1. Protezione dati e tutela del lavoratore, dallo Statuto al Jobs Act

I quattro decreti attuativi della l. 183/2014, all'esame della Commissione, realizzano una rilevante riforma del diritto e delle politiche del lavoro, incidendo per vari aspetti sul diritto alla protezione dei dati personali.
E' significativo che la prima norma sulla riservatezza del nostro ordinamento nasca con lo Statuto dei lavoratori, in quell'articolo 4 che, sotto la rubrica "della libertà e dignità del lavoratore", ne sancisce l'intangibilità della sfera individuale, rispetto a controlli datoriali altrimenti pervasivi.
Nella sua applicazione ormai più che quarantennale, la norma si è dimostrata un fondamentale presidio di libertà del lavoratore rispetto al rischio di una sua totale espropriazione, magari anche con il consenso (inevitabilmente coartato) dell'interessato, in posizione troppo debole per opporvisi.
Ma ovviamente l'equilibrio complessivo di questa disciplina è stato reso possibile anche da un'interpretazione evolutiva, che ha adattato norme pensate per l'organizzazione fordista del lavoro alla realtà dell'internet delle cose, della sorveglianza di massa, del corpo elettronico.
Quest'esigenza di "sincronizzazione" della norma rispetto alla realtà odierna è anche alla base della delega di cui all'art. 1, comma 7, lett.f), l. 183, che demanda al Governo, sul punto, "la revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore". L'inciso "sugli impianti e sugli strumenti di lavoro" è stato aggiunto in seconda lettura, dal momento che il testo approvato dal Senato ampliava l'oggetto della delega alla revisione della disciplina "dei controlli a distanza".
La precisazione indurrebbe dunque a ritenere che l'oggetto della delega sia limitato alla (revisione della) disciplina dei controlli sui soli impianti e strumenti di lavoro, aventi ad oggetto essenzialmente la tutela del patrimonio aziendale, di esigenze organizzative e produttive e della sicurezza del lavoro.

2.La revisione della disciplina dei controlli a distanza in ambito lavorativo nell'AG 176

L'art. 23 dello schema di decreto sembrerebbe intervenire su un ambito più ampio. Le innovazioni principali apportate all'art. 4 dello Statuto sono:

a) abolizione del generale divieto (penalmente sanzionato) di utilizzo "di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", sebbene ovviamente le condizioni di legittimità dei controlli siano poi delimitate nei commi successivi;

b) espressa legittimazione dei controlli c.d. difensivi (per la tutela del patrimonio aziendale, che pure la giurisprudenza, sia pur con qualche limite, già ammetteva), la cui disciplina è ricondotta alla procedura generale concertativo-autorizzativa;

c) mutamento della procedura concertativa: tra le semplificazioni previste per la procedura concertativo-autorizzativa, si segnala l'esclusione dell'indicazione delle modalità di realizzazione dei controlli a distanza dal contenuto dell'autorizzazione amministrativa. Si sopprime inoltre la previsione della possibilità d'impugnazione della decisione autorizzativa, da parte delle rsa, dei sindacati o dello stesso datore. *Si dovrebbe tuttavia ritenere applicabile anche a questo atto autorizzativo la disciplina generale delle impugnazioni degli atti amministrativi*. La violazione delle regole sulla procedura concertativa radica responsabilità penale, ai sensi dell'art. 38 dello Statuto;

d) espressa esclusione, dalla procedura concertativo-autorizzativa, dei controlli realizzati mediante gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (es. computer, smartphone) e gli strumenti di registrazione degli accessi e delle presenze" (ad es. i badge).
Come precisato dallo stesso Ministro, tuttavia, i controlli realizzati mediante tali strumenti beneficiano dell'esonero dalla procedura autorizzativa solo nella misura in cui siano effettuati utilizzando le normali funzionalità degli apparecchi forniti in dotazione, appunto, per rendere la prestazione e non inserendo specifici sistemi modificativi dei dispositivi, finalizzati al controllo personale del lavoratore.
Non dovrebbe, dunque, avvalersi dell'esonero il datore di lavoro che intenda dotare di particolari software atti al monitoraggio del lavoratore i dispositivi (il pc o il telefono) forniti al dipendente per ragioni di servizio.
Nell'escludere l'applicazione della disciplina "del primo comma" a queste ipotesi, tuttavia, la norma prescinde non solo dalla procedura autorizzativa, ma anche da quei requisiti finalistici (funzionalità del controllo a esigenze produttive, organizzative ecc.) previsti dal primo comma per i controlli a distanza. Requisiti che concorrono indubbiamente a circoscrivere, sia pur in misura parziale, l'ambito dei monitoraggi datoriali.
Se quest'esclusione fosse imputabile a un mero errore di drafting (escludere non la sola procedura autorizzativa ma l'intero "comma primo"), sarebbe opportuno chiarirlo.
In assenza di questa precisazione, infatti, il solo requisito finalistico applicabile ai controlli in esame resta quello (alquanto ampio, come si dirà) del terzo comma, che legittima l'utilizzo dei dati così acquisti per "tutti i fini connessi al rapporto di lavoro";

e) i dati raccolti mediante i controlli suddetti (a distanza o "sugli strumenti di lavoro") possono essere utilizzati "a tutti i fini connessi al rapporto di lavoro", purché sia data al lavoratore "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto" dal Codice in materia di protezione dei dati personali di cui al d.lgs. 30 giugno 2003, n. 196 (*infra:* Codice).
La possibilità del controllo dell'adempimento della prestazione, mediante gli strumenti "di lavoro", diverrebbe in tal modo un "effetto naturale del contratto", in senso civilistico, in quanto finirebbe con il discendere naturalmente dalla costituzione del rapporto di lavoro. E' un'innovazione non irrilevante, soprattutto rispetto all'indirizzo giurisprudenziale che, ad esempio, ha escluso l'utilizzabilità dei dati ottenuti con controlli difensivi, per provare l'inadempimento contrattuale del lavoratore (es. Cass., 16622/2012).
Tale modifica costituisce uno sviluppo forse solo indiretto del criterio di delega, almeno formalmente non comprensivo anche della fase – successiva al controllo- dell'utilizzazione delle informazioni così ottenute, nell'esercizio di poteri datoriali (direttivo, disciplinare) diversi dal potere di controllo.

Si tratta, evidentemente, di un'estensione delle possibilità di utilizzo dei dati ottenuti con questi controlli indubbiamente notevole ma non certo illimitata.
Infatti, i principi di legittimità e determinatezza del fine perseguito con il trattamento, nonché della sua proporzionalità, correttezza e non eccedenza, non solo escludono l'ammissibilità di controlli massivi, ma impongono comunque una gradualità nell'ampiezza e tipologia del monitoraggio, che renda assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori.
Ad esempio- riprendendo la Raccomandazione del CdE dello scorso aprile – ove il datore di lavoro riscontrasse la presenza di virus sui pc aziendali, dovrebbe dotarli di sistemi di filtraggio/blocco dei siti a rischio e non procedere al monitoraggio dei siti visitati. Analogamente il Garante, in più occasioni, ha sancito in capo al datore di lavoro l'obbligo di individuazione preventiva della lista

dei siti considerati correlati alla prestazione lavorativa, nonché dell'adozione di filtri per il blocco dell'accesso a determinati siti o del download di alcuni file.
Con vari provvedimenti, abbiamo chiarito che non sono consentite, al datore di lavoro, la lettura e registrazione sistematica delle e-mail e delle pagine web visualizzate dal lavoratore, la lettura e registrazione dei caratteri inseriti tramite tastiere e dispositivi analoghi, nonché l'analisi occulta di computer portatili affidati in uso.
In questa prospettiva, assai utile può essere l'adozione di una soluzione di privacy-by-design, ovvero la progettazione degli stessi strumenti mediante i quali effettuare i controlli in modo da minimizzare, fino ad escludere, il rischio di controlli invasivi o comunque di incisive limitazioni della riservatezza di chi a quei controlli possa essere sottoposto. E' significativo che tali soluzioni siano valorizzate dalla Bozza di Regolamento Ue sulla protezione dati e dalla Raccomandazione del 1^ aprile del Consiglio d'Europa.
Ovviamente, ai sensi dell'art. 11, c.2 del Codice, la violazione della disciplina di realizzazione dei controlli datoriali renderà inutilizzabili i dati così raccolti.
Ma diversamente dalla violazione della procedura concertativa, l'infrazione di tale norma sui limiti di utilizzo dei dati dei lavoratori non radica autonoma responsabilità penale, a meno che non integri, ovviamente, un trattamento illecito di dati personali, pur con tutte le rigidità previste dall'art. 167 del Codice.
Si potrebbe invece riflettere sull'opportunità di estendere la sanzione penale (o anzi codificarne una autonoma, visto che quella di cui all'art. 38 è davvero lieve e di carattere contravvenzionale) alla violazione del comma III del nuovo art. 4, che riguarda le condizioni di liceità dell'utilizzo dei dati dei lavoratori così raccolti. Risiede, infatti, in questa norma uno dei possibili argini rispetto al rischio di una sorveglianza totale (e abusiva, strumentale o comunque eccessivamente invasiva) sul lavoratore da parte del datore.

In ordine al terzo comma e alle condizioni di legittimità dei controlli svolti mediante gli "strumenti di lavoro" e l'informativa da rendersi all'interessato e il rispetto delle norme del Codice, vanno chiariti alcuni aspetti.
Il requisito della previa informazione del lavoratore- incompatibile con ogni forma di controllo occulto- costituisce un'esplicitazione di quanto già desumibile dalla disciplina di protezione dati, come abbiamo chiarito in numerosi provvedimenti (Linee Guida per l'utilizzo della posta elettronica e di internet nell'ambito dell'attività lavorativa del 2007; provvedimenti 11 settembre e 9 ottobre 2014 su sistemi di localizzazione mediante smartphone).
Il principale argine a un utilizzo pervasivo dei controlli sul lavoro sarà nella conformità alle norme del Codice.
In questo senso molto utili saranno i principi generali che, in attuazione della direttiva 95/46/CE, sinora hanno consentito al Garante di adeguare la disciplina del 1970 (cui lo stesso Codice rinvia) a una realtà da allora così fortemente mutata. Essenziali, in particolare:
-il principio di necessità- secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- il principio di correttezza che deve informare il trattamento in ogni suo profilo;
- la necessaria determinatezza, legittimità ed esplicitazione del fine perseguito dal trattamento, che dovrebbe concorrere a un'interpretazione "adeguatrice" del terzo comma del nuovo articolo 4 ;
-i principi di pertinenza e non eccedenza dei dati trattati, che impongono una minimizzazione nel ricorso al trattamento dei dati personali secondo le effettive necessità e con le modalità meno invasive possibile;
- il divieto di profilazione;
- la necessaria legittimazione soggettiva al trattamento, che impone di limitare ai soli soggetti preposti l'autorizzazione allo svolgimento di attività di monitoraggio sul lavoro;

-il rinvio, di cui all'art. 113, al divieto, sancito dallo Statuto, di indagini "sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".
Tali principi hanno consentito al Garante di delineare un congruo bilanciamento tra tutela del lavoratore e legittime esigenze datoriali (anche ai fini dell'applicazione dell'istituto di cui all'art. 24, c.1, lett.g), del Codice, che costituisce una esimente del consenso), con numerosi provvedimenti prescrittivi spesso adottati in sede di verifica preliminare, segnatamente per lo svolgimento di controlli sull'impiego di strumenti tradizionali (tipo posta elettronica e internet) ovvero per l'implementazione – a fini produttivi – di sistemi di localizzazione geografica dei dipendenti.
Tali principi potrebbero essere valorizzati, in particolare, con l'adozione del Codice deontologico per la gestione del rapporto di lavoro di cui all'art. 111 del Codice, sinora inattuato, al fine di sancire alcune minime garanzie nell' applicazione dei controlli sul lavoro.
L'equilibrio che l'applicazione di tali principi fornirebbe nel rapporto tra esigenze produttive e dignità del lavoratore è, del resto, auspicato dalla Raccomandazione del Consiglio d'Europa, di aprile scorso, sulla protezione dei dati in ambito lavorativo, che in particolare auspica :
-la minimizzazione dei controlli difensivi o comunque rivolti agli strumenti elettronici;
-l'assoluta residualità dei controlli, con appositi sistemi informativi, sull'attività e il comportamento dei lavoratori in quanto tale;
-il tendenziale divieto di accesso alle comunicazioni elettroniche del dipendente;
-la residualità del ricorso ai sistemi biometrici e il divieto di utilizzo di dati genetici per la valutazione dell'attitudine professionale del dipendente, salvi ovviamente i casi previsti dalla legge per particolari circostanze.

3.L'informatizzazione delle politiche del lavoro

Sia l'AG 176, all'art. 17, sia l'AG 177, in materia di servizi per il lavoro, agli artt. 13 ss., attuano i criteri di delega volti da un lato alla telematizzazione degli adempimenti amministrativi funzionali alla gestione del rapporto di lavoro e, dall'altro, all'informatizzazione delle politiche del lavoro.
Di questi due indirizzi sono espressione, in particolare, i fascicoli elettronici dell'azienda e del lavoratore, istituiti rispettivamente dagli artt. 17 dell'AG 176 e 14 dell'AG 177, che consentiranno indubbiamente una migliore gestione delle politiche attive per il lavoro semplificando, altresì, diversi adempimenti amministrativi. Tuttavia, i dati contenuti in questi fascicoli e nei sistemi informativi che li alimentano devono essere adeguatamente protetti, al fine di scongiurare accessi abusivi lesivi tanto della riservatezza del lavoratore, quanto dell'interesse pubblico alla corretta gestione delle politiche del lavoro.
E' un punto importante: l'asimmetria che ha caratterizzato, sinora, il rapporto tra processo di informatizzazione delle pp.aa. e sicurezza dei dati personali detenuti dalle stesse è uno dei fattori principali della vulnerabilità dei nostri sistemi informativi, come ha documentato una ricerca dell'Università La Sapienza. E' dunque essenziale che le banche dati di nuova costituzione e anche soltanto la loro interconnessione siano realizzate nel rispetto dei requisiti di sicurezza previsti dal Codice e che, per quanto possibile, la loro vulnerabilità sia contrastata riducendo "la superficie d'attacco". In questo senso, ogniqualvolta le finalità (ad es. di monitoraggio dell'efficacia delle politiche occupazionali) siano ugualmente perseguibili anche con **dati anonimi**, dovrebbe evitarsi l'utilizzo di dati identificativi: circostanza che non sembra, invece, adeguatamente prevista per i flussi informativi disciplinati dagli artt. 13 ss. dell'AG 177.
In particolare, andrebbe adeguatamente valutata l'opportunità di consentire **lo scambio reciproco** - tra Miur e Anpal[1] e in base a una mera convenzione tra i due enti- di dati individuali (oltre ai relativi risultati statistici) per mere finalità di monitoraggio degli esiti occupazionali dei giovani in uscita da

[1] Agenzia nazionale per le politiche attive del lavoro

percorsi di istruzione e formazione (art. 13, c.6). Nella sua formulazione attuale, la norma non impone il ricorso a dati anonimi (ancorché, appunto, individuali e non aggregati), che sarebbe invece opportuno prescrivere almeno qualora non si documenti l'indispensabilità dell'utilizzo di dati identificativi.

Analoga previsione andrebbe inserita all'art. 14, c.3, relativamente all'accesso per fini statistici e di monitoraggio delle politiche attive e passive del lavoro, da parte del Ministero del lavoro, al **sistema informativo unico delle politiche del lavoro**, istituito presso l'Anpal dall'art. 13. Tale previsione è tanto più necessaria in ragione della particolare estensione di questo sistema informativo, costituito: dal sistema informativo dei percettori di ammortizzatori sociali, dall'archivio informatizzato delle comunicazioni obbligatorie, dai dati relativi alla gestione dei servizi per l'impiego e delle politiche attive per il lavoro e dal sistema informativo della formazione professionale. Si tratta, peraltro, di un sistema la cui consultabilità andrebbe, almeno in certa misura, limitata o quantomeno precisata con criteri soggettivi di accesso proporzionali alle effettive esigenze perseguite di volta in volta. Nella formulazione proposta, infatti, si prevede espressamente (e genericamente) che le informazioni del sistema informativo unico per le politiche del lavoro costituiscano il "**patrimonio informativo comune**", per lo svolgimento dei rispettivi fini istituzionali, del Ministero del lavoro, dell'Anpal, dell'Isfol[2], dell'Inps, dell'Inail, delle regioni e province autonome, nonché dei centri per l'impiego.

In ragione della diversità, appunto, delle finalità istituzionali perseguite da ciascuno di questi enti, sarebbe opportuno disciplinare specificamente (anche con fonte subordinata, allo stato tuttavia non prevista, su cui il Garante sarà sentito ex art. 154) l'ambito oggettivo di accesso di ciascuno, precisando anche le modalità di realizzazione di questo flusso informativo. Una migliore precisazione meriterebbe poi la categoria degli "altri soggetti interessati" alla lettura dei dati contenuti nel sistema informativo unico delle politiche del lavoro, cui l'Anpal può consentire l'accesso ai sensi dell'art. 13, comma 5, sia pur "nel rispetto del diritto alla protezione dei dati personali" (inciso sicuramente doveroso ma probabilmente non interamente risolutivo).

Analoga precisazione meriterebbero poi le condizioni e i limiti che incontrano il Ministero e l'Isfol nell'accesso, per fini di "monitoraggio e valutazione", a "tutti i dati gestionali trattati dall'Anpal" e, rispettivamente, al **sistema informativo unico delle politiche del lavoro** (art. 16, c.2).

I dati censiti nel nuovo sistema costituiscono poi l'oggetto del **fascicolo elettronico del lavoratore,** istituito dall'art. 14 e "liberamente accessibile", on line, da parte dei "singoli soggetti interessati". Anche tale norma andrebbe perfezionata, al fine di chiarire meglio i criteri di legittimazione soggettiva (e oggettiva) all'accesso, ovvero chi effettivamente possa consultare quelle informazioni (alcune verosimilmente anche di carattere sensibile), con quale grado di "invasività" (ad es. limitando l'accesso ai dati identificativi ai soli casi nei quali essi siano indispensabili) e con quali garanzie per la sicurezza dei dati e dei sistemi stessi. Ulteriori cautele potrebbero poi essere precisate in sede di normativa di attuazione (che sarebbe opportuno prevedere), rispetto alla quale il Garante potrebbe fornire un contributo in sede di parere. Una particolare attenzione ai profili di sicurezza dei flussi informativi andrebbe poi riservata nella tipula delle convenzioni previste tra le amministrazioni interessate e "altri soggetti del Sistan al fine di integrare le banche dati" in possesso del Ministero del lavoro, dell'Anpal, dell'Isfol, dell'Inps e dell'Inail (art. 14, c. 6).

Una consultazione del Garante sarebbe necessaria anche rispetto alla definizione, da parte dell'Anpal, delle procedure per il conferimento, da parte delle regioni e province autonome, dei dati sulla formazione del lavoratore da inserirsi nel fascicolo elettronico (art. 15, c.1). Una più puntuale disciplina meriterebbe poi il **sistema informativo della formazione professionale**, istituito dall'art. 15, gestito dell'Anpal per essere messo a disposizione delle regioni e comprensivo dell'albo nazionale degli enti di formazione e dei "dati individuali relativi alle attività formative avviate e ai soggetti coinvolti".

[2] Istituto per lo Sviluppo della Formazione Professionale dei Lavoratori

L'articolo 16 disciplina le attività dell'ANPAL, del Ministero del lavoro e delle politiche sociali e dell'ISFOL concernenti il monitoraggio e la valutazione sulla gestione delle politiche attive per il lavoro, sui servizi per l'impiego e sui risultati conseguiti dai soggetti, pubblici e privati, accreditati a svolgere tali funzioni. Il comma 4 prevede, allo scopo di assicurare una valutazione indipendente delle politiche per il lavoro, l'allestimento, da parte dell'ANPAL, di banche dati informatizzate anonime, alle quali abbiano accesso determinati soggetti a fini di ricerca.
Un ulteriore miglioramento è auspicabile poi per l'art. 17 dell'AG 176, che tra l'altro costituisce, presso la Banca dati delle politiche attive e passive (già istituita dal d.l. 76/2013), **il fascicolo elettronico dell'azienda** -contenente tutte le informazioni sui datori di lavoro ricavabili dalle comunicazioni obbligatorie – e che rileva ai nostri fini solo in quanto concerna imprenditori individuali, dal momento che le persone giuridiche non sono più soggetti di diritto ai fini privacy. Il miglioramento auspicato concerne tuttavia il conferimento alla banca dati, da parte dei soggetti tenuti ad alimentarla, dei dati relativi, tra gli altri, ai collaboratori e ai lavoratori autonomi, agli studenti e ai cittadini stranieri soggiornanti in Italia per ragioni di lavoro. Dal momento che tali dati possono anche rivestire natura sensibile, oltre a una più puntuale regolamentazione di questo flusso informativo, sarebbe opportuno acquisire il parere del Garante sul decreto attuativo che dovrà, ai sensi del comma 2 del citato art. 17, disciplinare i soggetti legittimati a inserire, aggiornare e consultare le suddette informazioni, nonché le relative modalità.
Il comma terzo dello stesso articolo, invece – che "esonera" le amministrazioni interessate dall'obbligo di comunicare al Garante il trattamento in questione, ai sensi dell'art. 39 del Codice– sembra poi ultronea, dal momento che la procedura di cui all'art. 39 (comma 1, lett.a) è necessaria nei casi nei quali il trattamento non abbia copertura normativa; circostanza che, evidentemente, non ricorre nella fattispecie.
Il Garante potrà poi fornire un contributo in sede di parere sul decreto attuativo dell'art. 8 dell'AG 176, relativo alla costituzione, all'interno della Banca dati delle politiche attive e passive, della **Banca dati del collocamento mirato** (riservato ai lavoratori disabili), al fine di assicurare garanzie adeguate ai dati sensibili che saranno così trattati.
Importante sarà poi il rispetto delle norme del Codice nell'attuazione delle norme (artt. 20-21) dello stesso AG 176 sulla telematizzazione delle comunicazioni in materia di **malattie professionali e infortuni sul lavoro**. La doverosa semplificazione e riduzione dei tempi delle procedure deve, infatti, essere circondata di altrettante garanzie nella protezione di dati sensibili (e, per parte datoriale, spesso anche giudiziari), come il Garante ha in più occasioni avuto modo di sottolineare, proprio rispetto a un settore del diritto del lavoro così importante.