LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 1 / 2023

Alessandro Bellavista

Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori

Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori

Alessandro Bellavista

Sommario: 1. Premessa.- 2. La teoria della sopravvivenza dei controlli difensivi. – 3. Il Garante per la protezione dei dati personali e la sorveglianza elettronica.- 4. Il «decreto trasparenza» e l'utilizzo di sistemi decisionali e di monitoraggio automatizzati.- 5. Il principio del controllo umano e la valutazione d'impatto sulla protezione dei dati.

1.**Premessa**

Nella storia dell'umanità, i rapporti tra tecnologia e diritti della persona sono sempre stati controversi. Difatti, molto spesso le innovazioni tecnologiche hanno rappresentato una sorta di cavallo di Troia per rompere equilibri consolidati e per affermare la preminenza del potere che si avvaleva di queste[1]. In particolare, le nuove tecnologie hanno sempre offerto l'occasione per giustificare narrazioni ad uso e consumo di chi le possiede e le può utilizzare. In altri termini, l'argomento tecnologico è stato (e viene tuttora) usato per sostenere che tutto ciò che la tecnologia rende possibile sia ammissibile e che, anzi, non potrebbe essere limitato od ostacolato da posizioni differenti. Quanto sia devastante un ragionamento del genere lo si coglie chiaramente qualora si prendano in esame le moderne tecnologie riproduttive e genetiche. In questo modo, per esempio, al di là degli sconfinati problemi etici che emergono a tale proposito, il diritto non potrebbe porre alcun limite a nessuna forma di maternità surrogata oppure alla clonazione umana.

In realtà, le cose stanno diversamente. Il valore primario attribuito alla persona impone una risposta negativa alla domanda «se tutto quel che è tecnicamente possibile sia pure eticamente lecito, politicamente e socialmente accettabile, giuridicamente ammissibile»[2]. Il diritto del lavoro, come sistema di protezione del lavoratore nei confronti dei poteri predominanti del datore, non sarebbe nemmeno nato se non si fosse affermato un punto di vista contrapposto all'imperativo tecnologico: un punto di vista che appunto metteva, e mette tuttora, al centro l'esigenza della salvaguardia della persona che lavora. Si pensi alla questione della tutela della salute nei luoghi di lavoro. Le normative a protezione della salute e sicurezza dei lavoratori si sono evolute proprio allo scopo di

[1] Cfr. A. SUPIOT, *Homo Juridicus. Saggio sulla funzione antropologica del diritto*, Milano, 2006, 139 ss.

[2] S. RODOTA', *Discorso del Presidente*, Garante per la protezione dei dati personali, *Relazione per l'anno 1997*, Roma, 1998.

frenare tecnologie e forme di organizzazione del lavoro indifferenti al rispetto della persona del lavoratore (e di quella di qualunque cittadino) la quale invece gode della piena considerazione da parte dei moderni ordinamenti giuridici e delle relative Costituzioni.

Proprio per contrastare la deriva tecnologica molteplici fonti normative ormai affermano la natura di diritto fondamentale dello specifico diritto alla protezione dei dati personali, il quale comprende un complesso di posizioni soggettive atte a difendere la persona di fronte ai rischi derivanti dal trattamento dei suoi dati personali. Da ciò consegue che la paventata «asimmetria» tra esigenze di garanzia della persona e tecnologia può essere risolta, almeno in via tendenziale, imponendo alla seconda non solo barriere normative concernenti il suo utilizzo, ma anche modalità di costruzione e di funzionamento che attenuino o limitino allo stretto indispensabile i pericoli anzidetti. Per questo motivo si parla oggi di tecnologie *privacy friendly* che trovano espressione nei concetti giuridici di *privacy by design* e di *privacy by default*. Si tratta di principi che, di recente, sono stati consacrati nel Regolamento generale sulla protezione dei dati personali (cosiddetto RGPD). Sicché, i diritti della persona, tra cui oggi rientrano a pieno titolo anche il diritto alla *privacy* e alla protezione dei propri dati personali, assurgono al rango di diritti fondamentali sia nell'ordinamento nazionale sia in quello multilivello.

È acquisizione indiscussa che, in Italia, il trattamento dei dati personali nel rapporto di lavoro è governato dall'integrazione delle regole generali del RGPD con la disciplina speciale lavoristica rilevante in materia: e cioè, soprattutto, gli artt. 4 e 8 l. 20 maggio 1970, n. 300 (da ora St. lav.). Basti sottolineare che l'interazione tra la disciplina generale del trattamento dei dati personali e le disposizioni lavoristiche permette di aumentare il grado di tutela dei lavoratori nei confronti di ogni fase del trattamento delle informazioni che li concernono**.** In linea di massima, per un verso, le regole speciali lavoristiche incidono sulle regole generali. Infatti, quest'ultime sono da interpretare alla luce delle speciali norme lavoristiche, con l'effetto di mantenere, proprio nell'area dei rapporti di lavoro, l'operatività dei principi lavoristici che assumono portata più restrittiva rispetto a quelli della disciplina generale. Per altro verso, la normativa generale copre gli spazi non occupati dalle regole speciali del diritto del lavoro e quindi introduce garanzie da queste non previste: si pensi, per esempio, ai principi riguardanti le modalità del trattamento, ai molteplici diritti spettanti all'interessato nei confronti del titolare del trattamento, alle misure in materia di sicurezza del trattamento, alle forme di tutela gestite dal Garante per la protezione dei dati personali.

Un tema sempre più attuale, di fronte all'incessante sviluppo tecnologico, riguarda l'area di liceità delle forme di sorveglianza utilizzabili dal datore di lavoro. A questo riguardo viene, anzitutto, in rilievo, l'art. 4 St. lav. che regola l'uso di «impianti audiovisivi e altri strumenti di controllo sul luogo di lavoro»**.** La disposizione è stata

riformulata con i d.lgs. 14 settembre 2015 n. 151 e 24 settembre 2016, n. 185 (provvedimenti questi rientranti nelle riforme del cosiddetto *Jobs Act*), al precipuo scopo di adeguarla all'innovazione tecnologica.

2.**La teoria della sopravvivenza dei controlli difensivi**

L'avvento del nuovo testo dell'art. 4 St. lav., a seguito della novella del *Jobs Act*, ha incrementato il dibattito (invero mai sopito) circa gli spazi di legittimità del potere di controllo tecnologico (a distanza) del datore di lavoro sui comportamenti del lavoratore.

La questione principale (tra le tante)[3] concerne la sopravvivenza o meno dei cosiddetti «controlli difensivi» sotto il vigore del nuovo testo normativo. Più precisamente, ci si chiede se, ancora oggi, sia possibile ammettere controlli tecnologici, sui comportamento illeciti del lavoratore, che non rientrano nel perimetro applicativo dell'art. 4 St. lav.

Questo dubbio appare paradossale. In effetti, se si considera che la cosiddetta teoria dei controlli difensivi è stata elaborata dalla giurisprudenza sulla base del vecchio testo dell'art. 4 St. lav., una conclusione logica dovrebbe essere quella di ritenere che la novella non poteva non tenere conto di quella elaborazione, dei problemi e delle criticità da essa suscitati, nonché degli orientamenti giurisprudenziali in questa materia non sempre coerenti e univoci.

Ma tant'è. Al momento l'idea della sopravvivenza dei controlli difensivi ha trovato accoglimento in alcune corti di merito e finanche presso la Suprema Corte[4] che ha recepito le suggestioni di una parte della dottrina.

Tale approdo ermeneutico, per quanto finemente argomentato, conduce ad una disapplicazione, e perciò ad sostanziale abrogazione, di un enunciato normativo, facendo prevalere un illimitato e idiosincratico bilanciamento giudiziale nei confronti di quello prefigurato nel dettaglio dal legislatore; e, in ultima analisi, determinando la creazione di una vera e propria nuova norma del tutto antitetica rispetto a quella coniata dallo stesso legislatore.

Sicché, sulla base della rivitalizzata teoria dei controlli difensivi, la disapplicazione dell'art. 4 St. lav. comporta l'esenzione, da un lato, dalla procedura codeterminativa del c. 1 della disposizione; dall'altro, e soprattutto, dall'osservanza dell'obbligo, di cui al c. 3 del medesimo testo normativo, di informare preventivamente il lavoratore della possibilità di essere sottoposto al controllo a distanza.

[3] Cfr., ampiamente, A. INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Bari, 2018, 156 ss.; nonché, volendo, A. BELLAVISTA, *Privacy e rapporti di lavoro*, in *GDPR normativa privacy. Commentario*, a cura di G. M. RICCIO – G. SCORZA – E. BELISARIO, 2° ed., Milano, 2022, 905 ss.

[4] Cass. 22 settembre 2021, n. 25732; ID. 12 novembre 2021, n. 34092.

Questa posizione non è (per fortuna) unanime. In effetti, in altra parte della giurisprudenza di merito e di Cassazione[5], e nella dottrina prevalente, è diffusa la tesi secondo cui il cosiddetto controllo difensivo è assoggettato alla procedura codeterminativa del c. 1; e, comunque, va sempre osservato l'obbligo di informare preventivamente il lavoratore della possibilità del controllo. E se ciò non accadesse, i dati sarebbero illegittimamente raccolti e quindi inutilizzabili.

Orbene, va anzitutto osservato che la riedizione della teoria dei controlli difensivi, sotto il nuovo regime giuridico, appare presentare molteplici aporie logiche, che in pratica sono simili (se, *mutatis mutandis*, non del tutto analoghe) a quelle in cui incorreva la stessa teoria di fronte al vecchio testo dell'art. 4 St. lav. Questa disposizione, infatti, è onnicomprensiva: e cioè, essa, ieri come oggi, prende in considerazione il controllo a distanza (e cioè tramite strumenti tecnologici) sull'«attività dei lavoratori». E il concetto di «attività dei lavoratori» (che è diverso dall'espressione «attività lavorativa» contenuta negli artt. 2 e 3 St. lav.) è talmente ampio da abbracciare qualunque tipo di comportamento dei dipendenti: anche quello che si concreta in un illecito. Quindi, ogni forma di controllo tecnologico dovrebbe rientrare nel campo applicativo della disposizione.

D'altra parte, l'inserimento nel nuovo testo del c. 1, dell'art. 4 St. lav., quale presupposto giustificativo dell'installazione dell'apparecchiatura di controllo, della finalità di «tutela del patrimonio aziendale», è un chiaro indice della scelta del legislatore di ricondurre i controlli difensivi proprio nel campo di applicazione della suddetta parte dell'art. 4 St. lav. In effetti, ogni forma di comportamento illecito del lavoratore, comunque sia classificabile, è inesorabilmente diretto a ledere il patrimonio aziendale. E, ovviamente, se il controllo difensivo ricade nel perimetro dell'art. 4 St. lav., da ciò consegue che non si possa prescindere anche dall'ottemperare all'obbligo di preventiva informazione di cui al c. 3 del medesimo art. 4 St. lav.

Peraltro, nelle pronunce della Cassazione favorevoli alla sopravvivenza della teoria dei controlli difensivi è rintracciabile un uso non appropriato della giurisprudenza della Corte europea dei diritti dell'uomo sul rispetto della vita privata nei luoghi di lavoro. In pratica, quest'ultima giurisprudenza rappresenta, per la Cassazione, un argomento per giustificare la disapplicazione dell'art. 4 St. lav. e lasciare campo libero ad un imprevedibile e soggettivo bilanciamento giudiziale.

Questa soluzione è criticabile, poiché, com'è noto, secondo la Corte costituzionale, il dialogo tra le norme internazionali (della Convenzione europea dei diritti dell'uomo) e quelle interne dovrebbe portare ad un ampliamento delle tutele garantite al diritto fondamentale che viene in esame (che qui è il diritto al rispetto della vita privata nei luoghi di lavoro)[6]. Infatti, la Consulta afferma che «in materia di diritti

[5] Cass. 4 novembre 2021, n. 31778.
[6] Cfr. Corte cost. 30 novembre 2009, n. 317.

fondamentali, il rispetto degli obblighi internazionali non può mai essere causa di una diminuzione di tutela rispetto a quelle già predisposte dall'ordinamento interno, ma può e deve costituire strumento efficace di ampliamento della tutela stessa (sentenza n. 317 del 2009): vale, in altre parole, il principio della massima espansione delle tutele e della conseguente prevalenza della fonte che conferisce la protezione più intensa»[7]. Cosa questa che invece non si verifica seguendo il ragionamento della Cassazione. E, d'altronde, fino a tempi recenti, il richiamo della suddetta giurisprudenza della Corte di Strasburgo è stato sempre operato dalla prevalente dottrina italiana in funzione espansiva della tutela del lavoratore nei confronti della sorveglianza elettronica. Da quando, invece, la Corte europea dei diritti dell'uomo ha ammesso la legittimità di un controllo occulto, svolto attraverso la videosorveglianza[8], allora questo precedente, riguardante l'ordinamento spagnolo, è stato utilizzato per giustificare lo scardinamento dei limiti alla vigilanza elettronica posti dall'art. 4 St. lav.

3.**Il Garante per la protezione dei dati personali e la sorveglianza elettronica**

A ben vedere, la teoria dei controlli difensivi non trova alcun riscontro presso il Garante per la protezione dei dati personali. Infatti, questa Autorità, per un verso, tende a fare rientrare tutti gli strumenti di controllo nell'area di operatività della procedura codeterminativa di cui al c. 1 dell'art. 4 St. lav.: e quindi a configurare come eccezionale l'ipotesi di esenzione da siffatta procedura sancita dal successivo c. 2. Per altro verso, il medesimo Garante, proprio con riferimento al nuovo testo dell'art. 4 St. lav., ha ripetutamente sottolineato che «l'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali»[9].

Peraltro, i sostenitori della teoria dei controlli difensivi trascurano che, anche disapplicando *in toto* l'art. 4 St. lav., e quindi (non solo il dovere di informativa preventiva, ma) anche il riferimento, lì contenuto, all'obbligo di osservanza della disciplina della protezione dei dati personali, quest'ultimo obbligo risorge dalle ceneri per effetto del Codice

[7] Così, Corte cost. 9 luglio 2014, n. 223.

[8] Corte europea dei diritti dell'uomo, 17 ottobre 2019, Lòpez Ribalda *and Others v*. Spain.

[9] Garante per la protezione dei dati personali, provv. 13 maggio 2021, n. 9669974; ID., provv. 15 aprile 2021, n. 9670738.

della *privacy* e della diretta applicazione del già menzionato Regolamento generale sulla protezione dei dati personali (cosiddetto RGPD). E tale normativa concreta principi e regole assai dettagliati che vincolano fortemente la valutazione di legittimità della sorveglianza e che vanno ben al di là degli sfumati criteri indicati dalla Cassazione, nelle pronunce poc'anzi citate: criteri, e questo va rimarcato, tanto evanescenti da fare correre il rischio che la soluzione del caso concreto sfoci nel più ampio soggettivismo giudiziario.

Per giunta, il Garante per la protezione dei dati personali ha sottolineato la stretta connessione tra l'art. 88 RGPD e le già vigenti disposizioni lavoristiche in materia di trattamento dei dati personali nel rapporto di lavoro. Secondo il Garante, infatti, «il Codice» (cosiddetto della *privacy*: e cioè, il d.lgs. 30 giugno 2003, n. 276), «confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro (artt. 113 "Raccolta di dati e pertinenza", e 114 "Garanzie in materia di controllo a distanza")». E «per effetto di tale rinvio, e tenuto conto dell'art. 88, paragrafo 2, RGPD, l'osservanza degli artt. 4 e 8 St. lav. e dell'art. 10 d.lgs. n. 276/2003 (nei casi in cui ne ricorrono i presupposti) costituisce una condizione di liceità del trattamento». Sicché, «tali norme costituiscono nell'ordinamento interno quelle disposizioni più specifiche e di maggiore garanzia di cui all'art. 88 RGPD – a tal fine oggetto di specifica notifica del Garante alla Commissione, ai sensi dell'art. 88, paragrafo 3, RGPD – la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione…determina anche l'applicazione di sanzioni amministrative pecuniarie ai sensi dell'art. 83, paragrafo 5, lettera d), RGPD»[10].

E così, nell'ultima relazione del Garante, si legge che «l'Autorità è tornata sul tema dell'impiego degli strumenti tecnologici nei diversi contesti lavorativi, evidenziando il rapporto tra la disciplina di settore (l. n. 300/1970) e la disciplina di protezione dei dati, che, pur costituendo normative autonome, dotate ciascuna di un proprio apparato sanzionatorio, posto a tutela di beni giuridici distinti e complementari, sono comunque integrate attraverso richiami incrociati che regolano le condotte del datore di lavoro (artt. 113, 114 e 171 del Codice; v. anche art. 4, c. 3, l. n. 300/1970)». Pertanto, il Garante afferma, a chiare lettere, che «il mancato rispetto della predetta disciplina» (cioè, di quella speciale lavoristica) «può comportare l'applicazione di sanzioni amministrative pecuniarie (cfr. artt. 83, paragrafo 5, lettera d) e 88 RGPD, nonché art.

[10] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provv. 28 ottobre 2021, n. 9722661, e *ivi* sono menzionati i precedenti provvedimenti che affermano lo stesso principio.

114 del Codice, in riferimento all'art. 4, l. n. 300/1970), nonché può integrare la fattispecie di reato prevista dall'art. 171 del Codice»[11].

Di conseguenza, sarà molto probabile che i controlli difensivi «liberi» dall'art. 4 St. lav., ammessi dalla Cassazione e da una parte della dottrina, verranno invece folgorati, in vario modo, dal Garante. Il che ovviamente contribuirà all'aumento dell'incertezza del quadro giuridico e soprattutto ostacolerà le scelte delle imprese di implementazione degli strumenti tecnologici. E tutto questo assume contorni paradossali se si tiene conto del fatto che proprio una delle letture più ragionevoli della novella dell'art. 4 St. lav. è stata quella di ritenere che essa realizzasse la tanto auspicata integrazione tra la disciplina speciale lavoristica in materia di controlli sui lavoratori e la disciplina generale della *privacy*. Purtroppo, come s'è appena visto, la teoria della sopravvivenza dei controlli difensivi produce l'effetto contrario: non quello dell'integrazione del quadro normativo, bensì quello della sua polverizzazione e balcanizzazione.

4. **Il «decreto trasparenza» e l'utilizzo di sistemi decisionali e di monitoraggio automatizzati**

Di recente, è stato varato il d.lgs. 27 giugno 2022, n. 104, denominato «attuazione della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea». Il decreto (detto anche «decreto trasparenza» da parte degli addetti ai lavori) contiene alcune significative modifiche al d.lgs. 26 maggio 1997, n. 152 («attuazione della direttiva 91/533/CEE concernente l'obbligo del datore di lavoro di informare il lavoratore delle condizioni applicabili al contratto o al rapporto di lavoro»).

Anzitutto, nel d.lgs. n. 152/1997 è stato inserito l'art. 1-*bis* (intitolato «ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati»). Il c. 1 di tale disposizione prevede che «il datore di lavoro o il committente pubblico e privato», (tale normativa, in base al c. 7, si applica anche alle cosiddette collaborazioni autorganizzate e etero-organizzate), «è tenuto ad informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori»; e che «resta fermo quanto disposto dall'art. 4, l. n. 300/1970».

[11] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Relazione annuale 2021, Roma, 2022, 164 s.

Il successivo c. 2 aggiunge che «i fini dell'adempimento degli obblighi di cui al c. 1, il datore di lavoro o il committente è tenuto a fornire al lavoratore, unitamente alle informazioni di cui all'art. 1, prima dell'inizio dell'attività lavorativa, le seguenti ulteriori informazioni: a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi di cui al c. 1; b) gli scopi e le finalità dei sistemi di cui al c. 1; c) la logica ed il funzionamento dei sistemi di cui al c. 1; d) le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi di cui al c. 1, inclusi i meccanismi di valutazione delle prestazioni; e) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità; f) il livello di accuratezza, robustezza e cybersicurezza dei sistemi di cui al c. 1 e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse». E nel c. 5 si legge che «i lavoratori, almeno 24 ore prima, devono essere informati per iscritto di ogni modifica incidente sulle informazioni fornite ai sensi del c. 2 che comportino variazioni delle condizioni di svolgimento del lavoro».

Il c. 3 dell'enunciato sottolinea che «il lavoratore, direttamente o per il tramite delle rappresentanze sindacali aziendali o territoriali, ha diritto di accedere ai dati e di richiedere ulteriori informazioni concernenti gli obblighi di cui al c. 2»; e che «il datore di lavoro o il committente sono tenuti a trasmettere i dati richiesti e a rispondere per iscritto entro trenta giorni».

Di notevole importanza è il c. 4, per il quale «il datore di lavoro o il committente sono tenuti a integrare l'informativa con le istruzioni per il lavoratore in merito alla sicurezza dei dati e l'aggiornamento del registro dei trattamenti riguardanti l'attività di cui al c. 1, incluse le attività di sorveglianza e monitoraggio»; e che «al fine di verificare che gli strumenti utilizzati per lo svolgimento della prestazione lavorativa siano conformi alle disposizioni previste dal» RGPD, «il datore di lavoro o il committente effettuano un'analisi dei rischi e una valutazione d'impatto degli stessi trattamenti, procedendo a consultazione preventiva del Garante per la protezione dei dati personali ove sussistano i presupposti di cui all'art. 36 del» RGDP «medesimo».

Inoltre, il c. 6 della stessa disposizione stabilisce che «le informazioni e i dati di cui ai c. da 1 a 5 del presente articolo devono essere comunicati dal datore di lavoro o dal committente ai lavoratori in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico»; e che «la comunicazione delle medesime informazioni e dati deve essere effettuata anche alle rappresentanze sindacali aziendali ovvero alla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale. Il Ministero del lavoro e delle politiche sociali e

l'Ispettorato nazionale del lavoro possono richiedere la comunicazione delle medesime informazioni e dati e l'accesso agli stessi».

Come si vede questa nuova disciplina impone al datore di lavoro un ampio obbligo di informazione preventiva, a favore del lavoratore e delle organizzazioni sindacali, sulla gestione del rapporto di lavoro attraverso strumenti tecnologici e in particolare tramite sistemi decisionali automatizzati, governati da procedure algoritmiche, e meccanismi di sorveglianza elettronica. La violazione di tale obbligo è punita con apposite sanzioni amministrative. E peraltro, di fronte all'inottemperanza del suddetto obbligo, ad opera del datore di lavoro, al di là dell'applicazione della sanzione amministrativa, le organizzazioni sindacali potrebbero ovviamente anche agire mediante l'azione per la repressione della condotta antisindacale.

Per quanto l'interpretazione di questo nuovo blocco normativo possa presentare qualche non trascurabile difficoltà, è però evidente che esso contribuisce ad avvelenare i pochi pozzi disponibili per la teoria (della sopravvivenza) dei controlli difensivi. Ciò perché, come s'è visto, il decreto introduce un ampio obbligo di informazione preventiva, a carico del datore di lavoro, che tocca le varie forme di sorveglianza elettronica e i sistemi decisionali automatizzati. E, ovviamente, il suddetto diritto di informazione del lavoratore (e delle organizzazioni sindacali) va integrato con il più ampio ventaglio di diritti a favore del lavoratore/interessato garantiti dal RGPD e, in particolare, con quelli più specifici di cui all'art. 22 RGPD che scattano nel caso di processi decisionali automatizzati.

Inoltre, scaturiranno maggiori possibilità di un controllo, da parte dei lavoratori e dei loro rappresentanti, dell'esercizio del potere datoriale attraverso il cosiddetto «*management* algoritmico» (dominato dall'intelligenza artificiale) qualora fosse approvata la proposta (del 9 dicembre 2021) della Commissione europea di direttiva del Parlamento e del Consiglio «relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali». Ciò soprattutto se questa proposta di direttiva fosse perfezionata, in modo tale da allargare l'applicazione delle garanzie ivi previste in ordine al «*management* algoritmico» a tutti i lavoratori ad esso esposti e non solo a quelli delle piattaforme digitali. Comunque, va segnalato che questa proposta di direttiva ha rappresentato la fonte d'ispirazione per il legislatore che ha inserito le disposizioni poc'anzi esaminate nel nuovo «decreto trasparenza».

Da ultimo, estremamente interessante è la circolare del Ministero del lavoro del 20 settembre 2022, che si sofferma sulla nuova disciplina del «decreto trasparenza». Per ciò che concerne le questioni qui affrontate, secondo la circolare «dalla lettura della disposizione» (e cioè del nuovo art. 1-*bis*, d.lgs. n. 152/1997) possono individuarsi due distinte ipotesi che il decreto ha voluto regolare per gli aspetti informativi, qualora il datore di lavoro utilizzi sistemi decisionali o di monitoraggio automatizzati che siano: a) finalizzati a realizzare un procedimento decisionale in grado di incidere sul rapporto di lavoro; b) incidenti sulla

sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori».

Ad avviso della circolare, «premesso che il legislatore ha inteso occuparsi di strumenti tecnologici e modelli organizzativi in costante evoluzione, con particolare riferimento alla fattispecie *sub* a), sulla base delle conoscenze e delle esperienze attualmente disponibili, si può ritenere che per sistemi decisionali o di monitoraggio automatizzati si intendono quegli strumenti che, attraverso l'attività di raccolta dati ed elaborazione degli stessi effettuata tramite algoritmo, intelligenza artificiale, ecc., siano in grado di generare decisioni automatizzate». Di particolare rilievo è l'affermazione che «nell'ipotesi descritta, l'obbligo dell'informativa sussiste anche nel caso di intervento umano meramente accessorio». Sicché, «nella sostanza, il decreto legislativo richiede che il datore di lavoro proceda all'informativa quando la disciplina della vita lavorativa del dipendente, o suoi particolari aspetti rilevanti, siano interamente rimessi all'attività decisionale di sistemi automatizzati».

La circolare, così, precisa che «ad esempio, l'obbligo dell'informativa sussiste nelle seguenti ipotesi: 1) assunzione o conferimento dell'incarico tramite l'utilizzo di *chatbots* durante il colloquio, la profilazione automatizzata dei candidati, lo *screening* dei curricula, l'utilizzo di *software* per il riconoscimento emotivo e test psicoattitudinali, ecc.; 2) gestione o cessazione del rapporto di lavoro con assegnazione o revoca automatizzata di compiti, mansioni o turni, definizione dell'orario di lavoro, analisi di produttività, determinazione della retribuzione, promozioni, ecc., attraverso analisi statistiche, strumenti di *data analytics* o *machine learning*, rete neurali, *deep-learning*, ecc.».

La circolare sottolinea che «diversamente, non sarà necessario procedere all'informativa nel caso, ad esempio, di sistemi automatizzati deputati alla rilevazione delle presenze in ingresso e in uscita, cui non consegua un'attività interamente automatizzata finalizzata ad una decisione datoriale».

Poi nella circolare si legge che «discorso a parte merita, invece, la previsione *sub* b), riguardante "le indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori"». E che «anche in questa ipotesi il datore di lavoro ha l'obbligo di informare il lavoratore dell'utilizzo di tali sistemi automatizzati, quali, a puro titolo di esempio: *tablet*, dispositivi digitali e *wearables*, gps e geolocalizzatori, sistemi per il riconoscimento facciale, sistemi di *rating* e *ranking*, ecc.» Infine, la circolare precisa che «si deve ritenere che l'obbligo informativo introdotto dal citato art. 1-*bis* del d.lgs. n. 152/1997 trovi applicazione anche in relazione all'utilizzo di sistemi decisionali o di monitoraggio automatizzati integrati negli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, allorquando presentino le caratteristiche tecniche e le funzioni descritte in precedenza».

È evidente che il recente legislatore ha fatto un importante passo in avanti sulla via della tutela della *privacy* e dei diritti di autodeterminazione informativa dei lavoratori. Il che pone nuovi forti ostacoli a qualunque tentativo di legittimare forme occulte e indiscriminate di sorveglianza tecnologica.

Beninteso, il «decreto trasparenza» si muove nella direzione di introdurre nuovi diritti di informazione a favore dei lavoratori e dei loro rappresentanti. Ciò significa che lo spazio di legittimità delle forme di trattamento dei dati personali da esso considerate resta governato dalla speciale disciplina lavoristica applicabile in materia (infatti lo stesso «decreto trasparenza» richiama l'art. 4 St. lav.), nonché da tutte le altre regole vigenti sulla protezione dei dati personali.

Tra quest'ultime spicca l'art. 22 RGPD che pone forti limiti al «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione». Anzitutto, la disposizione consente tale specifico tipo di trattamento solo quando sia necessario; e, pertanto, non vi sia la possibilità di adottare altri metodi più rispettosi e meno invasivi della *privacy* dell'interessato. Peraltro, in considerazione dei particolari rischi che promanano da siffatto trattamento, una volta che esso sia stato ritenuto ammissibile, gli artt. 13 e 14 RGPD rafforzano gli ordinari diritti di informazione dell'interessato; e lo stesso art. 22 RGDP impone che «il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[12].

5.**Il principio del controllo umano e la valutazione d'impatto sulla protezione dei dati**

Un'ultima considerazione riguarda il principio del cosiddetto controllo umano che assume particolare rilievo di fronte all'espansione massiccia delle tecnologie digitali e, soprattutto, dei sistemi decisionali automatizzati. Per garantire l'effettività della tutela della persona, il principio del controllo umano va interpretato in senso ampio. E cioè, non è sufficiente che sia assicurato solo un mero diritto dell'interessato al riesame di una decisione automatizzata da parte di un funzionario dell'impresa datrice di lavoro, come avviene nella citata proposta di direttiva sul lavoro nelle piattaforme e nello stesso art. 22 RGPD. È altresì indispensabile che siano assicurate forme di controllo individuale e, soprattutto, collettivo sulle scelte manageriali di introdurre sistemi decisionali automatizzati. Il che potrebbe pienamente giustificare l'introduzione di veri e propri moderni diritti di codeterminazione in

[12] Cfr., ampiamente, le indicazioni del GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679,* 3 ottobre 2017 (con aggiornamento del 6 febbraio 2018).

questa materia. Ciò, per esempio, attraverso la previsione di procedure congiunte (svolte da rappresentanti del datore di lavoro e dei lavoratori) di validazione preventiva di tali sistemi nonché di monitoraggio continuo sul loro uso corretto.

S'è già accennato, peraltro, che il nuovo art. 1-*bis*, c. 4, d.lgs. n. 152/1997, impone una valutazione di impatto, alla stregua degli artt. 35 e 36 RGPD, sugli «strumenti utilizzati per lo svolgimento della prestazione lavorativa». E nell'ambito di questi rientrano, ovviamente, i sistemi decisionali e di monitoraggio automatizzati.

A questo proposito è necessario tenere conto delle «linee guida in materia di valutazione d'impatto» elaborate dal Gruppo di lavoro *ex* art. 29, che ha svolto la meritoria funzione di contribuire all'applicazione coerente negli stati membri della direttiva n. 95/46 e che, oggi, a seguito dell'entrata in vigore del RGPD, è stato sostituito dal Comitato europeo per la protezione dei dati (da ora CEPD). Nel periodo interlocutorio tra il varo del RGPD (2016) e la sua entrata in vigore (2018) il Gruppo di lavoro ha elaborato una serie di documenti per facilitare l'effettiva applicazione del RGPD. E il CEPD, all'atto del suo insediamento, ha fatto propria l'opera svolta dal Gruppo di lavoro.

In base alle suddette linee guida[13] «la valutazione d'impatto sulla protezione dei dati» (da ora anche DPIA) «è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali, valutando detti rischi e determinando le misure per affrontarli». Sicché, «le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento». Pertanto, in sintesi, la DPIA (che deve essere condotta prima di procedere al trattamento) è «un processo inteso a garantire e dimostrare la conformità» e quindi concreta il principio fondamentale di *accountability* su cui è imperniato il RGDP.

Come precisa il Gruppo di lavoro «in linea con l'approccio basato sul rischio adottato dal regolamento, non è obbligatorio condurre una DPIA per ciascun trattamento. Infatti, è necessario svolgere una DPIA soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1)». Ma «il semplice fatto che le condizioni che comportano l'obbligo di realizzare una DPIA non siano soddisfatte non diminuisce tuttavia l'obbligo

[13] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679*, adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017.

generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati». Di conseguenza, «in pratica, ciò significa che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento» integri il presupposto della DPIA e cioè «un rischio elevato per i diritti e le libertà delle persone fisiche».

Il Gruppo di lavoro, attraverso una lettura coordinata dell'art. 35 RGDP, con le altre disposizioni e i considerando del medesimo testo, ha elaborato ben nove criteri per individuare i trattamenti che richiedono una DPIA. E, in forza dell'interlocuzione con il CEPD prevista dal RGPD, il Garante italiano per la protezione dei dati personali ha predisposto, l'11 ottobre 2018, un elenco di dodici trattamenti soggetti alla DPIA. Tra questi rientrano alcuni pertinenti in modo specifico all'area dei rapporti di lavoro. Infatti, il Garante parla di «trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti»; di «trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso *app*, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato»; «trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato».

Di fatto, leggendo in modo integrato i criteri del Gruppo di lavoro e quelli del Garante, gran parte dei trattamenti svolti nell'ambito dei rapporti di lavoro risultano soggetti all'obbligo della DPIA. Il che, alla stregua dell'art. 36 RGPD, comporta il dovere del titolare di consultare il Garante se, come sottolinea il Gruppo di lavoro, egli «non è in grado di trovare misure sufficienti per ridurre i rischi ad un livello accettabile (ossia, i rischi residui restano comunque elevati)». E così il Garante potrà, in forza dell'art. 58 RGPD, prescrivere tutte le misure correttive per garantire la conformità del trattamento alle regole e ai principi del RGPD.

Importante è poi la previsione del paragrafo 9 dell'art. 35 RGPD, secondo cui, nell'ambito della DPIA, «se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti». E, a giudizio del Gruppo di lavoro, «tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto»; tra cui «una domanda posta ai rappresentanti del personale».

Come si vede, emerge in sostanza la necessità non solo del mero coinvolgimento delle organizzazioni dei lavoratori, ma anche dell'ottenimento della loro approvazione in merito al relativo trattamento, a garanzia per giunta dello stesso titolare. Infatti, il Gruppo di lavoro sottolinea che «qualora la decisione finale del titolare si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate»; e che «il titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò pregiudicherebbe la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile».

D'altra parte, il fatto che il Gruppo di lavoro parli del solo coinvolgimento dei rappresentanti del personale e non dei singoli lavoratori deriva dalla circostanza che, com'è noto, nell'area dei rapporti di lavoro, il consenso del singolo dipendente, a causa dell'endemica situazione di debolezza contrattuale in cui si trova quest'ultimo, non sarebbe mai liberamente prestato. E perciò, proprio in quest'ambito, il consenso del lavoratore non può, quasi mai, rappresentare un valido presupposto di legittimazione del trattamento dei dati personali del medesimo.

Lo stesso Gruppo di lavoro, nell'individuare i criteri, di cui s'è poc'anzi detto, utili a selezionare i trattamenti che richiedono una DPIA, fa riferimento ai «dati relativi a interessati vulnerabili (considerando n. 75)»: e cioè, «il trattamento di questo tipo di dati è un criterio» (che impone la DPIA) «a causa dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti». E per il Gruppo di lavoro «gli interessati vulnerabili possono includere…i dipendenti…e, ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento».