Regolamento Ue n. 2016/679).* (V. Nuzzo, *I software che registrano la durata delle telefonate nei call center sono strumenti di lavoro?,* in *Ridl* n. 2/2018, 307-308).

Per altra parte della dottrina è sufficiente che lo strumento sia indirettamente correlato all'attività lavorativa, ne ottimizzi l'esecuzione, la renda più sicura e più efficiente con benefiche ricadute sull'organizzazione del lavoro[185]. Includere anche gli strumenti che ottimizzano la prestazione non comprometterebbe le tutele del lavoratore garantite dai limiti di finalità, minimizzazione, trasparenza e proporzionalità che regolano le modalità di trattamento dei suoi dati e che si applicano indipendentemente dalla distinzione introdotta dal nuovo articolo 4 St. lav. fra strumenti di controllo e strumenti di lavoro[186].

Altro possibile elemento distintivo degli strumenti da includere nel comma 2 è l'esistenza di una relazione "attiva" tra lavoratore e strumento utilizzato per rendere la prestazione: dovrà trattarsi di uno strumento nella disponibilità operativa del dipendente e da questi effettivamente ed attivamente utilizzato, di cui il lavoratore non risulta essere soggetto meramente passivo come accade con gli strumenti di controllo[187].

Sul tema è intervenuto anche il Ministero del Lavoro con il comunicato del 18 giugno 2015: "l'espressione per rendere la prestazione lavorativa comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale

---

[185] Per una interpretazione restrittiva si esprimono P. Tullini, secondo la quale *l'interpretazione restrittiva si lascia preferire in ragione della ratio derogatoria dell'art. 4 co. 2, St. lav.*, e V. Nuzzo: *gli applicativi di cui il lavoratore non si avvalga per rendere la prestazione lavorativa, ma funzionali all'organizzazione del lavoro, non rientrano nella deroga all'accordo.* (V. Nuzzo I *software* che registrano la durata delle telefonate nei *call center* sono strumenti di lavoro? in *Rivista Italiana di Diritto del Lavoro*, 2/2018, 307). In senso contrario A. Ingrao, secondo la quale: *l'espressione "per rendere la prestazione" non impedisce di includere nell'area dell'esonero tutti quegli strumenti che pur non essendo essenziali rispetto all'adempimento, si limitino a facilitare, ottimizzare o rendere maggiormente efficiente la prestazione, in modo che possa essere "utilmente inserita" nell'organizzazione datoriale*. (A. Ingrao, *op. cit.*, 190). E così anche Maresca: *una formulazione ampia all'interno della quale non sembra possibile differenziare gli strumenti allorché siano utilizzati per organizzare oppure per eseguire la prestazione lavorativa, limitando a questi ultimi la previsione dell'art. 4, co. 2 e riconducendo gli altri al co. 1. […] si tratta di una distinzione priva di riscontro testuale*. (Maresca, *op. cit.).*

[186] A. Ingrao, *op. cit.*, 186.

[187] *Solo se il lavoratore ha un ruolo attivo nel suo utilizzo e, cioè, se quello strumento viene concretamente impiegato dal dipendente nello svolgimento delle mansioni. Quello che conta, in altri termini, è che lo strumento sia nella disponibilità operativa del dipendente e da questi effettivamente utilizzato nell'adempimento della prestazione, diversamente da quanto avviene con gli strumenti di controllo di cui all'art. 4, comma 1, rispetto ai quali il lavoratore è, invece, sempre soggetto meramente passivo*. (M. Marazza, *op. cit*., 11-12). V. anche M.T. Salimbeni, *op. cit*. secondo la quale si può parlare di strumento di lavoro *solo nelle ipotesi in cui il meccanismo che genera il controllo è nella gestione del lavoratore che lo attiva o disattiva per rendere la prestazione* (*op. cit*., 609) e I. Alvino che li identifica negli strumenti che il lavoratore impieghi direttamente per lo svolgimento della prestazione lavorativa, *ossia quegli strumenti il cui funzionamento richieda una partecipazione attiva del lavoratore, che se ne avvale per rendere la prestazione* (I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori*, *op. cit.*, 24).

In senso contrario P. Tullini: *Non consente una maggiore precisione neppure la tesi secondo cui gli strumenti di lavoro ai sensi del co. 2 sarebbero solo quelli che richiedono un ruolo attivo del lavoratore, mentre le tecnologie suscettibili di autorizzazione preventiva implicano una condizione di passività del soggetto controllato. Se si accogliesse tale interpretazione […] l'area dell'esonero risulterebbe ampliata a dismisura* (P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa*, in P. Tullini (a cura di), *op. cit.*, 107).

mezzo che serve al lavoratore per adempiere la prestazione (una volta si sarebbero chiamati gli "attrezzi di lavoro"): ciò significa che, nel momento in cui tale strumento viene modificato per controllare il lavoratore, si fuoriesce dall'ambito della disposizione"[188].

È considerazione condivisa che debba sussistere una stretta correlazione fra strumento di cui il lavoratore viene dotato e mansioni assegnate, sia per la componente *hardware*, pc, tablet, smartphone, che per i *software* su di essi installati, che dovranno essere valutati caso per caso. Non rientrano nella definizione i sistemi che rappresentino un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa, ma per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro[189]. Nel momento in cui uno strumento viene modificato con l'installazione di appositi software di localizzazione o filtraggio al fine di controllare il lavoratore, non siamo più nell'ambito della disposizione del comma 2 e il pc, il tablet o il cellulare si trasformano da strumento che "serve" al lavoratore per rendere la prestazione, in strumenti che servono al datore per controllare il lavoratore [190].

---

[188] È estremamente critico sull'intervento del Ministero, Cosattini che così scrive: *Non sanno, o fingono di non sapere, i tecnici del Ministero, che oggigiorno la stragrande maggioranza degli strumenti informatici è già dotata di sistemi di geolocalizzazione e/o rilevazione di traffico e quant'altro fin dall'immissione in commercio, senza necessità di dar corso a chissà quale "modifica"; e considerazioni analoghe si possono verosimilmente fare per altre tipologie di strumenti utilizzati dal lavoratore, come i macchinari: è agevole ipotizzare che essi vengano forniti già dotati di software che consentano la rilevazione dei dati di lavorazione, senza necessità di alcuna modifica, o se così ancora non fosse è più che plausibile che le industrie produttrici siano in grado di adeguarsi velocemente alle nuove esigenze....; per non parlare poi degli strumenti di registrazione degli accessi e delle presenze, che certo non risentono delle "precisazioni" fornite con la citata nota ministeriale.* (L. A. Cosattini, *Le modifiche all'art. 4 Stat. lav. sui controlli a distanza, tanto rumore; per nulla? op. cit*., 990).

[189] *Quanto al rapporto tra hardware e software sembra chiaro che un conto è lo strumento di lavoro computer, tablet o smartphone e, ben altra, cosa sono gli applicativi informatici su di essi installati. Anch'essi, se in grado di esprimere una funzionalità di controllo dell'attività, destinati ad essere autonomamente qualificati come "strumenti di controllo" o "strumenti di lavoro". Si tratta di un approccio qualificatorio che postula inevitabilmente accertamenti tecnici, talvolta anche complessi, sulle funzionalità del software di volta in volta preso in considerazione* […] *Un caso interessante che si può a tal riguardo considerare è, probabilmente, quello del sistema software utilizzato nei call center per consentire ai dipendenti di gestire le telefonate in ingresso o uscita (cosiddetta "barra telefonica"). Uno strumento di lavoro digitale che per i tecnici del settore si compone inscindibilmente dell'interfaccia gestita dal lavoratore (il telefono virtuale) e delle funzionalità che tracciano e registrano i dettagli dell'attività lavorativa. Se il software è inscindibile, e consente il tracciamento dei dati senza ulteriori applicativi, è ragionevole affermare, per le considerazioni sopra esposte, che si ricada nel campo di applicazione dell'art. 4, comma 2. Ond'è che l'utilizzo dei dati tramite di esso tracciati sarà consentito solo nel rispetto dell'art. 4, comma 3, dello statuto* (M. Marazza, *op. cit.*, 22, 23).

[190] L'Autorità Garante ribadisce "il divieto di installare strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica. Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò anche quando i singoli lavoratori ne siano consapevoli. In particolare, non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire - a volte anche minuziosamente - l'attività di lavoratori. È il caso, ad esempio, della lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori...; della riproduzione sistematica delle pagine web visitate dal lavoratore; della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

Anche il Garante ha precisato che nella nozione di strumenti di lavoro rientrano i sistemi e le apparecchiature che consentono il fisiologico e sicuro funzionamento dell'organizzazione aziendale, anche al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore, ma non sono strumenti di lavoro tutti quei "sistemi *software* che consentono, con modalità non percepibili dall'utente (c.d. in *background*) e in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente), operazioni di monitoraggio, filtraggio, controllo e tracciatura costanti e indiscriminati degli accessi a internet o al servizio di posta elettronica"[191].

La casistica è varia ed evidenzia incertezze ed oscillazioni interpretative. Uno dei casi più controversi riguarda i sistemi di geolocalizzazione in uso al lavoratore, per i quali la valutazione resta subordinata ad un'indagine da effettuare di volta in volta in base alla indispensabilità dell'applicativo rispetto alla effettiva mansione del lavoratore: nel caso in cui lo strumento sia assegnato ad un lavoratore adibito a servizi sul campo di assistenza alla clientela e l'applicativo serva a coordinare tali servizi, si dovrebbe stare nel campo di applicazione del comma 2, mentre così non è se il lavoratore non ha alcuna mobilità territoriale ed il sistema non è funzionale alla sua prestazione[192]. Sarà necessario verificare

---

dell'analisi occulta di computer portatili affidati in uso"). Si pensi, ad esempio, a BlackBox Security Monitor, un programma gratuito che può essere installato sul computer e che consente tecnicamente di "spiare" tutto ciò che su di esso accade: scatta istantanee del desktop, salva una lista di tutti i programmi avviati e dei siti internet visitati, memorizza persino i tasti della tastiera che sono stati digitati: *Il sol fatto che sia installato sullo strumento di lavoro non può certo farlo rientrare nella deroga di cui al co. 2 altrimenti si toglierebbe virtualmente qualsiasi spazio al primo comma, eccezion fatta per i soli impianti audiovisivi e poco altro*. (R. Del Punta, *La nuova disciplina dei controlli cit*., 100).

[191] Si veda la pronuncia dell'Autorità Garante che ha coinvolto l'Università degli Studi D'Annunzio di Chieti e Pescara (luglio 2016), dove si precisa che la casella di posta elettronica è funzionale alla prestazione lavorativa del Segretario amministrativo del Dipartimento, (comma 2), ma non certo a quella dell'addetto alla guardiania, che pure potrebbe avere la mail aziendale, ma ai sensi del primo comma dell'art. 4, non del secondo. E si veda anche, Audizione Garante Comm. lav. Camera Deputati 9 luglio 2015, par.2.: secondo cui i controlli mediante gli strumenti dell'art. 4, co. 2, St. lav. beneficiano dell'esonero dalla procedura autorizzativa solo se «effettuati utilizzando le normali funzionalità degli apparecchi forniti per rendere la prestazione e non inserendo specifici sistemi modificativi dei dispositivi, finalizzati al controllo personale del lavoratore. Non dovrebbe, dunque, avvalersi dell'esonero il datore di lavoro che intenda dotare di particolari software atti al monitoraggio del lavoratore i dispositivi (il PC o il telefono) forniti al dipendente per ragioni di servizio.

[192] Conseguentemente se il GPS è utile a fini organizzativi per individuare la posizione sul territorio e quindi unicamente per distribuire in modo efficiente il lavoro di consegna plichi, ma di esso non si avvale il fattorino per rendere la prestazione, rientrerà nell'ipotesi di cui al comma 1 art. 4 St. lav. costituendo uno strumento organizzativo e non di lavoro (M.T. Carinci in Tullini, P. (a cura di), *op. cit.*, 53). Per l'opposta interpretazione vedi I. Alvino: *In questa ipotesi si può ritenere che il sistema di rilevazione satellitare sia annoverabile fra gli strumenti di lavoro, poiché l'esistenza e il funzionamento dello stesso è essenziale affinché il datore di lavoro possa trarre vantaggio dalla esecuzione della mansione (la consegna dei pacchi).* (I. Alvino, *I nuovi limiti al controllo a distanza,* in LLI n.1/2016, 25).

Anche la Circolare INL n. 2 del 7 novembre 2016 fornisce indicazioni operative sull'utilizzazione di impianti GPS ai sensi dell'art. 4, co.1 e 2, L. n. 300/1970: in essa è specificata *la riconducibilità al co. 2 dell'art. 4 dei soli strumenti strettamente funzionali a rendere la prestazione lavorativa, tenuto conto che l'interpretazione*

concretamente il rapporto di "funzionalità" rispetto alla prestazione del lavoratore, con la conseguenza che, in sua mancanza, l'utilizzo di tali strumenti sarebbe soggetto all'accordo sindacale o all'autorizzazione amministrativa, di cui al primo comma art. 4 St. lav.[193]

Quello fra strumenti di lavoro e strumenti di controllo è un discrimine molto sottile, soprattutto per gli strumenti informatici intrinsecamente e volutamente polifunzionali, rispetto ai quali è arduo distinguere tecnologie di controllo e prestazionali o verificare l'inscindibilità o meno delle funzioni di lavoro e da quelle di controllo. Nell'ipotesi in cui la funzione di controllo sia connaturata inscindibilmente e *ab origine* allo strumento di lavoro, senza essere conseguenza di una modifica successivamente apportata al dispositivo, risulta più arduo superare le difficoltà interpretative.

Il punto, come osserva acutamente A. Sitzia, non riguarda tanto l'installazione di programmi di controllo *ad hoc* per rendere possibile un controllo sull'attività posta in essere dai lavoratori, ma il fatto che gli strumenti informatici sono spesso in se stessi strumenti di controllo con un'intrinseca capacità di acquisire e memorizzare informazioni sull'attività svolta dal lavoratore attraverso i file log. Questi ultimi registrano la sequenza cronologica delle operazioni effettuate e rendono possibile un ampio e incisivo monitoraggio[194].

---

letterale del disposto normativo porta a considerare quali strumenti di lavoro quegli apparecchi, dispositivi e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano stati posti in uso e messi a sua disposizione. In linea di massima, e in termini generali, si può ritenere che i sistemi di geolocalizzazione rappresentino un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro. Solo in casi del tutto particolari – qualora i sistemi di localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa (e cioè la stessa non possa essere resa senza ricorrere all'uso di tali strumenti) […] si può ritenere che gli stessi finiscano per "trasformarsi" in veri e propri strumenti di lavoro e pertanto si possa prescindere […] sia dall'intervento della contrattazione collettiva che dal procedimento amministrativo di carattere autorizzativo previsto dalla legge.

[193] *Si pensi agli applicativi installati in strumenti in dotazione ai lavoratori, e finalizzati all'analisi delle chiamate registrate dei clienti, così da ricavarne informazioni essenziali per una migliore commercializzazione dei prodotti: rientrano nell'ambito del 1° comma; si consideri il cronotachigrafo: in questo caso, nonostante la funzione dello strumento ecceda quanto è richiesto dalla prestazione del singolo conducente, si deve tenere conto che lo stesso è una componente necessaria, in quanto obbligatoria per legge, della strumentazione di bordo dei veicoli commerciali e industriali, per cui non sembra avere senso richiedere un'autorizzazione; oppure il telepass, tanto più se installato su auto aziendali destinate allo svolgimento di specifici servizi, si deve considerare uno strumento direttamente funzionale all'efficienza della singola prestazione, oltre che ormai fortemente compenetrato con essa nell'odierna pratica lavorativa, per cui siamo nell'ambito del 2° comma.* (R. Del Punta, *op. cit*., 77).

[194] *La questione interpretativa più grave attiene proprio a questi "file", i quali, ove possano dirsi necessari per il funzionamento del programma al quale accedono, consentono un controllo lecito ma in certi casi molto invasivo, soprattutto qualora sia reso possibile il monitoraggio sull'uso di Internet e della posta elettronica sulle attività svolte dal lavoratore attraverso l'utilizzo delle strumentazioni informatiche di cui egli sia stato dotato per ragioni di servizio*. (A. Sitzia, *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, in *LLI* n. 1/2016, 90).

Strumenti di lavoro più o meno sofisticati hanno innegabilmente un'insita capacità di controllo a distanza dell'attività lavorativa, rispetto alla quale il legislatore nulla specifica, riservandosi di tutelare la dignità e la riservatezza del lavoratore con le previsioni contenute nel successivo comma 3 dell'art. 4 St. lav.

Il risultato sembra essere che l'uso di strumenti riconducibili a questa categoria svincola la capacità di controllo, incorporata negli stessi, a condizione che non sia il risultato di una modifica apportata dal datore allo strumento di lavoro al fine di esercitare il controllo. In questo senso L. Ficari sostiene che la nuova disciplina prevede un "controllo a distanza svincolato" *e la conseguente valutazione di legittimità di controlli esercitati a mente del nuovo disposto*[195].

La delicatezza della questione risiede anche nel fatto che gli strumenti tecnologici spesso non distinguono e non tengono separate i contenuti personali da quelli lavorativi e aziendali e si configurano come strumenti ad uso promiscuo, di lavoro e privato, potendo intercettare ogni azione, e immagazzinare, catalogare, incrociare una serie enorme di dati sia personali sia riguardanti la prestazione di lavoro, resa o non resa.

Proprio per il rischio insito i questi strumenti il confronto e l'accordo sindacale poteva essere quanto mai necessario, secondo Valeria Nuzzo[196].

In ogni caso oggi ci viene in soccorso la normativa sulla protezione dei dati, con il Regolamento UE 2016/679. Se la scelta dei mezzi di lavoro è da ricondurre nell'ambito delle scelte organizzative e produttive dell'imprenditore che individua gli strumenti ritenuti più opportuni e funzionali al perseguimento degli obiettivi dell'impresa, la libertà dell'imprenditore di organizzare l'attività produttiva risulta limitata, dopo l'entrata in vigore del Regolamento UE 2016/679, non solo dai principi di minimizzazione, di necessità e non eccedenza del trattamento dei dati, già previsti dal Codice Privacy, ma ancor di più dal principio della *privacy by design,* operante sin dalla fase di progettazione degli strumenti e dei processi produttivi. Il rispetto di tale principio è in grado di incidere *ab origine* sulle scelte organizzative datoriali, doverosamente condizionate dalla ricerca di strumenti di lavoro che abbiano il minore impatto possibile sulla riservatezza di chi lavora[197].

---

[195] L. Ficari, *I controlli effettuati attraverso gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa,* in A. Levi (a cura di) *op. cit.*, 92.

[196] *Si tratta spesso di strumenti polifunzionali, in cui la funzione specifica considerata dal comma 2 (sottratta alle garanzie del comma 1 dell'art. 4 St. Lav.) può cumularsi con altre, compresa quella del controllo (occulto, palese, a distanza fisica o a distanza temporale) sull'attività dei lavoratori* […] e per questo *il confronto sindacale (e l'accordo) poteva essere più necessario.* (V. Nuzzo, *op.cit.*, 77).

[197] *Il principio della privacy by design, letto insieme a quello della accountability, della responsabilizzazione dei titolari del trattamento dei dati, si sostanzia in una serie di vincoli per il datore di lavoro relativi anche alla sua organizzazione di impresa. L'idea dell'accountability permea tutto il Regolamento Ue e mira a*

E questo risponde in ultima analisi alla ponderazione di interessi di cui al secondo comma dell'art. 41 C.

3.4.1 *Segue:* Il controllo esercitato attraverso gli strumenti di lavoro

Altro delicato nodo interpretativo è se attraverso gli strumenti di lavoro, liberamente scelti ed assegnati dal datore, sia anche possibile un controllo sull'esatto adempimento della prestazione finalizzato alla gestione del rapporto di lavoro. Il punto è se la deroga contenuta nel comma 2, art. 4 St. lav. debba leggersi come comprensiva tanto della procedura sindacale o amministrativa, quanto della necessità di esigenze giustificative qualificate, legittimanti l'impiego degli strumenti di controllo. Seguendo questa ultima interpretazione la deroga prevista dal comma 2 dell'art. 4 St. lav. liberalizzerebbe l'uso degli strumenti di lavoro e, con essi, la possibilità di controlli diretti alla verifica dell'adempimento: lo strumento di lavoro abiliterebbe il datore di lavoro all'esercizio del controllo sulla prestazione senza limiti finalistici.

In sede di audizione alle Camere sullo schema dei decreti legislativi attuativi del Jobs Act, il Presidente Soro ha richiamato l'attenzione sulle conseguenze di una tale interpretazione: *Nell'escludere l'applicazione della disciplina "del primo comma" a queste ipotesi, tuttavia, la norma prescinde non solo dalla procedura autorizzativa, ma anche da quei requisiti finalistici (funzionalità del controllo a esigenze produttive, organizzative ecc.) previsti dal primo comma per i controlli a distanza. Se quest'esclusione fosse imputabile a un mero errore di drafting, sarebbe opportuno chiarirlo. In assenza di questa precisazione, infatti, il solo requisito finalistico applicabile ai controlli in esame resta quello (alquanto ampio, come si dirà) del terzo comma, che legittima l'utilizzo dei dati così acquisiti per "tutti i fini connessi al rapporto di lavoro".* E prosegue prefigurando le conseguenze di tale "liberalizzazione": *La possibilità del controllo dell'adempimento della prestazione, mediante gli strumenti "di lavoro", diverrebbe in tal modo un "effetto naturale del*

incidere sin dalla genesi delle scelte datoriali: la "libertà" di decidere come strutturare l'attività economica è infatti fortemente limitata dall'obiettivo della effettiva tutela della riservatezza di quanti prestino lavoro nella organizzazione datoriale e, dunque, vincolata al presupposto che gli impianti e/o gli strumenti produttivi adottati non determinino un controllo più penetrante di quello necessario. Questa ponderazione di valori e interessi in gioco […] *deve spingersi a verificare se il medesimo risultato pratico cui è finalizzato l'esercizio del potere imprenditoriale possa essere conseguito sacrificando in misura minore la dignità di chi lavora*. (V. Nuzzo, *I software che registrano la durata delle telefonate nei call center sono strumenti di lavoro?*, in *RIDL*, n. 2/2018, 312).

contratto", in senso civilistico, in quanto finirebbe con il discendere naturalmente dalla costituzione del rapporto di lavoro[198].

Si tratta di una delle disposizioni sulle quali si sono appuntate le maggiori critiche e che lascia la dottrina in disaccordo, sostanzialmente divisa fra coloro che leggono la lettera della legge come apertura ad un controllo sulla prestazione esercitato attraverso gli strumenti di lavoro e chi ritiene che le previsioni del comma 2 operino in deroga ai vincoli procedurali ma non a quelli finalistici, essendo il principio della limitazione delle finalità un principio inderogabile, in base al quale devono sussistere finalità determinate e diverse dal controllo sull'adempimento della prestazione. Il controllo impersonale a distanza, resta lesivo della dignità di chi lavora, anche e soprattutto nel caso sia posto in essere tramite gli strumenti di lavoro. Il loro uso consente di acquisire una enorme quantità di dati e notizie sulle modalità di svolgimento dell'attività lavorativa, e non solo, ed esonerarli oltre che dalla disciplina autorizzativa, anche dal vincolo finalistico può significare una notevole perdita di tutele in capo al lavoratore.

In dottrina molte voci si esprimono nel senso della esplicita legittimazione di un controllo diretto sull'adempimento della prestazione effettuato tramite strumenti utilizzati dal lavoratore per rendere la prestazione stessa, con il possibile utilizzo delle rilevazioni effettuate per contestare al lavoratore l'inadempimento.

Secondo Maria Teresa Carinci il limite finalistico per cui lo strumento di lavoro deve essere strettamente funzionale all'esecuzione della prestazione lavorativa non impedisce, ma anzi legittima il controllo diretto sull'esecuzione della prestazione, esercitato tramite gli strumenti preordinati all'adempimento della specifica prestazione. Proprio l'eliminazione del divieto generale di controlli a distanza dal testo della norma sarebbe funzionale all'apertura ad un controllo sulla prestazione. L'Autrice si domanda se in questo modo sia venuto meno anche ogni argine alle modalità di quel controllo, se il datore di lavoro sia totalmente libero di strutturare la propria organizzazione e di scegliere liberamente gli strumenti di lavoro che, unendo inestricabilmente funzioni prestazionali e di controllo, gli garantiscano le più ampie possibilità di monitorare i propri dipendenti. La risposta in senso negativo trova il suo fondamento nella disciplina in materia di dati personali, oggi contenuta nel Regolamento UE 2016/679, cui il terzo comma dell'art. 4 St. lav. esplicitamente rinvia:

[198] A. Soro, Audizione sugli schemi dei decreti legislativi attuativi del c.d. Jobs Act presso la Commissione lavoro della Camera dei deputati e del Senato (9 e 14 luglio 2015).

l'argine a tutela della dignità e libertà del prestatore è rappresentato dal rispetto delle condizioni alle quali è subordinata l'utilizzazione delle informazioni raccolte[199].

Dato il carattere patrimoniale dell'interesse creditorio del datore, secondo Marco Marazza, anche il puntuale adempimento dell'obbligazione lavorativa concorre alla valorizzazione del patrimonio aziendale e questo renderebbe la vigilanza sull'attività lavorativa legittima e soggetta al limite procedurale di cui al comma 1 dell'art. 4 St. lav.[200]

Partendo dal quadro normativo vigente, anche Patrizia Tullini ritiene archiviato il divieto di controllo tecnologico sull'attività lavorativa risalente alla primitiva disciplina statutaria. L'esonero di cui al comma 2 sembra riguardare l'intera prima parte dell'art. 4 St. lav. e con questa apertura della riforma sembrerebbe legittimarsi la sorveglianza diretta sulla prestazione. Oggi il datore è abilitato a servirsi delle informazioni raccolte per via diretta, attraverso il monitoraggio degli strumenti di lavoro, oppure per via indiretta mediante i sistemi di sorveglianza autorizzati ai sensi del comma 1, per tutti i fini connessi al rapporto di lavoro, tanto da concludersi che il controllo sui lavoratori è lecito e possibile[201]. Tullini però avanza dubbi in merito alla coerenza con la normativa europea[202].

Andrea Sitzia sostiene che il legislatore del 2015 con la novella abbia inteso dare fondamento a quel potere di controllo tecnologico fortemente negato nel precedente assetto normativo: gli strumenti di lavoro possono essere impiegati anche per effettuare controlli a distanza dell'attività dei lavoratori, fermi restando i limiti stabiliti dallo Statuto dei lavoratori (in particolare quelli posti dall'articolo 8 St. lav.), quelli posti a salvaguardia della dignità e riservatezza del lavoratore e il rispetto della normativa privacy[203].

---

[199] M.T. Carinci, *op. cit.* 54 e ss.

[200] *Il riferimento alle esigenze di tutela del patrimonio aziendale* […] *legittimerebbe un deciso ampliamento delle finalità di controllo di tali strumenti. Anche il puntuale adempimento dell'obbligazione lavorativa concorre alla valorizzazione del patrimonio aziendale, se preso in considerazione dal punto di vista del diritto di credito dell'imprenditore ad una prestazione di lavoro che ha, indubbiamente, un contenuto patrimoniale*. (M. Marazza, *op. cit.*, 16).

[201] P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa,* 15 in Tullini, P. (a cura di) *Web e lavoro. Profili evolutivi e di tutela*. Giappichelli, Torino, 2017.

[202] 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 P. Tullini, (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, 111.

[203] *Il legislatore del 2015, con il secondo comma dell'art. 4 St. lav., ha ammesso, per contro, il controllo tecnologico nel senso che, al di fuori dell'applicazione del primo comma fermi i limiti della rilevanza ai fini della valutazione dell'attitudine professionale (art. 8 St. lav.), del rispetto della dignità del lavoratore, della riservatezza sua e di terzi, e del rispetto della tutela generale civilistica in materia di privacy; in questo senso è forse possibile affermare che, nei limiti di cui si è detto, il legislatore, novellando l'art. 4, abbia fondato quel vero e proprio potere di controllo di cui la dottrina, nella vigenza della vecchia normativa, negava l'esistenza.*(A. Sitzia, *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore),* in *Labour Law Issues* n. 1/2016, 88).

Anche Arturo Maresca, pur riconoscendo una *presunzione assoluta di legittimità* del controllo indotto dagli strumenti di lavoro, individua nel comma 3 dell'art. 4 il presidio a tutela del lavoratore: il legislatore non impone vincoli interdittivi all'impiego degli strumenti di lavoro, ma prevede tutele per il dipendente per quanto riguarda le informazioni raccolte dal datore di lavoro tramite gli stessi strumenti[204].

Allo stesso modo Marco Barbieri ritiene che né il limite procedurale né quello finalistico si applichino agli strumenti di cui al secondo comma: come la lettera della legge rende chiaro, nelle due ipotesi, degli strumenti di lavoro e di registrazione di accessi e presenze, il datore di lavoro è esonerato sia dal limite finalistico che da quello procedurale, ma questo non significa che il datore di lavoro sia liberato da qualunque vincolo nell'uso di strumenti da cui derivi o possa derivare il controllo a distanza della prestazione[205].

Secondo questi interpreti stando alla lettera della norma, si avrebbe una deroga piena all'applicazione della disciplina di cui al comma 1, sia con riferimento alla procedura concertativo-autorizzativa che dei vincoli finalistici. Rispetto ai controlli operati sugli e tramite gli strumenti di lavoro, non sussiste limite di finalità, pur permanendo limiti quanto alle modalità dettati dalla disciplina generale di tutela dei dati personali: entro questi limiti, il controllo pare poter interessare direttamente la prestazione lavorativa.

Tutti gli Autori citati individuano nell'applicazione della normativa posta a tutela dei dati personali lo strumento di tutela dei lavoratori, l'argine al controllo sulla prestazione

---

[204] A. Maresca, *op. cit.*, 512. V. anche Santoro-Passarelli: *Analizzando il secondo e il terzo comma del novellato art. 4 St. lav., G. Santoro Passarelli ha ravvisato nel comma 3 il vero baluardo a tutela di dignità e riservatezza del lavoratore. Se è vero che la norma sembra spostare l'equilibrio tra gli interessi contrapposti alla produttività e alla dignità e riservatezza del lavoratore a favore del primo piuttosto che dei secondi, rendendo più flessibile, in ragione della loro utilità a svolgere la prestazione, il ricorso a strumenti di lavoro tecnologicamente avanzati ma dai quali deriva la possibilità di controllo. Ciò non significa, però, che il controllo dell'attività lavorativa attraverso gli strumenti utilizzati per svolgere la prestazione, venuta meno la necessità di autorizzazione sindacale o amministrativa, sia del tutto liberalizzato: il comma 3, infatti detta le condizioni ed i limiti dell'utilizzabilità ai fini disciplinari delle informazioni raccolte*. (G. Santoro-Passarelli, *Sulle categorie del diritto del lavoro "riformate",* in WP C.S.D.L.E. Massimo D'Antona, 27/1/2016.).

[205] M. Barbieri, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in Tullini, P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, 193-194. Si veda anche Dagnino che segnala le *intrinseche potenzialità di controllo degli strumenti, che possono essere assai pervasive o, addirittura, porsi in contrasto con la ratio specifica dell'articolo 4 dello Statuto dei lavoratori, individuata nella necessità di garantire che la vigilanza sul lavoro operata tramite tecnologie non si configuri in una forma tale («continua ed anelastica») da eliminare gli spazi di riservatezza ed autonomia del lavoratore nello svolgimento della prestazione.* (E. Dagnino, *Tecnologie e controlli a distanza*, in *DRI* 4/2015, 988). È critico Filippo Olivelli che richiama il principio costituzionale di tutela della dignità del lavoratore quale argine al potere di controllo esercitato dal datore attraverso gli strumenti di lavoro: *il legislatore del 2015 permettendo il controllo – evidentemente anche occulto – sugli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", senza l'accordo o l'autorizzazione richiesta al primo comma, ha ora consentito la verifica dell'attività del lavoratore facendo venir meno quel contenimento del potere organizzativo e direttivo del datore di lavoro che era, invece, la ratio dell'art. 4 Stat. Lav. così come predisposto nel 1970.* F. Olivelli, *Lo "stratagemma" di facebook come controllo difensivo occulto: provocazione o tutela del patrimonio aziendale*?, in ADL n. 6/2015, 1318.

attraverso gli strumenti di lavoro: quanto previsto nel comma 3 dell'art. 4 vale ad escludere che il controllo dell'attività lavorativa attraverso gli strumenti utilizzati per rendere la prestazione sia del tutto liberalizzato.

Tra le voci critiche si segnala Anna Trojsi che definisce illusoria per le caratteristiche stesse degli strumenti tecnologici, che non consentono di separare materialmente strumento di lavoro e strumento di controllo, la giustificazione espressa in sede parlamentare per cui deve trattarsi di controlli aventi per oggetto gli impianti e gli strumenti di lavoro, non le persone dei lavoratori[206]. Secondo l'Autrice il controllo sugli strumenti di lavoro comporta inevitabilmente il controllo sul lavoratore, sulle sue attività, lavorative e non, e su aspetti personali, attraverso la memorizzazione e l'elaborazione elettronica di tutte le operazioni svolte e con esse di informazioni e dati personali del lavoratore. Per questa difficoltà di separare il controllo sullo strumento di lavoro dal controllo sul lavoratore, l'unica garanzia per il lavoratore è operare selettivamente sulle informazioni: le uniche informazioni utilizzabili dal datore di lavoro sono quelle concernenti l'esecuzione della prestazione lavorativa, incluse quelle quantitative sull'utilizzo privato dello strumento, mentre sussiste il divieto di raccolta e trattamento di ogni altro dato ricavabile da tali strumenti[207].

Tra coloro che non ritengono si possa concordare con una interpretazione della deroga contenuta nel secondo comma dell'art. 4 St. lav. volta a "liberalizzare" l'uso degli strumenti di lavoro e di registrazione degli accessi e, con essi, la possibilità di controlli diretti alla verifica dell'adempimento, c'è Valeria Nuzzo: se il controllo impersonale a distanza è giudicato lesivo della dignità di chi lavora, lo è a maggior ragione laddove manchi la negoziazione sindacale. Nuzzo ne segnala i pericoli per la dignità e la libertà personale, denunciando il rischio della sottoposizione del lavoratore ad uno strumento in grado di verificare luoghi, tempi e modi della prestazione, di spiare e memorizzare l'attività svolta e produrre un effetto dissuasivo e di soggezione molto simile all'effetto Panopticon, con il datore/controllore onnipresente e onniveggente. È invece opportuno guardare oltre il dato letterale, alla coerenza del sistema, ai valori e ai principi costituzionali, all'assetto generale

---

[206] A. Trojsi, *Il comma 7, lettera f), della legge delega n. 183/2014: tra costruzione del Diritto del lavoro dell'era tecnologica e liberalizzazione dei controlli a distanza sui lavoratori,* in Rusciano - Zoppoli (a cura di) CSDLE W.P. Massimo D'Antona, *Jobs Act e contratti di lavoro dopo la legge delega 10 dicembre 2014 n. 183,* 130.
Nel testo emendato alla Camera è stata inserita la precisazione per cui i "controlli a distanza", ai quali intende riferirsi il legislatore, sono quelli "sugli impianti e sugli strumenti di lavoro", con un mutamento dell'ottica in cui sono considerati gli impianti e gli strumenti di lavoro: da strumento di controllo a distanza sui lavoratori (come erano concepiti dall'art. 4 St. lav.) ad oggetto (obiettivo, destinatario) del controllo datoriale.

[207] A. Trojsi, *Al cuore del nuovo art. 4, co. 2, st. lav.: la delimitazione della fattispecie degli «strumenti utilizzati per rendere la prestazione lavorativa»* in *Rivista Italiana di Diritto del Lavoro*, n.2/2017, 317.

di tutele, delineato dallo stesso Statuto e dal Codice della privacy, al divieto di controlli a distanza, che pur in assenza di un'esplicita enunciazione resta immanente al sistema, ed in virtù di questa valutazione di sistema, Nuzzo conclude che non si può intendere come totale la deroga di cui al comma 2 dell'art. 4 St. lav. Consentire al datore un controllo continuativo e pervasivo, attraverso lo strumento di lavoro, sarebbe incompatibile con la tutela della persona, della sua dignità e della sua riservatezza[208].

Ad una lettura coerente del dato normativo rispetto al quadro giuridico europeo (in particolare dell'art. 5 Reg. 2016/679 UE) fa riferimento Valerio Pinto, secondo il quale la norma novellata non ha introdotto una deroga al principio di finalità, in base al quale i dati personali possono essere raccolti e registrati al fine di perseguire uno scopo predeterminato ed esplicitato, oltre che legittimo. Non sembra accettabile un'esenzione dal rispetto del principio di finalità, che in quanto principio radicato nel diritto sovranazionale non appare derogabile a livello nazionale. È sicuramente ammessa la verifica dell'impiego scorretto ed abusivo degli strumenti di lavoro ma l'Autore ritiene certamente escluso che la norma deroghi al divieto del controllo occulto, al principio che i controlli sulla prestazione siano effettuati da personale apposito. Ammettere il controllo impersonale sulla esecuzione della prestazione volto all'individuazione degli inadempimenti del lavoratore creerebbe un pericoloso disallineamento rispetto alla diversa soluzione prevista dagli impianti di videosorveglianza e dagli altri sistemi con analoghe funzionalità che potrebbe essere sfruttato dai datori di lavoro per aggirare il divieto[209].

Anche A. Ingrao sulla base di una lettura integrata del complesso sistema normativo, di cui l'art. 4 St. lav. è parte, ritiene erronea dal punto di vista del diritto della protezione dei dati personali un'interpretazione della norma che conduca alla deroga del principio di limitazione della legittima finalità: il controllo a distanza, configurandosi come trattamento di dati personali dei lavoratori, deve soggiacere alla disciplina in materia prevista dal Regolamento europeo. Una interpretazione del secondo comma dell'art. 4 come eccezione al principio di limitazione della finalità consentirebbe al datore di lavoro di svolgere attraverso gli strumenti di lavoro o di registrazione degli accessi e delle presenze, trattamenti di dati personali

[208] V. Nuzzo, *op. cit.*, 100 – 103 e 113.

[209] V. Pinto, *I controlli difensivi del datore di lavoro sulle attività informatiche e telematiche del lavoratore,* in P. Tullini, (a cura di) *op.cit.,* 148-149. Pinto aggiunge *Più difficile è stabilire se le informazioni registrate per il tramite degli strumenti di lavoro possano essere utilizzate per soddisfare esigenze diverse dall'individuazione degli inadempimenti da parte del lavoratore (certamente esclusa, come si è sostenuto) e dalla prevenzione dell'impiego scorretto ed abusivo degli strumenti di lavoro (sicuramente ammessa).*

multifunzionali, mentre il principio di limitazione della finalità ha, a parere dell'Autrice, carattere inderogabile[210].

I rischi connessi alla possibilità di raccogliere informazioni ulteriori e quelli collegati alla sorveglianza continua del dipendente che lo strumento di lavoro può consentire, sono evidenti nell'ambiente lavorativo di un'impresa fortemente digitalizzata come il colosso dell'e-commerce, Amazon. Nell'organizzazione del lavoro dei magazzini Amazon uno strumento di lavoro, indispensabile per svolgere la prestazione e assegnato liberamente senza mediazione sindacale, consente il controllo diretto sulla prestazione lavorativa e la raccolta l'utilizzo delle informazioni anche per scopi disciplinari[211].

Di fronte a risorse insite nello strumento di lavoro potenzialmente lesive della libertà e dignità umana, l'attenzione deve concentrarsi sulle garanzie e sulle tutele che ci vengono dal rispetto della normativa privacy, oggi dal Regolamento 2016/679 UE, improntando i controlli datoriali a gradualità nell'ampiezza e nella tipologia, rendendo residuali i controlli più invasivi, legittimati solo a fronte di specifiche anomalie e dopo aver fatto ricorso a misure preventive meno limitative dei diritti dei lavoratori.

---

[210] *La portata apparentemente derogatoria del c. 2, non è idonea a sottrarre gli strumenti di lavoro e quelli di registrazione degli accessi e delle presenze al principio di finalità e alla sua funzione limitativa, ma possiede un'implicazione soltanto procedurale. Di conseguenza, nell'ipotesi di "trattamento" con strumenti di lavoro non si può ritenere che il datore di lavoro sia facoltizzato a utilizzare indistintamente le informazioni purché il loro contenuto sia ricollegabile al contratto di lavoro, ma è obbligato, anche in questo caso, a predeterminare in concreto, esplicitare e rispettare per tutto il trattamento determinate finalità legittime.* A. Ingrao, *op. cit*., 162.

[211] Nei magazzini Amazon attraverso un lettore di codice a barre con GPS integrato, il dipendente è costantemente localizzato, e attraverso il lettore gli vengono indicati il percorso più breve per raggiungere il prodotto da prelevare dagli scaffali e i passaggi successivi da compiere per l'imballaggio. Questo consente all'azienda di monitorare i ritmi di lavoro e di raccogliere informazioni sulla produttività di ciascuno, valutando, ad esempio, se il dipendente è più lento rispetto al tempo considerato utile per spostarsi da una postazione all'altra, e di utilizzarle per richiami o sanzioni disciplinari per scarso rendimento. A. Ingrao, *op. cit.,* 175. Il braccialetto elettronico di cui tanto si è parlato dovrebbe sostituire il lettore ottico ora in uso: *il braccialetto Amazon sembra essere proprio uno di quegli strumenti "in cui la tecnologia indirizza, scandisce e registra le singole operazioni, previene errori e difetti, corregge in tempo reale le modalità della prestazione. I lavoratori subordinati possono essere completamente eterodiretti dal sistema intelligente che "automatically knows the next step".* I "people o HR analytics" funzionano in modo simile, attraverso software incorporati negli strumenti utilizzati per rendere la prestazione sono preordinati ad acquisire dati sul rendimento e non solo *(si pensi ai più noti "keyloggers", che ricostruiscono il numero di battiti sulla tastiera in un certo tempo). La sequenza alla base del loro funzionamento è quella tipica di un algoritmo: il dato è raccolto attraverso un certo dispositivo, analizzato da un algoritmo che lo rielabora per produrre un dato inferenziale. Ogni forma di indagine finalizzata all'analisi di dati sul rendimento dei lavoratori rientra nella fattispecie disciplinata dall'art. 4 st. lav. e come tale costituisce una raccolta automatizzata di dati personali.* A. Ingrao, *op. cit.,* 181.

3.5 Strumenti di registrazione degli accessi e delle presenze

L'altra eccezione contenuta nel comma 2 dell'art. 4 St. lav. seleziona gli strumenti, esonerati dall'applicazione della disciplina generale prevista nel primo comma, non in base alla funzione ma all'oggetto della rilevazione, gli accessi e le presenze: è il fatto stesso di essere destinati alla registrazione di tali dati che sottrae i dispositivi alle garanzie del primo comma dell'art. 4 St. lav.

Anche in questo caso il legislatore ha probabilmente inteso positivizzare un precedente orientamento giurisprudenziale secondo il quale la consegna di strumenti per registrare l'orario di entrata e di uscita dai locali aziendali non necessitava dell'autorizzazione preventiva, in quanto tesa a misurare solo il *quantum* della prestazione[212].

Si pone in primo luogo un problema di identificazione: sono da includere nella categoria tanto gli strumenti di rilevazione "fisica" degli ingressi quanto quelli virtuali di verifica dell'accesso al *digital workplace*, i software che verificano gli accessi e le presenze virtuali posti in essere dal lavoratore accedendo alla rete informatica aziendale?

A favore di un'interpretazione estensiva che include gli accessi virtuali si esprime Marazza, per il quale non v'è ragione di circoscrivere il concetto di accesso alla sola ipotesi di accesso in un ambiente fisico, ma è preferibile estenderlo anche gli accessi digitali alle reti informatiche, con la possibilità di includere anche l'utilizzo, nel rispetto delle prescrizioni del Garante, di dati biometrici[213].

In disaccordo con questa ricostruzione che considera equivoca è Alessandra Ingrao che esclude un'interpretazione estesa anche gli accessi virtuali, ravvisandovi il rischio di sottrarre ai vincoli procedurali tutti quei programmi che, consentendo di registrare orario e sito visitato dal prestatore durante l'accesso in rete, permettono di controllarne continuativamente i comportamenti, a discapito del suo diritto alla dignità[214]. Questi software infatti per le loro caratteristiche di funzionamento operano in *background*, senza che il lavoratore ne sia sempre consapevole, possono profilare il controllato e monitorare il

[212] Trib. Milano 26 marzo 1994; Trib. Napoli, 23 settembre 2010 (con nota di F. Fusco) in *Riv. it. dir. lav*, n.1/2011, 31. V. anche Cass. 17 luglio 2007, n. 15892.

[213] M. Marazza, *op. cit.*, 24. Sulla stessa linea E. Dagnino, *Tecnologie e controlli a distanza,* in *Diritto delle relazioni Industriali*, 4/2015, 988.

[214] A. Ingrao, *op. cit*., 194. Di analogo parere O. Dessì secondo la quale *gli strumenti che memorizzano l'ingresso e la presenza dei lavoratori nelle reti informatiche aziendali, si ritiene che non siano soggetti all'art. 4, 2° comma, St. lav.* […] *siffatti software registrando la presenza di lavoratori in un contesto virtuale permettono al datore di monitorare indirettamente l'insieme delle sue condotte sul luogo di lavoro* (*Il controllo a distanza sui lavoratori*, Edizioni Scientifiche Italiane, Cagliari, 2017, 102) e anche V. Nuzzo, *op. cit.*, 159.

suo comportamento senza soluzione di continuità, per finalità non giustificate dal legittimo interesse del datore di lavoro all'adempimento della prestazione.

Un'eccezione alla ricostruzione restrittiva dovrebbe identificarsi nel caso del telelavoratore (oggi del "lavoratore agile") per il quale l'accesso e l'uscita dal sistema informatico potrebbero essere equiparati ad un controllo sull'ingresso e sull'uscita dai locali di lavoro effettuato con un *badge*[215].

Altra questione interpretativa sollevata riguarda l'espressione "accessi e presenze": la formula deve essere considerata un'endiadi oppure individua due fattispecie distinte?

Propende per la prima ricostruzione Nuzzo, secondo la quale l'espressione è da intendere come variazione semantica di uno stesso concetto: la deroga sarà limitata all'ingresso e all'uscita del lavoratore intesa come sistema di accertamento dell'accesso e della presenza in azienda durante l'orario di lavoro. Assegnare ai concetti di "accesso e presenza" significati distinti significherebbe eccedere la *ratio legis* e svincolare dall'accordo sindacale o dall'autorizzazione amministrativa l'impiego di dispositivi in grado di rilevare gli spostamenti endo-aziendali e la permanenza in luoghi specifici, o persino alla scrivania, consentendo un monitoraggio continuo del lavoratore e una ricostruzione completa dei movimenti e del comportamento tenuto in azienda[216].

Ciò su cui la dottrina appare concorde è il divieto di utilizzare strumenti che non si limitano a registrare l'accesso o la presenza del lavoratore in una determinata area, ma lo seguano nei suoi spostamenti, lo monitorano costantemente nei suoi movimenti con rischio di privarlo di ogni spazio di riservatezza. In questo senso Maria Teresa Salimbeni sostiene che se gli strumenti di rilevazione dell'accesso e della presenza all'interno del perimetro aziendale si identificassero anche con quelli idonei a registrare la mobilità interna dei lavoratori e a verificare se essi siano o meno alla propria postazione di lavoro e come e dove eventualmente si spostino, vi sarebbe un evidente contrasto con i principi di dignità e libertà personale di cui all'art. 2 Cost., che sono ancora il fondamento del divieto di controllo a distanza

---

[215] C. Zoli, *Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge 300/1970,* in VTDL 4/2016, 645.

[216] V. contra I. Alvino che valorizza la congiunzione *e* posta tra i due termini per sottolineare l'autonomia concettuale dei due concetti: *La congiunzione "e" collocata fra i termini "accessi" e "presenze" assume un valore disgiuntivo destinato ad esprimere che il concetto di "accesso" ha un suo autonomo significato da considerare indipendentemente da quello di "presenza". Lo strumento al quale la disposizione fa riferimento non è dunque solo quello che consente di rilevare gli accessi del lavoratore sul luogo di lavoro, ai soli fini della rilevazione della presenza e dunque del rispetto dell'orario di lavoro, ma qualunque strumento idoneo a registrare l'accesso e/o la presenza in determinati locali aziendali.* (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,* in LLI I/2016, 22).

dell'attività dei lavoratori attraverso impianti audiovisivi e altre apparecchiature in virtù di una considerazione di carattere sistematico. L'art. 4, sia pur novellato, è parte del Titolo primo dello Statuto dei lavoratori che resta espressione di quei valori. L'Autrice propone per questo un'interpretazione restrittiva dell'espressione "strumenti di registrazione degli accessi e delle presenze", riferita esclusivamente ai sistemi di accertamento dell'accesso e della presenza in azienda durante l'orario di lavoro, necessari, in sostanza, per controllare il rispetto dell'orario di lavoro, non l'attività di lavoro o la mobilità interna[217].

Al tempo stesso è innegabile che l'espressione "accessi e presenze" sia più ampia di quella "accessi ed uscite" e per questo la si estende alla verifica dell'accesso ad aree aziendali riservate, in caso perché pericolose, mediante tesserino magnetico, o agli spostamenti da una palazzina all'altra o ad un piano diverso da quello in cui il dipendente normalmente opera per i quali si richiede il badge.

Sul tema della tracciabilità dei movimenti del lavoratore all'interno dei luoghi di lavoro, la questione più controversa ed interessante la pongono quegli strumenti di registrazione degli accessi e delle presenze particolarmente invasivi, in quanto in grado di per sé di seguire costantemente il dipendente: si pensi ai badge con tecnologia Rfid (Radio-frequency identification)[218], alle *app* di localizzazione installate su smartphone o tablet e ai gps.

Le tecnologie Rfid, in particolare, installate sul badge ma anche su oggetti o etichette, consentono di individuare costantemente la posizione "geografica" di chi le detiene con gravi effetti sulla libertà di movimento e sulla dignità dei lavoratori, soprattutto se questi strumenti vengono liberati dai vincoli procedurali e finalistici di cui al comma 1 e fatti

---

[217] M.T. Salimbeni RIDL, 4/2015, 589 Secondo l'Autrice *sarebbe lecito il controllo su movimenti e accessi interni con impianti di rilevazione, anche audiovisivi, purché sussistano esigenze organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale che li giustifichino: si pensi all'ipotesi di aree in cui si producono materiali pericolosi accostabili soltanto da alcuni dipendenti appositamente attrezzati, o all'esigenza di tutelare la segretezza di determinati processi produttivi. Non occorrerebbe l'accordo con rsu/rsa o associazioni sindacali comparativamente più rappresentative: e in questo consisterebbe la disapplicazione (parziale) del primo comma*.

[218] Il Garante nel Provvedimento generale del 9 marzo 2005 precisa che "ove si intenda utilizzare tali tecniche per verificare accessi a luoghi di lavoro, o comunque sul luogo di lavoro, va tenuto conto che lo Statuto dei lavoratori vieta l'uso di impianti e apparecchiature pe finalità di controllo a distanza dell'attività dei lavoratori e, nel caso in cui il loro impiego risulti necessario per altre finalità, prescrive alcune garanzie (art. 4 L.300/1970; art. 114 del Codice) alle quali si affianca l'osservanza dei richiamati principi di necessità, finalità e proporzionalità del trattamento dei dati". Il chip Rfid consente la trasmissione di tutti i dati acquisiti tramite lettura magnetica del badge del singolo lavoratore, riguardanti non solo l'ingresso e l'uscita dal luogo di lavoro ma anche le sospensioni, i permessi, le pause *così realizzando in concreto, un controllo costante e a distanza circa l'osservanza da parte degli stessi (dipendenti) del loro obbligo di diligenza, sotto il profilo del rispetto dell'orario di lavoro, rientrante nella fattispecie prevista dal secondo comma dell'art. 4 L. n. 300/1970.* Si tratta per la Suprema Corte di strumento di controllo a distanza e non di mero rilevatore di presenza, *tenuto anche conto che il sistema in oggetto consente di comparare immediatamente i dati di tutti i dipendenti, realizzando così un controllo continuo, permanente e globale.* (Cass. sez. lav. 14/7/2017, n. 17531 e analogamente Cass. Sez. Lav. 13/5/2016 n. 9904).

rientrare nel comma 2 dell'art. 4 St. lav.[219]. L'insidia rappresentata da questi strumenti è che attraverso di essi si potrebbe realizzare un monitoraggio continuo sul prestatore: si renderebbero visionabili e controllabili tutti i dettagli del comportamento del singolo lavoratore, inclusa la sua prestazione e produttività, con possibili conseguenze disciplinari in caso di scarso rendimento.

Sul tema dell'utilizzo di applicativi e software per la rilevazione delle presenze è intervenuto in più occasioni il Garante per la protezione dei dati personali, che ha subordinato a due condizioni essenziali la legittimità di sistemi finalizzati alla rilevazione delle presenze, ma in grado di localizzare continuamente il dipendente o di accedere ad altre informazioni personali del lavoratore. Sia nel caso della tecnologia RFID inserita nel badge dei dipendenti che dell'installazione sullo smartphone privato dei dipendenti di un'applicazione con funzione di localizzazione geografica, la legittimità degli stessi è condizionata sia all'informazione data ai lavoratori sulle modalità di funzionamento del sistema con la piena consapevolezza del lavoratore nell'utilizzo dello stessa (in possesso di *user id* e *password*, poteva consapevolmente cliccare sull'icona ingresso e poi su quella uscita per indicare la fine della giornata lavorativa), che alla possibilità di raccogliere esclusivamente i dati relativi all'entrata o all'uscita del lavoratore e non dati ulteriori ed estranei rispetto alle finalità di gestione del rapporto di lavoro, senza alcun controllo sull'attività lavorativa o sui dati personali contenuti nello smartphone[220].

---

[219] A. Ingrao, *op. cit*. pag. 174-175. Nei magazzini Amazon la prestazione di coloro che controllano le merci in arrivo e le dispongono sugli scaffali e di coloro che si occupano dell'imballaggio è organizzata attraverso un lettore di codici a barre con GPS integrato che indica la posizione del lavoratore, il percorso per raccogliere i prodotti o quello da fare per raggiungere le scatole necessarie per l'imballaggio. E quale ulteriore evoluzione di questi codici a barre si profila all'orizzonte l'utilizzo del famigerato braccialetto indossato dai lavoratori. L'evoluzione del codice a barre è il braccialetto elettronico con trasmettitori ad ultrasuoni in grado di percepire e segnalare l'esatta posizione delle mani del lavoratore. Da segnalare che a Livorno è già in uso un braccialetto elettronico che permette all'azienda di controllare che gli operatori ecologici abbiano correttamente svuotato i cassonetti della spazzatura. V. anche R. Di Meo, *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *Labour Law Issues* n.1/2018

[220] Si veda in riferimento ai sistemi di rilevazione delle presenze, il provvedimento dell'8 settembre 2016, con il quale il Garante privacy ha accolto un'istanza di verifica preliminare, presentata da due società appartenenti ad un gruppo che si occupa di ricerca, selezione e somministrazione di lavoro a tempo determinato – Manpower - in ordine alla possibilità di richiedere ai propri dipendenti (impiegati presso altre ditte o che svolgono sistematicamente attività fuori sede) di installare una *app* sugli smartphone di loro proprietà, ai fini della rilevazione di inizio e fine dell'attività lavorativa. Il Garante ha prescritto alle società di perfezionare il sistema nella prospettiva della "privacy by design", applicando il principio di necessità, anche alla luce dei possibili errori nell'accuratezza dei sistemi di localizzazione, ferme restando una serie di accortezze da adottare (ad esempio, sullo schermo del telefonino dovrà risultare sempre ben visibile un'icona indicante che la funzione di localizzazione è attiva e l'applicazione dovrà essere configurata in modo tale da impedire il trattamento, anche accidentale, di altri dati contenuti nel dispositivo di proprietà del lavoratore). Il Garante afferma inequivocabilmente che *qualora lo strumento dovesse essere programmato in modo da recepire anche informazioni ultronee rispetto ad un utilizzo lecito, ebbene in tale ipotesi si ritiene che i dati raccolti dall'Azienda non siano utilizzabili contro il lavoratore proprio perché esorbitanti rispetto allo scopo, e dunque*

In più occasioni gli interventi del Garante sono venuti in soccorso per adattare e concretizzare nel contesto specifico delle relazioni di lavoro i principi introdotti nel nostro ordinamento dalla disciplina sulla privacy consentendo di avvicinare le due normative.

3.6 Il ruolo del Garante per la protezione dei dati personali tra Codice privacy e Statuto dei lavoratori

In molti dei suoi interventi e soprattutto nelle Linee Guida, il Garante per la protezione dei dati personali ha espresso la consapevolezza che l'acquisizione e il trattamento dei dati personali dei lavoratori attraverso strumenti informatici costituisca la maggiore minaccia per la loro riservatezza. Non è un caso che tra le prescrizioni deliberate dal Garante in materia di lavoro, quelle più note e applicate siano le Linee guida per l'utilizzo di internet e della posta elettronica adottate con deliberazione 1 marzo 2007, n. 13 (pubblicata in G.U. 10 marzo 2007)[221] e il Provvedimento in materia di videosorveglianza, 8 aprile 2010, (pubblicata in G.U. n. 99 29 aprile 2010).

In ossequio al carattere multilivello della tutela della riservatezza del lavoratore, le previsioni fissate dalla normativa generale devono integrarsi con la specificità delle regole e dei principi lavoristici ricavabili dalle norme statutarie, e questo avviene anche attraverso il "filtro" interpretativo elaborato dal Garante.

I limiti posti dal Garante al datore di lavoro con le prescrizioni delle linee guida operano su di un piano diverso da quello dello Statuto dei lavoratori, ma finiscono per interagire ed affiancarsi con quanto stabilito nell'articolo 4 St. lav.[222].

Le Linee guida forniscono concrete istruzioni operative ed esprimono una esigenza di coordinamento tra le norme generali e le garanzie del lavoro, rafforzano il quadro regolativo, integrando i presupposti di legittimità fissati dallo Statuto con il rispetto dei principi di necessità, correttezza, proporzionalità, pertinenza e non eccedenza in materia di protezione e trattamento dei dati personali.

---

non necessari e finalisticamente inammissibili perché utilizzati per una finalità di controllo non consentita dall'ordinamento.

[221] Il provvedimento recepisce le indicazioni espresse dal Gruppo di lavoro ex art. 29 nell'Opinion n. 8/2001, così sintetizzate*: ogni rilevazione, uso o memorizzazione di informazioni sui lavoratori con mezzi elettronici rientra nel campo di applicazione della legislazione di protezione dei dati e questo vale anche per il controllo, da parte del datore di lavoro, dell'accesso dei lavoratori alla posta elettronica o a Internet.*

[222] Sulla questione giuridica dell'efficacia generale e vincolatività delle Linee guida non vi è univocità interpretativa. Vedi tra gli altri L. Perina, *L'evoluzione della giurisprudenza e dei provvedimenti del Garante in materia di protezione dei dati personali dei lavoratori subordinati,* in *Riv.it. dir. lav*. 2/2010, 305 e P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *Riv.it. dir. lav*. 3/2009, 323.

Come si legge nelle premesse delle Linee guida per posta elettronica e internet, il Garante intende fornire indicazioni pratiche ed elementi di certezza per le aziende affinché la verifica del corretto utilizzo di internet e della posta elettronica da parte del dipendente possa dirsi rispettoso della normativa in materia di protezione dei dati personali.

Le indicazioni sono dunque ispirate ad un approccio empirico che tiene conto dei comportamenti abituali di gran parte dei lavoratori, che utilizza la comunicazione elettronica aziendale o l'accesso ad Internet anche per finalità private (il cyberlacking) e al tempo stesso delle esigenze datoriali. Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità del lavoratore, garantendo la protezione della sua sfera di riservatezza nelle relazioni personali e professionali, anche rispetto ad un uso moderato degli strumenti informatici per fini personali, ma in una cornice di reciproci diritti e doveri nella quale salvaguardare anche gli interessi datoriali ad un corretto uso delle risorse aziendali.

Il Garante della Privacy ha previsto che il datore di lavoro sia chiamato, nell'esercizio delle sue prerogative, a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri degli strumenti informatici e a minimizzare l'uso di dati riferibili ai lavoratori. Grava sul datore di lavoro l'onere di indicare chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. I trattamenti devono poi rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza dei principi di minimizzazione e di necessità del trattamento dei dati, per ridurre al minimo l'utilizzazione di dati personali e identificativi, e di pertinenza e non eccedenza per un esercizio graduale e proporzionato del controllo in relazione alle specifiche esigenze aziendali. Il datore dovrà prevenire con idonee misure organizzative e tecnologiche l'uso anomalo o abusivo degli strumenti, ancor prima di attivare la rilevazione dei comportamenti illeciti, al fine di limitare il trattamento dei dati del lavoratore, connesso al controllo sull'impiego degli strumenti elettronici, solo ove "necessario" e comunque "non oltre il necessario". Il Garante invita a prevenire con opportuni accorgimenti tecnici l'uso non autorizzato degli strumenti assegnati al dipendente, ad adottare "misure opportune" per prevenire l'accesso abusivo ad *internet*, così da limitare il ricorso a controlli successivi: i sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente, attraverso procedure di sovra-registrazione, i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria; in assenza di particolari esigenze tecniche o di sicurezza, la conservazione

temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario e predeterminato a raggiungerla; debbono essere applicati filtri che prevengano determinate operazioni ritenute inconferenti con l'attività lavorativa, l'*upload* o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato) o l'accesso a determinati siti inseriti in una sorta di *black list* di siti non consultabili in quanto considerati non correlati con la prestazione lavorativa; devono essere adottate tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi dei lavoratori (c.d. privacy enhancing technologies– PETs) così che il trattamento di dati avvenga in forma anonima ed aggregata allo scopo di conciliare le esigenze di monitoraggio e manutenzione del sistema internet con la segretezza dei singoli accessi operati dai lavoratori.

Considerato che rispetto alle tradizionali apparecchiature di sorveglianza, quelle informatiche permettono una pluralità di "trattamenti ulteriori" senza la piena consapevolezza dei lavoratori, si determina un preciso obbligo di protezione a carico del datore, responsabile della corretta informazione e di ogni azione preventiva a salvaguardia della riservatezza dei dipendenti. A questo fine il Garante suggerisce l'adozione di un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente e da sottoporre ad aggiornamento periodico: una *policy* interna contenente le norme sul corretto utilizzo del sistema informatico aziendale in cui vengano indicate chiaramente quali siano le modalità di uso degli strumenti messi a disposizione ritenute corrette, la misura dell'utilizzo per ragioni personali di servizi di posta elettronica di Internet consentito al lavoratore, e se, in che misura e con quali modalità, vengono effettuati dei controlli, nonché le conseguenze, anche di tipo disciplinare, che il datore di lavoro si riserva di trarre qualora constati un indebito utilizzo delle risorse informatiche. La frequente impossibilità di tenere distinta attività lavorativa e attività non lavorativa, per un verso, e l'irragionevolezza di un divieto assoluto di impiego di internet e della posta elettronica per esigenze personali durante l'orario di lavoro, per l'altro, impone di procedere ad una puntuale informazione del lavoratore. La prospettiva prevenzionistica intorno alla quale oggi ruota il Regolamento europeo, era già prevista sotto il profilo organizzativo, nel momento in cui si prevedeva che prima di procedere all'installazione delle apparecchiature informatiche si valutasse "l'impatto sui diritti dei lavoratori" e si configurassero filtri per non consentire all'azienda di raccogliere informazioni inconferenti rispetto allo scopo. Al datore si richiede di privilegiare gli interventi di prevenzione rispetto a quelli repressivi e,

solo quando i primi abbiano fallito, è ammesso il controllo (successivo) nelle forme stabilite dalla normativa statutaria.

Con riferimento alla posta elettronica, l'uso dell'account di posta elettronica aziendale espone la privacy del lavoratore in modo particolare, poiché la corrispondenza può contenere anche messaggi di tipo personale: con riguardo al contenuto dei messaggi, ai dati esteriori e agli eventuali allegati, si dovrà tener conto della garanzia costituzionale di segretezza della corrispondenza (artt. 2 e 15 Cost.) e della tutela penale dell'inviolabilità dei segreti (art. 616, comma 4, c.p.) [223].

Il Garante ha recepito le raccomandazioni comunitarie con riguardo alla predisposizione di indirizzi di posta condivisi fra più lavoratori, e suggerito di impiegare tutti quegli accorgimenti volti, da un lato, ad esplicitare al lavoratore la natura non personale della corrispondenza elettronica e dall'altro a consentire al datore di accedere al contenuto della corrispondenza del lavoratore garantendo a quest'ultimo la possibilità di preservare i dati personali che potrebbero nella stessa reperirsi, magari dotando il lavoratore oltre che di un indirizzo di "servizio" anche di un indirizzo per uso personale. Si invitano i datori a predisporre dei meccanismi di risposta automatica in caso di assenza del lavoratore con segnalazione dell'indirizzo di altro dipendente a cui rivolgersi, oppure a consentire al lavoratore di delegare un collega per verificare il contenuto dei messaggi e inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa, o inserire un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi [224].

Nel Provvedimento in materia di videosorveglianza il Garante conferma il divieto di utilizzare sistemi di videosorveglianza per il controllo a distanza dei lavoratori, di effettuare riprese al fine di verificare l'osservanza dei doveri di diligenza, il rispetto dell'orario di

[223] Il Gruppo di lavoro *ex* articolo 29 aveva elaborato una lista di attività in grado di determinare elevati rischi per i diritti e le libertà degli individui, tra cui il controllo sistematico e il coinvolgimento di soggetti "vulnerabili" che richiedevano una valutazione di impatto. Nel rapporto di lavoro tale valutazione sarà necessaria non solo in presenza di trattamenti automatizzati o algoritmici, ma tutte le volte in cui il controllo delle attività includa la postazione del lavoratore o la sua attività su internet. Si identifica il rischio di violazione dei diritti fondamentali del lavoratore nelle attività di analisi, ricostruzione dell'attività attraverso i *log file* fino alla profilazione consentita dai sistemi informatici e per la quale si richiedono particolari cautele e tutele.

[224] Si veda in proposito Cass. Pen. Sez. 5, 31/3/2016, n. 13057, dove si afferma che qualora "siano attivate caselle di posta elettronica – protette da password personalizzate – a nome di uno specifico dipendente, quelle "caselle" rappresentano il domicilio informatico proprio del dipendente, sicché l'accesso abusivo alle stesse, da parte di chiunque (quindi, anche da parte del superiore gerarchico), integra il reato di cui all'art. 615/ter cod. pen. […]. La casella rappresenta uno "spazio" a disposizione – in via esclusiva – della persona, sicché la sua invasione costituisce, al contempo, lesione della riservatezza". Inoltre, l'assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

lavoro (ad esempio orientando la telecamera sul *badge*) e la correttezza nell'esecuzione della prestazione lavorativa.

La conservazione delle immagini è consentita per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato del personale, comunque non inferiore a sei mesi, e si prescrivono precise indicazioni sulla localizzazione delle telecamere e sulle modalità di ripresa. Nel rispetto dei richiamati principi di necessità, proporzionalità e finalità, occorre evitare riprese particolareggiate nei casi in cui le stesse non siano indispensabili in relazione alle finalità perseguite e il titolare del trattamento dovrà garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati.

A causa della complessità della materia e dell'alta conflittualità, le linee guida emesse dall'Autorità Garante si sono dimostrate un efficace strumento di indirizzo per le imprese, incentivate a fornirsi di specifici regolamenti atti a definire in maniera chiara e preventiva la politica aziendale in materia, e per i dipendenti resi consapevoli dei propri diritti e delle limitazioni in vigore.

3.6.1 Segue: Alcune decisioni dell'Autorità Garante per la protezione dei dati personale

L'Autorità Garante è intervenuta in diverse occasioni in merito all'uso degli strumenti informatici e al conseguente trattamento dei dati personali dei lavoratori: si è espressa, in particolare, sul ricorso a software che consentono un controllo indiretto e continuativo del lavoratore attraverso la memorizzazione delle pagine internet visitate, sull'insidiosa distinzione fra strumenti di lavoro e strumenti di controllo e sull'uso di apparecchiature che consentono la localizzazione continua del dipendente. In queste occasioni ha contribuito a chiarire alcuni degli aspetti più problematici, realizzando di fatto il coordinamento e l'integrazione fra disciplina generale in materia di protezione dei dati personali e disciplina speciale relativa ai rapporti di lavoro.

Per quanto riguarda il primo tema il Garante si è espresso in più di un'occasione nel senso dell'illiceità delle operazioni di controllo attraverso software che operano in background, con modalità non percepibili dall'utente, e realizzano un monitoraggio e tracciatura massivi, prolungato nel tempo, condotto in modo sistematico ed anelastico e con una conservazione dei dati per un arco temporale troppo ampio. Sono questi, afferma il Garante, sistemi di controllo "in contrasto col divieto legislativo posto dalla disciplina tanto previgente quanto

vigente" e ne consegue che il dato trattato in violazione della normativa privacy, senza il rispetto dei principi del Codice e delle modalità di trattamento dei dati stessi, è inutilizzabile (art. 11, comma 2 Codice Privacy).

Con provvedimento del 2 aprile 2009 doc. web n. 1606053, il Garante si è pronunciato in senso contrario all'utilizzo di un software, denominato *Squid*, idoneo alla registrazione dei *file log* di navigazione web, ritenendo che l'installazione del software con funzionalità appositamente configurate per il tracciamento sistematico e continuativo degli accessi ad Internet del dipendente e con la conseguente memorizzazione di tutte le pagine web visualizzate dallo stesso, violi l'art. 4 St. lav., ancor più in assenza di procedure codeterminative o autorizzazione[225].

Particolarmente articolato il provvedimento con il quale il Garante ha dichiarato illegittimo il controllo esercitato da parte dell'Istituto Poligrafico sulla navigazione *web*, posta elettronica e dati del traffico telefonico dei propri dipendenti. Quanto al primo, posto in essere attraverso il software *Websense*, oltre a consentire il filtraggio della navigazione su siti non attinenti allo svolgimento dell'attività lavorativa, permetteva di registrare sistematicamente e memorizzare per un anno ogni accesso e tentativo di accesso a siti internet effettuato da ciascun lavoratore. *Websense* inoltre categorizzava le pagine visitate da ogni dipendente, raggruppandole in una molteplicità di classi predefinite (*entertainment*, *vehicles*, *marketing*, *sex*, etc.) per poi generare un *report* individuale: l'attivazione di questa funzione è stata dichiarata dal Garante contraria all'art. 8 St. lav., in quanto permetteva al datore di lavoro di acquisire, mediante non consentite indagini, dati personali e sensibili del prestatore di lavoro. Sul versante del diritto alla protezione dei dati personali, la creazione di *report* individuali costituiva profilazione dell'utente e, come tale, avrebbe dovuto formare oggetto d'informativa *ad hoc*, di notificazione al Garante ed essere espressamente accettata dall'interessato. Adempimenti questi che nel caso di specie difettavano integralmente.

Le censure del Garante relative alla posta elettronica attenevano all'archiviazione delle *email* sul *server* aziendale per periodi giudicati più lunghi del necessario (da 6 mesi ad 1 anno) e alla possibilità, per soggetti non identificati a priori, di visualizzare "in chiaro" tali messaggi.

Infine, l'Istituto utilizzava, in assenza di provvedimento sindacale e di informativa ai lavoratori, un s*oftware VoIP* di analisi del traffico telefonico che registrava i dettagli delle

[225] Già in un provvedimento del 2 febbraio 2006 il Garante aveva affermato che per poter contestare l'indebito utilizzo dei beni aziendali è sufficiente verificare il numero di accessi ad Internet ed i tempi di connessione senza necessità di esaminare il contenuto dei siti visitati, cosa quest'ultima che rende il trattamento dei dati sproporzionato, non rispondente ai principi della minimizzazione e della non eccedenza.

chiamate in uscita di ciascun dipendente senza indicarne la finalità e i tempi conservazione e con una funzione *alert* che inviava una *email* ad un indirizzo definito dal datore in presenza di chiamate verso numeri esterni preimpostati. Il Garante aveva inquadrato l'*alert* come strumento di controllo vietato ai sensi dell'art. 4, co. 1, St. lav.: la sua installazione non era giustificabile se non con l'intenzione esclusiva del datore di controllare il lavoratore e, quindi, ne aveva disposto la disattivazione immediata[226]. Si tratta di violazioni che comportano l'inutilizzabilità dei dati raccolti *ex* art. 11, d.lgs. n. 196/2003.

Tra i provvedimenti più recenti merita di essere segnalata la decisione n. 303 del 13 luglio 2016 nella quale il Garante ha ritenuto illecito l'utilizzo di software che consentono operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminate degli accessi ad Internet o al servizio di posta elettronica, in background e in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore, ossia senza alcun impatto o interferenza sul lavoro del dipendente. Nell'occasione il Garante ha negato la legittimità di apparati e programmi informatici che effettuino una verifica continua e indistinta degli accessi a internet e all'email, operanti con modalità non percepibili dall'utente e ha precisato che internet e posta elettronica non sempre si configuravano come strumenti utilizzati per rendere la prestazione[227].

Il secondo tema attiene all'individuazione dello strumento utilizzato per rendere la prestazione, ai fini dell'applicazione dell'art. 4, comma 2: la questione ha recentemente interessato il *call center* di Sky Italia Network Service S.r.l., (decisione 8 marzo 2018 doc web n.8163433). Nell'occasione il Garante ha dichiarato illecito, ai sensi dell'art. 4 St. lav. e della normativa in materia di *privacy*, un *software* che gestiva le chiamate degli abbonati, con la conseguente inutilizzabilità dei dati trattati in violazione di legge. Alla base della

---

[226] La Corte dichiarava la violazione dell'art. 4, co. 2, St. lav. discostandosi dal Garante.
A. Ingrao, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, in Ridl 2/2017. Nel caso di specie, infatti, il datore di lavoro valorizzava le esigenze difensive, per giustificare ex ante la legittimità dell'installazione degli strumenti di controllo e non, invece, per utilizzarne gli esiti come materiale probatorio a supporto di un licenziamento disciplinare.

[227] È rilevante verificare se l'accesso ad internet e la posta elettronica siano ricompresi tra gli strumenti utilizzati per rendere la prestazione lavorativa e per questo esclusi dal campo di applicazione del co. 1 dell'art. 4 St. Lav., installati liberamente senza vincoli sindacali o amministrativi, o se per le mansioni svolte non lo sono. Nel caso di specie il software, utilizzato per il controllo della navigazione *web* e della posta elettronica istituzionale dei dipendenti di una Università, non può essere considerato strumento utilizzato dal lavoratore per rendere la prestazione lavorativa, o applicativo strettamente funzionale alla prestazione lavorativa, anche sotto il profilo della sicurezza (ai sensi e per gli effetti dell´art. 4, comma 2), ne consegue che il trattamento è illecito per essere stato esercitato in violazione dei principi di liceità e correttezza, di necessità, pertinenza e non eccedenza e dell'obbligo di informativa degli interessati e i dati sono inutilizzabili.
Altre decisioni sul tema approfondiscono il principio: Provv. n. 139 del 7 aprile 2011, doc. web n. 1812154 *Vietato il trattamento di dati personali del dipendente ricavati da file e documenti acquisiti nell'ambito di operazioni di backup effettuate sul server aziendale*; Provv. n. 308 del 21 luglio 2011, doc. web n. 1829641 *Il Garante privacy al Poligrafico: più tutele per i lavoratori*; Provv. 23 dicembre 2010, doc. web n. 1786116.

decisione vi è la constatazione che il sistema non si limitava a consentire la mera associazione tra la chiamata e l'anagrafica del cliente per facilitare l'attività di gestione della richiesta, come se si trattasse di un mero archivio informatico dei rapporti con la clientela, ma consentiva "ulteriori elaborazioni", tra cui la memorizzazione di dati personali degli operatori, e di *report* relativi all'attività telefonica in generale. La registrazione di queste informazioni consentiva di ricostruire, anche indirettamente, l'attività effettuata dagli operatori. Il sistema risultava quindi "idoneo a realizzare un controllo, anche solo potenziale e in via indiretta, dell'attività lavorativa" e non poteva qualificarsi come uno strumento utilizzato dal lavoratore per rendere la prestazione lavorativa, ai sensi dell'art. 4 comma 2. Piuttosto, veniva fatto rientrare tra quegli strumenti organizzativi dai quali può indirettamente derivare il controllo a distanza dell'attività dei lavoratori, con conseguente necessità di attivare le procedure previste dall'art. 4 comma 1. La decisione è motivata dal fatto che le finalità che la società intende perseguire nel caso concreto sono riconducibili ad esigenze organizzative e produttive, ma non risultano essere state attivate le garanzie procedurali prescritte dalla legge e nessun accordo sindacale in relazione all'applicativo è stato stipulato[228].

Ad analoghe conclusioni è giunto il Garante nel caso del sistema di gestione delle attese allo sportello adottato da Poste Italiane, con il Provvedimento 479 del 16 novembre 2017 (doc. web n. 7355533), *Trattamento di dati personali mediante un sistema utilizzato per la gestione delle attese allo sportello.* È emerso come il sistema "Gestore attese" fosse dotato di funzionalità che permettevano oltre alla visualizzazione del nominativo del dipendente sul display di Sportello e di Sala Consulenza, la visualizzazione e il controllo in tempo reale di una serie di dati, tra cui in particolare il tempo medio di gestione delle diverse tipologie di operazioni, con la possibilità di estrapolare *reports* riferiti ai singoli operatori nominativamente individuati, e di accedere in tempo reale e in via continuativa ai dati su base individuale relativi a tutte le postazioni e a tutti gli operatori in servizio in un dato momento presso un determinato ufficio. Il sistema non configurandosi come strumento utilizzato per rendere la prestazione lavorativa (art. 4, comma 2, l. n. 300/1970) e non essendo nella disponibilità del singolo operatore, rientrava in quegli strumenti rispondenti a finalità organizzative, dai quali può indirettamente derivare il controllo a distanza

[228] A. Trojsi, *op. cit.* Si veda anche la circolare n. 4 del 26/7/2017 dell'Ispettorato nazionale del lavoro, *Indicazioni operative sull'istallazione e utilizzazione di strumenti di supporto all'attività operativa ordinaria dei Call Center*, dove si parla di sistemi, che ancorché non idonei a effettuare controlli diretti, sono comunque atti a realizzare un più generale monitoraggio dell'attività telefonica.

dell'attività dei lavoratori, con conseguente necessità di attivare le procedure previste dalle disposizioni statutarie. In assenza della dovuta informativa ai dipendenti e senza la stipula di specifico accordo con le parti sindacali, il Garante ha ritenuto il conseguente trattamento di dati illecito e sproporzionato, con la conseguente inutilizzabilità dei dati trattati in violazione di legge.

Rispetto alla terza grande questione che ha interessato il Garante, ossia la legittimità dell'utilizzo di dispositivi che consentono la localizzazione dei dipendenti, l'Autorità ha prescritto a tutela della riservatezza dei dipendenti una serie di accorgimenti e di stringenti misure di sicurezza alle quali ha subordinato la possibilità di utilizzo degli strumenti di geolocalizzazione.

Con un recentissimo provvedimento n. 232 del 18 aprile 2018, *Verifica preliminare. Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali*[229], il Garante si è pronunciato a favore dell'installazione su dispositivi smartphone o tablet di un sistema di geolocalizzazione (c.d. NavNet), prevedendo però una serie di accorgimenti e cautele. Tra le altre si indicano: configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva e consentire la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa; configurare il sistema in modo da oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore; individuare profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili; individuare i tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite; predisporre periodiche verifiche e test sulla funzionalità del sistema e la conseguente predisposizione di correttivi a tutela della qualità dei dati trattati[230].

[229] Sicuritalia S.p.A. ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in relazione al trattamento dei dati personali connesso alla prospettata installazione dell'applicazione NavNet, completa di funzionalità di localizzazione geografica, sui dispositivi smartphone o tablet consegnati alle guardie giurate incaricate di effettuare i servizi di vigilanza forniti dalla società.

[230] Si veda anche la decisione 8 settembre 2016 n. 350 [5497522] (verifica preliminare richiesta dalla società Manpower srl) relativa ad un sistema di rilevazione delle presenze del personale attraverso una *app* installata sullo *smartphone* di proprietà del lavoratore, che trasmette all'azienda la localizzazione del lavoratore all'interno della struttura aziendale, si è espresso a favore dell'uso dell'*app*, a precise condizioni. La società dovrà impegnarsi a cancellare il dato relativo alla posizione del lavoratore, avendo verificato preventivamente l'associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore, conservando, eventualmente, il solo dato relativo alla predetta sede di lavoro, alla data e all'orario cui si riferisce la timbratura; a configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona ben visibile che indichi che la funzionalità di localizzazione è attiva e ad adottare specifiche misure idonee a garantire che l'applicativo installato sul dispositivo del dipendente non possa effettuare trattamenti di dati ultronei, dati relativi al traffico telefonico, agli sms, alla posta elettronica o alla navigazione in internet o altro contenuto dello smartphone, ma limitarsi alle informazioni di geolocalizzazione, impedendo l'accesso ad altri dati.

Infine, merita un cenno un tema di grande attualità come quello dei profili reputazionali sul web, di cui il Garante si è occupato nel provvedimento n. 488 del 24 novembre 2016, *Piattaforma web per l'elaborazione di profili reputazionali*. Il provvedimento del Garante si occupa per la prima volta di un sistema tecnologico finalizzato a fornire, a partire dall'analisi dei dati, elementi di conoscenza dei singoli individui tramite una sintesi espressa da un punteggio*:* il Garante interdice il calcolo del rating reputazionale dei soggetti interessati mettendo in evidenza i rischi e le criticità che un simile trattamento comporta dal punto di vista del Codice Privacy. In generale si esprimono perplessità sull'opportunità stessa di rimettere a un sistema automatizzato ogni determinazione in merito ad aspetti particolarmente delicati e complessi, quali quelli connessi alla reputazione dei soggetti coinvolti. A prescindere dall'oggettiva difficoltà di misurare situazioni, parametri e variabili non sempre classificabili o quantificabili, occorre evidenziare che la suddetta (acritica) valutazione potrebbe fondarsi su atti, documenti o certificati viziati *ex ante* da falsità ideologica, ovvero caratterizzati da alterazioni materiali non facilmente riscontrabili da parte di pur esperti "consulenti" reputazionali. Il rischio, neanche tanto remoto, è quello di creare profili reputazionali inesatti e non rispondenti alla reale rappresentazione e, quindi, all'identità personale, intesa anche quale immagine sociale dei soggetti presi in esame (art. 2 del Codice; Provv. 9 marzo 2006 (doc. web n.1269316); Trib. Roma 7 dicembre 2015)[231]. Come ribadito anche in questa sede dal Garante, dignità e identità personale compongono il fondamento valoriale della normativa per il trattamento dei dati, ma assumono una specifica e ulteriore rilevanza all'interno della relazione di lavoro, dove sono minacciate dalle nuove

Il Garante per la privacy si è occupato di rilevazione delle presenze tramite l'utilizzo dei sistemi biometrici, che consentono, con l'impiego di specifici software ed apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare e ha previsto rispetto a questi sistemi ulteriori cautele e limitazioni all'utilizzo.

[231] Il Garante ha dichiarato illecito e contrario a numerose disposizioni del Codice della privacy il trattamento dati connesso ai servizi della "Infrastruttura immateriale Mevaluate per la qualificazione reputazionale", una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti le persone fisiche e giuridiche.

Il progetto di piattaforma sottoposto al vaglio dell'Autorità era volto a predisporre un servizio a pagamento avente ad oggetto sia la creazione di profili reputazionali a favore degli utenti interessati, che la creazione di profili «contro terzi», attraverso il caricamento di documenti concernenti aspetti personali e professionali. A tali documenti, valutati da appositi "consulenti" al fine di garantirne genuinità e integrità, sarebbe stato applicato un algoritmo matematico, in grado di generare un "rating reputazionale" per ogni interessato espressivo sia dell'affidabilità generale che di quella riferita a singoli settori (penale, civile, fiscale lavoro e impegno civile, studi e formazione). Il Garante ha riscontrato significative violazioni ai principi e alle regole del Codice Privacy e rilevanti rischi per la dignità e l'identità personale dei soggetti sottoposti a profilazione dichiarando pertanto illecita la realizzazione della piattaforma e il connesso trattamento dei dati. Le valutazioni e classificazioni cui Mevaluate è finalizzata sono infatti in grado di condizionare la proiezione sociale di un individuo, in considerazione sia della limitata qualità dei dati di partenza che della "oggettiva difficoltà di misurare situazioni, parametri e variabili, come anzitutto la reputazion, non sempre agevolmente classificabili o quantificabili" (punto 2.5 ultimo cpv).

tecniche di profilazione e di trattamento automatizzato che mettono in pericolo il diritto al controllo sulle informazioni (c.d. auto-determinazione informativa). L'immagine del lavoratore, costruita attraverso metodi di raccolta ed elaborazione automatica dei dati, può violare la dignità e l'identità personale e condizionare il diritto al lavoro.

A differenza della tutela della dignità che orienta larga parte dell'ordinamento giuslavoristico, la protezione dell'identità personale non ha fino ad ora assunto un autonomo ambito di affermazione a vantaggio dell'individuo coinvolto in un rapporto di lavoro e dovrà essere considerata adeguatamente in futuro[232].

[232] Si veda sul tema l'analisi di A. Donini, *Tecniche avanzate di analisi dei dati e protezione dei lavoratori,* in *Diritto delle Relazioni Industriali*, fasc.1/2018, 222.

Capitolo 4 L'utilizzabilità dei dati nell'ambito del rapporto di lavoro: limiti e tutele

Avrebbero potuto analizzare e mettere su carta, nei minimi particolari, tutto quello che s'era fatto, s'era detto e s'era pensato; ma l'intimità del cuore, il cui lavoro è in gran parte un mistero anche per chi lo possiede, restava imprendibile.

G. Orwell, *1984*

E se oggi, più di venti anni fa, la protezione dei dati è condizione necessaria per la libertà e per la democrazia, è anche e soprattutto perché la nostra più effettiva e reale dimensione di vita è, paradossalmente, quella digitale: densa di straordinarie e impensabili opportunità, ma anche di insidie, rispetto alle quali siamo sempre più esposti.

Antonello Soro

4.1 L'utilizzabilità dei dati acquisiti attraverso il controllo a distanza: dalle ambiguità statutarie alla novella del 2015

Il vero nodo problematico della disciplina emerge quando il focus si sposta dal momento statico del controllo a quello dell'utilizzazione delle risultanze dello stesso e attiene alle condizioni e ai limiti di utilizzabilità delle informazioni raccolte dal datore di lavoro.

Nella precedente formulazione dell'art. 4 St. lav. la norma si limitava a disciplinare il momento dell'installazione degli strumenti di controllo, mentre taceva sul momento successivo, sull'utilizzabilità delle informazioni acquisite e sui suoi limiti.

Come ci ricordava Massimo D'Antona, *il divieto di controllo a distanza si preoccupa esclusivamente di "come" le informazioni vengono acquisite e vuole evitare che quel "come" sia offensivo della dignità del lavoratore. Ma non vieta che una pluralità di informazioni sul lavoratore, acquisite non illegittimamente ma memorizzate a sua insaputa,*

vengano combinate e raccolte in un archivio elettronico, in una banca dati, e all'occorrenza elaborate ed utilizzate a sua pregiudizio e senza diritto di contraddittorio[233].

L'(in)utilizzabilità delle informazioni acquisite attraverso il controllo, definito preterintenzionale, è stata considerata *la maggiore aporia del modello statutario*[234]. La norma taceva sull'utilizzabilità dei dati raccolti da strumenti di controllo a distanza il cui impiego era stato autorizzato per finalità diverse e questo alimentava incertezze ed ambiguità interpretative in ordine all'utilizzabilità degli stessi, soprattutto per fini disciplinari[235]. Appariva pacifico che non si sarebbero potute utilizzare le prove sull'eventuale comportamento illecito del lavoratore, raccolte attraverso una forma di sorveglianza illegittima, ma che fare delle informazioni acquisite dagli impianti e dalle apparecchiature autorizzate per finalità organizzative o delle immagini riprese da una telecamera installata per ragioni di sicurezza e che mostrano un lavoratore in flagranza di illecito? Il datore di lavoro doveva far finta di ignorarlo perché lo strumento attraverso il quale lo aveva rilevato era stato autorizzato a fini diversi?

Erano evidenti le contraddizioni e le difficoltà applicative di una simile conclusione, tanto che per uscire dall'*impasse* la giurisprudenza, facendo da cassa di risonanza all'ambiguità normativa, aveva elaborato la categoria dei controlli difensivi (a loro volta controversi), operanti al di fuori della procedura del comma 2 art. 4 St. lav. (vecchio testo) per tutelare l'azienda rispetto a condotte illecite dei suoi dipendenti, aprendo così all'utilizzabilità dei dati derivanti dal controllo "involontario".

Secondo la maggior parte degli interpreti dal divieto espresso di controlli a distanza, stabilito dall'originaria versione statutaria, discendeva quale corollario che le informazioni acquisite mediante impianti autorizzati ad altri fini non avrebbero potuto essere utilizzate per sanzionare eventuali inadempimenti, essendo l'autorizzazione riferita esclusivamente ad esigenze tecnico organizzative o di sicurezza del lavoro. Anche dati legittimamente acquisiti dovevano essere considerati inutilizzabili per finalità differenti da quelle di tutela dell'interesse che ne condizionava la legittimità dell'acquisizione. La tesi dell'inutilizzabilità per eccedenza dei fini delle informazioni raccolte attraverso controlli

[233] M. D'Antona, *Dibattito,* in R. De Luca Tamajo, R. Imperiali D'Afflitto, C. Pisani, R. Romei, *op. cit.*, 208-209.

[234] V. Nuzzo, *op. cit.*, 90.

[235] A. Maresca evidenzia l'ambivalenza del vecchio art. 4 *che, com'è noto, alimentava non poche incertezze applicative in ordine all'utilizzabilità dei dati derivanti dal controllo, potendosi ritenere che alla legittimità di tale controllo conseguisse ineluttabilmente la facoltà del datore di lavoro di avvalersene, ma anche, all'opposto che, il limite stabilito dal legislatore del 1970 ai controlli a distanza in funzione di «esigenze organizzative e produttive» o dettate «dalla sicurezza del lavoro» operasse pure con riferimento all'utilizzo dei dati acquisiti. La questione si può ritenere oggi risolta con il co. 3 dell'art. 4.* (Maresca, *op. cit*., 512).

preterintenzionali legittimi si fondava sulla *ratio* del divieto di controlli a distanza e trovava conferma nel fatto che gli stessi accordi sindacali spesso contenevano clausole d'inutilizzabilità a fini disciplinari dei dati legittimamente raccolti dal datore di lavoro nell'esercizio del proprio potere[236].

A causa dell'ambiguità normativa trovava spazio anche l'opinione secondo la quale il datore poteva utilizzare i dati per fini estranei rispetto alle esigenze aziendali che avevano giustificato a monte l'installazione degli strumenti di controllo: le ragioni aziendali tipizzate dal legislatore condizionavano l'autorizzazione all'installazione dell'impianto, ma non limitavano le potenzialità del controllo preterintenzionale ed il successivo trattamento dei dati raccolti per finalità connesse al rapporto di lavoro. E si argomentava *a contrario* facendo riferimento alle stesse restrizioni di utilizzo a fini disciplinari divenute usuali negli accordi sindacali, che, secondo questo orientamento interpretativo, costituivano deroghe al generale principio di utilizzabilità delle informazioni, ricavabile dal testo previgente dell'art. 4, comma 2, St. lav.[237].

---

[236] In questo senso M. Barbieri secondo il quale c'era poco spazio per le incertezze: *La situazione previgente era tutto sommato abbastanza chiara: i dati acquisiti legittimamente erano utilizzabili per le finalità per le quali era legittimo raccoglierli e trattarli; in difetto della legittimità della raccolta e del trattamento, anche solo per eccedenza dai fini, non erano utilizzabili. Legittimità della raccolta e del trattamento e utilizzabilità dei dati erano insomma funzionalmente e inderogabilmente collegate.* (M. Barbieri, in P. Tullini, (a cura di) *op. cit.*, 191). Analogamente P. Lambertucci, a parere del quale *la vecchia disposizione conteneva anche un divieto assoluto di utilizzabilità dei dati raccolti mediante impianti legittimamente installati ai fini del rapporto di lavoro, trovando conferma tale argomentazione nel fatto che gli stessi provvedimenti autorizzativi precludevano tale facoltà di utilizzo dei dati.* E ancora: *le rilevazioni devono essere effettuate in coerenza con le legittime finalità dell'impiego di tali strumenti, cioè per soddisfare esigenze organizzative, produttive o attinenti alla sicurezza del lavoro, restando fermo che* […] *l'utilizzazione, anche casuale, dell'impianto per finalità di controllo dei lavoratori deve considerarsi sempre illegittima.* (P. Lambertucci, *op. cit.*, 8). M.T. Salimbeni considera *forzata un'interpretazione evolutiva dell'articolo 4, che ha riconosciuto la legittimità dell'uso dei dati ricavati dagli strumenti informatici di lavoro per controllare illeciti del dipendente, anche contrattuali* (*op. cit*., 597).
Scettico invece R. Del Punta che denuncia l'ipocrisia di un'interpretazione fedele al testo della norma: *dalla norma sarebbe stato lecito desumere, quindi, l'assoluta inutilizzabilità delle informazioni raccolte con la modalità a distanza*. *Da cui la giustificazione delle clausole che esplicitavano tale inutilizzabilità, contenute in taluni accordi sindacali e, di regola, nei provvedimenti autorizzativi delle DTL. Ma la dose di ipocrisia stava, nel contempo, nel far finta di credere che questo regime potesse reggere al lume di un pur misurato realismo. Nel ritenere possibile, insomma, che il datore di lavoro che avesse sorpreso il lavoratore intento a sottrarre materiale aziendale, potesse fingere di non averlo visto e rinunciare a perseguirlo sul piano disciplinare*. Secondo Del Punta il *punto di vista radicale dell'inutilizzabilità delle informazioni raccolte era sempre meno sostenibile alla luce degli sviluppi giurisprudenziali nonché del buon senso* (R. Del Punta, *op. cit.,* 77).
[237] Questa è la ricostruzione di M. Marazza: *è proprio il contenuto di quei provvedimenti che confermava l'utilizzabilità dei dati e giustificava, di conseguenza, la specificazione di misure restrittive dei poteri datoriali che altrimenti la norma avrebbe consentito* (M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in W. P. CSDLE "Massimo D'Antona", 2016, 15). In senso favorevole all'utilizzo anche disciplinare delle informazioni raccolte mediante impianti di controllo legittimamente autorizzati e installati ma per finalità diverse, si veda anche Cass. 23 febbraio 2010, n. 4375. La stessa soluzione era già stata indirettamente ammessa da Cass., 17 luglio 2007, n. 15892 e Cass. 22 marzo 2011, n. 6498 che consente l'utilizzo a fini disciplinari di immagini registrate da videocamere installate

Il legislatore del 2015, con il comma 3 del novellato art. 4 St. lav., intende far calare il sipario sulle incertezze interpretative emerse e chiarire definitivamente che le informazioni acquisite attraverso il controllo a distanza, sia con gli strumenti di controllo che attraverso gli strumenti utilizzati per rendere la prestazione o per registrare gli accessi e le presenze, sono utilizzabili a tutti i fini connessi al rapporto di lavoro, per qualsiasi atto di gestione del rapporto stesso, certamente a fini disciplinari, ma anche per valutazioni di rendimento e produttività del lavoratore, a fini retributivi e premiali. Il legislatore circonda però di tre ordini di limiti l'utilizzabilità dei dati: si deve trattare di informazioni legittimamente acquisite nel rispetto dei primi due commi dell'art. 4 St. lav., il lavoratore deve essere stato informato adeguatamente circa le modalità di uso degli strumenti e l'effettuazione dei controlli, e infine le informazioni devono essere raccolte e trattate nel rispetto di quanto disposto dal D.lgs. 196/2003, dalla disciplina posta a protezione dei dati personali, che oggi trova il suo riferimento nel Regolamento UE 2016/679[238].

La novella ha inteso distinguere il momento della raccolta da quello della eventuale, successiva utilizzazione dei dati raccolti, legittimando per precise finalità la prima e subordinando a specifiche condizioni la seconda[239].

Giampiero Proia individua nella raccolta e nell'utilizzo dei dati operazioni concettualmente e materialmente distinte, che prefigurano autonome e distinte operazioni di trattamento di dati, a loro volta disciplinate da limiti e condizioni diverse: la raccolta di informazioni è consentita se deriva dall'impiego di strumenti legittimamente installati in azienda o utilizzati

---

legittimamente per finalità di protezione dei lavoratori, senza che l'accordo sindacale prevedesse l'utilizzo a fini disciplinari.

Si segnala che dopo la novella dell'art. 4 St. lav. nei moduli predisposti dall'Ispettorato Nazionale del Lavoro per chiedere l'autorizzazione all'installazione degli impianti e degli strumenti, non è prevista la preclusione all'utilizzabilità delle informazioni raccolte per finalità disciplinari. Si viene a creare così una disparità rispetto agli accordi sindacali, dove la clausola di inutilizzabilità può ancora essere inserita, rappresentando gli accordi sindacali uno scambio di volontà fra soggetti privati nell'esercizio della rispettiva autonomia negoziale. Si indurrebbe così il datore di lavoro a preferire l'autorizzazione amministrativa (A. Ingrao, *op.cit*., 205). V. anche Maresca, *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, in *Ipsoa* quotidiano, 22/2/2016.

[238] A parere di M. Marazza la nuova formulazione del terzo comma apre prospettive che vanno ben oltre l'esercizio del potere disciplinare e la gestione delle politiche premiali. *Basti considerare, del resto, all'impatto che il novellato art. 4 della legge n. 300/1970 può assumere, applicato unitamente all'art. 2103 c.c., nella strutturazione di modelli di mappatura di competenze anche in vista delle progressioni di carriera. Ciò alla luce della possibilità di poter trattare (tramite gli strumenti di lavoro) dati di enorme impatto nella valutazione delle prestazioni di lavoro nell'ambito di percorsi professionali che risulteranno sempre più connotati (per effetto dell'ampliamento dello ius variandi) da una notevole rotazione di incarichi, tra l'altro funzionale all'accrescimento di professionalità ed alla individuazione delle mansioni più confacenti alle competenze e propensioni della persona*. (M. Marazza, *op. cit*., 26).

[239] Secondo Cosattini a seguito della novella le prove raccolte con i controlli a distanza risulterebbero inutilizzabili se raccolte in assenza delle condizioni di cui al comma 3 e finalizzate al rapporto di lavoro, utilizzabili anche in assenza delle condizioni di cui al comma 3 se finalizzate alla repressione e/o prevenzione di reati. (Cosattini A.L., *op. cit.*, 991).

dal lavoratore per rendere la prestazione, ai sensi dei primi due commi dell'art. 4, mentre l'adeguata informazione ed il rispetto della disciplina della privacy sono condizioni richieste per l'utilizzabilità delle informazioni a qualsiasi fine connesso al rapporto di lavoro, non ai fini della raccolta[240]. In altre parole, secondo autorevole dottrina, la disposizione non riguarderebbe più l'esercizio del potere di controllo e le sue modalità, ma una fase successiva che interviene dopo il controllo, quando questo si è esaurito e le informazioni sono entrate nella disponibilità del datore di lavoro che potrà utilizzarle, a distanza di tempo o di luogo rispetto al momento della loro acquisizione[241].

Subordinando l'utilizzabilità dei dati raccolti al rispetto di quanto previsto dal Codice della privacy, la novella pone almeno formalmente fine alla tradizionale incomunicabilità tra le due discipline e rende evidente la necessità di una effettiva integrazione fra le stesse: si istituisce un rapporto diretto ed esplicito tra l'esercizio del potere datoriale e le garanzie per il trattamento delle informazioni personali, tra il sistema di tutele lavoristico contenuto nello Statuto dei lavoratori e quello extra-lavoristico del Codice privacy, un rapporto di definitiva e circolare integrazione tra i due piani di regolazione. Ne consegue l'obbligo per l'interprete di perseguire una lettura quanto più possibile unitaria delle norme che regolano la sorveglianza tecnologica svolta in occasione del rapporto di lavoro, con quelle che disciplinano la protezione dei dati personali, incluso il sistema di fonti regolative promananti dall'Autorità Garante, linee guida, deliberazioni, prescrizioni e provvedimenti paragiurisdizionali, che si consolidano quali parametri di riferimento al fine di perseguire l'ambito bilanciamento di interessi[242].

---

[240] G. Proia, *op. cit.*, 547.

[241] A. Maresca: *accade spesso che questi due aspetti* [esercizio del controllo ed utilizzo dei dati derivanti da tale controllo] *vengano sovrapposti e percepiti come se fossero riconducibili ad un unico atto catalogabile come esercizio del potere di controllo. Ciò accade perché molto spesso l'avvenuto controllo, cioè l'acquisizione del dato, si manifesta in modo visibile soltanto quando si procede alla sua utilizzazione nei confronti del singolo lavoratore.* […] *La disposizione non riguarda l'esercizio del potere di controllo e le sue modalità, ma una fase successiva che si colloca a valle del controllo, anzi quando esso si è esaurito, essendo le «informazioni» entrate nella disponibilità del datore di lavoro che potrà utilizzarle, a distanza di tempo o di luogo dal momento della loro acquisizione. Per chiarire il punto occorre fare riferimento (almeno) a tre fasi cronologicamente e funzionalmente distinte: la prima riguarda l'acquisizione dei dati relativi all'attività lavorativa, come conseguenza automatica della tecnologia utilizzata dal dipendente per svolgere l'attività lavorativa; la seconda concerne la conservazione dei dati, cioè la loro memorizzazione; la terza — che è meramente eventuale — attiene all'utilizzazione dei dati per la gestione del rapporto di lavoro. La sequenza delle tre fasi connota e caratterizza la tipologia dei controlli tecnologici prevista dall'art. 4; controlli che, appunto, vengono definiti "a distanza" per segnare lo spazio di luogo o di tempo che intercorre tra il momento o il luogo in cui il dato inerente all'attività lavorativa viene a formarsi, quello della raccolta/acquisizione, quello della conservazione e, infine, dell'utilizzazione* (Maresca, *op. cit.*, 512).

[242] Si veda A. Sitzia, *Videosorveglianza occulta, privacy e diritto di proprietà: la corte EDU torna sul criterio di bilanciamento*, in ADL n. 2/2018, 514. Vedi anche la lettura molto critica di M.T. Salimbeni: *L'espressione "a tutti i fini connessi al rapporto di lavoro" non può che significare disciplinari e valutativi, nonché giudiziali. L'utilizzo dei dati a questi fini viene condizionato al rispetto del decreto legislativo n. 196/2003 e*

Quali sono gli effetti del rinvio al Codice privacy in termini di rapporto tra le due discipline, generale e speciale? Il rinvio opera in termini di raccordo sistematico o di deroga? Prevale la norma speciale o è la normativa di *data protection*, in quanto normativa di carattere generale, a sopperire al fatto che la disciplina lavoristica non preveda vincoli relativi alle concrete modalità attuative dei trattamenti dei dati nel contesto di lavoro?

M. Marazza ritiene che con il comma 3 dell'art. 4 St. lav. si realizzino inediti livelli di penetrazione del diritto della privacy nell'ambito del rapporto di lavoro, affermandosi un sistema di garanzie essenzialmente individuale e non più collettivo[243]. Sul posizionamento sistematico della previsione statutaria rispetto alla disciplina in materia di protezione dei dati personali, l'Autore ritiene che le disposizioni del Codice Privacy siano applicabili solo ove non espressamente derogate, proprio in virtù del carattere di norma speciale dell'art. 4 St. lav.: la nuova norma detta regole per alcuni aspetti derogatorie rispetto a quelle comuni della privacy e supera ogni diversa previsione del Codice Privacy in materia di finalità del trattamento[244].

---

all'informativa resa ai lavoratori circa le modalità d'uso degli strumenti e di effettuazione dei controlli: sia pur importante questa ulteriore garanzia era già desumibile dai principi enunciati dal Garante nelle Linee guida del 2007, della cui vincolatività nessuno ha mai dubitato e la cui importanza è testimoniata dalla Raccomandazione del Consiglio d'Europa, adottata in data 1 aprile 2015, che ha amplificato a livello dell'Unione europea le indicazioni in esse contenute. Lo stesso richiamo al d.lgs. n. 196/2003 appare superfluo, secondo l'Autrice, perché l'uso dei dati personali era già automaticamente assoggettato alla disciplina generale sui dati che da tempo costituisce normativa di riferimento in materia e che già integrava il divieto di controllo sui lavoratori quando questo si svolgesse attraverso le risultanze informatiche. E inoltre [il legislatore del 2015] *Invertendo il rapporto sistematico che nel nostro ordinamento esiste tra norma generale e norma speciale ha affermato la priorità di una disciplina che nessun bisogno aveva di essere richiamata, retrocedendo in realtà sia sul campo delle tutele sostanziali sia su quello della chiarezza normativa.* (M. T. Salimbeni, *La riforma dell'articolo 4 dello statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Rivista Italiana di Diritto del Lavoro*, 4/2015, 589).

[243] Vedi anche A. Maresca: *si può, forse, osservare che la maturata valutazione negativa del controllo sindacale come presidio della riservatezza del lavoratore, ha suggerito al legislatore di realizzare tale contemperamento attraverso misure più coerenti con la dimensione individuale degli interessi da tutelare e che, come si dirà nel prosieguo, si focalizzano sulla trasparenza e proporzionalità dei controlli (art. 4, co. 3).*

[244] *L'art. 4* è *destinato a prevalere anche in ragione della sua natura di norma speciale che disciplina la tutela della riservatezza di un soggetto "interessato" qualificato (qual è il lavoratore subordinato) rispetto ad uno strumento di trattamento del dato altrettanto tipizzato (qual è lo "strumento di controllo a distanza"). La questione è di grande importanza perché sta a significare che l'esplicita autorizzazione legislativa al trattamento dei dati rilevati mediante strumenti di controllo per "tutti i fini connessi al rapporto di lavoro" (art. 4, comma 3), previo il rispetto dei commi 1 e 2 e fermo l'adempimento dell'obbligo di informativa, supera ogni diversa previsione del Codice Privacy in materia di consenso al trattamento e/o di finalità dello stesso* (M. Marazza, *op. cit*., 25-26). Vedi in senso contrario M. Barbieri: *non si può condividere la tesi che l'esplicita autorizzazione legislativa al trattamento dei dati rilevati mediante strumenti di controllo per tutti i fini connessi al rapporto di lavoro* [...] *supera ogni diversa previsione del Codice Privacy in materia di consenso al trattamento e/o di finalità dello stesso: a me non pare proprio che l'art. 4, co. 3, novellato, esoneri dal rispetto della normativa sulla privacy, con particolare riferimento alla finalità del trattamento, giacché letteralmente l'utilizzabilità delle informazioni raccolte ai fini del rapporto di lavoro deve pur sempre avvenire nel rispetto del d. lgs. n. 196/2003.* (M. Barbieri, *L'utilizzabilità delle informazioni raccolte*, in Tullini, P. (a cura di) *op. cit.*, 194).

Tale interpretazione, secondo P. Tullini, eccede la stessa intenzione della riforma: la tutela che il Codice Privacy riconosce a "chiunque", a qualsiasi interessato al trattamento delle informazioni che lo riguardano, risulterebbe derogata proprio nei luoghi di lavoro. Tale interpretazione si porrebbe in contrasto anche con le disposizioni europee per cui i dati sono utilizzabili solo se la finalità e la modalità del controllo siano corrette per se stesse e coerenti tra loro[245]. Secondo l'Autrice non convince neanche l'interpretazione più sfumata di G. Proia che identifica specificamente tra gli ambiti di prevalenza della norma lavoristica quello dell'utilizzabilità delle informazioni a tutti i fini connessi al rapporto di lavoro: le disposizioni del D.lgs. n. 196/2003 non sono applicabili in quanto derogate o specificate dalla norma speciale, destinata a prevalere. Secondo l'Autore, con questa previsione il legislatore non ha operato un salto nel buio in quanto esiste già una disciplina sostanziale che limita i poteri del datore di lavoro ed evita abusi: il divieto di qualsiasi indagine su fatti che non rilevano ai fini della valutazione dell'attitudine professionale del lavoratore (art. 8 St. lav.) e le disposizioni che vietano gli atti aventi finalità discriminatoria o ritorsiva rappresentano un sicuro baluardo a tutela del dipendente[246].

In ogni caso, come precisato dal Presidente Soro, l'ampliamento delle possibilità di utilizzo dei dati ottenuti con questi controlli non è illimitata poiché i principi di legittimità e determinatezza del fine perseguito con il trattamento, nonché della sua proporzionalità, correttezza e non eccedenza, non solo escludono l'ammissibilità di controlli massivi, ma impongono comunque una gradualità nell'ampiezza e tipologia del monitoraggio, che renda assolutamente residuali i controlli più invasivi.

I vincoli e gli strumenti di tutela sembrano spostarsi piuttosto dal perché al come del controllo, alle sue modalità.

4.2 L'adeguata informazione

Nell'ambito della disciplina generale a tutela della protezione dei dati personali, il consenso del soggetto passivo del trattamento dei dati, l'interessato, adeguatamente informato dal

[245] P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa*, in P. Tullini (a cura di), *op. cit*., 112.

[246] *A mio avviso, pur essendo facile prevedere che tale, complessa, opera darà vita ad un acceso dibattito, la norma lavoristica prevale su quella generale per quanto riguarda tre profili: i) la previsione che legittima la raccolta delle informazioni derivanti dall'uso legittimo degli strumenti consentiti; ii) la previsione della «utilizzabilità» di tali informazioni «a tutti i fini connessi al rapporto di lavoro»; iii) la implicita esclusione della necessità del consenso del lavoratore ai fini del trattamento dei dati personali consistente nella raccolta e nella utilizzazione di quelle stesse informazioni*. (G. Proia, *op. cit*., 547).

titolare e responsabile del trattamento, è presupposto necessario ed indispensabile per rendere giuridicamente lecito il trattamento dei dati personali. Nell'ottica giuslavorista (dove vige l'indisponibilità o solo parziale disponibilità dei diritti) si traduce nella previsione statutaria di un'adeguata informazione al lavoratore e realizza una tutela della persona del dipendente fondata sul principio di trasparenza.

Il principio cardine della trasparenza intorno al quale ruota la disciplina sulla protezione dei dati personali si traduce nell'informazione resa dal datore di lavoro al lavoratore come condizione per l'utilizzabilità dei dati. L'obbligo di rendere edotto il lavoratore in ordine alle modalità di utilizzo degli strumenti e ai controlli a cui è sottoposto costituisce un modo efficace per proteggerlo, non dal controllo, che si è già realizzato nei limiti previsti dal legislatore ai commi 1 e 2 dell'art. 4, ma dall'utilizzo dei dati, consentendo la conoscibilità e la verifica del corretto procedimento nel trattamento dei dati e la consapevolezza dei potenziali effetti, anche disciplinari, nell'ambito del rapporto di lavoro. I limiti posti dal legislatore nel comma 3 operano come limiti riferiti complessivamente ai poteri datoriali di gestione del rapporto di lavoro, non esclusivamente al potere di controllo: il datore potendo utilizzare le informazioni per valutazioni relative al rendimento del lavoratore o alle competenze professionali, oltre ad avvalersene per valutazioni disciplinari. Il dovere di informazione implica la trasparente rappresentazione di tutto l'iter, dalle modalità d'uso dello strumento alla raccolta e conservazione dei dati[247].

Maresca mette in guardia sugli effetti indotti ed ulteriori della trasparenza e della consapevolezza di essere controllati che accentuerebbe la condizione di soggezione del lavoratore, intravedendosi nelle parole di Maresca un timore per l'effetto Panopticon[248].

Il legislatore stabilisce che deve essere data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli: in dottrina si è ritenuto che tale formulazione non rappresenti un'endiadi, ma identifichi due adempimenti differenti[249]. Il primo rimanda alla policy aziendale sull'uso degli strumenti, il disciplinare interno al quale

[247] La conoscibilità del controllo non ne disinnesca la potenzialità lesiva ma la consapevolezza della procedura consente di verificare il rispetto degli adempimenti. Anche il principio di buona fede di cui all'art. 1375 c.c. (Esecuzione di buona fede. Il contratto deve essere eseguito secondo buona fede) implica un dovere di trasparenza da parte del titolare nei confronti dell'interessato.

[248] *Lo strumento attuativo di tale trasparenza — cioè l'informazione al lavoratore — può comportare effetti indotti di altra natura, proprio perché realizza in capo al dipendente la piena e formalizzata cognizione del controllo a cui è assoggettato. Si tratta, in particolare, non soltanto dell'effetto dissuasivo tipico di ogni controllo, ma anche dell'accentuazione della condizione di soggezione del lavoratore nel momento in cui assume la consapevolezza di essere sottoposto, ancorché legittimamente, ad un controllo, realizzato tecnologicamente, che viene a connotare la situazione di subordinazione nei confronti del datore di lavoro* (A. Maresca, *op. cit.*, 512).

[249] A. Ingrao, *op. cit.*, 118.

rinvia anche il Regolamento europeo, come misura di *accountability*, di responsabilizzazione del titolare del trattamento dei dati, mentre l'informazione sulle modalità di effettuazione dei controlli, sulle caratteristiche del monitoraggio ricorda da vicino l'informativa che il titolare del trattamento dei dati personali è tenuto ad inviare al soggetto interessato, ai sensi dell'art. 13 d.lgs. 196/2003 (oggi abrogato e sostituito dagli articoli 13 e 14 Reg. 2016/679UE). Potrebbe apparire un mero duplicato dell'obbligo previsto dall'art. 13 del Codice della privacy e da una parte della dottrina è considerata una *species* dell'informativa di cui all'art. 13 D.lgs. 196/2003[250].

In realtà, i due istituti restano distinti, quello giuslavoristico rappresenta un atto unilaterale che non richiede alcuna manifestazione di consenso da parte del lavoratore[251], consente al lavoratore la conoscenza *ex ante* degli adempimenti dovuti e assicura il persistere del divieto di controlli occulti, è finalizzato ad abilitare il datore di lavoro ad utilizzare i dati acquisiti a tutti i fini connessi al rapporto di lavoro, compresi quelli disciplinari. La funzione principale dell'informazione nella disciplina della privacy è invece quella di rappresentare il presupposto logico necessario per l'acquisizione del consenso dell'interessato e lo strumento di acquisizione di informazioni generali sulle finalità e modalità di trattamento, per verificarne il rispetto ed eventualmente azionare i previsti strumenti di tutela. L'informativa sulla modalità di effettuazione dei controlli dovrà contenere l'indicazione della base giuridica che legittima il datore alla raccolta, specificare perché il controllo è necessario, il tipo di strumento utilizzato, le finalità del trattamento, gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali, il tempo massimo di conservazione dei dati o i criteri utilizzati per determinare tale periodo, i diritti dei lavoratori quali interessati al trattamento, l'indicazione del nominativo e dei contatti del Data Protection Officer, se nominato. L'obbligo dell'informativa e il principio di trasparenza che lo ispira si sono diffusi

[250] *Quanto al consenso, invece, pare corretto osservare che la legge condiziona il trattamento dei dati al solo adempimento dell'obbligo di informativa, che è un atto unilaterale che non richiede alcuna manifestazione di consenso da parte dell'interessato, osservato il quale le "*informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili*" (art. 4, comma 3). Peculiarità che esclude la necessità di acquisire il consenso del lavoratore e che ben si giustifica se si considera che i dati da trattare sono raccolti tramite strumenti di lavoro (art. 4, comma 2), il cui utilizzo non può certo dipendere da una manifestazione di volontà del lavoratore, o, comunque, tramite strumenti di controllo preventivamente autorizzati dall'accordo collettivo o dal provvedimento amministrativo per finalità legislativamente tipizzate (art. 4, comma 1)* (M. Marazza, *op. cit.*, 27).

[251] In senso contrario A. Sitzia che conclude nel senso della necessità del consenso, v. *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. Lav. e il consenso (del lavoratore)*, in *LLI* n.1/2016. Secondo Marazza solo nel caso in cui il datore di lavoro intendesse utilizzare i dati raccolti per finalità diverse da quelle connesse al rapporto di lavoro, sarebbe condivisibile ritenere che trovi ordinaria applicazione non solo il principio dello scopo determinato e legittimo, da verificare caso per caso, ma anche la regola del consenso. (Marazza, *op.cit*., 27).

nelle prassi gestionali delle imprese, generando la consapevolezza di poter essere controllati, la possibilità del controllo in luogo del divieto assoluto e la trasparenza dei confini entro i quali il controllo può essere esercitato.

Non è escluso che tale informativa e quella di cui al Codice della privacy in futuro si possano unificare per i neoassunti, venendo incorporate in un unico documento.

La legge dà indicazioni generali sul contenuto della informativa e richiede adeguatezza: requisito da intendere come leggibilità, effettiva comprensibilità dei contenuti da parte del destinatario, e come specificità rispetto al tipo di strumento e di controllo a distanza effettuato. L'informativa dovrà contenere informazioni chiare, complete e sintetiche, per essere comprese agevolmente dal prestatore e non generalizzate, ma mirate in base al rischio che il singolo strumento può presentare per i diritti fondamentali del lavoratore, in grado di consentire a ciascun lavoratore di avere contezza del funzionamento degli strumenti che utilizza o che può utilizzare, del controllo che ne deriva e delle modalità con le quali saranno raccolti e trattati i suoi dati personali.

Pur in assenza di indicazioni specifiche da parte del legislatore, è opportuno che l'informazione al lavoratore rispetti il requisito della forma scritta per essere documentabile e tracciabile l'invio al lavoratore. Se il contenuto non è generalizzabile per tutti i dipendenti ma differenziato a seconda delle mansioni e degli strumenti di lavoro, allo stesso modo la comunicazione dell'informativa sarà individuale o specificamente indirizzata a gruppi di lavoratori che svolgono le stesse mansioni o usano gli stessi strumenti[252].

È indubbio che l'informativa svolga una funzione essenziale proprio con riferimento agli strumenti impiegati ai sensi del secondo comma dell'art. 4, tra i quali certamente sono da ricomprendere internet e posta elettronica. Non a caso la formulazione dell'attuale comma 3, art. 4 St. lav. riprende testualmente la prescrizione del Garante nelle Linee guida per posta elettronica ed internet (punto 3.1 e 3.2)[253]. Se per gli impianti ricadenti nella disciplina del

[252] Vedi A. Maresca, *op. cit.* e v. anche la circolare di Confindustria, *Il nuovo art. 4 dello Statuto dei lavoratori: profili privacy*, in www.aib.bs.it/Allegati/2015/wdm_doc_allegati_58552_allegati.pdf nella quale si legge: Tale circostanza non sembrerebbe escludere la redazione di disciplinari interni, validi per gruppi di lavoratori che svolgono le stesse mansioni ovvero per gruppi di lavoratori che, pur svolgendo mansioni differenti, utilizzano i medesimi strumenti (v. Linee Guida per l'utilizzo della posta elettronica e internet, par. 3.2). In ogni caso, sarebbe opportuno che la diffusione di tali disciplinari tra i lavoratori interessati avvenisse con modalità tali da assicurarne la comunicazione personale (es. consegna del disciplinare, invio del disciplinare per e-mail).

[253] Il Garante aveva chiarito, con riferimento a internet e alla posta elettronica, che "grava sui datori di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle

comma 1 saranno gli accordi sindacali a determinare, in linea di massima, sia le modalità di uso dei dispositivi che quelle di effettuazione dei controlli, per gli strumenti di lavoro assegnati dal datore di lavoro manca il suddetto accordo e sarà il datore di lavoro a decidere liberamente e unilateralmente le relative regole di uso e ad informare preventivamente il lavoratore sulle condizioni d'uso degli strumenti di lavoro e sulle connesse possibilità di effettuare i controlli[254].

A fronte delle possibili forme di controllo sulla prestazione lavorativa, collegate all'uso di strumenti di lavoro utilizzati per rendere la prestazione, assegnati liberamente dal datore di lavoro, la tutela della riservatezza viene garantita in una dimensione principalmente individuale, in cui l'adeguatezza dell'informativa funge da elemento cardine di protezione della libertà e dignità della persona all'interno dell'impresa, soprattutto nei casi nei quali non interviene la procedura sindacale o amministrativa[255].

Il rischio, tuttavia, è che la previsione abbia una portata più formale che sostanziale: sarà agevole per i datori di lavoro attrezzarsi con modelli di informativa più o meno articolati che spieghino al lavoratore come e quando siano posti in essere i controlli attraverso l'utilizzo dello strumento di lavoro da parte del dipendente e non saranno in molti i lavoratori che chiederanno modifiche limitative alla portata dei potenziali controlli o che si rifiuteranno di firmare.

---

dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative".

Da notare che il Garante nel provvedimento *Linee guida in materia di trattamento di dati personali per profilazione on line* (19 marzo 2015), ha caldeggiato la scomposizione dell'informativa in due testi: uno approfondito ed uno sintetico.

[254] *Nell'ipotesi d'installazione di strumenti di controllo la ricorrenza di tale esigenza [tutela del patrimonio aziendale] sarà verificata in concreto attraverso la procedura codeterminativa, mentre [nel caso di trattamento d'informazioni sui prestatori raccolte da uno strumento utilizzato per rendere la prestazione] sarà il datore di lavoro nella "valutazione di impatto privacy" (art. 35 Reg.) a dimostrare la ricorrenza del suo "legittimo interesse", ossia della presenza di una base giuridica che giustifichi la legittimità del trattamento.* (A. Ingrao, *op. cit.*,163).

[255]Vedi Trib. Roma 13 giugno 2018 n. 57668 che dichiara inutilizzabili le informazioni raccolte per mancanza di un'adeguata informazione, considerato che la policy aziendale non prevedeva né disciplinava in alcun modo l'esperimento di controlli e che il novellato art. 4 pone espressamente il rispetto dell'obbligo di adeguata informazione a condizione dell'utilizzabilità del dato.

V. anche C. App. Torino 27 marzo 2017 che dichiara inutilizzabili le comunicazioni Skype di un lavoratore in quanto la preventiva comunicazione sull'uso consentito degli strumenti in dotazione risultava mancante.

4.3 Le condizioni legittimanti e i principi regolatori del trattamento dei dati personali

Il Regolamento 2016/679UE nel Capo II ripropone i principi applicabili al trattamento dei dati personali, distinguendo i presupposti legittimanti il trattamento (o basi giuridiche) (art. 6) e i principi applicabili al trattamento dei dati personali (art. 5) che regolano specificamente le modalità esecutive dello stesso.

Il fondamento di liceità del trattamento si basa sulla ricorrenza di almeno una delle condizioni di legittimità indicate nell'articolo 6 Reg. UE 2016/679, che legittimano a monte il trattamento dei dati personali: l'esecuzione di un contratto di cui l'interessato è parte, l'obbligo legale del trattamento, la salvaguardia degli interessi vitali dell'interessato, l'esecuzione di un compito di interesse pubblico, il consenso dell'interessato e il perseguimento del legittimo interesse del titolare. Quest'ultimo nel rapporto di lavoro rappresenterebbe il necessario presupposto di legittimità, piuttosto che il consenso del lavoratore che potrebbe non essere liberamente espresso, dato il rapporto geneticamente squilibrato tra le parti. Nel nostro ordinamento la legittimità dell'interesse datoriale al trattamento dei dati è tipizzata in qualificate esigenze aziendali, organizzative, di sicurezza del lavoro e di tutela del patrimonio aziendale, come indicate nel comma 1 dell'art. 4 St. lav. Il punto è che il legittimo interesse datoriale deve essere contemperato con i diritti e le libertà fondamentali del prestatore di lavoro, soprattutto con il diritto alla protezione dei suoi dati personali: l'equilibrio tra interessi confliggenti dovrebbe essere ricercato applicando modalità operative del trattamento conformi ad un quadro di principi che orientano il trattamento di dati[256].

[256] Articolo 5 Principi applicabili al trattamento di dati personali 1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla

Una volta individuati i presupposti giuridici che legittimano il trattamento dei dati, la disciplina europea obbliga il datore di lavoro, in quanto titolare del trattamento, per tutta la durata del trattamento ad esercitare il proprio potere in conformità a dati principi che regolano le modalità del trattamento e ad attuare misure adeguate per prevenire il rischio di lesione della dignità e dei diritti fondamentali dei lavoratori, quale soggetto interessato (artt. 5 e 24 Reg. UE). I principi regolatori del trattamento dei dati personali mutuati dalla normativa sulla privacy, già richiamati nelle Linee guida del Garante, oltre che nella giurisprudenza della Corte europea dei diritti dell'uomo, si applicano così anche al trattamento dei dati del lavoratore. In conformità a questi principi il datore di lavoro dovrà configurare i sistemi informativi e informatici in modo da effettuare il trattamento per scopi determinati, espliciti e legittimi, non eccedenti rispetto alle finalità per le quali i dati sono raccolti e ridurre al minimo l'utilizzazione dei dati personali e l'invasività del controllo, in funzione del principio di pertinenza e non eccedenza[257].

Se è vero che sia il legislatore lavoristico a "chiamare in soccorso" nella materia del controllo datoriale, la generale tutela posta a protezione delle informazioni personali in funzione limitativa del potere di controllo tecnologico, questo avviene al fine di inglobare i principi di trasparenza, limitazione della finalità e minimizzazione, in quanto reputati idonei a disciplinare le operazioni di raccolta e utilizzo dei dati personali dei lavoratori, nonché tutte quelle operazioni intermedie di trattamento che il datore di lavoro necessariamente compie sui loro dati personali[258].

L'art. 5 Reg. individua sette principi che definiscono le modalità lecite di trattamento dei dati personali ed attribuisce un nome "ufficiale" a ciascun principio: trasparenza, limitazione della finalità, minimizzazione, liceità, correttezza, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.

Si possono distinguere due gruppi differenti di principi: con il primo gruppo, che comprende i principi di liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione e responsabilizzazione, il legislatore europeo ha inteso obbligare il titolare del trattamento a

perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

[257] Il datore di lavoro prima d'installare le apparecchiature, sceglie la ragione, le modalità e l'oggetto del controllo; di conseguenza decide la tecnologia che intende utilizzare e, quindi, predefinisce le impostazioni di tali dispositivi, al fine di effettuare il controllo in un certo periodo temporale e in uno spazio determinato. A seguito della captazione, il dato prescelto rimane impresso nella memoria del dispositivo, in un certo formato e per un certo periodo, restando potenzialmente visibile a diversi soggetti all'interno dell'organizzazione per scopi differenziati (A. Ingrao, *op. cit.*, 53).

[258] A. Ingrao, *op. cit.*, 155.

conformare la propria azione a determinate regole, che integrano e definiscono le modalità di esercizio del potere di controllo a distanza.
Il secondo gruppo di principi intende garantire requisiti di qualità dei dati personali durante tutta la durata del trattamento: l'esattezza e l'integrità dei dati, se necessario periodicamente aggiornati, la limitazione della conservazione in una forma che consenta l'identificazione degli interessati per un tempo non superiore a quello necessario per il conseguimento delle finalità del trattamento, la sicurezza, in particolare, la protezione da trattamenti non autorizzati o illeciti, nonché dalla perdita, dalla distruzione o dal danno accidentale.
Il primo gruppo di principi è quello di nostro immediato interesse e di prima applicazione perché idoneo a governare le modalità esecutive del trattamento dei dati personali dei lavoratori acquisiti attraverso l'esercizio del potere di controllo a distanza.

4.3.1 Il principio di limitazione della finalità

I dati personali sono trattati in modo lecito (non è lecito l'utilizzo di informazioni già oggetto di divieti di trattamento ai sensi degli artt. 4 e 8 St. lav.), corretto (secondo buona fede) e trasparente (informativa) nei confronti dell'interessato.
Particolarmente rilevante nell'impianto di protezione dei dati personali è il principio di limitazione della finalità, in base al quale i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e in seguito trattati in modo che non sia incompatibile con tali finalità (art. 5, p.1, lett. b, Reg.). Tale principio ha costituito sin dalla Convenzione 108/1981 la pietra angolare della protezione della persona da raccolte automatizzate di dati[259], obbliga il datore di lavoro, prima di eseguire il controllo, a predeterminare ed esplicitare nella informativa e nella valutazione d'impatto privacy, di cui rispettivamente agli artt. 13 e 35 Reg., gli scopi legittimi del monitoraggio selezionandoli tra quelli "connessi al rapporto di lavoro" e di rispettarli per la durata del trattamento [260].
Gli obiettivi del trattamento sono specificati con precisione prima della raccolta e degli stessi è data informazione all'interessato: le informazioni raccolte sono soggette poi ad un vincolo di finalità che ne inibirebbe l'impiego per finalità diverse e "incompatibili" con quelle

[259] A. Ingrao, *op. cit*.,156-157.
[260] *Il principio di limitazione delle finalità si traduce in un obbligo posto in capo al datore di lavoro di selezionare le ragioni obiettive (gli scopi) della raccolta dei dati fra quelle legittimamente ammesse dall'ordinamento, di comunicarle all'interessato e di rispettarle per la durata del trattamento. (Il tracciamento del percorso motivazionale del titolare circa le ragioni del trattamento fa parte dell'esplicitazione della base giuridica del trattamento ai sensi dell'art. 6 Reg*.) (A. Ingrao, *op. cit*).

inizialmente stabilite. Il vincolo di finalità sulle informazioni raccolte perdura per tutto il loro utilizzo, che dovrà essere adeguato, proporzionato e graduato rispetto alla finalità indicata. Come si concilia il principio di limitazione delle finalità con l'utilizzabilità dei dati personali a tutti i fini connessi al rapporto di lavoro, il fatto che il datore di lavoro è tenuto a determinare prima dell'inizio del trattamento uno scopo lecito e determinato, a renderlo noto cristallizzandolo nell'informativa e a rispettarlo per tutta la durata del trattamento sino alla cancellazione dei dati?

Che la questione non sia di facile gestione lo dimostrano le previsioni del Regolamento europeo laddove consentono l'utilizzo dei dati raccolti anche per finalità diverse da quelle originarie purché "compatibili" con queste ultime. È prevista una valutazione di compatibilità tra le finalità ulteriori e quelle inizialmente dichiarate, da effettuare caso per caso sulla base di un test denominato *compatibility assessment*, elaborato dal Gruppo di lavoro ex art. 29 sotto la vigenza della Direttiva 95/46/CE, ma destinato a trovare applicazione anche con il Regolamento. Il test tiene conto di diversi fattori: la relazione tra la finalità per le quali sono state raccolte e quelle ulteriori che si vogliono raggiungere, il rapporto di continenza tra le finalità iniziali e quelle ulteriori, il contesto nel quale sono stati raccolti i dati e la ragionevole aspettativa dell'interessato, le misure adottate dal titolare per garantire trattamenti ulteriori leali e prevenire illegittimi effetti rispetto agli interessati[261].

In dottrina si è evidenziata una possibile contraddizione interna al sistema: l'utilizzabilità a tutti i fini connessi al rapporto di lavoro è subordinata al rispetto della normativa privacy e la normativa privacy a sua volta prevede il rispetto del principio di limitazione della finalità, un fine inizialmente dichiarato ed un trattamento proporzionato e non eccedente rispetto a quel fine.

Sotto il profilo della finalità, il Garante della Privacy ha esplicitamente sostenuto che tale principio non impone soltanto di raccogliere i dati per uno scopo specifico, lecito e determinato, ma anche che tali dati non possono essere utilizzati per trattamenti ulteriori, secondo modalità incompatibili con lo scopo: lo scopo perseguito in concreto dal datore di lavoro non deve essere infatti incompatibile con le finalità per le quali i dati personali sono stati raccolti[262]. Ne potrebbe conseguire che un impianto di videosorveglianza autorizzato

[261] A proposito del *compatibility assesment* vedi il parere n. 3/2013 del Gruppo di lavoro ex art. 29.

[262] Il seguente passaggio, tratto dal provvedimento del Garante n. 434 del 2 ottobre 2014, *Sistemi di localizzazione e videosorveglianza. Utilizzo dei dati per fini disciplinari e tutela dei lavoratori*, relativo all'installazione di un sistema di localizzazione dei veicoli della società A.MA.CO. s.p.a. di Cosenza, chiarisce la problematica: *Ritenuto altresì che nel caso di specie i dati personali dei dipendenti sono trattati attraverso il sistema di localizzazione per esigenze organizzative e produttive e che pertanto eventuali operazioni di trattamento effettuate allo scopo ulteriore di contestare illeciti disciplinari ai dipendenti non siano conformi*

solo per ragioni di sicurezza sul lavoro consentirà l'utilizzo dei dati esclusivamente per finalità di tutela dell'integrità psicofisica del dipendente e non per fini disciplinari. La finalità di sicurezza posta alla base dell'installazione di una telecamera non potrebbe ricomprendere in sé il diverso scopo disciplinare di utilizzo del dato.

Come abbiamo visto una parte degli interpreti supera questa contraddizione in base alla considerazione che la previsione della disciplina generale soccombe di fronte ad una norma speciale che autorizza esplicitamente il trattamento delle informazioni raccolte per ogni utilizzo connesso al rapporto di lavoro[263].

Di contrario avviso sono altri Autori: Patrizia Tullini sostiene che una interpretazione derogatoria della normativa generale sul punto della utilizzazione dei dati eccederebbe la stessa intenzione della riforma. In coerenza con le fonti europee, il legislatore italiano si è mostrato propenso al raccordo sistematico attraverso reciproci rinvii, anziché alla deroga rispetto alla normativa in materia di riservatezza. L'uso delle informazioni "a tutti i fini connessi al rapporto di lavoro" non concede la facoltà di andare oltre il contenuto oggettivo del rapporto di lavoro e l'aspettativa del corretto adempimento dell'obbligazione debitoria. La raccolta di informazioni personali incontra limiti imperativi e non derogabili, in caso contrario risulterebbe compromesso l'equilibrio degli interessi stabilito dallo Statuto, quello del lavoratore alla piena autonomia della sfera privata e quello datoriale al ragionevole affidamento sull'esatto svolgimento della prestazione, e la stessa coerenza interna dello Statuto, richiamata anche dal Codice Privacy. La facoltà attribuita al datore di lavoro di servirsi delle informazioni raccolte non può abilitare il superamento dei vincoli posti dall'art. 8 St. lav., né consentirgli di andare oltre il contenuto oggettivo del rapporto di lavoro e la legittima aspettativa all'esatto adempimento della prestazione[264].

---

al principio di finalità del trattamento (cfr. art. 11, comma 1, lett. b) del Codice); ritenuto che tali ulteriori trattamenti non siano altresì conformi alla disciplina posta in materia di controllo a distanza dei dipendenti, laddove vieta di installare dispositivi allo scopo di effettuare un controllo sull'attività lavorativa (cfr. art. 4, l. 20.5.1970, n. 300). Il Garante ha ritenuto illecito il trattamento effettuato a mezzo del sistema di localizzazione dei veicoli aziendali e prescritto di non utilizzare i dati trattati per finalità di contestazione disciplinare per violazione del principio di finalità e della vigente disciplina in materia di controlli a distanza dei lavoratori.

[263] M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in Working Papers CSDLE Massimo D'Antona, 2016, 15. Anche secondo Giampiero Proia rimangono presidiate dalla norma lavoristica le finalità del controllo: i dati possono essere utilizzati a tutti i fini connessi al rapporto di lavoro e le norme sulla privacy non possono limitare le finalità, ma solo disciplinare la misura e le modalità del controllo. Tuttavia lo stesso Autore non manca di evidenziare una contraddizione interna alla nuova disciplina per cui l'uso delle informazioni raccolte, anche se legittimato a qualsiasi fine connesso al rapporto di lavoro, risulta in concreto circoscritto per effetto dell'applicazione del principio del Codice della privacy, nel momento in cui il datore di lavoro è tenuto a comunicare preventivamente al lavoratore le specifiche finalità di ogni tipologia di trattamento dei dati e a rispettare i principi di pertinenza e non eccedenza rispetto alla finalità indicata (G. Proia, *op. cit*., 547).

[264] P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa*, 114.

Fortissime perplessità sulla nuova formulazione del terzo comma dell'art. 4 St. lav. sono espresse da M. T. Salimbeni che intravede una minaccia alla dignità e alla riservatezza del lavoratore: autorizzando l'uso "a tutti i fini connessi al rapporto di lavoro" di tutte le informazioni raccolte ai sensi sia del primo sia del secondo comma, si neutralizzerebbe la disposizione del primo comma che consente l'impiego degli strumenti dai quali derivi anche la possibilità di controllo a distanza dei lavoratori esclusivamente per esigenze organizzative e produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale e non di controllo sull'attività dei lavoratori[265].

Secondo Maresca il legislatore stesso traccia il confine tra le materie disciplinate direttamente dall'art. 4 e quelle rimesse al D.lgs. n. 196/2003 che concorre con la disciplina statutaria a concretizzare la complessiva tutela del lavoratore in materia di controlli a distanza, attraverso l'integrazione delle due discipline, senza sovrapposizioni. In materia di utilizzabilità dei dati raccolti a tutti i fini del rapporto di lavoro dovrà applicarsi il comma 3 dell'art. 4 St. lav., mentre per quanto attiene invece alla misura e alla modalità dei controlli a distanza, non contenendo l'art. 4 alcuno specifico riferimento, sono chiamati in causa i principi enunciati dalla normativa privacy, in particolare con riferimento alla necessità e pertinenza del controllo, alla non eccedenza ed alla temporanea conservazione dei dati raccolti. Con l'applicazione di questi principi gli interpreti dovranno confrontarsi nella parte in cui ad essi è subordinata la legittimità del trattamento[266].

Valeria Nuzzo ci offre una chiave di lettura che rappresenta la possibile via d'uscita dall'impasse interpretativa: si dovrebbe leggere la formula "a tutti i fini connessi al rapporto di lavoro" aggiungendovi "purché compatibili con la finalità della raccolta"[267].

Non è un caso che il Presidente Soro abbia messo in guardia sul fatto che prescindere dai requisiti finalistici previsti dal primo comma e applicare il solo requisito finalistico previsto dal terzo comma, che legittima l'utilizzo dei dati acquisti per tutti i fini connessi al rapporto

---

Si veda anche P. Tullini, *La digitalizzazione del lavoro*, in P. Tullini, (a cura di) *Web e lavoro*, 17. In senso contrario alla derogabilità del principio di limitazione della finalità si esprime anche A. Ingrao (*op. cit.*, 161).

[265] *La disposizione del terzo comma desta fortissime perplessità, nel merito e nella forma, se letta in combinato con il primo comma. Quanto al merito del terzo comma, non può non rilevarsi come, autorizzando l'uso «a tutti i fini connessi al rapporto di lavoro» di tutte le informazioni raccolte, ai sensi sia del primo sia del secondo comma, in pratica si neutralizza la disposizione del primo comma che consente l'impiego degli «impianti audiovisivi» e degli «altri strumenti dai quali derivi anche la possibilità di controllo a distanza dei lavoratori» ai soli fini di esigenze organizzative e produttive, di sicurezza del lavoro, di tutela del patrimonio aziendale (non certo quindi di controllo sull'attività dei lavoratori). Se la limitazione posta dal primo comma ha lo scopo di mantenere in vita il divieto di utilizzare impianti di controllo invasivi della dignità e della riservatezza del lavoratore la palese smentita che ne deriva ad opera del terzo comma rischia di essere ingiustificata e contraria ai principi costituzionali.* (M.T. Salimbeni, *op. cit.*, 589).

[266] A. Maresca, *op. cit*., 525.

[267] V. Nuzzo, *La protezione del lavoratore dai controlli impersonali*, *op. cit.*, 219.

di lavoro, significa ampliare le potenzialità del controllo a distanza, fino alla possibilità del controllo dell'adempimento della prestazione, mediante gli strumenti di lavoro[268].
Le esigenze di protezione dei diritti di dignità e riservatezza dei lavoratori esposti ad un elevato rischio per effetto dell'amplificazione del potere informatico datoriale e delle sue potenzialità di controllo, imporrebbero un approccio restrittivo nell'ambito del rapporto di lavoro.

4.3.2 I principi di necessità e proporzionalità

Da leggere in combinazione con il principio di limitazione della finalità sono i principi di pertinenza, non eccedenza e proporzionalità (art. 5, lett. c Reg. UE 679/2016): la conformità del trattamento dei dati dei lavoratori al Codice privacy si concretizza in un trattamento adeguato, pertinente e non eccedente rispetto alla finalità indicata.
In un'evoluzione del principio di minimizzazione dei dati, oggi sviluppato nei concetti di *privacy by design* e di *privacy by default*, nell'ambito dell'organizzazione aziendale il datore è tenuto ad adottare una strategia di prevenzione da cui si evinca che sistemi ed impianti sono configurati in modo da ridurre al minimo l'utilizzazione di dati personali riferibili ai lavoratori e di dati identificativi, dando preferenza ai dati anonimi, e in modo che non sia possibile raccogliere dati ulteriori rispetto a quelli strettamente necessari[269].
L'organizzazione deve privilegiare misure che siano in grado di prevenire piuttosto che reprimere comportamenti illeciti da parte dei lavoratori: i controlli del datore di lavoro sono ammissibili soltanto se strettamente proporzionati e non eccedenti lo scopo indicato, limitati nel tempo e nell'oggetto, previsti da preventive policy aziendali, mirati e fondati su precisi presupposti utili a impedire la sorveglianza massiva e totale del lavoratore[270].

---

[268] Anche le nuove norme vanno interpretate alla luce del principio di proporzionalità riaffermato di recente dalla Corte Europea dei diritti dell'uomo rispetto al controllo della mail aziendale in orario di lavoro. A. Soro, Audizione in Parlamento sugli schemi di decreti legislativi attuativi del Jobs Act (9 e 14 luglio 2015).
[269] Si veda anche il considerando 39 del Regolamento: *le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati.*
[270] *I principi di legittimità e determinatezza del fine perseguito con il trattamento, nonché della sua proporzionalità, correttezza e non eccedenza, non solo escludono l'ammissibilità di controlli massivi, ma impongono comunque una gradualità nell'ampiezza e tipologia del monitoraggio, che renda assolutamente*

Già nelle Linee guida su posta elettronica ed Internet il Garante stabiliva l'obbligo di intervenire con accorgimenti tecnici volti a configurare come *extrema ratio* l'esecuzione di controlli individuali. Ne consegue l'illiceità del trattamento quando la finalità perseguita nel singolo caso poteva essere perseguita mediante la gestione di dati anonimi o comunque attraverso modalità meno invasive che consentano l'identificazione dell'interessato solo in caso di stretta necessità[271].

La combinazione di questi principi limita l'invasività e la continuità dei controlli ed il Garante è intervenuto a stabilire l'illegittimità del trattamento quando la legittima esigenza datoriale poteva essere soddisfatta con mezzi meno invasivi[272].

Del rispetto dei suddetti principi è responsabile il titolare del trattamento: il principio di responsabilizzazione o *accountability* (art. 5, p.2 Reg.) si sostituisce all'impostazione autorizzatoria, propria della Direttiva 95/46/CE, e si sostanzia in una serie di adempimenti e responsabilità a carico del datore di lavoro: dall'adozione di regolamenti interni sull'uso di strumenti informatici all'attuazione dei principi di *privacy by default* e *by design*, alla conservazione delle evidenze documentali circa la conformità dei trattamenti. Grava sul titolare l'onere probatorio della dimostrazione della liceità dei trattamenti per non incorrere nelle sanzioni amministrative comminate dal Garante e nell'inutilizzabilità dei dati, (art. 2-decies del d.lgs. 196/2003 come modificato dal D. Lgs. 101/2018).

residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritto dei lavoratori. (A. Soro, Audizione alle Camere 9-14 luglio 2015).

[271] Il Garante nel provvedimento n. 1229854 del 2 febbraio 2006, *Internet: proporzionalità nei controlli effettuati dal datore di lavoro*, ha accolto il ricorso presentato dal lavoratore in quanto il datore di lavoro avrebbe potuto dimostrare l'illegittimità del comportamento del lavoratore verificando l'accesso ingiustificato alla rete, senza necessità di acquisire anche i contenuti delle pagine web visitate e con questi dati sensibili del lavoratore.

L'Autorità Garante ha sottolineato l'obbligo di predisporre programmi che provvedano alla cancellazione periodica dei dati relativi agli accessi ad internet ed al traffico telematico, con la sola eccezione dei dati la cui conservazione sia necessaria, purché però limitata al tempo utile a raggiungere la legittima finalità prevista. Incide anche sulla determinazione del tempo di conservazione dei dati che deve essere predeterminato dal titolare del trattamento avendo riguardo allo scopo che si prefiggeva di realizzare nel caso concreto. Salva la ricorrenza di particolari esigenze tecniche o di sicurezza i sistemi informatici devono essere configurati in modo tale da cancellare automaticamente i dati personali relativi ai lavoratori.

[272] In un caso sanzionato dal Garante il datore di lavoro, per evitare sottrazioni o smarrimenti di camici ospedalieri in uso al personale medico e infermieristico, ha utilizzato un microchip di geolocalizzazione sotto il bottone di ciascun indumento e per questo ha eseguito un trattamento illecito, sproporzionato. Non vi è necessità di raccogliere dati associati al nome del proprietario del camice e di rivelare la sua posizione geografica in modo continuativo durante tutto l'orario di lavoro.

4.4 L'inutilizzabilità dei dati

Sebbene il Presidente Soro identifichi nella conformità alle norme del Codice il principale argine a un utilizzo pervasivo dei controlli sul lavoro e nonostante l'opera svolta dal Garante, è forte l'impressione che l'applicazione della disciplina generale sulla *privacy* nel rapporto di lavoro continui a produrre una percentuale considerevole di adempimenti, ma non un effettivo progresso nella tutela della dignità del lavoratore. L'argine che la disciplina generale sembra opporre all'esercizio illegittimo del controllo datoriale e alla conseguente illegittima acquisizione dei dati personali dei lavoratori resta debole.

Molte le incertezze applicative rispetto all'effettiva portata della disposizione generale dell'art. 11, co. 2, oggi riprodotta nell'art. 2-decies del Codice, come modificato dal d. lgs. 101/2018, per cui *i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'art. 160-bis*[273].

Le Corti civili nel verificare la legittimità dei controlli a distanza, raramente hanno valorizzato il rispetto di questi principi quale elemento essenziale per la decisione, motivata sulla base del mancato rispetto di questi[274].

Per questo si segnalano due sentenze che dall'eccedenza delle modalità del controllo e dalla sproporzione fra trattamento dei dati personali e finalità perseguita fanno discendere l'inutilizzabilità a fini disciplinari dei dati personali raccolti.

La prima è una sentenza del Tribunale di Milano 23 aprile 2015 che evidenzia e valorizza la questione dell'eccesso delle modalità del controllo rispetto allo scopo, *il controllo è stato effettuato con modalità assolutamente eccessive essendo indagato qualsiasi atto del ricorrente.* L'"ossessivo controllo", così definito dal Tribunale, l'assoluta e palese sproporzione fra i mezzi usati (alcuni mesi di pedinamento) e lo scopo perseguito,

[273] Art. 160-*bis Validità, efficacia e utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento.* La validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali.

[274] Nonostante il disposto di legge contenuto nell'art. 2 decies, d.lgs. n. 196/2003, le Corti penali riconoscevano l'utilizzabilità processuale e l'ammissibilità di mezzi istruttori indipendentemente dalle modalità di raccolta dei dati, in considerazione del principio di prevalenza rispetto alle disposizioni a tutela della riservatezza "dell'esigenza di ordine pubblico relativa alla prevenzione dei reati, ove siano concreti ed effettivi sospetti di attività illecite poste in essere all'interno dei luoghi di lavoro" Cass. pen. sez. V, 12 luglio 2011, n. 34842 e Cass. pen., sez. V, 1 giugno 2010, n. 20722.

giustificano l'inutilizzabilità di tutto il materiale probatorio raccolto e l'accoglimento delle ragioni del lavoratore[275].

L'altra è una pronuncia di Cass. civ. sez. I, 1 agosto 2013, n. 18443, la Corte rileva un trattamento di dati eccedente rispetto alla finalità perseguita quando il datore di lavoro, pur potendo diversamente dimostrare l'illiceità della condotta di un suo dipendente acquisisca e diffonda informazioni ulteriori e non indispensabili per far valere un suo diritto in sede giudiziaria. Nel caso di specie la condotta illecita del dipendente era consistita in reiterati e non autorizzati accessi alla rete sul luogo di lavoro e sarebbe stato sufficiente provare l'accesso indebito alla rete e i tempi di collegamento senza trattare informazioni indicative anche degli specifici contenuti dei singoli siti web visitati dal dipendente, operando un trattamento di dati sensibili non proporzionato rispetto alle finalità perseguite e non rispondente al principio di minimizzazione dei dati. Questo motiva il rigetto del ricorso avverso il provvedimento del Garante[276].

Malgrado queste pronunce, nel contesto occupazionale il rimedio dell'inutilizzabilità del dato illegittimamente acquisito/trattato dal datore di lavoro non sembra sufficiente a garantire adeguata dissuasività a tutela della privacy, forse anche per la mancata definizione dei profili sostanziali e processuali[277].

Come ultima osservazione si vuole segnalare che la normativa prevede che la violazione delle disposizioni di cui agli articoli 4, primo e secondo comma, e 8 St. lav., sia punita con le sanzioni di cui all'art. 38 St. lav., disposizioni penali, mentre il legislatore non ha

[275] Tribunale Milano sez. lav. sent. 1221 del 23 aprile 2015 (rel. Riccardo Atanasio). In parziale riforma della sentenza, la Corte di appello di Milano sez. lav. 4 agosto 2015 n. 755 (Rel. Monica Vitali) stabilisce che gli eventuali aspetti di violazione della privacy possono ricondursi semmai alle modalità con cui l'agenzia incaricata ha svolto il proprio mandato – e, dunque, potrebbero legittimare pretese di risarcimento del danno nei confronti di soggetti terzi diversi dal datore di lavoro. La sentenza è stata annotata da C. Giaconi in *GiustiziaCivile.com,* 2 marzo 2016: *Affinché un controllo difensivo realizzato ricorrendo ad investigatori privati possa dirsi compatibile con gli artt. 4 e 8 st. lav. nonché con le specifiche disposizioni in materia di privacy, invero, è necessario che lo stesso sia rispettoso di alcuni requisiti. Il controllo non dovrà essere invasivo, dovrà essere inevitabile e giustificato da un iniziale fondato sospetto sulla realizzazione di condotte illecite da parte del lavoratore controllato*. Una registrazione capillare di tutte le attività del lavoratore è ritenuta eccessiva, uno strumento di acquisizione di dati personali palesemente irrispettoso dei principi di necessità, di proporzionalità, di non eccedenza rispetto alle finalità del trattamento stesso, come previsto dal Codice Privacy. Si veda in senso contrario Tribunale di Padova, ord. Sez. lav., 8 novembre 2018, n. 6897, nella quale il Tribunale ha ritenuto legittimi i controlli effettuati da un'agenzia investigativa privata, incaricata da parte datoriale, avendo ritenuto che le condotte del lavoratore configurassero degli illeciti e non dei semplici inadempimenti contrattuali.

[276] Si trattava di un giudizio di impugnazione del provvedimento interdittivo del Garante.

[277] Proia ricorda che nei casi di violazione del diritto di informativa, la conseguenza dell'inutilizzabilità non viene applicata se il titolare abbia provveduto a fornire tardivamente l'informativa. Lo stesso Garante opera, al riguardo, un ulteriore self restraint, affermando, sulla base dell'art. 160, co. 6, del Codice, che, nel caso di produzione in giudizio di atti contenenti i dati personali, ogni valutazione sulla loro "utilizzabilità" "è rimessa esclusivamente all'autorità giudiziaria adita" (G. Proia, *op. cit*., 547).

introdotto alcuna fattispecie penale per l'inosservanza datoriale degli obblighi di cui al comma 3. La violazione della normativa sull'utilizzabilità dei dati acquisiti mediante il controllo a distanza dell'attività del lavoratore non costituisce reato, anche se il Garante in sede di audizione sui decreti attuativi del Jobs Act, aveva suggerito di estendere la sanzione penale anche alla violazione del comma 3 o di prevedere un'autonoma fattispecie di reato per la violazione dei limiti e delle condizioni utilizzabilità dei dati personali dei lavoratori. In quell'occasione il Garante aveva avvertito che risiede proprio nel comma 3 uno dei baluardi rispetto al rischio di una sorveglianza totale: è proprio il mancato rispetto dei limiti di cui al comma 3 che si annida il rischio di una sorveglianza sul lavoratore totale ed eccessivamente invasiva.

D'altra parte, in un contesto nel quale la digitalizzazione è ampiamente applicata ai processi produttivi e le potenzialità della tecnologia sono adoperate per raccogliere, trasmettere, combinare e riutilizzare le informazioni per scopi non sempre trasparenti, non appare neanche più sufficiente un mero rinvio ai principi della normativa privacy. È il Garante europeo ad ammonirci: In questo contesto, anche i principi generali del trattamento dei dati personali – necessità, proporzionalità, correttezza, trasparenza, finalità e minimizzazione della raccolta – incontrano ostacoli e limiti oggettivi di operatività. Del resto, l'adesione formale a tali principi non appare più sufficiente, ma occorre sollecitare una riflessione teorica più approfondita sulla dimensione etica del trattamento dei dati, correlando il diritto alla riservatezza e alla tutela dei dati personali ai valori della dignità e libertà individuale riconosciuti dall'art. 1 della Carta europea dei diritti fondamentali[278].

[278] *In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing.* Vedi P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa,* in P. Tullini, (a cura di) *Web e lavoro. Profili evolutivi e di tutela,* 11.

Conclusioni

Non è il caso né di avere paura né di sperare, bisogna cercare nuove armi.

Gilles Deleuze**,** Poscritto sulle società di controllo.

Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro.

S. Rodotà Discorso conclusivo alla Conferenza internazionale sulla protezione dei dati (settembre 2004).

È stato il filosofo Gilles Deleuze,[279] nel descrivere il funzionamento dei meccanismi di potere nel tardo capitalismo, ad introdurre la nozione di "società del controllo", una società nella quale non esiste un punto di sorveglianza centrale ben visibile e che genera timore, come nel Panopticon, dove la sorveglianza si sviluppa rigidamente in senso verticale, ma esiste un monitoraggio continuo, una sorveglianza insidiosa e trasversale che invade qualsiasi aspetto della vita, un Grande Fratello che raccoglie informazioni e le trasforma in algoritmi, e nella quale veniamo incoraggiati a non preoccuparci di essere controllati, fino al punto di intendere la cessione dei dati come un prezzo necessario per usufruire dei vantaggi della interconnessione.

In questo panorama la rivoluzione digitale esercita un ruolo cruciale: non è solo una rivoluzione tecnologica che investe le attività di produzione e di consumo, ma una rivoluzione culturale che coinvolge anche le attività di cittadinanza.

La diffusione dei computer, la digitalizzazione delle informazioni con la creazione di banche dati, l'avvento di Internet e dei motori di ricerca e la proliferazione dei social network sono accadimenti che hanno determinato una sostanziale modifica dell'angolo prospettico: al centro dell'attenzione non ci sono più quelle informazioni sulla persona che riguardavano un numero ristretto di individui e potevano rivestire interesse per la cronaca in quanto facevano notizia, ma tutte quelle informazioni, anche minime e di per sé poco significative, che riguardano ognuno e che necessariamente e costantemente vengono messe in

[279] Gilles Deleuze (1925-1995), filosofo francese, è autore di un saggio intitolato *Poscritto sulle società di controllo* (1990).

circolazione in un sistema economico e sociale che affida all'informatica e ad Internet lo svolgimento delle attività pubbliche e private.

Nell'ambiente digitale prende forma un nuovo modo di vivere e di lavorare, come testimonia la "vita a punti" dei cinesi[280], che è qualcosa di più e di diverso dalla mera digitalizzazione dei processi di produzione e di azione pubblica e sembra tracciare la via di una tecnologia al servizio di un controllo onnipresente sul cittadino, fino al paradosso di un totalitarismo digitale.

Rispetto al secondo dopoguerra quando l'affermazione della inviolabilità della sfera privata rispetto alle altrui interferenze, alle ingerenze nelle "vite degli altri", ha dato origine al diritto alla privacy, oggi l'espropriazione della sfera di diritti e libertà personali e della stessa autodeterminazione individuale[281] si propone in forme meno visibili, ma più insidiose. E soprattutto non è più solo delle invasioni nella sfera privata che ci dobbiamo preoccupare, ma piuttosto del modo in cui si interviene nella costruzione della sfera privata, utilizzando le enormi quantità di informazioni personali disponibili per estrarre profili individuali, per ritagliare della persona quello che interessa il mercato e creare così modelli di comportamento prevalenti in una pericolosa ottica di classificazione e di normalizzazione del singolo individuo[282]. Viviamo in un flusso continuo di dati, la nostra vita è uno scambio

---

[280] Il Social Credit System cinese utilizzato per valutare l'"affidabilità" dei cittadini, migliorare la "fiducia" nel Paese e promuovere una cultura di "sincerità" e di "credibilità giudiziaria", realizza una sorta di trasposizione sul piano sociale dei sistemi di valutazione dell'affidabilità creditizia, e funziona assegnando un "punteggio" ai cittadini sulla base della valutazione delle abitudini di acquisto, delle frequentazioni più o meno esibite, dei contenuti pubblicati in rete, penalizzando quelli socialmente o politicamente indesiderabili, con inevitabili effetti di normalizzazione. Come una sorta di programma-fedeltà, il conseguimento di uno *scoring* alto, agevola la fruizione di servizi pubblici e privati, l'esercizio di molti diritti e libertà, mentre un punteggio basso preclude l'accesso al credito, a sistemi assicurativi o previdenziali, a determinate professioni, persino a prestazioni di welfare: una sorta di misura di prevenzione fondata non su indizi di reità ma sulla mera indesiderabilità della condotta, secondo i parametri unilateralmente decisi dal Governo. (A. Soro, *La protezione dei dati personali nell'era digitale,* NGCC, 2/2019, 343).

[281] Si veda per un approfondimento Faleri che individua un vero e proprio diritto all'autodeterminazione informativa, secondo il quale ciascun soggetto deve avere la possibilità di decidere da solo le sorti delle informazioni che riguardano la sua persona. Il diritto all'autodeterminazione costituisce una posizione giuridica soggettiva di non facile realizzazione, soprattutto nel settore dei rapporti di lavoro dove l'affermazione formale del principio di autodeterminazione non è sufficiente a garantire l'autodeterminazione effettiva (C. Faleri, *Autonomia individuale e diritto alla riservatezza,* in *Riv. It. Dir. Lav.*, n.1/2000, 304).

[282] *Le tecnologie elettroniche, con la possibilità di organizzare, unificare e far permanere informazioni disperse o destinate a scomparire, hanno introdotto un modo inedito di costruzione della sfera privata.* […] *Queste nuove modalità di costruzione della sfera privata non danno luogo soltanto a invasioni lecite o indebite, ma determinano un profondo mutamento della qualità stessa della sfera privata, permettono la disponibilità di masse enormi di informazioni personali "che possono essere utilizzate per estrarre profili individuali e di gruppo, per individuare comportamenti prevalenti, con la concreta possibilità di definire criteri di normalità e di cercare di imporli"* (S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, 67-68). In proposito vedi anche A. Soro: *Se prive di regole, le nuove tecnologie possono alimentare un regime della sorveglianza tale da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere. E questo non solo per lucido calcolo di profitto o per politiche statali illiberali, ma anche solo per assuefazione alla cessione indiscriminata*

continuo di informazioni, e in questa raccolta onnivora di dati perdiamo di vista il fatto che il dato rappresenta la proiezione del sé nella dimensione digitale e tanto più il dato personale viene ridotto ad una cifra, ad una merce da sfruttare, tanto più la persona, sempre più frammentata e identificata con quella parziale informazione, è ridotta ad un'astrazione priva di individualità e, dunque, di dignità, in una "decontestualizzazione" che è già di per sé una falsa rappresentazione della realtà[283].

Attraverso trattamenti automatizzati di grandi quantità di dati personali, aggregati, combinati, incrociati e conservati nelle banche dati, senza alcun riferimento al loro contesto originario e con finalità ultime di trattamento sempre meno trasparenti, persone/lavoratori divenuti di vetro, per visibilità e vulnerabilità, vedono minacciati i loro diritti fondamentali[284]. Per rispondere alle nuove esigenze di tutela di lavoratori/persone elettroniche, Rodotà aveva invocato un *habeas data*, ispirato all'*habeas corpus* quale strumento per la salvaguardia e lo sviluppo della libertà personale, che fondasse un nuovo approccio all'idea di libertà e di privacy esteso anche all'ambiente elettronico[285].

---

e disattenta, di quei frammenti di libertà che sono i dati e che incorporano sempre più relazioni tra persone e rapporti di potere. (A. Soro, *La protezione dei dati personali nell'era digitale*, NGCC, 2/2019, 343).

[283] V. S. Niger, *op. cit*., 205. Uno dei rischi conseguenti alla diffusione dei *big data* risiede nel pericolo di assumere decisioni basate su trattamenti automatizzati di dati destinati a valutare taluni aspetti della personalità del singolo individuo, quali il rendimento professionale, il credito, l'affidabilità, il comportamento.

L'automatizzazione della fase decisionale e gestionale (*management by algorithm*) negli aspetti organizzativi e di gestione del personale sembra poter produrre un rischio di de-umanizzazione del lavoro, laddove non sia il processo produttivo ad adattarsi alle caratteristiche dell'uomo, ma l'uomo a doversi inserire in esso e rispondere automaticamente ad esigenze di miglioramento della performance.

Da notare come le recensioni *on line* degli utenti rispetto alla prestazione svolta da coloro che operano a chiamata per conto di un'azienda che fornisce servizi su una piattaforma digitale, presentano qualche affinità in termini di rischi con la sorveglianza a distanza: la recensione *on line* rilasciata dagli utenti è diretta alla valutazione dell'attività eseguita dagli operatori a chiamata e il feedback negativo potrebbe essere utilizzato dal datore a tutti i fini che ritiene opportuni, incluso il licenziamento. Non si potrebbero con facilità estendere alla valutazione delle prestazioni su piattaforma le tutele dell'art. 4, ma potrebbe venire in aiuto il diritto a non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, previsto dall'art. 22 del Reg.

[284] Già nel gennaio 2008 il Times aveva rivelato che Microsoft stava mettendo a punto un programma (commercializzabile, secondo la stessa multinazionale, in tre/cinque anni) capace di controllare minuto per minuto i dipendenti. Utilizzando microcamere e sensori wireless raccoglieva informazioni che vanno dalla temperatura corporea al battito cardiaco, dall'espressione facciale alla posizione assunta alla scrivania, dai tasti digitati sulla tastiera ai siti Internet visitati. E negli Stati Uniti i risultati dell'indagine sulla sorveglianza elettronica sul posto di lavoro per il 2007 attestavano che il 70% dei datori di lavoro aveva monitorato la navigazione in Internet dei dipendenti registrando e archiviando i contenuti; circa il 30 % dei lavoratori era stato ripreso e aveva subito una qualche conseguenza per uso illegittimo di e-mail e Internet; il 10% monitorava blogosfera e social networking alla ricerca di commenti sull'azienda; quasi il 50% monitorava l'uso del telefono e nel 20% dei casi si registravano le telefonate o i messaggi lasciati in segreterie telefoniche. (M. Paissan, *E-mail e navigazione in internet: le linee del Garante*, in P. Tullini (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, 13).

[285] G. Ziccardi, *Internet controllo e libertà, Trasparenza, sorveglianza e segreto nell'era tecnologica,* Raffaello Cortina Editore, 2015, 71. V. anche S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Bari, 2014.

In questo scenario di grandi cambiamenti organizzativi e produttivi si inserisce il tema dei controlli sul luogo di lavoro, in un contesto nel quale anche la prestazione lavorativa si esprime attraverso un flusso di dati, che consente di potenziare la sorveglianza aziendale e di procedere alla profilazione stessa dei lavoratori[286]. Nell'industria 4.0, caratterizzata da un alto livello di automazione e da processi produttivi digitalizzati, nella quale il lavoratore mentre governa la macchina dissemina tracce digitali, è arduo per definizione segnare la linea di confine tra l'esercizio legittimo del potere datoriale di organizzazione e controllo e la tutela dei diritti del lavoratore di riservatezza, identità e di autodeterminazione[287].

Anche il potere di controllo a distanza subisce una mutazione genetica e la disciplina statutaria, pur dopo la novella del 2015, mal si presta ad essere applicata all'ambiente digitale della *smart factory*, lasciando intravedere alcune aree di criticità[288]. Una di queste è rappresentata proprio dalla difficoltà di distinguere gli strumenti di lavoro dagli strumenti di controllo, oggetto di una disciplina diversificata di portata potenzialmente esplosiva. Sottrarre alla disciplina limitativa ed autorizzativa imposta dal comma 1 dell'art. 4 l'intero armamentario delle dotazioni informatiche, ormai parte integrante ed imprescindibile del corredo del lavoratore e al tempo stesso in grado di acquisire una mole enorme di dati e

---

[286] Il principale utilizzo dei Big Data riguarda la produzione di beni e servizi a misura del cliente, la riduzione dei costi, il miglioramento dell'efficienza e della produttività aziendale, ma ha implicazioni rischiose per il controllo totale sul soggetto/lavoratore, per il maggiore squilibrio contrattuale che produce e per le possibili pratiche discriminatorie. *Sono invece rimaste in ombra le rischiose implicazioni della raccolta massiccia e dell'analisi dei dati personali dei lavoratori (HR Analytics): dall'aumento dell'asimmetria informativa nel rapporto di lavoro, allo squilibrio contrattuale, alla diffusione di inedite pratiche discriminatorie* (P. Tullini, *Il controllo a distanza,* in *Controlli a distanza e tutela dei dati personali del lavoratore*, *op. cit*., 120).

[287] *Alla frammentazione della persona umana, della sua autenticità, si accompagna una moltiplicazione delle "persone elettroniche", tante quante sono gli archivi o banche che custodiscono i diversi dati rilevanti. Una siffatta "deriva tecnologica" che comporta questa nostra nuova condizione di "donne e uomini di vetro" o, rectius, di "lavoratrici e lavoratori di vetro", non può che concretizzarsi in una minaccia per i diritti fondamentali per l'individuo – e […] del lavoratore, ed in particolare per la sua riservatezza, identità personale ed autodeterminazione a cui non è possibile non reagire.* (C. Colapietro, *Digitalizzazione del lavoro e tutela della riservatezza della persona,* in P. Tullini (a cura di) *Web e lavoro, op. cit.,* 23).

[288] Lo schema di decreto legislativo contenente la modifica dell'art. 4 St. lav. è giunto alla promulgazione quasi inalterato, disinvoltamente ignorandosi le voci preoccupate che da più parti si erano fatte sentire. Trasmesso alle Camere per il necessario parere parlamentare, la stessa Camera dei Deputati, che pure ha espresso il proprio parere favorevole al decreto, aveva formulato le seguenti significative osservazioni: "all'articolo 23, comma 1, capoverso Art. 4, apportare le seguenti modificazioni: a) al primo comma, premettere il seguente: È vietato l'uso di impianti audiovisivi e di altri strumenti che abbiano quale finalità il controllo a distanza dell'attività dei lavoratori; b) al secondo comma, sostituire le parole: La disposizione di cui al primo comma non si applica agli con le seguenti: L'accordo e l'autorizzazione di cui al secondo comma non sono richiesti per l'impiego degli e sostituire le parole: agli strumenti di registrazione con le seguenti: per l'installazione degli strumenti di registrazione; c) sostituire il comma 3 con il seguente: I dati registrati dagli strumenti di cui al terzo comma sono utilizzabili a condizione che sia data al lavoratore preventiva e adeguata informazione delle loro modalità d'uso, nonché dei casi e dei limiti di effettuazione degli eventuali controlli, che in ogni caso debbono avvenire nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196". Lette con il senno di poi queste osservazioni appaiono particolarmente significative: se accolte avrebbero risolto molte delle questioni interpretative sollevati in dottrina.

notizie sulle modalità di svolgimento della prestazione e sulla persona stessa, può significare una perdita di tutele in capo al lavoratore subordinato davvero significativa[289].

Nella *smart factory* non solo il controllo a distanza, parte integrante dell'ambiente digitale, spesso non è distinguibile dal processo produttivo e dall'organizzazione del lavoro, ma le tecnologie intelligenti, le piattaforme automatizzate e gli altri strumenti tecnologici utilizzati per rendere la prestazione lavorativa, scelti e assegnati in assenza di confronto sindacale, si configurano come apparati sofisticati, dotati di una pluralità di funzioni, in grado di soddisfare molteplici esigenze aziendali, dallo svolgimento dell'attività lavorativa al riscontro di errori e inadempimenti, dalla misurazione qualitativa e quantitativa della prestazione, al monitoraggio della mobilità dei lavoratori. Sono strumenti in grado di catturare in modo continuativo informazioni relative sia alla prestazione che alla persona, sfuggendo spesso alla consapevolezza del lavoratore e rispetto ai quali sembrano offrire scarsa tutela, forse più formale che sostanziale, le garanzie individuali di carattere informativo introdotte dal terzo comma dell'art. 4 St. lav. [290].

Si consideri anche che restano fuori dalle previsioni statutarie i cosiddetti sistemi di controllo passivi che si fondano sull'acquisizione di informazioni fornite spontaneamente dagli stessi lavoratori-utenti della rete: opinioni espresse sui social network (Facebook, Twitter o Istagram), esperienze professionali indicate su Linkedin, siti internet visitati, visualizzazioni di giornali online o di negozi virtuali, offrono una rappresentazione a 360 gradi della personalità e delle attitudini dei soggetti[291]. I social network operano quali giganteschi collettori di dati nei quali la persona immette volontariamente informazioni personali, relative alla propria sfera privata e anche lavorativa. In qualche caso, come quello degli addetti al *social media marketing,* si identificano in un vero e proprio strumento di lavoro,

---

[289] Cosattini parla di possibile *tabula rasa* di ogni forma di tutela, attesa l'ampiezza delle locuzioni utilizzate dal Legislatore (L. A. Cosattini, *op. cit*., 989).

[290] *La funzione di controllo costituisce una parte integrante e inscindibile dell'organizzazione produttiva "intelligente", sicché risulterebbe probabilmente frustrato in partenza il tentativo di considerare in modo separato – come suggerisce l'art. 4, co.1 e 2, St. Lav. – le tecnologie "esclusivamente" finalizzate al controllo per specifiche ragioni aziendali e quelle destinate all'esecuzione della prestazione.* (P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in P. Tullini (a cura di) *Web e lavoro*, op. cit., 17, 18). Questi rischi evidentemente si accentuano quando la prestazione lavorativa sia completamente esternalizzata, sia resa sfruttando le risorse del web e la connettività da remoto con l'impresa.

[291] L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?* in *Rivista italiana di diritto del lavoro*, 3/2016, 345. Anche sull'*effetto boomerang per cui gli stessi soggetti che hanno inserito i dati finiscono con il rimanerne imprigionati e condizionati. Sempre più spesso rigurgiti del passato impattano sul presente, in quanto le nuove tecnologie hanno alterato il concetto di memoria e di tempo storico, allontanando la capacità di dimenticare e riproponendo, senza alcuna contestualizzazione, interi frammenti di una più complessa, e magari rinnovata, identità*.

ma in tutti casi costituiscono uno strumento di "dossieraggio" suscettibile di rappresentare una minaccia, forse sottovalutata, per i diritti di riservatezza e libertà dei lavoratori[292].

Rispetto a queste insidie dovrebbero venire in soccorso le previsioni della normativa europea a tutela dei dati personali. Il principio di *privacy by design*, volto a tutelare il dato sin dal momento della progettazione di sistemi e strumenti e il principio di *privacy by default,* inteso a tutelare la vita privata per impostazione predefinita, impongono di valutare preliminarmente e di ridurre al minimo l'impatto sulla riservatezza dei dati, da tutelare sin dalla fase di sviluppo e progettazione degli strumenti. Il titolare del trattamento è tenuto ad adottare policy interne e misure tecniche e organizzative adeguate, quali la pseudonimizzazione e la minimizzazione dei dati, al fine di tutelare i diritti degli interessati.

Altra criticità emersa nel corso dell'analisi è ravvisabile nella contraddizione interna alla norma statutaria che consente l'utilizzabilità dei dati a qualsiasi fine connesso al rapporto di lavoro, subordinandola al rispetto della normativa sulla privacy, la quale a sua volta impone quale condizione di legittimità il principio della limitazione della finalità. Si configura una sorta di circolo vizioso per cui i dati per essere utilizzabili a tutti i fini dovranno essere acquisiti e trattati nel rispetto del principio di finalità, dunque per il fine indicato preventivamente e in modo compatibile, proporzionato e non eccedente rispetto ad esso.

L'impasse non è di poco conto perché l'utilizzo delle informazioni raccolte per qualsiasi fine connesso al rapporto di lavoro, soprattutto se raccolte attraverso strumenti di lavoro, liberamente scelti dal datore al di fuori del confronto con il sindacato, espanderebbe i poteri dell'imprenditore e rischierebbe di comprimere la sfera di dignità e riservatezza del lavoratore. Anche in questo caso in dottrina si è fatto appello alle disposizioni sulla tutela dei dati personali dettate dal Regolamento europeo, e si è auspicata un'interpretazione sistematica e costituzionalmente orientata del dato letterale, una lettura della norma che in virtù del sistema complessivo di tutele, interpreti restrittivamente l'espressione "tutti i fini connessi al rapporto di lavoro", intendendola come "tutti i fini compatibili con la finalità della raccolta"[293]. In effetti, se da un lato il potere di controllo a distanza risulta ampliato dalla dilatazione delle finalità di utilizzo dei dati, dall'altra sono le modalità di esercizio di quel potere indicate dalla normativa sulla privacy e conformi ai principi di proporzionalità,

[292] Al di là delle precedenti considerazioni critiche preoccupa la sottovalutazione della pericolosità del "veicolo": sui social network, tra cui naturalmente Facebook, la riservatezza è notoriamente un mito. (P. Tosi – E. Puccetti, *Chat Facebook: se la riservatezza legittima la denigrazione del datore di lavoro*, in *Giurisprudenza italiana*, gennaio 2019, 143).

[293] V. Nuzzo, *op. cit.*, 219.

non eccedenza e trasparenza, a costituire un baluardo a difesa della riservatezza del lavoratore.

Da ultimo, la scelta compiuta nel novellare l'art. 4 St. lav. di spostare il focus della disciplina e con esso l'equilibrio interno verso la dimensione individuale, introducendo requisiti di legittimità per lo specifico atto di controllo e rafforzando la consapevolezza del singolo lavoratore attraverso l'adeguata preventiva informazione, può rappresentare un ulteriore elemento di criticità della nuova disciplina del controllo a distanza. Nello spostarsi dal piano collettivo a quello individuale, il baricentro delle tutele viene a poggiare sulla tenuta del funzionamento delle regole dettate dalla normativa sulla privacy e se nella pratica non si potenzia il raccordo fra le due discipline potrebbe tradursi in un'operazione inadeguata e insufficiente per assicurare il contemperamento dei diritti[294].

È vero che fino ad oggi il tema del coordinamento fra le disposizioni statutarie e la disciplina sul trattamento dei dati personali ha vissuto dell'attività del Garante della Privacy e del costante lavoro di dottrina e giurisprudenza, ma la conclusione condivisa ed auspicata dagli interpreti e dagli studiosi è che entrambe le normative debbano essere applicate in modo concorrente, integrandosi le une con le altre. È di fondamentale importanza integrare i due piani normativi ed effettuare un raccordo mirato con il Regolamento europeo, in una sintesi che sia comprensione dei significati e del funzionamento dell'assetto regolativo della privacy e di quello del lavoro, pur diversi in termini di valori e di strumenti operativi, ma che devono confrontarsi offrendo anche alle aziende la certezza di una prassi consolidata[295].

La via da seguire è quella di ricorrere alla normativa di protezione dei dati quale fondamentale presidio di garanzia, tanto in termini di diritti esercitabili dall'utente quanto in termini di responsabilizzazione dei protagonisti attivi nella articolata filiera in cui si snodano questi trattamenti[296]. In questi termini si dovranno in parte ripensare le categorie giuridiche, riscrivendole con un approccio multidisciplinare e con la duttilità necessaria ad accogliere una realtà in costante evoluzione.

Concludo condividendo l'auspicio del Presidente Soro: Il passo che resta da fare, raccogliendo una delle sfide più importanti che il legame tra tecnologia, nuovi diritti e

---

[294] P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa*, in P. Tullini (a cura di) *op. cit.*, 119.

[295] Vedi le riflessioni di L. Calafà, in A. Levi, *op. cit.*, 147. Tra l'altro l'Autrice ravvisa un'occasione mancata nel fatto che non siano state previste procedure periodiche codeterminative da sviluppare con il Garante al fine di elaborare principi e criteri direttivi che tengano conto delle pronunce della giurisprudenza elaborate dopo la scomparsa del divieto generale previsto nell'art. 4 dello Statuto e favoriscano la più ampia integrazione fra le due discipline.

[296] A. Soro, *Persone in rete*, *op.cit.*, 160.

prevenzione pone alle nostre generazioni, è quello del riconoscimento universale del diritto alla protezione dei dati personali, quale primo presupposto di libertà del XXI secolo[297].

[297] A. Soro, *op. cit.*, 165-166.

Bibliografia

AIMO, M., *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, Napoli, 2002.

ALVINO, I. *L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica,* in *Diritto delle Relazioni Industriali*, n. 4/2014, 999 e 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 *Labour Law Issues* Vol. 2, N.1, 2016, 3 e ss.

ANGIELLO, L. *I controlli del datore di lavoro sui dipendenti: perduranti incertezze,* in *Il lavoro nella giurisprudenza*, n. 3/2019, 298 e ss. (Nota a Tribunale di Padova, Sez. lav., 8 novembre 2018, n. 6897 ord.).

ARCELLA, G. *GDPR: il Registro delle attività di trattamento e le misure di accountability*, in *Notariato* n. 4/2018, 394 e ss.

BARBERA A. *Commentario della Costituzione. Principi fondamentali,* a cura di Giuseppe Branca, Zanichelli, Bologna, 1975.

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

BAUMAN, Z. LYON, D. *Sesto potere. La sorveglianza nella modernità liquida*, Editori Laterza, Bari, 2013.

BARRACO, E. - SITZIA, A. *Un de profundis per i "controlli difensivi" del datore di lavoro?* in *Il lavoro nella giurisprudenza* n. 4/2013, 383 e ss. (Nota a Cass. Civ., Sez. lav., 1 ottobre 2012, n. 16622).

BARRACO, E. - SITZIA, A. *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie,* Wolters Kluwer, Milano, 2016.

BELLAVISTA, A., *Tutela delle persone e di altri soggetti rispetto al trattamento dati personali,* in *Il lavoro nella giurisprudenza*, n. 5/1996, 375 e ss.

BELLAVISTA, A., *Sorveglianza, privacy e rapporto di lavoro,* in *Diritto dell'Internet*, n. 5/2006, 437 e ss.

BELLAVISTA, A., *Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in *Il lavoro nella giurisprudenza*, n. 8/9 2014, 737.

CAIRO, L. - VILLA, U. *I controlli a distanza a quattro anni dal Jobs Act*, in *Il lavoro nella giurisprudenza*, n. 7/2019, 676 e ss.

CALAFÀ, L. *I limiti derivanti dalla disciplina della tutela della riservatezza*, in Levi, A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il Jobs Act*, Giuffrè, Milano, 2016.

CALIFANO, L. *Tecnologie di controllo del lavoro, diritto alla riservatezza e orientamenti del Garante per la protezione dei dati personali*, in Tullini, P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017.

CARINCI, M.T. *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. Lgs. 151/2015): spunti per un dibattito*, in *Labour Law Issues*, Vol. 2, n. 1/2016.

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

CARNELUTTI, F. *Il diritto alla vita privata,* in *Riv. Trim. Dir. Pub*., 1955, 3 ss.

CARTA, C. *Documenti ''personali'' o ''privati'': il caso dei files salvati sul computer aziendale*, in *La nuova giurisprudenza civile commentata n.* 9/2018, 1259 e ss.

CARTA, M. *Diritto alla vita privata ed Internet nell'esperienza giuridica europea ed internazionale*, in *Diritto dell'informazione e dell'informatica*, n. 1/2014, 1 e ss.

CASILLO, R. *La dignità nel rapporto di lavoro,* in *Rivista di diritto civile,* n. 5/2008, 593 e ss.

CASSANO, G. *Prime pronunce sul nuovo art. 4 della l. n. 300/1970*, in *Diritto delle Relazioni Industriali*, n. 1/2019, 302 e ss. (Nota a Trib. La Spezia 25 novembre 2016, Trib. Milano 24 ottobre 2017 e Trib. Padova 19 gennaio 2018).

CIPRIANI, A., GRAMOLATI, A., MARI, G. (a cura di) *Il lavoro 4.0. La quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, Firenze, 2018.

CIUCCIOVINO, S. *Le nuove questioni di regolazione del lavoro nell'industria 4.0 e nella gig economy: un problem framework per la riflessione,* in *Diritto delle Relazioni Industriali,* n. 4/2018, 1043 e ss.

COLAPIETRO, C. *Digitalizzazione del lavoro e tutela della riservatezza della persona*, in Tullini, P. (a cura di) *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Torino, 2017.

COLAPIETRO, C. *Dignità e riservatezza del lavoratore nell'uso di tecnologie digitali,* in *Giornale di diritto del lavoro e di relazioni industriali*, n. 3/2017, 439 e ss.

COSATTINI, L. A. *Le modifiche all'art. 4 Stat. lav. sui controlli a distanza, tanto rumore; per nulla?*, in *Il lavoro nella giurisprudenza*, n. 11/2015, 985 e ss.

COSCIA, C. *Le modifiche all'art. 4 Stat. lav.: dignità e riservatezza del lavoratore continuano a prevalere sulla tutela del patrimonio aziendale*, in *Diritto penale e processo*, n. 7/2018, 872 e ss. (Nota a Cassazione Penale, Sez. III, 31 gennaio 2018, n. 4564).

COSTANTINI, F. *Il Regolamento (UE) 679/2016 sulla protezione dei dati personali,* in *Il lavoro nella giurisprudenza*, n. 6/2018, 545 e ss.

CRISCUOLO, C. *Potere di controllo e computer aziendale,* in *Rivista Italiana Diritto del lavoro*, n. 2/2019, 9 e ss.

CUFFARO, V. *Il diritto europeo sul trattamento dei dati personali,* in *Contratto e Impresa*, n. 3/2018, 1098 e ss.

CUFFARO, V. *Quel che resta di un codice: il D. Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Il Corriere giuridico* n. 10/2018, 1181 e ss.

DAGNINO, E. *Tecnologie e controlli a distanza*, in *Diritto delle Relazioni Industriali*, fasc.4, 2015, 988.

DAGNINO, E. *People Analytics: lavoro e tutele al tempo del management tramite big data*, in *Labour Law Issues* vol. 3 n. 1, 2017.

DAGNINO, E. *Una questione di fiducia: la reputazione ai tempi delle piattaforme online tra diritto alla privacy e prospettive di mercato*, in *Diritto delle Relazioni Industriali*, 1/2017, 247 e ss.

D'ATENA, A. *In tema di principi e valori costituzionali,* in *Giurisprudenza Costituzionale*, n. 6/1997, 3065 e ss.

DE LUCA TAMAJO, R., IMPERIALI D'AFFLITTO, R., PISANI, C., ROMEI, R., *Nuove tecnologie e tutela della riservatezza dei lavoratori,* Franco Angeli, Milano, 1988.

DE MARCO, E. *Controlli a distanza e privacy del lavoratore*, in Giurisprudenza Italiana, marzo 2018, 682 e ss. (Nota a Cassazione penale, Sez. V, 9 ottobre 2017, n. 46428).

DEL FEDERICO, C. *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive,* in Tullini, P. (a cura di) *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Torino, 2017.

DEL PRATO, E. *Regole deontologiche delle professioni e principio di sussidiarietà: l'esperienza italiana*, in *Rivista di diritto civile*, n. 4/2014, 764 e ss.

DEL PUNTA, R. *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015),* in *Rivista Italiana di Diritto del Lavoro*, n.1/2016, 77 e ss.

DESSÌ, O. *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.* Edizioni scientifiche italiane, Napoli, 2017.

DI MEO, R. *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon,* in Labou Law Issues, n.1/2018.

DONINI, A. *Tecniche avanzate di analisi dei dati e protezione dei lavoratori,* in *Diritto delle Relazioni Industriali*, n.1/2018, 222 e ss.

DONINI, A. *Il mercato dei servizi sul web: il rapporto di lavoro su piattaforma digitale*, in Tullini, P. (a cura di) *Web e lavoro. Profili evolutivi e di tutela,* Giappichelli, Torino, 2017.

DONINI, A. *Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy,* in *Labour Law Issues,* Vol. 3, n. 1, 2017.

ESPOSITO, M. S. *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Diritto dell'informazione e dell'informatica*, n. 4-5/2019, 1071 e ss.

FACCIOLI, E. - CASSARO, M. *Il "GDPR"e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design,* in *Il Diritto Industriale*, n. 6/2018, 561 e ss.

FALERI, C. *Autonomia individuale e diritto alla riservatezza,* in *Rivista italiana di diritto del lavoro,* n. 1/2000, 303 e ss.

FAVRETTO, C. *Controlli difensivi sul PC aziendale: l'area grigia della libertà e della dignità del lavoratore quale limite al potere datoriale,* in *Argomenti di diritto del lavoro,* n. 2/2017, 443 e ss.

FORLIVESI, M., *Il controllo della vita del lavoratore attraverso i social network,* in Tullini, P. (a cura di) *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Torino, 2017.

FORMICI, G. *Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza*, in *Osservatorio Costituzionale*, 1/2018.

FUSCO, F. *Il pomo della discordia: il badge come strumento di controllo a distanza?,* in *Rivista Italiana di Diritto del Lavoro,* n. 2/2011, 31 e ss. (Nota a Tribunale di Napoli 29 settembre 2010 e Tribunale di Napoli 23 settembre 2010).

GALARDI, R. *Il controllo sugli accessi ad Internet al vaglio della Cassazione,* in *Rivista Italiana di Diritto del Lavoro,* n. 2/2010, 564 e ss. (Nota a Cassazione, Sez. lav. 23 febbraio 2010, n. 4375).

GERMANI, E. – FEROLA, L. *Il Wearable computing e gli orizzonti futuri della privacy*, in *Diritto dell'informazione e dell'informatica*, n. 1/2014, 75 e ss.

GRAGNOLI, E. *Dalla tutela della libertà alla tutela della dignità e della riservatezza dei lavoratori*, in *Argomenti di diritto del lavoro*, n.1/2007, 1211 e ss.

GRAGNOLI, E. *L'uso della posta elettronica sui luoghi di lavoro e la strategia di protezione elaborata dall'Autorità Garante,* in Tullini, P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro, Trattato di diritto commerciale e di diritto pubblico dell'economia*, vol. cinquantottesimo, Cedam, Padova 2010.

GRAMANO, E. *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi*, in *Diritto delle Relazioni Industriali*, n. 1/2018, 265 e ss. (Nota a Trib. Roma, Ord. 24 marzo 2017).

GRAUSO, M. *Radio Frequency Identification Technology e tutela della persona*, in *Diritto dell'Internet*, n. 6/2005, 623 e ss.

GUIDETTI SERRA, B. *Le schedature Fiat. Cronache di un processo e altre cronache*, Rosenberg&Sellier, Torino, 1984.

IAQUINTA, F. INGRAO, A. *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, in *Diritto delle Relazioni Industriali*, n. 4, 2014, 1027 e ss.

INGRAO, A. *Il controllo a distanza effettuato mediante Social network*, in *Labour Law Issues*, Vol. 2, N. 1, 2016, 105 e ss.

INGRAO, A. *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, in *Rivista Italiana di Diritto del Lavoro*, n. 1, 2017, e ss. 46.

INGRAO, A. *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018.

INGRAO, A. *I controlli difensivi tra passato e presente: privacy del lavoratore e inutilizzabilità dei dati*, in *Nuova giurisprudenza civile commentata*, n. 4/2019, 649 e ss. (Nota a Trib. Padova, sez. lav., 24.12.2018).

INGRAO, A. *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in *Diritto delle Relazioni Industriali*, n. 3/2019, 895 e ss.

INGRAO, A. *Il potere di controllo a distanza sull'ozio telematico e il limite del diritto alla privacy del lavoratore*, in *Rivista Italiana di Diritto del Lavoro*, n. 3/2019, 414 e ss. (Nota a Cassazione, sez. lav. n. 3133, 1.2.2019).

INGRAO, A. *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour Law Issues*, Vol. 5, N. 2, 2019, 128 e ss.

IULIANI, A. *Note minime in tema di trattamento dei dati personali*, in *Europa e diritto privato*, n. 1/ 2018, 293 e ss.

LAMBERTUCCI, P. *I poteri del datore di lavoro nello Statuto dei Lavoratori dopo l'attuazione del C.D. Jobs Act del 2015: primi spunti di riflessione,* in *Argomenti di diritto del lavoro*, n. 3/2016, 514 e 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 Working Papers CSDLE, Massimo D'Antona, 2015.

LAMBERTUCCI, P. *La disciplina dei "controlli a distanza" dopo il Jobs Act: continuità e discontinuità con lo Statuto dei lavoratori,* in F. Carinci (a cura di), *Jobs Act: un primo bilancio. Atti del XI Seminario di Bertinoro-Bologna del 22-23 ottobre 2015,* ADAPT University Press, 2016, 270.

LANOTTE, M. *La ridefinizione dei limiti al potere di controllo a distanza,* in A. Levi (a cura di), *Il nuovo art. 4 sui controlli a distanza,* Giuffré, Milano 2016.

LATTANZI, R. *Dallo Statuto dei lavoratori alla disciplina di protezione dei dati personali, Rivista italiana diritto lavoro,* n.1/2011, 151 e ss.

LEVI, A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act,* Giuffrè, Milano, 2016.

LEVI, A., *Il controllo difensivo a distanza e l'inoperatività dell'art. 4 dello Statuto*, in *Il lavoro nella giurisprudenza* n. 5/2018, 471 e ss. (Nota a Cassazione Civile, Sez. lav., 10 novembre 2017, n. 26682).

LUCCHINI GUASTALLA, E. *Trattamento dei dati personali e danno alla riservatezza*, in *Responsabilità civile e previdenza*, n. 3, maggio-giugno 2003, 632 e ss.

LUCCHINI GUASTALLA, E. *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, n. 1/2018.

LUGARESI, N. *Uso di Internet sul luogo di lavoro, controlli del datore di lavoro e riservatezza del lavoratore*, in Tullini, P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro, Trattato di diritto commerciale e di diritto pubblico dell'economia*, vol. cinquantottesimo, Cedam, Padova 2010.

MAIO, V. *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica,* in *Argomenti di diritto del lavoro,* n. 6/2015, 1186 e ss.

MAIO, V. *Il diritto del lavoro e le nuove sfide della rivoluzione robotica*, in *Argomenti di diritto del lavoro*, n. 6/2018, 1414 e ss.

MARAZZA, M. *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in Working Papers CSDLE Massimo D'Antona, 2016.

MARAZZA, M. *I controlli a distanza del lavoratore di natura "difensiva",* in Tullini, P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore,* Giappichelli, Torino, 2017.

MARCIANTE, M. *Recenti sviluppi in tema di videosorveglianza nei luoghi di lavoro in ambito CEDU,* in *Giurisprudenza Italiana*, maggio 2018, 1157 e ss.

MARESCA, A. *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, Ipsoa Quotidiano, 22 febbraio 2016.

MARESCA, A. *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei Lavoratori*, in *Rivista Italiana di Diritto del Lavoro*, n. 4/2016, 512 e ss.

MASTRELIA, D. *Gestione dei big data in una prospettiva orientata alla tutela della privacy degli individui,* in *Il Diritto Industriale*, 4/2018, 364 e ss.

MIRAGLIA, V. *Il controllo a distanza dell'attività dei lavoratori: il limite invalicabile*, in *Giurisprudenza italiana,* giugno 2018, 1459 e ss.

NIGER, S. *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali,* CEDAM, Padova, 2006.

NUZZO, V. *I software che registrano la durata delle telefonate nei call center sono strumenti di lavoro?* in *Rivista Italiana di Diritto del Lavoro*, n.2/2018.

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

OLIVELLI, F. *Lo "stratagemma" di Facebook come controllo difensivo occulto: provocazione o tutela del patrimonio aziendale?* in *Argomenti di diritto del lavoro*, n. 6/2015, 1303 e ss.

OLIVELLI, F. *Il difficile bilanciamento tra la tutela della privacy e le esigenze di controllo del datore di lavoro,* in *Rivista Italiana Diritto del Lavoro*, n.2/2013, 328 e ss. (Nota a Tribunale di Ferrara 27 agosto 2012, n. 172).

PAISSAN, M. *E-mail e navigazione in internet: le linee del Garante*, in Tullini, P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro, Trattato di diritto commerciale e di diritto pubblico dell'economia,* vol. cinquantottesimo, Cedam, Padova 2010.

PERINA, L. *L'evoluzione della giurisprudenza e dei provvedimenti del Garante in materia di protezione dei dati personali dei lavoratori subordinati*, in *Rivista italiana di diritto del lavoro*, 2/2010, 305 e ss.

PETTINELLI, R. *Controlli difensivi: storia di un anacronismo,* in *Argomenti di diritto del lavoro*, 6/2018, 1591 e ss. (Nota a Tribunale di Roma, ord. 13 giugno 2018).

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

PIRAINO, F. *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civili commentate*, n. 2/2017, 369 e ss.

PISANI, C. *Il computer e l'art. 4 dello Statuto dei Lavoratori*, in De Luca Tamajo, R.- Imperiali D'Afflitto, R. - Pisani, C. - Romei, R. *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Franco Angeli, Milano, 1988.

PIZZOFERRATO, A. *Gli effetti del GDPR sulla disciplina del trattamento aziendale dei dati del lavoratore,* in *Argomenti di diritto del lavoro,* n. 4-5/2018, 1034 e ss.

PROIA, G. *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza*, in *Rivista Italiana di Diritto del Lavoro*, n. 4/2016, 547 e ss.

RECCHIA, G. A. Controlli datoriali difensivi: note su una categoria in via di estinzione, in Il lavoro nella giurisprudenza, 4/2017, 346 e ss. (Nota a Cassazione Civile, Sez. lav., 8 novembre 2016, n. 22662).

RICCI, A. *Il controllo informatico a distanza sul lavoratore fra giurisprudenza e Jobs Act. La web-sorveglianza nella modernità liquida,* in *Studium iuris* n. 3-4/2016, 306 e ss.

RICCI, M. *I controlli a distanza dei lavoratori tra istanze di revisione e flessibilità "nel" lavoro,* in *Argomenti di diritto del lavoro* n. 4-5/2016, 740 e ss.

RICCIO, G.M. *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e Regolamento privacy*, in *Nuova Giurisprudenza civile commentata*, n. 12/2018, 1805 e ss.

RODOTÀ, S. *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy,* in *Europa e Diritto privato*, n. 1/2004, 6 e ss.

RODOTÀ, S. *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, Roma, 2014.

ROMAGNOLI, U. *"Noi e loro": diritto del lavoro e nuove tecnologie,* in *Rivista trimestrale di diritto e procedura civile*, 1986, 377 e ss.

ROMEI, R. *Il dibattito dottrinale sull'art. 4 dello Statuto dei Lavoratori,* in De Luca Tamajo,R. - Imperiali D'Afflitto, R. - Pisani, C. - Romei, R. *Nuove tecnologie e tutela della riservatezza dei lavoratori,* Franco Angeli, Milano, 1988.

ROSSI, S. *Tutela della riservatezza e limiti ai controlli difensivi,* in *Giurisprudenza italiana*, febbraio 2019, 390 e ss.

ROTA, A. *Stampa 3D: un nuovo rischio da ignoto tecnologico?,* in *Labour Law Issues*, Vol.1, N. 1, 2015, 108 e ss.

RUSSO, M. *Quis custodiet ipsos custodes? I "nuovi" limiti all'esercizio del potere di controllo a distanza,* in *Labour Law Issues*, vol.2, n. 2/2016, 2 e ss.

SALAZAR, P. - FAILLA, L. *Facebook e rapporto di lavoro: nuove frontiere per i comportamenti extra-lavorativi,* in *Il lavoro nella giurisprudenza,* n. 6/2019, 635 e ss.

SANTORO-PASSARELLI, G. *Sulle categorie del diritto del lavoro "riformate",* in W.P. C.S.D.L.E. Massimo D'Antona, 27/1/2016.

SANTORO-PASSARELLI, G., *Lavoro eterorganizzato, coordinato, agile e il telelavoro: un puzzle non facile da comporre in un'impresa in via di trasformazione*, in W.P. C.S.D.L.E. Massimo D'Antona, 327, 2017.

SEGHEZZI, I. *I social network e le nuove frontiere dell'illecito disciplinare,* in *Il Lavoro nella giurisprudenza*, n. 6/2018.

SITZIA, A. *Privacy del lavoratore, poteri del datore di lavoro ed interessi confliggenti: un contemperamento è possibile?,* in *Nuova Giurisprudenza Civile Commentata* n. 1/2010, 71 e ss. (Nota a Cass. Civ., sez. lav., 30 giugno 2009, n. 15327).

SITZIA, A. *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali,* Cedam, Milano, 2013.

SITZIA, A. *I controlli a distanza dopo il "Jobs Act" e la Raccomandazione R(2015)5 del Consiglio d'Europa*, in *Il Lavoro nella giurisprudenza* n. 7/2015, 671 e ss.

SITZIA, A. *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 St. Lav. e il consenso (del lavoratore),* in *Labour Law Issues*, Vol.2, N. 1, 2016, 83 e ss.

SITZIA, A. - PIZZONIA, D. *Il controllo del datore di lavoro su Internet e posta elettronica: quale riservatezza sul luogo di lavoro?,* in *Nuova Giurisprudenza Civile Commentata* n.6/2016, 901 e ss. (Nota a Corte europea diritti dell'uomo 12.1.2016, ric. 61496/08).

SITZIA, A. *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza,* in *Argomenti di Diritto del Lavoro* 3/2017, 804 e ss.

SITZIA, A. *Videosorveglianza occulta, privacy e diritto di proprietà: la Corte EDU torna sul criterio di bilanciamento,* in *Argomenti di diritto del lavoro,* n. 2/2018, 499 e ss.

SITZIA, A. - CRAFA, S. *Impronte digitali, algoritmo e trattamento di dati personali: questioni di "law and technology",* in *Il lavoro nella giurisprudenza* 3/2019, 245 e ss. (Nota a Cass. Civ., Sez. II civ., 15 ottobre 2018, n. 25686, ord.).

SORO, A. *Persone in rete. I dati tra poteri e diritti*, Fazi Editore, Roma, 2018.

SORO, A. *La protezione dei dati personali nell'era digitale*, in *Nuova Giurisprudenza Civile Commentata*, n.2/2019, 343 e ss.

STOLFA, A. *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, in *Il lavoro nella giurisprudenza*, n. 5/2018, 530 e ss.

TEBANO, L. *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *Rivista Italiana Diritto del Lavoro*, n.1/2016, 345 e ss.

TEBANO, L. *Employees' Privacy and employers' control between the Italian legal system and European sources*, in *Labour Law Issues*, n. 2/2017.

TIRABOSCHI, M. *Il lavoro agile tra legge e contrattazione collettiva: la tortuosa via italiana verso la modernizzazione del diritto del lavoro,* in *Diritto delle Relazioni Industriali* 4/2017, 921 e ss.

TOMMASI, C. *La nuova disciplina europea sulla protezione dei dati personali*, in *Studium Iuris*, n. 1/2019, 6 e ss.

TROJSI, A. *Il diritto del lavoratore alla protezione dei dati personali,* Giappichelli, Torino, 2013.

TOSI, P. – PUCCETTI, E. *Chat Facebook: se la riservatezza legittima la denigrazione del datore di lavoro,* in *Giurisprudenza italiana,* gennaio 2019, 137 e ss. (Nota a Cassazione civile, Sez. lav., 10 settembre 2018, n. 21965).

TROJSI, A. *Il comma 7, lettera f), della legge delega n. 183/2014: tra costruzione del Diritto del lavoro dell'era tecnologica e liberalizzazione dei controlli a distanza sui lavoratori*, in M. Rusciano-L. Zoppoli (a cura di), *Jobs Act e contratti di lavoro dopo la legge delega 10 dicembre 2014, n. 183*, in W.P. C.S.D.L.E. "Massimo D'Antona" 3/2014.

TROJSI, A. *Al cuore del nuovo art. 4, co. 2, St. Lav.: la delimitazione della fattispecie degli "strumenti utilizzati per rendere la prestazione lavorativa"*, in *Rivista Italiana di Diritto del Lavoro*, n. 2/2017, 265 e ss.

TULLINI, P. *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *Rivista italiana di diritto del lavoro*, n. 3/2009, 323 e ss.

TULLINI, P. *Economia digitale e lavoro non standard*, in *Labour Law Issues*, Vol. 2, n. 2/2016, 2 e ss.

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 Tullini, P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017.

TULLINI, P. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, Torino, 2017.

WARREN, D. S., BRANDEIS, D. L., *The right to privacy,* in *Harvard Law Review*, Vol. IV, N. 5, The Harvard Law Review Association, 1890, 193-220.

VERZARO, M. *Controlli tecnologici e utilizzabilità dei dati acquisiti tra finalità del trattamento e diritto alla protezione dei dati personali,* in *Rivista Giuridica del lavoro,* n.4/2018, 562 e ss. (Nota a Trib. Roma, sent. n. 2270 22.3.2018 e Trib. Roma, ord. n. 57668 13.6.2018).

VIDIRI, *G. Controlli datoriali sui dipendenti e tutela della privacy nel nuovo art. 4 Stat. lav.*, in *Il Corriere Giuridico* n. 11/2016, 1389 e ss.

ZICCARDI, G. *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche,* in *Labour Law Issues*, Vol. 2, N. 1, 2016.

ZICCARDI, G. *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, 2015.

ZOLI, C. *Il controllo a distanza del datore di lavoro, l'art. 4 l. n. 300/ 1970 tra attualità ed esigenze di riforma*, in *Rivista Italiana Diritto del Lavoro*, 1/2009, 485 e ss.

ZOLI, C. *Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n.300/1970,* in *Variazioni su temi di diritto del lavoro*, 4/2016, 635.

ZOLI, C. – VILLA, E. *Gli strumenti di registrazione degli accessi e delle presenze*, in P. TULLINI (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore,* Giappichelli, Torino, 2017.