

CENTRO STUDI DI DIRITTO DEL LAVORO "DOMENICO NAPOLETANO"
SEZIONE VENETO

RELAZIONE CHE IL **PROF. ALESSANDRO BELLAVISTA** (professore straordinario di diritto del lavoro nell'Università di Palermo) HA PREPARATO PER IL CONVEGNO DI VENEZIA DEL 12 APRILE 2002 CON TEMA:

"I poteri dell'imprenditore e la privacy del lavoratore"

Sommario: 1. Premessa.- 2. La legge n. 675/1996 e la disciplina speciale del diritto del lavoro.- 3. I controlli tecnologici e l'art. 4 St. lav.- 4. Controlli tecnologici e misure di garanzia. 5. Alcuni casi di controllo tecnologico.- 6. Ipotesi e limiti del controllo occulto.- 7. Profili del trattamento dei dati personali dei lavoratori nel rapporto di lavoro pubblico.- 8. Il controllo tecnologico nel lavoro pubblico.- 9. Principio di finalità, sistema del diritto del lavoro e uso dei dati personali.- 10. Autoregolamentazione e disciplina di settore per il trattamento dei dati personali dei lavoratori.- 11. Azione sindacale e contrattazione collettiva.

1. Premessa.

L'evoluzione tecnologica e i mutamenti delle forme organizzative delle imprese contribuiscono a creare sempre nuovi momenti di tensione in relazione all'assetto tra il legittimo esercizio dei poteri del datore e i contrapposti diritti dei prestatori di lavoro subordinato¹. Particolarmente significativa è la vicenda che riguarda il potere del datore di raccogliere informazioni sui dipendenti e di controllarne l'operato. La questione è strettamente connessa al codice genetico del rapporto di lavoro, perché tale relazione contrattuale è dominata da un permanente flusso informativo tra le due parti e inoltre la funzionalità della stessa sarebbe compromessa se il datore non potesse controllare alcune manifestazioni del comportamento del lavoratore². Pertanto, resta acceso il dibattito vertente

¹ Cfr. Carinci, *Rivoluzione tecnologica e diritto del lavoro*, in *Giorn. dir. lav. rel. ind.*, 1985, p. 203 ss.; Veneziani, *Nuove tecnologie e contratto di lavoro: profili di diritto comparato*, *ivi*, 1987, p. 1 ss.; Giugni, *Lavoro leggi contratti*, Il Mulino, Bologna, 1989, p. 121 ss.; Perulli, *Il potere direttivo dell'imprenditore*, Giuffrè, Milano, 1992; Bonazzi, *Il tubo di cristallo*, Il Mulino, Bologna, 1993; Revelli, *Economia e modello sociale nel passaggio tra fordismo e toyotismo*, in *Appuntamenti di fine secolo*, a cura di Ingrao-Rossanda, Manifestolibri, Roma, 1995, p. 161 ss.; Bronzini, *Dall'habeas corpus all' habeas mentem. Soft law e autoregolazione nel lavoro postfordista*, in *Dem. dir.*, 1996, p. 215 ss.; Zoli, *Subordinazione e poteri dell'imprenditore tra organizzazione, contratto e contropotere*, in *Lav. dir.*, 1997, p. 252 ss.

² Per tutti cfr. Simitis, *Reconsidering the premises of labour law: prolegomena to an Eu-regulation on the protection of the employees' personal data*, in *Scritti in onore di Gino Giugni*, tomo II, Cacucci, Bari, 1999, p. 1584 ss.; Däubler, *Arbeitnehmerdatenschutz - ein Problem der EG?*, in *Informationsgesellschaft und Rechtskultur in Europa*, a cura di Tinnenfeld-Philipps-Heil, Nomos, Baden-Baden, 1995, p. 11 ss.; Ghezzi-Romagnoli, *Il rapporto di lavoro*, 3° ed., Zanichelli, Bologna, 1995, p. 217 ss.

sull'individuazione dei limiti del potere del datore di controllare i dipendenti nonché di trattare le informazioni che li riguardano. Negli ultimi tempi, specie nel contesto italiano, s'è assistito ad una intensificazione dell'interesse su tali questioni; e che quindi meritano d'essere analizzate, almeno con riferimento a quegli aspetti su cui sembra al momento concentrarsi l'attenzione degli addetti ai lavori e soprattutto degli attori del mondo del lavoro.

Infatti, nuove applicazioni delle tecnologie informatiche permettono il ricorso a forme di raccolta d'informazioni e di sorveglianza estremamente ampie e dettagliate, di fronte alle quali è indubitabile l'esigenza di porre un argine a tutela dei diritti e delle libertà fondamentali del lavoratore, tra cui il cosiddetto diritto all'autodeterminazione informativa ovvero il diritto alla *privacy* che concerne il diritto del singolo di controllare l'uso e la circolazione dei propri dati personali³ e quindi di mantenere il controllo sulle informazioni che lo riguardano⁴.

Peraltro, il sistema giuridico italiano è caratterizzato dall'esistenza di regole generali e speciali applicabili all'attività del datore volta a sorvegliare l'operato del lavoratore e trattare le relative informazioni. Senonché, propria questa materia è contraddistinta da una permanente dialettica tra sistema normativo e progresso tecnologico e quindi propone un "tipico tema di armonizzazione strutturale del diritto alla società"⁵. E cioè, la realtà effettuale si presenta densa di casi e ipotesi di controllo a volte difficilmente afferrabili da fattispecie giuridiche coniate avendo presenti differenti contesti tecnologici ovvero in apparenza rese obsolete dalle continue novità tecnologiche. In effetti, i progressi scientifici e tecnologici sono in grado di rendere disponibili metodi di sorveglianza e di raccolta d'informazioni personali capaci di travolgere e di rendere inefficaci anche regole elaborate in tempi recenti, ma plasmate in funzione di un certo stadio di sviluppo tecnologico. Tutto ciò dimostra l'importanza, da un lato, di concepire meccanismi di garanzia non rigidi, ma il più possibile adattabili, grazie all'opera degli interpreti, alle innumerevoli sfaccettature dell'uso delle forme di sorveglianza; e, dall'altro, di accettare l'idea che la disciplina del trattamento delle informazioni personali e delle tecniche di sorveglianza non possa essere immutabile (o meglio destinata ad una lunga vita), ma anzi che debba essere costruita in modo tale da essere facilmente integrabile ovvero sostituibile mediante nuovi interventi regolativi, quando ciò fosse reso necessario dal mutamento del contesto tecnologico sulla cui base la medesima disciplina è stata elaborata⁶.

³ Cfr. Rodotà', *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 101; Stenico, *Il trattamento dei dati personali del lavoratore subordinato: dalla segretezza al controllo*, in *La tutela della privacy del lavoratore*, in *Quad. dir. lav. rel.ind.*, n. 24, 2000, p. 124 ss.

⁴ Diritto questo che ora trova esplicita affermazione (non solo nelle leggi nazionali sulla protezione dei dati personali, come quella italiana, ma anche) nell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea: cfr. il commento di Donati, in *L'Europa dei diritti*, a cura di Bifulco-Cartabia-Celotto, Il Mulino, Bologna, 2001, p. 83 ss.

⁵ Cfr. Giugni, *Lavoro leggi contratti*, cit., p. 355.

⁶ Cfr. Simitis, *Arbeitnehmerdatenschutzgesetz - Realistische Erwartung oder Lippenbekenntnis?*, in *Arbeit und Recht*, 2001, p. 432 ss. ; Rodotà, *Diritto, diritti, globalizzazione*, in *Riv. giur. lav.*, 2000, p. 776 s.

2. La legge n. 675/1996 e la disciplina speciale del diritto del lavoro.

Com'è noto, la disciplina base in materia di raccolta e trattamento delle informazioni personali è costituita, in Italia, dalla legge 31 dicembre 1996, n. 675. Questa normativa ha una portata generale è cioè regola ogni trattamento di dati personali che non sia svolto per fini esclusivamente personali. Questa osservazione va completata precisando che la stessa legge n. 675/1996 contiene varie e differenti forme di regolazione dei trattamenti di dati personali a seconda delle caratteristiche che essi presentano e delle finalità per cui sono svolti⁷.

Peraltro, tale normativa ha subito, fin da prima della sua entrata in vigore, diverse modifiche volte a correggere imperfezioni e lacune, ed inoltre è stata integrata e accompagnata da ulteriori testi normativi che si affiancano ad essa nel comporre l'attuale disciplina legale del trattamento dei dati personali. Il meccanismo che ha permesso tale celere opera di completamento e correzione della legge base è stato rappresentato dalla parallela legge 31 dicembre 1996, n. 676, che appunto conteneva un apposita delega al Governo per operare le già menzionate integrazioni e rettifiche della legge n. 675/1996. Siffatta delega è stata riaperta, dopo la prima scadenza, per ben due volte, proprio in ragione dell'esigenza di favorire la completa integrazione e l'eventuale immediata correzione della disciplina base.

Tuttavia, nonostante il legislatore delegato sia intervenuto sulla regolamentazione del trattamento dei dati personali assai frequentemente, per quanto concerne l'area dei rapporti di lavoro non è stata sfruttata quella parte della delega che avrebbe permesso di emanare una normativa specifica proprio per il trattamento dei dati personali nell'ambito del rapporto di lavoro, di cui è, in modo diffuso, avvertita la necessità⁸. Inoltre, è stata mantenuta una delle impostazioni originarie della legge n. 675/1996, sulla quale si sono addensate molte critiche, perché comporta una profonda diversificazione delle regole in ordine al trattamento dei dati personali dei lavoratori privati e pubblici. Ciò dipende dal fatto che la legge n. 675/1996 disciplina il trattamento in funzione del soggetto che appunto tratta i dati personali: e quindi, alla differente regolamentazione del trattamento dei dati da parte dei soggetti privati e pubblici corrisponde una diversa disciplina per i lavoratori privati e pubblici⁹.

A questo proposito, per ciò che concerne l'area dei *rapporti di lavoro privati* e il trattamento dei cosiddetti *dati ordinari o comuni e sensibili*, si devono distinguere (per assicurare una maggiore semplicità espositiva), secondo la loro scansione nel testo della legge, da un lato, le regole che concernono le modalità di raccolta e i requisiti che ogni fase del trattamento deve soddisfare (cfr. l'art. 9) e, dall'altro le norme che individuano i casi in cui è legittimato ovvero è ammesso il trattamento dei dati (e che riguardano quindi i cosiddetti presupposti di legittimazione al trattamento: gli artt. 11, 12 e 20, per il trattamento

⁷ Cfr. Rodotà', *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 583 ss.; Buttarelli, *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997.

⁸ Cfr. SIMITIS, *Arbeinehmerdatenschutzgesetz*, cit., p. 429 ss. e Id., *Reconsidering*, cit., p. 1590 ss.

⁹ Da ultimo, sulla disciplina del trattamento dei dati personali dei lavoratori, cfr.: Aimo, *I "lavoratori di vetro": regole di trattamento e meccanismi di tutela dei dati personali*, in *Riv. giur. lav.*, 2002, I, p. 45 ss.; Chieco, *Privacy e lavoro*, Cacucci, Bari, 2000; e gli scritti contenuti nel volume monografico: *La tutela della privacy del lavoratore*, in *Quad. dir. lav. rel. ind.*, n. 24, 2000.

dei cosiddetti dati ordinari o comuni; e l'art. 22 per il trattamento dei cosiddetti dati sensibili).

Più chiaramente, in forza della legge n. 675/1996, il trattamento di dati personali, dei lavoratori privati, è lecito solo in presenza di due condizioni che devono simultaneamente essere accertate. In primo luogo, ci deve essere uno dei *presupposti* - descritti, in via alternativa, dagli artt. 11 o 12 e 20 della legge n. 675/1996 (per il trattamento o la comunicazione e diffusione dei dati ordinari o comuni), e dall'art. 22 della legge n. 675/1996 (per il trattamento o la comunicazione e diffusione dei dati sensibili) - che permette di ammettere il trattamento (ovvero la comunicazione e diffusione dei dati). In secondo luogo, una volta ammesso il trattamento, ogni momento dello stesso deve rispettare le regole di principio stabilite dall'art. 9 della legge n. 675/1996. S'è già detto che il trattamento dei dati dei lavoratori pubblici è soggetto ad una disciplina differenziata - soprattutto con riferimento ai presupposti di legittimazione del trattamento - rispetto a quella dei lavoratori privati e su cui ci si soffermerà meglio in seguito. Ciò non esclude che anche riguardo al trattamento dei dati dei lavoratori pubblici opera l'art. 9 della legge n. 675/1996: quindi la lettura di tale disposizione spiega la sua efficacia - senza variazioni di rilievo - in entrambe le due tipologie di rapporto di lavoro. Come emerge dalla lettura dell'art. 1 della legge n. 675/1996 e dall'insieme della normativa, l'applicazione di essa nell'ambito del rapporto di lavoro non determina alcuna funzionalizzazione del potere datoriale, bensì - in modo coerente all'esperienza del diritto del lavoro italiano - fissa limiti esterni a tale potere e appunto modella una serie di regole dirette ad evitare che il trattamento dei dati dei lavoratori possa spingersi fino a ledere i diritti e le libertà fondamentali nonché la dignità di costoro.

Beninteso, l'art. 9, lettera a) della legge n. 675/1996 esordisce con una regola generale e di amplissima portata, disponendo che i dati personali devono essere "trattati in modo lecito e secondo correttezza". Come precisa l'art. 1 della legge n. 675/1996, il concetto di trattamento abbraccia anche la fase della mera raccolta dei dati personali. Pertanto, quando l'art. 9, lettera a), della legge impone che il trattamento dei dati personali avvenga *in modo lecito e secondo correttezza*, questo comporta che tale direttiva vada osservata anche nel momento della raccolta dei dati. Inoltre, lo stesso art. 9 della legge n. 675/1996 delinea in modo dettagliato i connotati del fondamentale *principio di finalità* che, in prima battuta, si manifesta, come afferma l'art. 9, lettera b), nella regola che i dati personali devono essere "raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi".

E' evidente l'ampio spettro delle due prescrizioni di *liceità del trattamento* e di *legittimità degli scopi* da esso perseguiti che emergono dall'art. 9 della legge n. 675/1996: esse possono assumere sfaccettature variabili in funzione dei contesti concreti, e il loro significato deve ovviamente essere colto anche attraverso il coordinamento con la normativa esistente.

In altri termini, non è solo la legge n. 675/1996 a definire quando il trattamento avvenga in modo lecito e persegua finalità legittime, ma la liceità del trattamento e la legittimità dei fini dello stesso discendono dalla loro conformità con tutte le altre norme dell'ordinamento di volta in volta rilevanti. A questo proposito, l'art. 43, comma 2, della legge n. 675/1996, stabilisce che "restano ferme le disposizioni della legge 20 maggio 1970, n. 300, e successive modificazioni, nonché, in quanto compatibili, le disposizioni della legge 5 giugno 1990, n. 135, e successive modificazioni"; e aggiunge che "restano altresì ferme le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento

di taluni dati personali". Ciò significa che le norme generali della legge n. 675/1996 vanno applicate in quanto compatibili con le norme speciali dello Statuto dei lavoratori (comprehensive dei principi da esse ricavati in via ermeneutica: e cioè del diritto vivente) nonché con tutte le altre che, nel campo lavoristico, stabiliscono in materia di trattamento di dati personali, "divieti e limiti più restrittivi" rispetto a quelle della legge n. 675/1996. Così, tutte queste disposizioni, in caso di insanabile contrasto con quelle della legge n. 675/1996, prevarranno su di esse¹⁰.

Sicché, il datore di lavoro, nel trattare dati sul conto dei lavoratori, resta obbligato all'osservanza delle regole e dei principi del sistema dogmatico del diritto del lavoro, come plasmato dalla combinazione dei contributi della legislazione, della dottrina e della giurisprudenza: e in particolare al rispetto degli artt. 2, 3, 4, 5, 6, e 8 dello Statuto dei lavoratori nonché degli artt. 5 (come risultante dalla lettura offerta dalla Corte costituzionale a seguito della sentenza n. 218/1994) e 6 della legge n. 135/1990. Tutte queste norme circoscrivono in modo più o meno esteso la possibilità del datore di raccogliere (e quindi trattare) alcune categorie di dati riguardanti i lavoratori o quantomeno limitano la facoltà di utilizzare alcune modalità di raccolta di dati, la cui conoscenza da parte del datore è di per sé lecita¹¹.

A questo punto, emerge chiaramente il ruolo cardine svolto dall'art. 8 St.lav. Sicché, tale norma continua ad individuare, in funzione delle specifiche caratteristiche di ogni rapporto di lavoro, categorie di dati "supersensibili" dei quali è vietato ogni momento del trattamento¹². Peraltro, nella prassi applicativa la disposizione ha assunto il valore di limite generale ai poteri del datore di lavoro, indipendentemente dall'integrazione della fattispecie penale da essa descritta. E questo perché si afferma che essa non solo vieta un'attività positiva d'indagine da parte del datore di lavoro sui fatti del lavoratore estranei al fine della valutazione dell'attitudine professionale, e cioè che non presentino alcuna correlazione funzionale con le mansioni da svolgere e quindi con l'esecuzione del contratto di lavoro, ma sancisce l'ulteriore principio (avente ovviamente rilievo meramente civilistico) secondo cui sarebbe illegittimo che si tenga conto nell'ambito del rapporto di lavoro di tali fatti comunque siano stati conosciuti¹³. Sicché, tale norma ha dimostrato di essere in grado di "varcare la soglia che ne delimita l'operatività all'area dei comportamenti illecitamente diretti ad acquisire notizie 'protette' per spingersi a sanzionare anche l'utilizzazione che il

¹⁰ Sul punto cfr. Buttarelli, *Banche dati e tutela della riservatezza*, cit., p. 555; e AIMO, *I "lavoratori di vetro"*, cit., p. 106 ss.

¹¹ Cfr., ampiamente, Aimo, *I "lavoratori di vetro"*, cit. p. 49 ss.; Lambertucci, *Trattamento dei dati personali e rapporto di lavoro*, in *La disciplina del trattamento dei dati personali*, a cura di Cuffaro-Ricciuto, Giappichelli, Torino, 1997, p. 423 ss.; Chieco, *Il diritto alla riservatezza del lavoratore*, in *Giorn. dir. lav. rel. ind.*, 1998, p. 1 ss.; nonché, volendo, Bellavista, *Il controllo sui lavoratori*, Giappichelli, Torino, 1995.

¹² Cfr. Lambertucci, *Svolgimento del rapporto di lavoro e tutela dei dati personali*, in *La tutela della privacy del lavoratore*, cit. p. 71 ss.

¹³ Cfr. Cass. sez. un., 23 luglio 1981, n. 5736, in *Foro. it.*, 1982, I, 111; Cass. sez. un., 11 dicembre 1979, n. 6452, *ivi*, 1980, I, 322; Broglio, *Il rilievo del comportamento "privato" del lavoratore nel "pubblico" del rapporto di lavoro*, in *Giur. it.*, 1987, I, sez. I, c. 317 ss.

datore di lavoro faccia di tali notizie nella gestione del contratto di lavoro"¹⁴. In altre parole, è evidente come tale principio desumibile dall'art. 8 St.lav. contribuisca a precisare le condizioni di liceità dell'intero trattamento e di legittimità degli scopi da esso perseguiti.

Beninteso, va precisato che questo principio generale, ricavato dall'art. 8 St.lav. (o, eventualmente, se si vuole, dallo Statuto nel suo complesso ovvero in particolare dalla combinazione degli artt. 1, 8 e 15 St.lav.), non può assumere un atteggiamento "integralista", nel senso di imporre al datore di utilizzare, nel corso della fase di selezione e nell'amministrazione del rapporto, solo le informazioni strettamente pertinenti alla valutazione dell'attitudine professionale del lavoratore. A parte il fatto che il concetto di attitudine professionale, proprio per temperare l'apparente rigidità della norma statutaria, è stato dilatato e reso abbastanza elastico dalle letture più diffuse, è logico ritenere che il suddetto principio generale (in modo coerente alla struttura di tali particolari componenti del sistema giuridico¹⁵) debba assumere, nella fase di concreta applicazione, contorni alquanto flessibili, mirando però ad assicurare in via tendenziale uno *stretto collegamento tra le informazioni acquisibili sui lavoratori e la struttura del concreto rapporto di lavoro*: e cioè di imporre che i suddetti dati, per potere essere legittimamente utilizzati, devono essere oggettivamente (alla stregua di standard e parametri di tipicità sociale) rilevanti ai fini della gestione dello specifico rapporto di lavoro che viene in questione e che l'uso di essi deve essere necessario per assicurare la *funzionalità* del medesimo rapporto¹⁶.

Comunque, tutto ciò comporta che l'applicazione delle regole di cui agli artt. 11, 12, 20 e 22 della legge n. 675/1996, per il trattamento dei dati ordinari e sensibili nel rapporto di lavoro privato, presuppone il preventivo accertamento della liceità della raccolta e dell'uso dei suddetti dati ordinari e sensibili ai sensi dell'interpretazione prevalente dell'art. 8 St.lav. Una volta fatto ciò, va valutata la legittimità del trattamento alla stregua delle appena citate regole della legge n. 675/1996. Ciò è stato confermato dalla prassi, perché, ogni volta che il Garante per la protezione dei dati personali s'è occupato di trattamenti di dati personali nell'area dei rapporti di lavoro, ha fatto esplicito richiamo alla necessità del rispetto delle disposizioni dello Statuto dei lavoratori, tra cui in particolare l'art. 8 St.lav. Peraltro, si consideri che il trattamento dei dati sensibili di cui all'art. 22 della legge n. 675/1996, è ammesso dal comma 1 di questa disposizione solo in presenza del consenso scritto dell'interessato e dell'autorizzazione del Garante. Beninteso, l'autorizzazione n.1/2002 (già n. 1/2000, n. 1/1999, n. 1/1998 e n.1/1997) del Garante al trattamento dei dati sensibili nei rapporti di lavoro privati, e l'autorizzazione n.5/2002 (e già n. 5/2000, n. 5/1999, n. 5/1998 e n. 5/1997) nella parte relativa all'attività di selezione del personale svolta da soggetti terzi rispetto alle parti del futuro rapporto, nell'individuare gruppi di dati sensibili di cui, a determinate condizioni, è lecito il trattamento nel rapporto di lavoro e nella fase di selezione del personale da assumere, hanno anche, seppure in via indiretta, fornito un utile contributo per meglio circoscrivere e definire l'ambito di operatività del divieto dell'art. 8 St.lav. e del principio da esso ricavato nei vari settori da esse considerati.

¹⁴ Chieco, *Il diritto alla riservatezza*, cit., p. 25.

¹⁵ Cfr. Guastini, voce *Principi di diritto*, in *Digesto IV, Disc. priv., Sez. civ.*, vol. XIV, 1996, p. 341 ss; Mengoni, *I principi generali del diritto e la scienza giuridica*, in *Dir. lav.*, 1992, I, p. 3 ss.

¹⁶ Cfr. Romagnoli, *Sub. art. 8*, in Ghezzi-Mancini-Montuschi-Romagnoli, *Statuto dei diritti dei lavoratori*, 2° ed., Zanichelli-II Foro italiano, Bologna-Roma, 1979, p. 143 ss.; Trojsi, *Sfera privata del lavoratore e contratto di lavoro*, in *La tutela della privacy del lavoratore*, cit., p. 195 ss.

Più in generale, i requisiti di liceità del trattamento e di legittimità degli scopi da esso perseguiti, di cui all'art. 9 della legge n. 675/1996, vanno individuati e concretati in funzione dello specifico contesto del rapporto di lavoro, proprio in base alla direttiva dell'art. 8 St.lav. E inoltre tali requisiti influenzano anche i margini operativi dei cosiddetti *presupposti di ammissibilità del trattamento*. Ciò equivale a dire che - né grazie al consenso dell'interessato né mediante gli altri presupposti ad esso equipollenti - si può estendere lo spettro del trattamento a dati o scopi che non risultano coerenti con i predetti requisiti di liceità e legittimità. In sostanza, la disciplina speciale del diritto del lavoro fissa una soglia (pur flessibile, ma non arbitraria) al di là della quale non può spingersi il trattamento dei dati personali del lavoratore. Più precisamente, questa disciplina speciale ribadisce che, nel rapporto di lavoro, vi è un grappolo di beni del lavoratore intangibili dal datore e indisponibili dal medesimo prestatore di lavoro mediante il proprio consenso¹⁷. E tale conclusione trova una forte conferma nella analoga e consolidata interpretazione della normativa tedesca (già BDSG 1990 e ora BDSG 2001), laddove parimenti i principi e le regole del diritto del lavoro condizionano la concretizzazione delle clausole generali contenute nella legge sulla protezione dei dati e quindi disegnano i confini della possibilità del datore di raccogliere dati sui lavoratori, di procedere al trattamento dei medesimi nonché l'ambito di efficacia del consenso del lavoratore al trattamento dei propri dati¹⁸. Analoga impostazione è adottata dai documenti internazionali attualmente più rilevanti nell'area del trattamento dei dati personali dei lavoratori. La raccomandazione No. R(89) 2 del Consiglio d'Europa del 18 gennaio 1989 sulla protezione dei dati personali utilizzati per finalità di lavoro e il codice di condotta (*Code of practice*) dell'Ufficio internazionale del lavoro del 1996 sulla protezione dei dati personali dei lavoratori scelgono entrambe un criterio generale secondo cui la *conditio sine qua non* per il trattamento dei dati personali dei lavoratori è costituita dalla diretta connessione di ogni singolo dato con lo specifico rapporto di lavoro in questione¹⁹. Di conseguenza, il consenso del lavoratore, quando è previsto, non rappresenta mai l'unico (e quindi sufficiente) presupposto di legittimità del trattamento, ma (soprattutto nel codice dell'Ufficio internazionale del lavoro) viene accompagnato da condizioni e procedure volte a garantire lo stretto ancoraggio tra singole tipologie di dati raccolti e usati e oggettive finalità di gestione del rapporto di lavoro. A tal punto che viene sancito il divieto di trattamento di alcune categorie di dati, anche qualora vi fosse il consenso del lavoratore, e viene esclusa la possibilità che costui possa rinunciare all'esercizio dei propri diritti nei confronti del titolare del trattamento.

3. I controlli tecnologici e l'art. 4 St. lav.

¹⁷ Cfr. Chieco, *Il diritto alla riservatezza*, cit., p. 26.

¹⁸ Cfr. Däubler, *Das Arbeitsrecht 2*, 11 ed., Rowohlt, Reinbek bei Hamburg, 1998, p. 317 ss.; Wedde, *Sub § 28*, in Däubler-Klebe-Wedde, *Bundesdatenschutzgesetz*, Basiskommentar, Bund, Köln, 1996, p. 214 ss.; Fitting e altri, *Betriebsverfassungsgesetz*, 17 ed., Vahlen, München, 1992, p. 1071; Däubler, *Das neue Bundesdatenschutz-gesetz und seine Auswirkungen im Arbeitsrecht*, in *Neue Zeitschrift für Arbeitsrecht*, 2001, p. 876 s.

¹⁹ Cfr. il principio 6.1. della raccomandazione del Consiglio d'Europa, nonché i punti 47 ss. della relazione che accompagna la medesima raccomandazione; nonché i principi 5.1. ss. del codice dell'Ufficio internazionale del lavoro e pag. 23 ss. del commento allegato: ILO, *Protection of workers' personal data*, Geneva, 1997.

Peraltro, i requisiti di liceità del trattamento e di legittimità degli scopi da esso perseguiti, fissati in via generale dall'art. 9 della legge n. 675/1996, devono essere, in modo più accurato, precisati alla luce dell'art. 4 dello Statuto dei lavoratori. E cioè: va sottolineato che quando il datore utilizza apparecchiature (di vario genere) per la raccolta di dati personali sul lavoratore allo scopo della sorveglianza sul suo comportamento, deve rispettare le prescrizioni di tale disposizione. Questo precetto influenza principalmente le modalità attraverso cui il datore può agire nel raccogliere informazioni sul conto del lavoratore: informazioni - come quelle riguardanti l'attività dei lavoratori - che di per sé sarebbero legittimamente raccogliibili, con mezzi diversi da quelli rientranti nel concetto di "apparecchiature", purché ovviamente fossero pertinenti all'area del rapporto di lavoro e all'adempimento dei relativi obblighi.

A questo riguardo va detto che l'art. 4 St.lav. è una disposizione di cui s'è discussa l'operatività nel nuovo contesto tecnologico dominato dall'informatizzazione del posto di lavoro. Tuttavia, la dottrina e la giurisprudenza prevalenti ritengono che la norma sia perfettamente applicabile anche a tutte le forme di controllo rese possibili dall'utilizzazione delle tecnologie informatiche²⁰. Com'è noto, l'art. 4, comma 1, St.lav. dice che "è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori". E il comma 2 aggiunge che "gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali"; nonché "in difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti".

Pertanto, il datore di lavoro non può unilateralmente decidere di installare un'apparecchiatura (e quindi anche uno specifico programma per computer) destinata a controllare a distanza l'attività dei lavoratori, ma deve rispettare la procedura delineata dal comma 2 dell'art. 4 St.lav. e quindi raggiungere un accordo con le rappresentanze sindacali aziendali: accordo in cui si accerta che l'installazione dell'apparecchiatura è richiesta da esigenze organizzative, produttive e di sicurezza del lavoro. Qualche dubbio può sorgere sulla circostanza se a seguito di tale accordo - o del provvedimento della direzione provinciale del lavoro che può intervenire, su richiesta del datore, in mancanza di accordo - sia possibile utilizzare l'apparecchiatura in questione proprio per controllare a distanza il comportamento dei lavoratori. La perplessità sorge perché la norma appare formulata in modo tale da escludere comunque che i risultati del controllo possano servire per verificare la regolarità del comportamento dei lavoratori, e perciò sembra solo consentire l'uso

²⁰ Così, Rossi, *La libertà e la professionalità dei lavoratori di fronte alle nuove tecnologie informatiche*, in *Quest. giust.*, 1983, p. 212 ss.; Zanelli, *Impresa, lavoro e innovazione tecnologica*, Giuffrè, Milano, 1985, p. 84 ss.; Ghezzi e Liso, *Computer e controllo dei lavoratori*, in *Giorn. dir. lav. rel. ind.*, 1986, rispettivamente p. 354 ss. e p. 366 ss.; Veneziani, *L'art. 4 St. lav.: una norma da riformare?*, in *Riv. giur. lav.*, 1991, I, p. 79 ss.; Garilli, *Tutela della persona e tutela della sfera privata nel rapporto di lavoro*, in *Riv. crit. dir. priv.*, 1992, p. 331 ss.; Bellavista, *Il controllo*, cit., p. 103 ss. Opinioni differenti sono espresse da Pisani, *I controlli a distanza sui lavoratori*, in *Giorn. dir. lav. rel. ind.*, 1987, p. 121 ss.; De Luca Tamajo-Imperiali D'Afflitto-Pisani-Romei, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Angeli, Milano, 1988 (e ivi anche scritti di Salimbeni); Romei, *I controlli e la tutela della privacy*, in *Telelavoro e diritto*, a cura di Gaeta-Pascucci, Giappichelli, Torino, 1998, p. 97 ss.

dell'apparecchiatura per il soddisfacimento di esigenze organizzative, produttive e di sicurezza del lavoro diverse dalla mera sorveglianza dei lavoratori²¹.

Beninteso, va considerato che oggi, il controllo attraverso gli strumenti informatici (ma talvolta anche con strumenti più tradizionali, come le telecamere) rappresenta spesso l'unica modalità per garantire che il lavoratore non commetta illeciti contrattuali o fatti ancora più gravi. Si pensi al caso in cui il lavoratore svolga la propria prestazione utilizzando un computer, mediante il quale abbia la possibilità di gestire denaro o di maneggiare dati estremamente riservati, la cui comunicazione o diffusione sia suscettibile di arrecare gravissimi danni al datore o a terzi. Pertanto, sembra ragionevole l'opinione secondo cui in casi del genere (e quindi in via di *extrema ratio*) - cioè quando non vi sia valida alternativa a tale tipo di controllo - sarebbe possibile l'utilizzazione di un'apparecchiature del genere a condizione che venga rispettata la procedura di cui al comma 2 dell'art. 4 St.lav.²² Non accettare tale soluzione compromissoria, porterebbe ad una drastica alternativa: o ritenere vietati tutti i controlli elettronici oppure tentare di sostenere l'inapplicabilità dell'art. 4 St.lav. nel nuovo contesto tecnologico. In pratica, pare possibile sostenere che tale disposizione consenta di ammettere controlli informatici diretti all'accertamento della regolarità del comportamento del dipendente, purché vengano rispettate le condizioni di cui al comma 2 della medesima disposizione: vale a dire, l'esistenza di specifiche esigenze aziendali (organizzative, produttive e di sicurezza del lavoro) nonché l'accordo con le rappresentanze sindacali. Più precisamente, va sottolineato che sembra ragionevole permettere tali controlli proprio quando le caratteristiche dell'attività lavorativa siano tali per cui sarebbe estremamente difficile (se non impossibile) svolgere controlli efficaci in forme diverse da quelle rese possibili dai sistemi informatici. A favore di questa opinione gioca, nella recente esperienza, la vicenda dell'introduzione in Italia del telelavoro (e cioè di casi in cui l'attività lavorativa si svolge a distanza dalla sede aziendale, facendo uso di un collegamento telematico), laddove la contrattazione collettiva, che ha regolato tale modalità lavorativa, ha espressamente riconosciuto la necessità di controlli telematici per consentire l'accertamento della regolarità dello svolgimento della prestazione lavorativa²³. Certo, su questo punto - e cioè a favore di una lettura dell'art. 4 St. lav. come quella qui suggerita - non esistono precedenti giurisprudenziale esplicitamente favorevoli. Anzi, diverse pronunce su questioni affini appaiono di segno contrario, anche se riguardanti casi in cui i controlli tecnologici assumevano ampia portata e facevano sorgere il forte sospetto di costituire strumenti per instaurare in azienda forme di vigilanza che andavano a toccare molteplici aspetti dell'attività dei lavoratori del tutto estranei all'adempimento degli obblighi lavorativi e alle esigenze di salvaguardia del patrimonio aziendale²⁴. Pertanto, si può pensare che modalità di

²¹ Cfr. Chieco, *Privacy e lavoro*, cit., p. 332 ss.

²² In tale direzione cfr. Bellavista, *Il controllo*, cit., p. 99 ss.; Chieco, *Telelavoro e Statuto dei lavoratori*, in *Lav. inf.*, 1999, n. 12, p. 9 ss.

²³ Cfr. *L'esperienza Tim dall'accordo del '97 ad oggi*, in *Lav. inf.*, 2000, n. 1, p. 19 ss.; Romei, *I controlli*, cit., p. 97 ss.; Pizzi, "Telelavoro": *prime esperienze applicative nella contrattazione collettiva italiana*, in *Dir. lav.*, 1996, p. 172 ss.; e *ivi* ampia documentazione sulla contrattazione collettiva.

²⁴ Cfr. P. Milano 5 dicembre 1984, in *Foro it.*, 1985, II, c. 285.

controllo informatico opportunamente limitate all'esclusivo perseguimento di giustificati interessi dell'azienda, e sottoposte al vaglio sindacale come previsto dal comma 2 dell'art. 4 St.lav., possano ottenere un giudizio positivo da parte di future pronunce della giurisprudenza. D'altra parte, esaminando attentamente la numerosa giurisprudenza sull'art. 4 St.lav., è rintracciabile in essa l'opzione prevalente per una interpretazione meno rigida della disposizione volta ad ammettere l'installazione di apparecchiature direttamente destinate a controllare l'attività del lavoratore, purché sia accertata la presenza di rigorose e oggettive condizioni di tipo organizzativo, produttivo e di sicurezza del lavoro, e sia rispettata la procedura di codeterminazione di cui al comma 2 dell'art. 4 St. lav.²⁵.

Un ulteriore argomento a sostegno della lettura della disposizione qui suggerita può essere ricavato dalla disposizione contenuta nel paragrafo 3 dell'allegato VII al d.lgs. n. 626/1994 (integrato e modificato con le correzioni apportate dall'art. 29 del d.lgs. n. 242/1996) che fissa "prescrizioni minime" costituenti parte integrante del titolo VI del d.lgs. n. 626/1994 in materia di "uso di attrezzature munite di videoterminali". Proprio nel citato paragrafo 3 dell'allegato VII – nella parte relativa all'interfaccia elaboratore/uomo – si trova la disposizione secondo cui "all'atto dell'elaborazione, della scelta, dell'acquisto del software, o allorché questo viene modificato... il datore terrà conto" che "nessun dispositivo o controllo quantitativo o qualitativo può essere utilizzato all'insaputa dei lavoratori" e che "il software deve essere adeguato alla mansione da svolgere".

In effetti, se la disposizione del paragrafo 3 dell'allegato VII esclude la possibilità del controllo informatico all'insaputa dei lavoratori, si potrebbe ritenere che essa presupponga l'ammissibilità del controllo informatico quando sia svolto in modo palese o quantomeno avendo preventivamente avvertito i lavoratori della possibilità del controllo. E se questa disposizione presuppone l'ammissibilità di un tipo di controllo informatico, ciò significa che essa accoglie l'idea della legittimità del medesimo controllo alla stregua della norma base del sistema: vale a dire dell'art. 4 St.lav. In altri termini, la disposizione va coordinata con l'enunciato di cui al comma 1 e con la procedura di cui al comma 2 dell'art. 4 St.lav. e da ciò si può ricavare che essa ammetta una lettura più flessibile dell'art. 4 St.lav., ma al tempo stesso stabilisce ben precisi limiti all'uso dei software dotati di potenzialità di controllo e applicabili "alle attività lavorative che comportano l'uso di attrezzature munite di videoterminale" alla stregua dell'art. 50 del d.lgs. n. 626/1994. Questo fa sì che una volta decisa l'ammissibilità del controllo soprattutto in base all'art. 4 St.lav. (e anche della legge n. 675/1996) bisognerà osservare le condizioni poste dal paragrafo 3 dell'allegato VII al d.lgs. n. 626/1994: condizioni che impongono la preventiva informazione del lavoratore della possibilità del controllo.

4. Controlli tecnologici e misure di garanzia.

Va subito detto che un'interpretazione flessibile dell'art. 4 St.lav., volta ad ammettere la possibilità di controlli diretti sull'attività dei lavoratori, svolti mediante apparecchiature tecniche, è ancorata all'adozione di un metodo esegetico assai prudente e che tenga conto di vari elementi.

Anzitutto, non va trascurato che nell'art. 4 St.lav., come dimostrano la genesi della disposizione e la sua lunga vicenda applicativa, v'è il ripudio di controlli svolti tramite

²⁵ Cfr. Cass. 17 giugno 2000, n. 8250, in *Not. giur. lav.*, 2000, p. 711; Stenico, *La tutela della riservatezza del lavoratore nell'esercizio della prestazione*, in *La tutela della privacy del lavoratore*, cit., p. 169 ss.; Chieco, *Telelavoro*, cit., p. 11 ss.; e Bellavista, *Il controllo*, cit., p. 106 ss.

apparecchiature tecniche che vadano oltre una "dimensione umana" e cioè siano totalizzanti e capaci di afferrare ogni momento dell'attività dei lavoratori. Poi, dovrebbe essere chiaro che l'art. 4 St.lav., proprio nel regolare una forma di controllo sui lavoratori, non fa altro che fissare dei limiti all'esercizio di un potere contrattuale del datore che interferisce con la libertà e la dignità del lavoratori: e quindi la disposizione interviene in un'area in cui vengono in gioco diritti fondamentali della persona umana, che, com'è noto, possono subire delle restrizioni in determinati contesti, in funzione della tutela di altri interessi ritenuti prevalenti, ma mai essere completamente annullati. D'altra parte sono troppo noti gli effetti devastanti, proprio a danno della libertà e dei diritti fondamentali del singolo, che possono essere provocati dall'uso indiscriminato delle forme di controllo e di trattamento dei dati personali rese possibili dalle nuove tecnologie²⁶.

Tutto ciò spinge ad utilizzare come chiave di lettura dell'enunciato normativo alcuni principi tipici cui si fa ricorso quando si tratta di vagliare la legittimità delle restrizioni ai diritti fondamentali²⁷: e cioè i principi di indispensabilità e di proporzionalità²⁸.

Beninteso, il controllo tecnologico può apparire legittimo, solo quando esso sia indispensabile, vale a dire quando non esiste alcuna altra possibilità, meno restrittiva per la libertà e la dignità del lavoratore, per il perseguimento di uno scopo del datore ritenuto nel caso concreto meritevole di tutela.

Quindi, va preliminarmente vagliata la presenza di un interesse del datore, ritenuto meritevole di apprezzamento e quindi di soddisfazione. Poi, come s'è già accennato, va accertato che per la garanzia di tale interesse sia indispensabile l'attivazione del controllo tecnico. E così, il parametro dell'indispensabilità induce a ritenere ammissibile il controllo tecnologico solo in via di *extrema ratio*. Inoltre, anche se il controllo è così valutato legittimo, esso deve comunque svolgersi nel modo che consenta di ridurre al minimo la lesione dei contrapposti interessi del lavoratore, pur realizzando lo scopo meritevole di tutela perseguito dal datore. Principi del genere non costituiscono una novità, ma anzi trovano significativo riscontro nell'esperienza comparata. Ad esempio, in Francia, il principio di proporzionalità è affermato esplicitamente, in via legislativa, come criterio base di verifica della legittimità delle restrizioni apportate ai diritti della persona e alle libertà individuali e collettive in funzione dell'esercizio dei poteri del datore. Sicché, facendo

²⁶ Cfr. Simitis, *Developments in the protection of workers' personal data*, in ILO, *Workers' privacy, Protection of personal data*, n. 2/1991, Geneva, 1992, p. 10 ss.; Lyon, *L'occhio elettronico*, Feltrinelli, Milano, 1997, spec. p. 100 ss. e p. 171 ss.

²⁷ L'impostazione esegetica prescelta nel testo si collega alle osservazioni già svolte in Bellavista, *Il controllo*, cit., p. 65 ss. e p. 99. Sulla stessa lunghezza d'onda, anche se con argomentazioni diverse, cfr. Chieco, *Telelavoro*, cit., p. 9 ss.; Stenico, *La tutela*, cit., p. 176 ss.; Ghezzi e Liso, *Computer e controllo dei lavoratori*, cit., rispett. p. 365 s. e p. 378 ss.

²⁸ Il fondamento dogmatico di tali principi può essere rintracciato nel ruolo primario assegnato alla tutela della persona nel sistema costituzionale, alla luce delle clausole generali di buona fede e correttezza e dell'art. 9 della legge n. 675/1996. Per suggestive indicazioni cfr. Rodotà', *Persona*, cit., p. 583 ss.; Perulli, *La buona fede nel diritto del lavoro*, in *Riv. giur. lav.*, 2002, I, p. 3 ss.; nonché Montuschi, *Ancora sulla rilevanza della buona fede nel rapporto di lavoro*, in *Arg. dir. lav.*, 1999, p. 723 ss.; Zachert, *Ein Mosaik von Arbeitnehmergrundrechten im Grundgesetz*, in *Betriebs-Berater*, 1998, p. 1310 ss.; Tullini, *Clausole generali e rapporto di lavoro*, Maggioli, Rimini, 1990; Zoli, *La tutela delle posizioni "strumentali" del lavoratore*, Giuffrè, Milano, 1988.

ricorso a tale principio, e ad altre regole generali, s'è mosso il Garante per la protezione dei dati francese (la CNIL) proprio nel valutare l'ammissibilità di forme di controllo informatico in azienda²⁹. E soprattutto va ricordata l'esperienza tedesca. Qui esiste una disposizione legale, il § 87 del *BetrVG* che si limita a sancire la necessità della codeterminazione del *Betriebsrat* quando il datore intenda installare apparecchiature destinate a controllare il comportamento o il rendimento del lavoratore³⁰. Ma tale disposizione non stabilisce che, una volta rispettata la procedura di codeterminazione, sia sempre lecita tale installazione. Anzi, la liceità dell'installazione di apparecchiature di controllo dipende, alla stregua di un costante orientamento della giurisprudenza e della dottrina, da una valutazione volta a bilanciare nel caso concreto l'interesse perseguito dal datore e le singole manifestazioni del diritto generale della personalità del lavoratore che vengono coinvolte dalla specifica forma di sorveglianza. E questa valutazione viene operata con molta prudenza, considerando e distinguendo le varie ipotesi che si possono presentare, cercando di ridurre al minimo l'intromissione nella sfera della personalità del lavoratore, pur consentendo la soddisfazione del legittimo interesse datoriale. Sicché, gli attori della procedura codeterminativa possono regolare in concreto l'uso della specifica forma di sorveglianza, ma devono tenere in conto l'esigenza di garantire il diritto generale della personalità del lavoratore: e quindi il loro potere regolativo non è illimitato, bensì orientato dall'esigenza di rispettare il diritto citato dalle cui specifiche manifestazioni sono desumibili articolati confini all'utilizzazione di ogni singolo mezzo di controllo³¹.

Un approccio così accorto alla problematica della sorveglianza tecnologica ha trovato concretizzazione nel codice di condotta sulla protezione dei dati personali dei lavoratori del 1996, elaborato in seno all'Ufficio internazionale del lavoro. Benché il codice non abbia alcuna forza vincolante, l'autorevolezza dell'organo da cui promana lo rende degno della massima attenzione sia da parte degli attori individuali e collettivi sia degli stessi legislatori nazionali. In primo luogo, il codice adotta un concetto di sorveglianza estremamente ampio. Infatti si dice che il termine "monitoring" (e quindi controllo o sorveglianza) "comprende (ma non è limitato a) l'uso di apparecchiature, come computer, macchine fotografiche, impianti audiovisivi, registratori di suoni, telefoni e altri mezzi di comunicazione, vari metodi per stabilire l'identità e la posizione, o ogni altro metodo di sorveglianza". E' evidente che una nozione così aperta del concetto di controllo è formulata proprio per evitare il problema che la disciplina sostanziale sia resa inapplicabile dall'affacciarsi di una nuova forma di sorveglianza (si pensi alle tecniche biometriche oggi sempre più diffuse) che

²⁹ Cfr. Commission nationale de l'informatique et des libertés (da ora CNIL), *La cybersurveillance sur les lieux de travail*, 5 febbraio 2002, reperibile sul sito Internet della Commissione.

³⁰ Per un quadro completo dei presupposti normativi che, nel sistema tedesco, consentono alla rappresentanza dei lavoratori di partecipare, con varie forme di intensità, alle decisioni del datore, privato e pubblico, di raccogliere e trattare dati personali dei lavoratori cfr. Simitis, *Zur Mitbestimmung bei der Verarbeitung von Arbeitnehmerdaten - eine Zwischenbilanz*, in *Recht der Datenverarbeitung*, 1989, p. 49 ss.

³¹ Cfr. Lindemann-Simon, *Betriebsvereinbarungen zur E-Mail-, Internet und Intranet-Nutzung*, in *Betriebs-Berater*, 2001, spec. p. 1953 ss.; Balke-Müller, *Arbeitsrechtliche Aspekte beim betrieblichen Einsatz von e-mails*, in *Der Betrieb*, 1997, p. 327 ss.; Simitis, *Mitbestimmung als Regulativ einer technisierten Kontrolle von Arbeitnehmern*, in *Neue Juristische Wochenschrift*, 1985, p. 403.

non è ricompresa in una enumerazione casistica e chiusa delle apparecchiature di controllo. E per inciso sia consentito sottolineare come questa modalità di costruzione della fattispecie presenti spiccate analogie con la formulazione dell'art. 4 St.lav. in cui l'espressione "altre apparecchiature" ha permesso, e pare possibile possa permettere ancora, una straordinaria vitalità della disposizione, nonostante siano trascorsi tanti anni dal momento in cui è stata varata. Peraltro, proprio questa analogia lascia intendere come l'art. 4 St.lav. costituisca una disposizione ben costruita per vivere in differenti contesti tecnologici, purché ovviamente si presentino le esigenze di tutela nei confronti del controllo tecnico codificate dal legislatore. E quindi emerge come la dottrina che ha cercato di restringere il campo di applicazione dell'art. 4 St.lav. agli strumenti simili a quelli esplicitamente menzionati dal legislatore del 1970 (impianti audiovisivi), come se le telecamere e i registratori esaurissero la *ratio* di tutela della norma, abbia sostenuto una tesi perfettamente legittima, ma fondata su argomenti parimenti controvertibili.

Sul piano sostanziale il citato codice di condotta afferma, in primo luogo, che "se i lavoratori vengono sorvegliati" (e cioè con uno dei metodi appena menzionati) "essi dovrebbero essere informati in anticipo delle ragioni del controllo, della tabella oraria, dei metodi e delle tecniche usate, nonché dei dati che vengono raccolti". E inoltre "i datori di lavoro devono ridurre al minimo l'intrusione nella *privacy* dei lavoratori". Quest'ultima espressione assume un'importanza fondamentale. Infatti, come si legge nel memorandum esplicativo che accompagna il codice, "i datori non sono liberi di scegliere il metodo e i mezzi di controllo che considerano i più adatti per i propri scopi; piuttosto essi devono considerare le conseguenze prodotte sulla *privacy* dei lavoratori e dare la preferenza ai mezzi di sorveglianza meno intrusivi". Come si vede, si suggerisce l'adozione di un principio volto a circoscrivere lo spazio del controllo mediante il ricorso a strumenti che, pur realizzando gli scopi prefissi, producano il minimo danno a carico dei contrapposti interessi dei lavoratori.

Il codice prevede anche la possibilità che il controllo sia continuo o occulto; ma a questo riguardo detta delle prescrizioni ancora più severe. Infatti, "il controllo occulto dovrebbe essere permesso soltanto quando è svolto conformemente alla legislazione nazionale o sussista una ragionevole sospetto di un'attività penalmente illecita o altri gravi comportamenti illeciti"; mentre il "controllo continuo dovrebbe essere permesso soltanto qualora è richiesto dall'esigenza di garantire la salute e la sicurezza o la protezione della proprietà". A questo proposito, il memorandum precisa "che è stato dimostrato come il controllo continuo sia una causa di una costante ansietà che può provocare lesioni fisiche e psicologiche". Perciò, tale controllo dovrebbe essere limitato ai casi in cui sia necessario per risolvere specifici problemi concernenti la salute e la sicurezza o la protezione della proprietà". Mentre, "il controllo occulto va ammesso nella misura in cui sia previsto da specifiche disposizioni della legislazione nazionale". E ciò "potrebbe essere inevitabile in relazione ad indagini riguardanti attività penalmente illecite o altri gravi comportamenti illeciti". Ma si aggiunge che "il codice sottolinea come il mero sospetto di un'attività illecita non sia sufficiente". E cioè il controllo occulto può essere attivato "solo se esistano motivi ragionevoli" sulla cui base si ritenga fondato tale sospetto. E un esempio di grave comportamento illecito è costituito dalla molestia sessuale, "che potrebbe non essere considerata come un comportamento penalmente rilevante"³².

³² Simitis, *Reconsidering*, cit., p. 1597 ss., sottolinea l'importanza di questi indicazioni per conformare una specifica regolazione comunitaria del trattamento dei dati personali dei lavoratori.

Di recente anche il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, di cui all'art. 29 della direttiva n. 95/46/Ce, del 24 ottobre 1995 - sulla cui base è stata varata la legge n. 675/1996 - ha sfornato un articolato parere sul trattamento dei dati personali nel rapporto di lavoro. Per quanto concerne la sorveglianza sui lavoratori, si afferma chiaramente che "qualsiasi controllo deve costituire una risposta proporzionata ai rischi che si fronteggiano e deve tenere conto delle legittime aspettative di *privacy* e degli altri interessi dei lavoratori". Inoltre, "qualsiasi dato personale ottenuto o usato nel corso della sorveglianza deve essere adeguato, pertinente e non eccessivo rispetto allo scopo per cui è giustificato il controllo". E "qualsiasi controllo deve essere svolto nel modo che sia il meno intrusivo possibile".³³

5. Alcuni casi di controllo tecnologico.

Alla luce delle considerazioni svolte nei paragrafi precedenti pare opportuno analizzare alcune forme di utilizzazione delle tecnologie informatiche a fini di controllo sull'attività dei lavoratori in questo momento particolarmente discusse.

Come s'è accennato, è sempre più diffuso l'uso del videoterminale come strumento di lavoro, nel senso che esso spesso costituisce l'indispensabile mezzo attraverso cui il lavoratore adempie la propria prestazione. Il caso più eclatante è appunto quello del telelavoro in cui la distanza tra l'azienda e il luogo di svolgimento effettivo del lavoro è colmata grazie al collegamento telematico. Ma in questa ipotesi possono rientrare tutti i casi in cui il lavoratore faccia uso di un computer come diretto strumento di lavoro. Si pensi ad un operatore del settore bancario e dell'intermediazione mobiliare, oppure a un lavoratore di un'azienda che produce software, che utilizza il computer per elaborare programmi e per intervenire sui sistemi informatici del proprio datore o di altri. Qui a volte il controllo può rappresentare l'unica modalità per accertare la regolarità del comportamento del lavoratore oppure per prevenire il compimento di illeciti. E pertanto adeguate misure di sorveglianza dovrebbero essere consentite proprio per permettere la realizzazione di tali obiettivi. Accertata la giustificazione del controllo e l'indispensabilità dello stesso, vanno poi precisate le modalità d'esercizio del medesimo. E a questo riguardo i lavoratori dovrebbero essere preventivamente informati dell'attivazione di forme di sorveglianza (arg. *ex* allegato VII al d.lgs. n. 626/1994) ed essa dovrebbe essere limitata alla misura strettamente indispensabile per il raggiungimento degli obiettivi prefigurati. Ciò ovviamente può variare da caso a caso: sicuramente deve essere possibile rintracciare in ogni momento il lavoratore che abbia la possibilità di operare degli spostamenti di denaro, oppure il dipendente che operi su aree particolarmente delicate del sistema aziendale. Mentre nel caso di un lavoro a distanza di tipo ordinario - la vendita o la propaganda di prodotti, la diffusione di informazioni commerciali, il servizio di prenotazione aerea o ferroviaria - il controllo andrebbe circoscritto all'accertamento di alcuni indici di rendimento: come per esempio il numero di contratti stipulati, o di contatti effettuati in una giornata; senza quindi che la sorveglianza possa estendersi a lambire ogni fase dell'attività del lavoratore. Qui emerge il ruolo fondamentale giocato dal comma 2 dell'art. 4 St.lav. Infatti, proprio grazie alla procedura codeterminativa prevista dalla disposizione, è possibile fissare in concreto le regole che dovrebbero garantire l'adeguato bilanciamento tra le legittime esigenze datoriali e i contrapposti interessi dei prestatori di lavoro. E' superfluo osservare che l'azione del soggetto sindacale non può arrivare a bloccare l'installazione del meccanismo di controllo,

³³ Data protection working party, opinion 8/2001, 13 settembre 2001, p. 4, e anche p. 25.

perché, nel caso in cui non si raggiungesse l'accordo, il datore potrebbe sempre ottenere un provvedimento sostitutivo da parte dell'autorità amministrativa, ovviamente qualora quest'ultime ritenesse giustificata la richiesta datoriale.

Altro caso di controllo su cui di recente s'è concentrata particolare attenzione, è quello effettuato sull'uso dei collegamenti Internet e della posta elettronica da parte dei lavoratori, per fini diversi da quelli ammessi dalla direzione aziendale³⁴.

Per quanto concerne l'uso di Internet, dalla parte delle aziende si sostiene la necessità di tale controllo per evitare che i dipendenti, durante l'orario di lavoro, si dedichino ad attività diverse da quelle corrispondenti al rispetto degli obblighi contrattuali (per esempio trascorrendo un notevole arco di tempo con collegamenti alle cosiddette chat-line o ai forum di discussione telematici), oppure per impedire che, grazie alle enormi potenzialità di tale forma di circolazione delle informazioni, i lavoratori provochino danni all'impresa, per esempio collegandosi a siti cosiddetti a pagamento (come quelli pornografici, o quelli che distribuiscono musica e altri giochi), con l'effetto che i relativi costi appunto vengano addossati all'azienda.

A questo riguardo va preliminarmente detto (e l'osservazione vale in generale per i rapporti tra tecnologia e diritti della persona) che il fatto che lo sviluppo tecnologico consente certe forme di sorveglianza, ciò non significa che il loro uso sia lecito alla stregua dei principi del sistema giuridico³⁵. Se si pensasse così verrebbero travolte le ragioni che hanno rappresentato la base della nascita e della permanenza di quel settore dell'esperienza giuridica che è costituito dal diritto del lavoro: il quale è permeato dallo sforzo di realizzare un costante bilanciamento tra le esigenze dell'impresa e i diritti della persona che lavora³⁶.

Beninteso, va poi messo in evidenza che la moderna tecnologia consente di evitare i rischi poc'anzi citati. In effetti, con costi irrisori i sistemi informatici aziendali potrebbero essere dotati di meccanismi (di cosiddetto filtraggio) tali da bloccare l'accesso, via Internet, a siti non autorizzati o non ritenuti utili ai fini lavorativi. In questo modo con semplici accorgimenti tecnici, non vi sarebbe nemmeno l'esigenza di effettuare controlli in quanto il comportamento indesiderato non potrebbe *a priori* essere realizzato. E pertanto, in questa ipotesi, è difficile realizzare l'integrazione del principio di indispensabilità del controllo tecnologico, che, come s'è visto in precedenza, rappresenta una delle tappe del percorso volto ad accertarne la legittimità. Sicché, se un datore ritenesse di dovere attivare una forma di controllo del genere, senza prima verificare la possibilità di utilizzare tecniche in grado di evitare la stessa necessità del controllo, porrebbe in essere una violazione dell'art. 4 St.lav. e anche della stessa legge n. 675/1996. In effetti, tale controllo realizzerebbe un trattamento non necessario alla stregua della lettera b) del comma 1, dell'art. 12 della legge n. 675/1996, oppure violerebbe il principio della pertinenza e della non eccedenza dei dati di cui alla lettera d) del comma 1 dell'art. 9 della medesima legge e quindi sarebbe del tutto illecito.

Non va trascurato che, come ammette lo stesso Garante per la protezione dei dati personali francese "un divieto generale e assoluto di utilizzare Internet per fini diversi da quelli professionali non sembra realistico in una società dell'informazione e della

³⁴ Cfr. ampiamente CNIL, *La cybersurveillance sur les lieux de travail*, cit., p. 2 ss.; Däubler, *Internet und Arbeitsrecht*, Bund, Frankfurt am Main, 2001.

³⁵ Cfr. Rodotà, *Tecnologie e diritti*, cit., p. 114 ss. e p. 143 ss.

³⁶ Per tutti, cfr. Mengoni, *Diritto e valori*, Il Mulino, Bologna, 1985, p. 127 ss.

comunicazione". E quindi "un uso ragionevole, non suscettibile di ridurre le condizioni d'uso a fini professionali e che non comprometta la produttività, appare generalmente e socialmente ammissibile nelle maggior parte delle imprese e delle amministrazioni pubbliche"³⁷.

Orbene, potrebbe verificarsi il caso in cui la particolare attività del lavoratore rende necessario che egli abbia un completo accesso a Internet oppure che la stessa impresa, per libera scelta diretta a creare un tranquillo clima aziendale, voglia consentire ai propri dipendenti, nei momenti di pausa, la possibilità di utilizzare la rete per motivi personali. Ma al tempo stesso sorge l'esigenza di evitare che si verifichino abusi e quindi uno sfruttamento abnorme del sistema telematico. Anche in questi casi, è possibile adottare soluzioni volte a restringere il controllo allo stretto indispensabile. Nell'ipotesi di lavoratori la cui particolarità della mansione rende necessario l'accesso libero ad Internet, potrebbero essere effettuati dei controlli congiunti tra azienda e sindacato per accertare se l'uso di Internet sia andato verso siti assolutamente non corrispondenti alle esigenze lavorative. I dati relativi alle varie connessioni andrebbero registrati, controllati a campione e successivamente cancellati³⁸.

Oppure, qualora l'impresa conceda ai lavoratori l'uso di Internet per motivi personali, durante le pause di lavoro o in altri spazi discrezionalmente individuati, l'uso abnorme potrebbe essere evitato ricorrendo ai meccanismi di filtraggio di cui s'è detto. Si tratterebbe di bloccare del tutto l'accesso a determinate tipologie di indirizzi ritenuti "deprecabili" e consentire la navigazione verso tutti quelli restanti: in effetti, è ben diverso il caso del collegamento ad un sito a pagamento (da cui si può scaricare musica, programmi per giochi elettronici, immagini pornografiche) o generalmente riprovevole, come quelli che espongono idee politiche, razziali e sessuali estreme, rispetto al caso del lavoratore che usi Internet per effettuare una prenotazione di un viaggio, si informi sull'orario di apertura di un museo, o si legga un documento sindacale. Altra soluzione potrebbe essere quella di accollare i costi del collegamento verso i siti non autorizzati per motivi di servizio, e pertanto non riconosciuti dal sistema informatico aziendale, direttamente in capo al lavoratore, e quindi in questo modo verrebbe indirettamente disincentivata la connessione a siti a pagamento (che, com'è noto, sono alquanto costosi). Resta l'ipotesi in cui v'è l'esigenza di evitare che l'uso di Internet distraiga il lavoratore dallo svolgimento della prestazione lavorativa, ovvero di impedire che il dipendente ricorra ad Internet per motivi personali anche al di fuori dei momenti autorizzati dall'azienda. Per soddisfare questa ragionevole esigenza andrebbero introdotti meccanismi in grado di individuare il ricorso alla rete telematica che superi l'arco temporale eventualmente consentito. Per esempio, se si assegnano tot minuti di collegamento libero durante l'arco della giornata, il sistema informatico inizierebbe a registrare i collegamenti che sfiorano la durata così stabilita e quindi si potrebbero accertare i comportamenti scorretti. Sicché, il dipendente, avendo conoscenza di non potere abusare delle facoltà concesse, sarà inevitabilmente portato a limitare i collegamenti per il tempo assegnato.

Ovviamente, le possibili forme di controllo qui brevemente suggerite andrebbero attivate rispettando la procedura codeterminativa di cui all'art. 4 St.lav., in modo tale da modellare le modalità di verifica alle specifiche esigenze concrete di ogni realtà aziendale.

³⁷ CNIL, *La cybersurveillance sur les lieux de travail*, cit., p. 10.

³⁸ Cfr. le indicazioni di Lindemann-Simon, *Betriebsvereinbarungen*, cit., p. 1955.

Alla luce delle considerazioni svolte, desta notevoli perplessità la recente decisione di un giudice che ha ritenuto legittimo il licenziamento per giusta causa di una lavoratrice, perché, invece di svolgere i propri compiti, avrebbe trascorso lunghi periodi di tempo collegandosi ad Internet, proprio in assenza di effettive necessità lavorative. La prova di tale comportamento illecito viene ottenuto non solo facendo ricorso alle testimonianze dei colleghi, ma anche alle registrazioni dei collegamenti operate dal fornitore del servizio Internet³⁹. Ciò che lascia sorpresi del percorso argomentativo del giudice è che non vi sia stata alcuna verifica della legittimità del controllo tecnico così svolto alla stregua dell'art. 4 St.lav.: come se appunto tale disposizione non fissasse limiti all'utilizzo del controllo tecnologico.

Riguardo all'utilizzazione della posta elettronica, oltre a tenere presente quanto già detto, vanno svolte ulteriori osservazioni. Anzitutto, la posta elettronica - sia che corre su linee esterne come Internet sia quella che circola sulle linee interne alle aziende: come Intranet - spesso rappresenta un indispensabile strumento di lavoro. Il datore di lavoro può avere la necessità di verificare il contenuto della posta elettronica per accertare che i dipendenti svolgano correttamente i propri compiti lavorativi. Poi sorge l'esigenza di evitare che i lavoratori usino la posta elettronica per motivi personali, distraendosi dai compiti contrattuali oppure di impedire che tramite la posta elettronica vengano rivelate informazioni aziendali riservate o segrete o vengano commessi gravi comportamenti illeciti, come la diffusione di messaggi diffamatori, la realizzazione di molestie sessuali, di forme di mobbing e così via. Tuttavia, pare possibile ritenere che, attraverso un approccio ragionevole ed equilibrato, queste condivisibili esigenze aziendali possano trovare adeguata soddisfazione.

Certo, non va trascurato di ricordare che qui si apre la questione se la posta elettronica sia assimilabile ad una forma di comunicazione e quindi goda della relativa tutela civile e penale. La risposta non può che essere positiva, anche alla luce delle indicazioni che provengono dal quadro legislativo (cfr. la legge 23 dicembre 1993, n. 547) e dalla pronunce del Garante italiano per la protezione dei dati personali⁴⁰. Però, nulla esclude che il controllo sulla posta elettronica possa essere giustificato in presenza di motivi particolarmente validi. D'altra parte, è noto come la portata dei diritti fondamentali possa atteggiarsi in modo differente a seconda del contesto in cui essi si esplicano. E che nel rapporto di lavoro, stante l'implicazione della persona del lavoratore nello svolgimento dello stesso, si assiste ad un continuo bilanciamento tra pretese datoriali e diritti dei prestatori di lavoro⁴¹.

Pertanto, se la posta elettronica rappresenta realmente un indispensabile strumento di lavoro, da cui possa evincersi il corretto adempimento dell'obbligazione lavorativa, il

³⁹ T. Milano 8 giugno 2001, in *D & L*, 2001, p. 1067 ss.

⁴⁰ Cfr. il comunicato stampa del Garante del 12 luglio 1999, in *Cittadini e società dell'informazione*, Bollettino, n. 9, 1999, p. 96 s. Sulla tutela penale delle comunicazioni informatiche o telematiche cfr. Dolcini-Marinucci, *Codice penale commentato*, Ipsoa, Milano, 2000, p. 3248 ss.; Pecorella, *Il diritto penale dell'informatica*, Cedam, Padova, 2000, p. 281 ss.

⁴¹ Cfr. Del Rey Guanter, *Diritti fondamentali della persona e contratto di lavoro: appunti per una teoria generale*, e Magnani, *Diritti della persona e contratto di lavoro: l'esperienza italiana*, entrambi in *Diritti della persona e contratto di lavoro*, in *Quad. dir. lav. rel. ind.*, n. 15, 1994, rispettivamente p. 9 ss. e p. 47 ss.; Valdés Dal-Ré, *I poteri dell'imprenditore e la persona del lavoratore*, in *Giorn. dir. lav. rel. ind.*, 1991, p. 45 ss.

controllo sulla stessa e quindi sul suo contenuto dovrebbe essere ritenuto ammissibile alla stessa stregua del più tradizionale controllo sulla documentazione cartacea utilizzata dal dipendente per lo svolgimento del proprio lavoro e grazie al cui esame appunto può essere accertata la correttezza delle operazioni svolte. Semmai, qui andrebbero adottati opportuni accorgimenti per evitare che la posta elettronica usata per motivi di servizio possa essere visionata ovvero danneggiata da personale non autorizzato, oppure che il controllo telematico si svolga con modalità da annullare ogni spazio di libertà del lavoratore, sia del tutto arbitrario, o impedisca al dipendente di contestare efficacemente le eventuali valutazioni negative scaturenti dal controllo.

Detto ciò bisogna distinguere se il datore intenda concedere ai propri dipendenti l'uso della posta elettronica per motivi personali. Se tale uso viene vietato, tuttavia non si può pensare di ritenere lecito qualsiasi controllo per verificare se i lavoratori rispettino il suddetto divieto. In effetti, anche qui basterebbe adottate opportuni accorgimenti tecnici per bloccare l'invio di messaggi non riconoscibili (e quindi non preventivamente autorizzati) dalla rete aziendale: e cioè verso indirizzi non di pertinenza professionale. Tuttavia, sembra alquanto irrealistico ipotizzare un'azienda moderna del tutto chiusa alla comunicazione esterna. Lo stesso Garante francese per la protezione dei dati personali (CNIL) ha affermato, nel suo già citato e approfondito rapporto, che "l'utilizzazione della posta elettronica, concessa per fini professionali, per inviare o ricevere messaggi a carattere personale, in proporzioni ragionevoli, corrisponde ad un uso generalmente e socialmente ammissibile"⁴². Sicché, come dimostra l'attuale esperienza, in genere il datore tenderà ad ammettere l'uso della posta elettronica per fini privati; ma qui sorgono le esigenze prima accennate di evitarne un uso dannoso per l'impresa. La soluzione preferibile sembra essere quella di assegnare ai lavoratori degli indirizzi di posta elettronica esclusivamente utilizzabili per fini privati: in questo modo, il sistema informatico potrebbe limitarsi ad accertare che il lavoratore non utilizzi la posta elettronica durante l'orario di lavoro, ma solo nelle pause o in altri momenti autorizzati. E così potrebbero anche essere attribuiti a carico dei lavoratori i relativi costi della comunicazione: e cioè si potrebbero utilizzare le stesse regole già da tempo suggerite e comunemente in uso nell'esperienza comparata riguardo alla possibilità di effettuare telefonate private con gli apparecchi aziendali⁴³.

Tuttavia, in certi casi queste misure potrebbero non essere sufficienti: per esempio, di fronte all'esigenza che l'uso per fini privati della posta elettronica costituisca lo strumento per commettere gravi illeciti. In particolare, l'unico modo per accertare se un dipendente usi la posta elettronica per comunicare a concorrenti del datore notizie riservate, è sicuramente costituito dal controllo sul contenuto dei messaggi inviati. Però, proprio in considerazione della particolare natura della posta elettronica - e cioè del fatto che è sempre una forma di comunicazione - il controllo sul contenuto dei messaggi privati di posta elettronica andrebbe attuato soltanto dopo rigorosissime verifiche della sua indispensabilità. E una soluzione idonea a garantire al massimo grado la trasparenza del procedimento, potrebbe consistere nel prevedere che l'effettivo controllo avvenga soltanto in presenza di fondati sospetti del

⁴² CNIL, *La cybersurveillance sur les lieux de travail*, cit., p. 11.

⁴³ Cfr. Balke-Müller, *Arbeitsrechtliche Aspekte*, cit., p. 328; Bellavista, *Il controllo*, cit., p. 109 ss.

comportamento illecito del lavoratore e con la presenza dei rappresentanti sindacali dei lavoratori⁴⁴.

6. Ipotesi e limiti del controllo occulto.

Peraltro, una garanzia a favore dei lavoratori è sicuramente quella della preventiva conoscenza della possibilità del controllo. Anzi, come s'è visto in precedenza, molto spesso la preventiva informazione sul tipo di controllo da attuare potrebbe svolgere una rilevante funzione dissuasiva dal tenere comportamenti illeciti. Le esperienze straniere più significative e l'esaminato codice di condotta dell'Ufficio internazionale del lavoro depongono chiaramente a favore del principio che in genere i lavoratori debbano essere informati preventivamente della possibilità del controllo e delle caratteristiche dello stesso⁴⁵.

Tuttavia, è evidente che talvolta la sorveglianza, per essere efficace, deve essere svolta in forma occulta, e quindi imporre la preventiva informazione dell'interessato, prima di ogni controllo, significherebbe rendere inutile la vigilanza. In considerazione di queste esigenze, come s'è accennato, lo stesso codice dell'Ufficio internazionale del lavoro ammette la possibilità del controllo occulto (e anche del controllo continuo) ma lo assoggetta a regole ancora più rigorose di quelle (già alquanto restrittive) a cui è sottoposto il controllo palese.

Sul piano sostanziale, l'ammissibilità del controllo occulto andrebbe valutata seguendo i già visti principi di indispensabilità e proporzionalità: e considerato il fatto che il controllo occulto assume connotati particolarmente insidiosi per la persona del lavoratore, esso dovrebbe costituire una misura del tutto eccezionale.

Nell'ordinamento italiano, bisogna tenere conto del fatto, che alla stregua dell'art. 10 della legge n. 675/1996 al dipendente spetta di essere preventivamente informato, da parte del datore, sulla caratteristiche più importanti dei trattamenti dei suoi dati personali che lo possono riguardare. Poiché il controllo non è altro che una forma di raccolta di dati personali e quindi di trattamento, l'avviso preventivo della possibilità di forme di controllo, costituisce sicuramente un contenuto imprescindibile dell'informativa a lui spettante: l'art. 10, comma 1, lett. a) della legge n. 675/1996 prevede come contenuto dell'informativa "le finalità e le modalità del trattamento cui sono destinati i dati". Ma tale regola procedurale non sembra escludere la facoltà del datore di attivare (ovviamente in casi eccezionali) forme di controllo occulto.

Infatti, alle ipotesi di controllo occulto (che sia in sé legittimo e cioè giustificato dal perseguimento di interessi meritevoli e non tutelabili in altro modo) pare applicabile l'art. 10, comma 4, della stessa legge che esclude l'obbligo di informativa nei confronti del soggetto interessato quando i dati sono trattati al fine di "far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento". A sostegno di questa conclusione depone una decisione del Garante per la protezione dei dati personali che ha riguardato il caso della raccolta di informazioni, per mezzo di un investigatore privato, allo scopo di verificare la sussistenza di una patologia addotta dal dipendente per giustificare alcuni

⁴⁴ Cfr. Lindemann-Simon, *Betriebsvereinbarungen*, cit., p. 1955; Balke-Müller, *Arbeitsrechtliche Aspekte*, cit., p. 328; Raffler-Hellich, *Unter welchen Voraussetzungen*, cit., p. 863 s.

⁴⁵ Nella stessa direzione cfr. CNIL, *La cybersurveillance sur les lieux de travail*, cit., p. 7 ss.; il principio 3.1 della raccomandazione del 1989 del Consiglio d'Europa; il parere del Gruppo ex art. 29 della direttiva 95/46/Ce, 13 settembre 2001, cit., p. 25.

periodi di assenza dal lavoro⁴⁶. D'altra parte, l'avviso preventivo della possibilità di forme di controllo (anche occulto) potrebbe rientrare nell'informativa che viene fornita all'atto della nascita del rapporto, senza che sia necessario ripetere l'informativa ogni volta che si faccia scattare la vigilanza. E un argomento a sostegno di questa lettura può essere rintracciato nella già citata disposizione contenuta nel paragrafo 3 dell'allegato VII al d.lgs. n. 626/1994, secondo cui "all'atto dell'elaborazione, della scelta, dell'acquisto del software, o allorché questo viene modificato... il datore terrà conto" che "nessun dispositivo o controllo quantitativo o qualitativo può essere utilizzato all'insaputa dei lavoratori". Ciò significa che una volta decisa l'ammissibilità del controllo, soprattutto in base all'art. 4 St.lav. e delle citate disposizioni della legge n. 675/1996 (artt. 9 e 12), bisognerà osservare le condizioni poste dal paragrafo 3 dell'allegato VII al d.lgs. n. 626/1994: condizioni che impongono la preventiva informazione del lavoratore della possibilità del controllo, ma permettono l'attivazione di specifici controlli occulti in casi particolarmente gravi, come, per esempio, quelli menzionati dal codice di condotta dell'Ufficio internazionale del lavoro.

Tutte le misure qui suggerite dovrebbero essere contenute, e ovviamente concretate in modo dettagliato, negli accordi o nei provvedimenti scaturenti dalla procedura codeterminativa di cui al comma 2 dell'art. 4 St.lav., che comunque costituirebbero la sede idonea per bilanciare le contrapposte esigenze in campo. Va sottolineato che il rispetto di siffatta procedura codeterminativa rappresenta solo uno dei tasselli per la legittimità dell'attivazione del controllo, perché devono essere sempre presenti anche le condizioni sostanziali di cui al comma 2 dell'art. 4 St.lav. (le esigenze organizzative, produttive e di sicurezza del lavoro, come qui interpretate) che giustificano il controllo: e quindi un accordo o un provvedimento amministrativo che ammettessero forme di sorveglianza in mancanza delle suddette condizioni sostanziali potrebbero essere impugnati dal dipendente dissenziente per ottenere una declaratoria di illegittimità.

7. Profili del trattamento dei dati personali dei lavoratori nel rapporto di lavoro pubblico.

Come s'è già accennato, un fatto estremamente importante è che la legge n. 675/1996 contiene un *regime differenziato* tra trattamento effettuato da soggetti privati (e da enti pubblici economici) e da soggetti pubblici: i primi possono trattare i dati ordinari o comuni alla stregua degli artt. 11 ss. e 20 e i dati sensibili rispettando l'art. 22, commi 1 e 2, della legge n. 675/1996 (nonché le autorizzazioni emanate in forza di tale ultima prescrizione e dell'art. 41, comma 7, della legge); i secondi (cioè i datori di lavoro pubblici), i dati ordinari o comuni ai sensi dell'art. 27, e i dati sensibili osservando l'art. 22, comma 3 (che è stato novellato dall'art. 5, comma 2, del dlgs. n. 135/1999). La diversità delle norme di riferimento non ha solo rilievo formale, ma si esprime anche in una *radicale divergenza della disciplina del trattamento* dei dati personali nei due settori. E, a seguito di ciò, sarebbe anche diversa la disciplina del trattamento dei dati personali tra lavoro privato e pubblico.

Fin dall'entrata in vigore della legge n. 675/1996 non è sembrato possibile colmare tale ingiustificata disparità di trattamento tra lavoro pubblico e privato attraverso una calibrata interpretazione della normativa esistente. Ciò perché, pur nella loro notevole generalità ed astrattezza, gli artt. 27 e 22, comma 3, sono chiaramente diretti a regolare ogni "trattamento

⁴⁶ Cfr. la Newsletter 8-14 gennaio 2001, nel sito Internet del Garante: Garanteprivacy.it.

da parte di soggetti pubblici" e quindi anche quello che riguarda i dati dei dipendenti dei medesimi soggetti.

Le due fonti di diritto internazionale attualmente più rilevanti in ordine al trattamento dei dati personali dei lavoratori, la raccomandazione del Consiglio d'Europa del 1989 (sui dati utilizzati per finalità di lavoro), e il Codice dell'Ufficio internazionale del lavoro dettano principi comuni ai trattamenti dei dati dei lavoratori dei due settori ed ammettono deroghe solo per alcuni frammenti dell'area pubblica *stricto sensu* (come la sicurezza dello Stato o la pubblica sicurezza e la lotta alla criminalità) ed esclusivamente in presenza di condizioni alquanto rigide; ma esse non sono giuridicamente vincolanti. Certo, il Governo italiano, se avesse esercitato quella parte della delega di cui alla legge n. 676/1996 che lo impegnava a varare una normativa specifica per il trattamento dei dati personali nel rapporto di lavoro, avrebbe dovuto tenere conto di tale indicazione della raccomandazione del Consiglio d'Europa. Si ricorda infatti che la suddetta raccomandazione era richiamata espressamente tra i principi e criteri direttivi che avrebbero dovuto guidare il Governo nell'esercizio della delega di cui alla legge n. 676/1996. Tuttavia, stante che la delega (più volte prorogata) è scaduta, la raccomandazione al momento potrebbe solo aiutare nell'interpretazione di disposizioni nazionali che abbiano un certo margine di elasticità semantica: cosa che non si verifica in questo frangente in cui è evidente il significato delle citate regole italiane. Semmai, alla stregua del diritto positivo, può essere prospettata una questione di legittimità costituzionale, per violazione dell'art. 3 Cost., degli artt. 27 e 22, comma 3, della legge n. 675/1996 in quanto applicabili *in toto* anche a tutti i rapporti di lavoro con le pubbliche amministrazioni: e il risultato più probabile è che la Corte costituzionale possa limitarsi a trovare ragionevole tale regime separato solo per alcuni specifici rapporti di pubblico impiego, in cui il rapporto di lavoro è massimamente permeato dal perseguimento dell'interesse pubblico o da motivi di sicurezza pubblica o di ordine pubblico (alla stregua delle indicazioni della citata raccomandazione del Consiglio d'Europa e anche del codice dell'Ufficio internazionale del lavoro).

Né un decisivo aiuto può provenire dalla direttiva comunitaria 95/46/Ce - che ha costituito la molla definitiva per il varo della legge n. 675/1996 - la quale detta prescrizioni tendenzialmente comuni ai trattamenti che avvengono nei due settori. Ma, a ben vedere, tale omogeneità delle regole è appunto solo tendenziale, perché vengono fatte salve ampie possibilità di deroga - giustificate "dall'esercizio di pubblici poteri" o da "un compito di interesse pubblico" - alle norme comuni e va tenuto conto che molti trattamenti posti in essere dai soggetti pubblici sfuggono *ab origine* alla competenza del legislatore comunitario: cfr., per esempio, il considerando 13 e gli artt. 7, 8, 13 della direttiva. Ma il punto centrale della questione è un altro: in considerazione della storia della legislazione della protezione dei dati personali, la preoccupazione maggiore della direttiva è stata quella di spingere gli Stati membri a garantire la tutela dei cittadini nei confronti dei trattamenti posti in essere da soggetti privati. Ciò perché la direttiva ha sullo sfondo i *deficit* di tutela delle legislazioni dei Paesi europei che sono nate per regolare i trattamenti in ambito pubblico (all'origine della problematica della protezione dei dati ritenuti i più pericolosi per le persone) e, mirando a realizzare questo obiettivo primario, solo a fatica e non sempre, sono state estese (e in genere in modo meno garantista) a toccare i trattamenti operati dai soggetti privati. Infatti, in Germania, dove - alla stregua della precedente legge federale sulla protezione dei dati personali del 1990 - il trattamento da parte di soggetti pubblici era assoggettato a regole più rigide di quelle operanti nell'area privata (e la stessa differenza si ripercuoteva sui trattamenti dei lavoratori dei due settori), la direttiva comunitaria è stata

vista come una ghiotta occasione per potere innalzare il livello di tutela nel settore privato⁴⁷.

Eppure, in Italia, la direttiva potrebbe essere invocata dai lavoratori pubblici (in forza della teoria dell'efficacia diretta solo verticale delle direttive qualora il regime del trattamento dei loro dati personali fosse inferiore agli standard comunitari - a questo riguardo non rileva che la tutela dei lavoratori pubblici sia meno forte di quella di cui godono i lavoratori privati - e qualora questo *gap* di tutela non potesse godere delle esenzioni consentite dalla normativa comunitaria; così, attraverso tale verifica si potrebbe pervenire alla eventuale disapplicazione della disciplina italiana.

Comunque, il Governo italiano ha con pervicacia confermato l'esistenza di un regime differenziato del trattamento tra lavoro pubblico e privato, quando, con il d.lgs. 11 maggio 1999, n. 135, emanato sulla base della legge delega n. 676/1996, ha definito "i principi generali in base ai quali i soggetti pubblici... sono autorizzati a trattare dati sensibili o attinenti a particolari provvedimenti giudiziari ai sensi degli artt. 22, comma 3 e 24" della legge n. 675/1996"; inoltre, ha individuato "alcune rilevanti finalità di interesse pubblico, per il cui perseguimento è consentito detto trattamento, nonché le operazioni eseguibili e i tipi di dati che possono essere trattati"; infine, ha dettato "alcune disposizioni integrative" della legge n. 675/1996⁴⁸. In particolare, l'art. 9 del d.lgs. n. 135/1999 afferma che "ai sensi dell'art. 1, si considerano di rilevante interesse pubblico le attività dirette all'instaurazione ed alla gestione di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato". Poi, il comma 2, dell'art. 9 del d.lgs. n. 135/1999 procede ad individuare tutta una serie di trattamenti che si intendono effettuati "per le finalità di cui al comma 1"; come "quelli svolti al fine di: a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette". In questo modo, attraverso l'enucleazione di un'ampia e articolata tipologia di trattamenti consentiti, i soggetti pubblici vengono messi in condizione di continuare a trattare tutti i dati sensibili pertinenti alla gestione dei rapporti di lavoro. Va sottolineato che l'elencazione contenuta nel comma 2, dell'art. 9, del d.lgs. n. 135/1999 appare meramente esemplificativa, poiché è introdotta dall'espressione "tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli svolti al fine di". Quello che conta è che il trattamento debba trovare giustificazione nel perseguimento della finalità di cui al comma 1 dell'art. 9 del d.lgs. n. 135/1999. Ovviamente, tutto ciò fa sì che la disciplina "speciale" del d.lgs. n. 135/1999 si applichi anche ai lavoratori pubblici.

Non è questa la sede per un'analisi dettagliata del d.lgs. n. 135/1999, ma va detto che sicuramente tale decreto assicura una dignitosa protezione ai dati di cui agli artt. 22 e 24 della legge n. 675/1996 dei dipendenti pubblici. Ciò che ancora non è condivisibile è la scelta di regolare con blocchi normativi differenti il trattamento dei dati dei lavoratori

⁴⁷ Cfr. Simitis, *Die EU-Datenschutzrichtlinie - Stillstand oder Anreiz?*, in *Neue Juristische Wochenschrift*, 1997, p. 287; Id., *Datenschutz - Rückschritt oder Neubeginn?*, *ivi*, 1998, p. 2474. Sulla nuova legge federale (BDSG 2001) del 2001 cfr. Däubler, *Das neue Bundesdatenschutzgesetz*, cit., p. 874 ss.

⁴⁸ Per una approfondita analisi cfr. Chieco, *Privacy e lavoro*, cit., p. 233 ss.; Gagnoli, *L'applicazione della legge n. 675 del 1996 al lavoro pubblico*, in *La tutela della privacy del lavoratore*, cit., p. 103 ss.

privati e pubblici. Vero è che sostanzialmente, se si confrontano le diverse discipline, le regole operazionali possono non divergere più di tanto. Anzi, attualmente, a seguito del d.lgs. n. 135/1999, il dipendente pubblico sembra più garantito, rispetto a quello privato, di fronte al trattamento dei dati di cui agli artt. 22 e 24. Ciò perché i rigorosi principi del d.lgs. n. 135/1999 riguardano entrambe tali categorie di dati, mentre quelli contenuti nell'autorizzazione del Garante relativa al trattamento dei dati a carattere giudiziario (e destinati anche ai trattamenti posti in essere da soggetti privati) - che sono in pratica identici a quelli degli artt. da 1 a 4 del d.lg.s. n. 135/1999 - si applicano solo al trattamento dei dati di cui all'art. 24 della legge n. 675/1996. Infatti, le regole contenute nell'autorizzazione generale che riguarda il trattamento dei dati di cui all'art. 22 nell'ambito dei rapporti di lavoro privati, sono più flessibili e meno dettagliate rispetto a quelle del d.lgs. n. 135/1999 e riguardanti il trattamento dei dati di cui agli artt. 22 e 24 attuati dai soggetti pubblici.

Beninteso, va sottolineato che, in questo modo, e cioè continuando a dedicare alle due aree del lavoro pubblico e privato normative formalmente (se non sostanzialmente) differenti, si corre il forte rischio di legittimare operazioni interpretative e applicative che diversifichino di fatto la disciplina concreta del trattamento dei dati personali dei lavoratori pubblici e privati. Tutto ciò lascia alquanto perplessi, perché non può trovare alcuna valida giustificazione soprattutto in considerazione del processo in atto di omogeneizzazione tra lavoro privato e pubblico: o, meglio, di diffusa penetrazione delle regole del diritto privato nell'area del lavoro pubblico. Peraltro, l'omogeneizzazione tra lavoro pubblico e privato (ovvero la privatizzazione del pubblico impiego) resterà un vago miraggio se, invece di eliminare le differenze normative ancora sopravvissute, si continuerà a varare regole non comuni ai due settori e che appunto esaltano la persistenza di tale storica divisione del diritto del lavoro italiano.

8. Il controllo tecnologico nel lavoro pubblico.

L'art. 9 del d.lg.s. n. 135/1999 contiene una prescrizione che condiziona la legittimità dei trattamenti dei dati dei lavoratori pubblici e che incide sulle possibilità di controllo elettronico sui lavoratori: infatti, il comma 3, di questa norma dice che "i dati raccolti mediante impianti audiovisivi o altre apparecchiature, anche informatiche o telematiche, richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro possono essere utilizzati unicamente per tali finalità, individuate secondo le procedure di cui all'art. 4 della legge 20 maggio 1970, n. 300, e all'art. 24 della legge 29 marzo 1983, n. 93". E che "gli interessati sono edotti delle modalità di tale trattamento, anche attraverso l'informativa di cui all'art. 10 della legge" n. 675/1996. Qui va osservato che il comma 3 dell'art. 9 del d.lgs. n. 135/1999 non si pronuncia sul confine della possibilità di raccolta di dati sui dipendenti attraverso le apparecchiature in questione: ma si affida all'interpretazione prevalente degli artt. 4 della legge n. 300/1970 e 24 della legge n. 93/1983. E quindi dovrebbero valere anche in quest'area tutte le considerazioni precedenti riguardanti la suggerita lettura dell'art. 4 St.lav. Comunque l'applicazione dell'art. 4 St.lav non dovrebbe divergere tra lavoro pubblico e privato. Peraltro, poiché il comma 3, dell'art. 9 del d.lgs. n. 135/1999, parla di "dati" senza alcuna specificazione, non è chiaro se tale espressione vada letta in modo coordinato con il comma 3, lett. b), dell'art. 1 del d.lgs. n. 135/1999; e quindi se vada riferita, come agevolmente ricavabile da un approccio sistematico, solo ai dati di cui agli artt. 22 e 24 oppure, come sarebbe più ragionevole, anche ai dati ordinari o comuni.

Comunque, qui sorge il problema dato dalla circostanza che le due norme prevedono differenti procedure per ammettere l'installazione delle apparecchiature in esame: e perciò l'operare dell'una esclude l'attivazione dell'altra. Peraltro, v'è il forte sospetto che l'art. 24 della legge n. 93/1983 sia stato abrogato o quantomeno sia inapplicabile. Infatti, l'art. 51 del d.lgs. n. 165/2001, che riproduce il contenuto dell'art. 55 del d.lgs. n. 29/1993, stabilisce l'applicazione della legge n. 300/1970 alle pubbliche amministrazioni. L'art. 72, comma 1, del d.lgs. n. 165/2001, non riprende più la formula dell'art. 74, comma 1 del d.lgs. n. 29/1993 che affermava l'abrogazione delle norme incompatibili con le disposizioni del d.lgs. n. 29/1993, tra cui quindi rientrava anche l'art. 55 del d.lgs. n. 29/1993, ma contiene un'elencazione delle norme abrogate tra cui non c'è l'art. 24 della legge n. 93/1983. Tuttavia, l'art. 69, comma 1 del d.lgs. n. 165/2001 sancisce che "le norme generali e speciali del pubblico impiego, vigenti alla data del 13 gennaio 1994 e non abrogate...cessano in ogni caso di produrre effetti dal momento della sottoscrizione, per ciascun ambito di riferimento, dei contratti collettivi del quadriennio 1998-2001".

E quindi l'art. 24 della legge n. 29/1983 sarebbe stato già abrogato in quanto incompatibile, alla stregua della vecchia formula dell'art. 74, comma 1, del d.lgs. n. 29/1993, con l'art. 55 del d.lgs. n. 29/1993 che determinava (senza alcuna riserva o eccezione) l'applicazione della legge n. 300/1970 (e perciò anche dell'art. 4 di questa legge) al pubblico impiego. Ovvero, se si ritenesse che l'art. 24 della legge n. 29/1983 non sia stato abrogato o sia stato rivitalizzato dalla successiva modifica del testo dell'art. 74 del d.lgs. n. 29/1993, ad opera dell'art. 72 del d.lgs. n. 165/2001, bisognerebbe tenere conto dell'art. 69, comma 1, del d.lgs. n. 165/2001, che condiziona implicitamente la disapplicazione della disposizione alla stipula, per ogni comparto, del contratto collettivo del quadriennio 1998-2001. Stante che la cosiddetta seconda tornata contrattuale, per il quadriennio 1998-2001, dovrebbe ormai essere completata, allora è ovvio ritenere che l'art. 24 della legge n. 93/1983 ha perso ogni efficacia in tutti i comparti dove è già stato stipulato il contratto collettivo del quadriennio 1998-2001 previsto dal d.lgs. n. 165/2001: e pertanto non vi dovrebbe essere alcun dubbio sulla piena operatività dell'art. 4 St.lav.

9. Principio di finalità, sistema del diritto del lavoro e uso dei dati personali.

E' forse superfluo osservare l'effettività della protezione dei dati personali è assicurata soltanto dalla stringente limitazione della possibilità di raccogliere e utilizzare i suddetti dati⁴⁹. Per quanto concerne la regolamentazione italiana del trattamento dei dati personali comune alle due aree (pubblico e privato) del rapporto di lavoro, va sottolineato che conseguono dal principio di finalità (di cui alla lettera b) dell'art. 9 della legge n. 675/1996 coordinato con l'art. 8 St. lav.), come si evince dall'art. 9 lettere c) e d) della legge n. 675/1996, i corollari che i dati personali devono essere "esatti, e se necessario, aggiornati" nonché "pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati". E infine il principio di finalità si specifica nel cosiddetto principio *del diritto all'oblio* vale a dire nel prevedere, alla stregua dell'art. 9, lettera d), che i dati personali devono essere "conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati".

Le prescrizioni citate (insieme ad altre della stessa legge), coordinate con le regole del sistema del diritto del lavoro, consentono di limitare alcuni rilevanti rischi per i diritti e le

⁴⁹ Cfr. Rodotà, *Persona*, cit. p. 589 ss.; Simitis, *Reconsidering*, cit., p. 1590 ss.

libertà dei lavoratori che scaturiscono soprattutto (ma non solo) dall'elaborazione automatica dei dati personali. Infatti, quando sono erette *barriere normative* che proibiscono o che quantomeno riducono, per quanto logicamente e realisticamente ammissibile, usi ulteriori dei dati rispetto a quelli per cui essi sono stati originariamente raccolti o registrati, si creano le precondizioni per evitare l'uso di siffatti dati per gli scopi più disparati. E' noto che il cosiddetto *uso multifunzionale dei dati* (vale a dire proprio l'uso dei dati per tutti gli scopi di volta in volta ritenuti utili e diversi da quelli per cui sono stati in origine raccolti) aumenta il rischio non solo della moltiplicazione illimitata degli effetti pregiudizievoli causati da dati inesatti o incompleti, ma anche quello di una decontestualizzazione di dati in partenza esatti e quindi della distorsione dell'informazione così veicolata. Beninteso, l'ancoraggio al principio di finalità e agli altri principi di base della legge n. 675/1996 e del diritto del lavoro dissolve la pretesa del datore di considerare il rapporto di lavoro come un unico collettore di informazioni e lo frantuma in una molteplicità di contesti informativi non comunicanti tra loro o comunicanti solo a certe condizioni. La decontestualizzazione è tendenzialmente evitata fissando limiti a sconfinata elaborazioni dei dati personali ed imponendo che questi dati, proprio per rispettare il principio di finalità e gli altri principi di base, vadano utilizzati mantenendo uno stretto collegamento con il loro contesto originario di riferimento.

Attenzione: l'unico modo certo per escludere del tutto i pericoli citati è rappresentato dal vietare l'uso dei dati per scopi diversi e ulteriori (oppure soprattutto per altri specifici scopi ritenuti assai pericolosi) rispetto a quelli che ne hanno legittimato la raccolta, la registrazione e l'uso originario, ovvero dalla tassativa e preventiva descrizione degli scopi leciti del trattamento. Disposizioni del genere si incontrano in particolare nella normativa varata dai singoli *Länder* tedeschi in relazione al trattamento dei dati personali dei lavoratori dipendenti da tali entità⁵⁰.

Tuttavia, tale impostazione può essere adottata solo quando viene coniata una normativa di settore che appunto contiene disposizioni assai dettagliate riguardo al trattamento dei dati personali dei soggetti coinvolti in ogni specifico ambito. Però, già da altre disposizioni del sistema italiano di protezione dei dati personali sono rintracciabili altre indicazioni che confermano l'idea della necessità di una rigorosa interpretazione del principio di finalità. In primo luogo, il d.lgs. 28 luglio 1997, n. 255 che tra l'altro ha introdotto - nell'originaria struttura dell'art. 7 della legge n. 675/1996 - ipotesi di trattamento per cui sono possibili forme di notificazione semplificata e per giunta l'esonero dall'obbligo della preventiva notificazione al Garante, ha stabilito che i trattamenti che godono di queste agevolazioni sono non solo tassativamente individuati in relazione ai fini da essi perseguiti, ma il beneficio opera nella misura in cui il trattamento resti strettamente vincolato agli scopi così fissati e, inoltre, sia quindi effettuato limitatamente alle categorie di dati, di interessati e di destinatari della comunicazione e diffusione, e al periodo di conservazione dei dati necessari per il perseguimento delle medesime finalità (cfr. l'art. 7, commi *5-bis*, *5-ter* e *5-quater*, della legge n. 675/1996: ora in via d'abrogazione a seguito della radicale riforma del sistema della notificazione del trattamento operata dall'art. 3 del d.lgs. 28 dicembre 2001, n. 467). Poi, il Garante - con le autorizzazioni al trattamento dei dati sensibili rispettivamente nei rapporti di lavoro e nell'ambito dell'attività di ricerca e selezione del personale svolta da soggetti esterni alle parti dell'eventuale rapporto - ha non solo individuato con accurata precisione le finalità che giustificano il trattamento dei dati

⁵⁰ Cfr. Simitis, *Reconsidering*, cit., p. 1594.

sensibili di volta in volta considerati, ma ha anche stabilito che "il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e forme di organizzazione dei dati strettamente correlate alle finalità" originarie che ne giustificano appunto il trattamento. E sicuramente tale regola, pur se dettata per i dati sensibili, proprio perché concreta, nello specifico settore dei rapporti di lavoro, il generale principio di finalità di cui all'art. 9 della legge n. 675/1996, non può non influenzare anche il trattamento dei dati cosiddetti ordinari o comuni⁵¹. Inoltre, il d.lgs. n. 135/1999, varato sulla base della legge delega n. 676/1996, contiene le disposizioni dei commi 5 e 6 dell'art.3 (che sono applicabili all'area dei rapporti di lavoro pubblici) secondo cui "i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo" e che i dati sensibili "non possono essere trattati nell'ambito dei test psico-attitudinali volti a definire il profilo o la personalità dell'interessato".

A questo punto, sorge la necessità di chiarire l'esatto significato della condizione, fissata dall'art. 9, lett. b) della legge n. 675/1996, secondo cui i dati personali possono essere "utilizzati in altre operazioni del trattamento in termini *non incompatibili*" con gli scopi (determinati, espliciti e legittimi) fissati all'atto della raccolta e della registrazione dei medesimi dati. E' evidente che più sono flessibili i criteri di misura della compatibilità tra gli scopi della raccolta o della registrazione dei dati e i cosiddetti "termini" in cui vengono successivamente utilizzati gli stessi dati nelle altre operazioni del trattamento, più è probabile il rischio che il principio di finalità affermato dalla prima parte di tale norma diventi un mero simulacro. Dal punto di vista letterale e grammaticale, "compatibile" equivale a conciliabile e tale aggettivo definisce l'idea secondo cui due elementi sono riconducibili "ad una sostanziale affinità qualitativa e di intenti" ovvero "adattabili"⁵². Perciò, nel particolare contesto del trattamento dei dati personali, la compatibilità pare debba essere valutata tenendo conto del risultato finale cui tende l'obiettivo originario (della raccolta e della registrazione) e quello successivamente perseguito nonché delle modalità attraverso cui si svolgono le operazioni del trattamento posteriori alla raccolta e alla registrazione. Pertanto, le "altre operazioni del trattamento" non saranno compatibili con lo scopo originario della raccolta e della registrazione quando produrranno un risultato finale abnorme rispetto a quello preventivabile al momento della raccolta e della registrazione ovvero si svolgeranno con modalità tali da compromettere i diritti della personalità e le libertà fondamentali dell'interessato protetti dalla stessa legge (arg. ex art. 1, della legge n. 675/1996).

Sul ruolo portante del principio di finalità pongono l'accento sia la raccomandazione del Consiglio d'Europa sia il codice dell'Ufficio internazionale del lavoro. In particolare, il codice sottolinea che "i dati personali dovrebbero, in via di principio, essere usati soltanto per gli scopi per cui sono stati in origine raccolti". Questa prescrizione appunto persegue l'obiettivo di evitare il pericolo di un uso illimitato dei dati raccolti e quindi il dissolvimento del medesimo principio di finalità. Ciò significa che il datore non può appellarsi a generiche motivazioni e unificare tutti i dati raccolti - per obiettivi diversi, ma sempre ricadenti nell'area della gestione del rapporto - sul conto del lavoratore per sottoporli ad altre fasi del trattamento. Invece, lo specifico fine della raccolta condiziona e limita la legittimità di ogni altra operazione sugli stessi dati. Inoltre, esclusivamente in via

⁵¹ Cfr. Chieco, *Il diritto alla riservatezza*, cit., p. 40.

⁵² Devoto-Oli, *Il dizionario della lingua italiana*, Le Monnier, Firenze, 1990.

di eccezione, il codice consente al datore, e solo a certe condizioni, di utilizzare i dati già raccolti per scopi *differenti* da quelle per le quali sono stati in origine raccolti i medesimi dati. In primo luogo, la nuova utilizzazione deve essere *compatibile* con lo scopo originario ed inoltre devono essere adottate le *misure necessarie* per evitare false interpretazioni dei dati nel nuovo contesto in cui vengono ad essere utilizzati. Il *memorandum* che accompagna il codice sottolinea che il concetto di trattamento compatibile con lo scopo originario determina la necessità di effettuare una comparazione tra la finalità primordiale e quella successiva e quindi il principio di finalità sarà rispettato solo se lo scopo successivo rientra nell'ambito di quello in origine perseguito. Sicché, "è perfettamente compatibile con lo scopo originario l'uso di dati riguardanti la qualificazione o il rendimento dei lavoratori nelle decisioni per assegnare nuovi benefici economici"; mentre l'uso dei dati raccolti allo scopo di governare i rapporti finanziari con i clienti dell'azienda è incompatibile con quello di emanare provvedimenti disciplinari a carico dei lavoratori in funzione del loro rendimento⁵³.

10. Autoregolamentazione e disciplina di settore per il trattamento dei dati personali dei lavoratori.

L'art. 1, comma 1, della legge 24 marzo 2001, n. 127, ha differito, entro il 31 dicembre 2001, il termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali. Così, il Governo avrebbe potuto emanare norme legislative sia integrative sia correttive della disciplina generale contenuta nella legge 31 dicembre 1996, n. 675 (e nelle normative collegate come il d.lgs. 13 maggio 1998, n. 171), sulla base dei principi e criteri direttivi indicati nella legge n. 676/1996. Sicché, in forza della delega contenuta nell'art. 1, comma 1, della legge n. 127/2001, il Governo ha recentemente varato il d.lgs. 28 dicembre 2001, n. 467 dal titolo "disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali". Il d.lgs. n. 467/2001 ha apportato significative modifiche alla legge n. 675/1996⁵⁴. Va qui concentrata l'attenzione sul capo II del decreto che ha come titolo "attuazione dei principi di protezione dei dati in determinati settori" e si compone di un'unica (ma lunga e di fondamentale importanza) disposizione, l'art. 20, la cui denominazione è "codici di deontologia e di buona condotta". Per il comma 1, dell'art. 20, "al fine di garantire la piena attuazione dei principi previsti dalla disciplina in materia di trattamento dei dati personali, ai sensi dell'articolo 31, comma 1, lett. h), della legge n. 675/1996, il Garante promuove entro il 30 giugno 2002 la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali nei settori indicati al comma 2, tenendo conto della specificità dei trattamenti nei diversi ambiti, nonché dei criteri direttivi

⁵³ Previsioni sostanzialmente analoghe a quelle del codice dell'Ufficio internazionale del lavoro contiene il principio 6.2. della raccomandazione del Consiglio d'Europa. Per un approfondimento delle questioni esaminate nel testo cfr. i *memorandum* esplicativi allegati alla raccomandazione del Consiglio d'Europa e al codice dell'Ufficio internazionale del lavoro; nonché, Simitis, *Reconsidering*, cit., p. 1593 ss.; Aimo, *I "lavoratori di vetro"*, cit., p. 106 ss.; Chieco, *Privacy e lavoro*, cit., p. 91 ss.; Bellavista, *La disciplina della tutela dei dati personali e il rapporto di lavoro: due anni dopo*, in CNEL, *Diritto alla riservatezza e rapporto di lavoro*, Roma, 1999, p. 25 ss.

⁵⁴ Sulle quali cfr. Busia, *Restyling per la tutela dei dati personali*, in *Guida al diritto*, 2002, n. 5, p. 34 ss.; Bellavista, *Novità per la protezione dei dati personali*, in *Dir. prat. lav.*, 2002, n. 5, p. 318 ss.

delle raccomandazioni del Consiglio d'Europa indicate nell'articolo 1, comma 1, lettera b), della legge n. 676/1996". Il successivo comma 2, dell'art. 20 individua sette categorie di trattamenti di dati personali che dovrebbero essere disciplinate dai suddetti codici.

Una di queste tipologie di disciplina settoriale fa esplicito riferimento, nella lettera b), del comma 2, dell'art. 20 del decreto n. 467/2001, all'adozione di codici di deontologia e di buona condotta che riguardano il trattamento di dati personali "necessari per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di *curricula* contenenti dati personali anche sensibili". Beninteso, va osservato che la scelta della via del codice di deontologia e di buona condotta proprio nell'area del rapporto di lavoro va, a prima vista, senza dubbio apprezzata. Ciò perché il ricorso ai codici di deontologia e di buona condotta – che, come si vedrà tra poco, sono il frutto dell'autoregolamentazione delle categorie interessate, anche se realizzata con l'assistenza del Garante - può rappresentare una significativa modalità per introdurre regole plasmate sulle specifiche esigenze e sulle molteplici ipotesi di trattamento dei dati personali presenti nel settore dei rapporti di lavoro. E inoltre la partecipazione dei soggetti rappresentativi dei datori di lavoro (e, eventualmente, come si vedrà tra poco, dei lavoratori) alla redazione del codice dovrebbe lasciare presagire che le relative disposizioni siano effettivamente rispettate dai singoli operatori.

Tuttavia, va nuovamente ricordato che in base all'art. 1, comma 1, della legge delega n. 676/1996, il Governo ha avuto concesso il potere di emanare norme legislative volte a dettare una specifica regolamentazione del trattamento dei dati personali nell'area dei rapporti di lavoro. Tale delega è stata prorogata per ben due volte, e da ultimo è cessata il 31 dicembre 2001. Pertanto, in questo momento, la via dell'adozione del codice deontologico in questo settore presenta l'aspetto positivo che esso può costituire lo strumento per sperimentare regole e principi, da inserire successivamente in un vero e proprio testo legislativo. Ma è evidente come la mancata adozione della specifica legislazione di settore entro il termine di scadenza della delega rappresenta la perdita di un'utile occasione per il varo di una normativa la cui importanza è indubbia: e quindi, sotto questo profilo, la scelta legislativa del codice di condotta appare come un'opzione residuale e dell'ultima ora.

Peraltro, peculiare interesse presenta la questione della rilevanza giuridica di tali codici deontologici. Anzitutto, il comma 1 dell'art. 20, del d.lgs. n. 467/2001 dice che "il Garante promuove... la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati"; e ciò dovrebbe avvenire "ai sensi dell'art. 31, comma 1, lett. h), della legge n. 675/1996". Secondo quest'ultima disposizione, il Garante ha il compito di "promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto". E ora il comma 2, dell'art. 20 del d.lgs. n. 467/2001 stabilisce che "il rispetto delle disposizioni in essi contenute" – vale a dire proprio quelle presenti nei codici di deontologia e di buona condotta sottoscritti rispettando la procedura indicata dal comma 1 dell'art. 20 del medesimo decreto – "costituisce condizione essenziale per la liceità del trattamento dei dati".

Pertanto, grazie alla previsione normativa appena citata, se ci fosse un codice del genere il Garante potrebbe valutare la conformità alle sue prescrizioni del trattamento

operato nel settore di riferimento e, in caso di contrasto tra le regole del codice e il trattamento in atto, avrebbe il potere di emanare i provvedimenti di divieto o di blocco di cui alla lettera l) del comma 1, dell'art. 31 della legge n. 675/1996. Infatti, questi provvedimenti sono adottabili, come dice la nuova formula della disposizione, "se il trattamento risulta illecito o non corretto". Né va dimenticato che la violazione di tali provvedimenti del Garante è folgorata con la sanzione penale del riformato art. 37 della legge n. 675/1996. Se il codice risulta sottoscritto dal titolare del trattamento, che pone in essere le violazioni alle sue prescrizioni non dovrebbe porsi alcun problema circa la sua efficacia. Ma più complessa è la questione se il codice non è sottoscritto da costui oppure se la sua adesione al codice non possa essere desunta dall'adesione all'associazione che lo abbia sottoscritto. In questi casi, per fondare la rilevanza giuridica del codice, si può utilizzare lo stesso tipo di argomentazioni utilizzate nell'area della disciplina dello sciopero nei servizi pubblici essenziali (di cui alla legge n. 146/1990) per affermare l'efficacia generale dei contratti collettivi e dei codici di autoregolamentazione, che determinano le cosiddette prestazioni indispensabili, anche nei confronti dei soggetti non aderenti alle associazioni che li abbiano rispettivamente sottoscritti o adottati⁵⁵. In sostanza, si potrebbe sostenere che il soggetto che non aderisce al codice di deontologia e di buona condotta è obbligato comunque a rispettarlo, non perché questo strumento abbia diretta efficacia nei suoi confronti, ma perché rappresenta, grazie alla mediazione della valutazione del Garante, una specificazione dei precetti contenuti nella legge n. 675/1996 e quindi un fatto al cui verificarsi la legge attribuisce determinati effetti. Così, si può anche affermare che ad avere efficacia generale non è in sé il codice, ma il provvedimento con cui il Garante, ai sensi dell'art. 31, comma 1, lettera h) della legge n. 675/1996, abbia valutato la "conformità alle leggi e ai regolamenti" dello stesso codice. In questo modo, la predisposizione del codice sarebbe solo il frammento di un procedimento più ampio, che termina con il provvedimento del Garante, e che ha lo scopo di assicurare che le regole dettate per specifici settori trovino il preventivo consenso del numero più ampio dei soggetti ivi operanti. D'altra parte, se il Garante può emanare provvedimenti che concretizzano le regole generali della legge n. 675/1996 e che inevitabilmente hanno efficacia generale nei confronti di tutti i potenziali destinatari (cfr. gli artt. 22, commi 2 e 4, 23, comma 1, 24-bis, 28, comma 4, lettera g), 31, comma 1, lettera l), 41, comma 7), nulla esclude che la stessa efficacia abbiano i provvedimenti del Garante adottati recependo le indicazioni delle categorie interessate, come appunto nel caso dei codici di deontologia e di buona condotta. A favore di questa soluzione depone lo stesso testo legislativo, laddove al comma 4, dell'art. 20 del nuovo decreto, si dice che "i codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e riportati in allegato al testo unico delle disposizioni in materia previsto dall'articolo 1, comma 4, della legge 24 marzo 2001, n. 127". In effetti, già la pubblicazione sulla Gazzetta ufficiale può costituire un indice dell'efficacia generale del codice, ma va richiamata l'attenzione sul fatto che la suddetta pubblicazione avviene a cura del Garante. E, com'è avvenuto nel caso del codice per i trattamenti di dati personali per scopi storici – previsto dagli artt. 6 e 7 del d.lgs. n. 281/1999, che hanno una struttura analoga all'art. 20 del d.lgs. n. 467/2001 – il Garante ha disposto la pubblicazione del suddetto codice, con un proprio provvedimento con cui ha accertato la conformità del codice alle leggi e ai regolamenti.

⁵⁵ Cfr. Giugni, *Diritto sindacale*, Cacucci, Bari, 2001, p. 248 ss.

Beninteso, è evidente la necessità che il codice di deontologia e buona condotta abbia un'efficacia estesa a tutti i soggetti appartenenti alla categoria di riferimento, perché, se non fosse così, si avrebbe il paradosso di una differenziazione delle regole vigenti per lo stesso tipo di trattamento e i soggetti non aderenti al codice avrebbero l'indubbio vantaggio di potere operare con meno limiti di chi invece abbia deciso di aderire al codice. Ma se si concorda con l'idea che il codice di cui all'art. 20 del d.lgs. n. 467/2001 abbia efficacia generale, sorge l'esigenza di garantire che al processo di formazione dello stesso partecipino associazioni, enti e istituzioni ampiamente rappresentativi della categoria di riferimento: ciò avrebbe l'utile risultato di ridurre al minimo i casi di dissenso e di dare a tutti i soggetti interessati la ragionevole certezza che il codice non costituisca un'imposizione esterna, ma il frutto di un processo nel corso del quale, grazie alla presenza degli enti più rappresentativi della categoria, vi sia stata l'effettiva possibilità di tenere conto delle aspettative e delle istanze dei singoli operatori del settore.

Come s'è visto, nel sistema della legge n. 675/1996, il Garante ha un forte potere d'influenza sul procedimento di redazione del codice e quindi non dovrebbe sussistere il pericolo che le disposizioni in esso contenute siano alquanto labili, proprio perché l'autoregolamentazione delle categorie interessate (e cioè dei datori di lavoro) si dovrebbe svolgere con l'assistenza e sotto la sorveglianza del Garante. Anzi, non è escluso che il Garante, proprio facendo uso del suo potere d'influenza, possa persuadere gli esponenti della categoria datoriale dell'opportunità e della convenienza di avviare momenti di consultazione con le organizzazioni rappresentative dei lavoratori. In questo modo, si potrebbe arrivare al varo di un codice, formalmente frutto dell'autoregolamentazione dei soggetti datoriali che trattano dati relativi ai lavoratori, ma che in sostanza rappresenti il prodotto di una procedura partecipativa anche culminante in un vero e proprio accordo collettivo.

Orbene, va rimarcato che la scelta legislativa a favore dei codici deontologici, per l'area dei rapporti di lavoro, costituisce senza dubbio, nell'immediato, un ripiego provvisorio e, per il futuro, una soluzione residuale che non può fare dimenticare la necessità del varo di un quadro di regole legali sufficientemente dettagliate all'interno delle quali l'autoregolamentazione avrebbe per giunta maggiore efficacia⁵⁶. Purtroppo, la base giuridica per questo auspicabile intervento legislativo è venuta meno a seguito dello scadere della delega di cui all'art. 1, comma 1, della legge n. 127/2001 e non sembra rintracciabile nell'ulteriore delega contenuta nel comma 4, dell'art. 1 della stessa legge. Infatti, questa disposizione dice che "il Governo emana, entro dodici mesi dallo scadere del termine di cui al comma 12 – che era il 31 dicembre 2001 – "e previa acquisizione dei pareri previsti nel comma 2, da esprimersi entro sessanta giorni dalla richiesta, un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse, coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurarne la miglior attuazione". Come si vede, qui l'affidamento al Governo del potere legislativo è ben circoscritto, e non può essere inteso nel senso che il Governo abbia la facoltà di emanare discipline innovative – come sarebbero quelle di settore – rispetto alle disposizioni vigenti. E pertanto, per raggiungere l'obiettivo indicato bisogna aspettare un rinnovo della delega ovvero un diretto intervento del Parlamento.

11. Azione sindacale e contrattazione collettiva.

⁵⁶ Cfr., ampiamente, Simitis, *Il contesto giuridico e politico della tutela della privacy*, in *Riv. crit. dir. priv.*, 1997, p. 569 ss.

Stante che il progresso tecnologico influenza necessariamente le modalità dell'azione sindacale e della contrattazione collettiva, anche in Italia, da tempo ci si interroga sull'individuazione degli spazi per il soggetto collettivo per agire efficacemente a tutela dei diritti individuali, nell'area della raccolta e del trattamento dei dati personali dei lavoratori⁵⁷. Va chiaramente sottolineato che le tesi favorevoli ad assegnare un forte ruolo all'organizzazione dei lavoratori in questa materia e quindi volte ad ampliare l'ambito di applicabilità di disposizioni esistenti (come l'art. 4 St.lav.) o a suggerirne l'introduzione di nuove, non sembrano muoversi in controtendenza rispetto alle opinioni e alle tendenze diffuse anche al di fuori dei confini nazionali⁵⁸. Peraltro, sia la raccomandazione del Consiglio d'Europa sia il Codice di condotta dell'Ufficio internazionale del lavoro - che attualmente costituiscono i due modelli base per la costruzione di una disciplina specifica del trattamento dei dati personali dei lavoratori - depongono chiaramente verso la costruzione di momenti di forte partecipazione del soggetto collettivo alle scelte datoriali di introdurre e utilizzare strumenti per la raccolta e il trattamento dei dati personali dei lavoratori⁵⁹. Come si legge nella relazione che accompagna il Codice di condotta dell'Ufficio internazionale del lavoro "la protezione dei lavoratori nei confronti dei rischi provocati dal trattamento dei loro dati personali e la capacità di difenderne gli interessi con successo, dipende in misura decisiva dall'esistenza di diritti collettivi". La stessa esperienza italiana dimostra con nettezza che le forme di intervento più rilevanti sulle scelte aziendali di controllare con strumenti tecnici i dipendenti, sono state attuate nel settore dei rapporti di lavoro grazie all'azione del soggetto sindacale: infatti, grazie alla connessione tra gli artt. 4, 8 e 28 St.lav., il sindacato ha fatto ricorso all'azione per la repressione della condotta antisindacale per ricorrere al giudice nel caso di pericolose utilizzazioni (per i diritti individuali e collettivi) di apparecchiature informatiche. Peraltro, l'emersione di tecniche e di poteri di controllo collettivo sul trattamento dei dati personali sembra anche trovare adeguato sostegno sul piano del diritto positivo. Infatti, nulla sembra escludere la fondatezza della tesi secondo cui la procedura codeterminativa del comma 2 dell'art. 4 St.lav. vada estesa anche ad ogni attività di raccolta e trattamento dei dati personali dei lavoratori svolta per mezzo di apparecchiature informatiche (e non solo)⁶⁰. E quindi il soggetto collettivo avrebbe a disposizione un formidabile strumento per influenzare le scelte aziendali dirette all'introduzione di innovazioni e a escogitare forme di trattamento dei dati dei lavoratori.

Certo, non va trascurato che, in Italia (e non solo), a tutela del corretto trattamento dei dati personali, vigila l'organo pubblico di controllo istituito dalla legge n. 675/1996 e cioè il Garante per la protezione dei dati personali. E va anche detto che, in questi primi anni di attività, il Garante è più volte intervenuto, proprio nell'area dei rapporti di lavoro, proprio

⁵⁷ Cfr. Lassandari, *Diritti della persona nel contratto di lavoro: le fonti e gli attori*, in *Diritti della persona e contratto di lavoro*, cit., p. 133 ss.; Douglas Scotti, *Alcune osservazioni in merito alla tutela del lavoratore subordinato di fronte al trattamento informatico dei dati personali*, in *Dir. rel. ind.*, 1993, p. 237 ss.; Garilli, *Tutela della persona*, cit., p. 338 ss.

⁵⁸ Cfr. Simitis, *Reconsidering*, cit., p. 1600 s.; Däubler, *Internet und Arbeitsrecht*, cit.; CNIL, *La cybersurveillance sur les lieux de travail*, cit., p. 7 ss.

⁵⁹ Cfr. Simitis, *Verarbeitung von Arbeitnehmerdaten*, in *Computer und Recht*, 1991, p. 169 ss.

⁶⁰ Così Chieco, *Privacy e lavoro*, cit., p. 334; Aimo, I "lavoratori di vetro", cit., p. 132; Bellavista, *Società della sorveglianza e protezione dei dati personali*, in *Contratto e impresa*, 1996, p. 75 ss.

per fissare paletti e condizioni al trattamento dei dati personali dei lavoratori. Per giunta, il Garante ha dimostrato una particolare sensibilità nei confronti dell'esigenza di garantire il rispetto dei diritti scaturenti dalla legge n. 675/1996 anche sul luogo di lavoro⁶¹: e ciò fa sicuramente ben sperare per il futuro. Tuttavia, risultati molto più pregnanti sul piano dell'effettività potrebbero essere raggiunti se su tali tematiche si sviluppasse una appropriata strategia del movimento sindacale, anche caratterizzata da innovativi momenti di collaborazione con l'autorità pubblica di vigilanza. In effetti, solo l'organizzazione sindacale sarebbe in grado di radicarsi sul luogo di lavoro e di svolgere una costante attività a presidio dei diritti dei lavoratori coinvolti dai processi aziendali di trattamento delle informazioni personali.

D'altra parte, l'azione sindacale e contrattuale, quantomeno come obiettivo minimo, dovrebbe avere la possibilità di conformarsi alla struttura organizzativa della nuova impresa telematica. Significative indicazioni in questa direzione provengono dagli accordi collettivi relativi all'introduzione di forme di telelavoro o anche da esperienze sviluppate in contesti aziendali più tradizionali, laddove all'introduzione di modalità di comunicazione e di esercizio dei poteri datoriali in via telematica, corrisponde la correlativa attribuzione all'organizzazione sindacale di contrapposti poteri di "agibilità telematica" nonché di utilizzazione dei sistemi aziendali di comunicazione per raggiungere i lavoratori più dispersi e per cercare di sviluppare gli indispensabili presupposti per la formazione di identità collettive⁶². Pur in un contesto in cui il potere aziendale tende a delocalizzarsi e a rendersi meno afferrabile e individuabile, ma non certo meno intenso rispetto al passato, la stessa tecnologia è in grado di consentire lo sviluppo di inedite forme di contropotere collettivo e quindi canali relazionali basati sulla dimensione sindacale e sulla rigenerazione degli spazi di comunicazione e dei rapporti di solidarietà tra i lavoratori⁶³.

Tuttavia, ancora più importante è che l'attore collettivo cerchi di evitare di muoversi soltanto su un piano difensivo e *a posteriori* rispetto a decisioni già adottate. Qui si pone il problema di come si possa influenzare l'adozione delle tecniche raccolta e di trattamento dei dati personali dei lavoratori. A questo proposito, è necessario che si diffonda la consapevolezza che la scelta di una determinata tecnologia non è mai neutra rispetto ai conseguenti effetti che si producono sui soggetti che la utilizzano. In altri termini, per assicurare un'adeguata tutela ai diritti dei lavoratori, è imprescindibile che le modalità della

⁶¹ Cfr. la ricca ricerca di Trojsi, *Gli interventi del Garante per la protezione dei dati personali in materia di lavoro*, in *La tutela della privacy del lavoratore*, cit., p. 233 ss.

⁶² Cfr. Nogler, *Qualificazione e disciplina del telelavoro*, in *Subordinazione e autonomia: vecchi e nuovi modelli*, in *Quad. dir. lav. rel. ind.*, n. 21, 1998, p. 129 s.

⁶³ Cfr. Bronzini, *Dall'habeas corpus all'habeas mentem*, cit., p. 224.; Klebe-Wedde, *Gewerkschaftsrechte auch per E-Mail und Intranet?*, in *Arbeit und Recht*, 2000, p. 401 ss. A questo riguardo, s'è discusso s'è il diritto d'affissione di cui all'art. 25 St. lav. possa essere esercitato con modalità adeguate alla nuova realtà informatica, per esempio attraverso apposite "bacheche elettroniche": in senso favorevole cfr. P. Milano, 3 aprile 1995, in *Riv. it. dir. lav.*, 1995, II, p. 758; di diverso avviso pare T. Foggia, 10 luglio 2000, in *Not. giur. lav.*, 2000, p. 560. Analogo problema s'è posto in Germania riguardo all'interpretazione del § 40, del *BetrVG*, dando luogo a valutazioni contrastanti; ma la recente riforma del *Betriebsverfassungsgesetz* dovrebbe avere risolto la questione in senso positivo: cfr. Däubler, *Die veränderte Betriebsverfassung*, in *Arbeit und Recht*, 2001, p. 285.

protezione dei dati personali, oltre a basarsi su regole giuridiche, si sviluppino attraverso l'opzione per tecnologie "amiche della privacy", e cioè che siano plasmate in modo da limitare la possibilità di raccolta e di trattamento di dati personali allo stretto necessario e che quindi creino un ostacolo fisico ad ulteriori elaborazioni dei medesimi⁶⁴. Ciò non sembra presentare né difficoltà d'ordine pratico né di tipo economico. Semmai, l'organizzazione sindacale si dovrebbe rendere conto che la regolazione del trattamento delle informazioni personali non rappresenta un argomento sofisticato o di poco conto, bensì una condizione indispensabile per la garanzia degli spazi di libertà e della dignità della persona anche sul luogo di lavoro⁶⁵.

⁶⁴ Cfr. Simitis, *Il contesto giuridico e politico*, cit., p. 579 ss.; Id., *Datenschutz*, cit., p. 2478.

⁶⁵ Cfr. Däubler, *Arbeitnehmerdatenschutz*, cit., p. 112 s.; Rodotà, *Tecnologie e diritti*, cit., p. 105 ss.; Simitis, *Reconsidering*, cit., p. 1582 ss.; Aimo, *I "lavoratori di vetro"*, cit., p. 48 ss.