Il potere di controllo elettronico del datore di lavoro e la *privacy* del lavoratore

di *Francesco Buffa*

Due sentenze del 2018 della Corte Edu riscrivono le linee fondamentali di protezione del lavoratore dal controllo elettronico datoriale, riconoscendo una sfera inderogabile di protezione della vita privata anche sul luogo di lavoro.

1. Legittimità dei controlli difensivi e dei controlli elettronici in presenza di *policy* aziendale

Fino allo scorso anno, nel panorama nazionale italiano giurisprudenziale, il potere di controllo elettronico del datore di lavoro aveva un riconoscimento ampio, sia in ragione del carattere difensivo del controllo, ossia del suo orientamento a dimostrare un illecito posto in essere dal lavoratore, sia, per altro verso, in presenza di *policy* aziendale recante espresso riferimento alle modalità e ai limiti del controllo.

Sotto il primo profilo, la stessa nozione di "controllo difensivo" è stata progressivamente allargata, fino a ricomprendere forme di accertamento di fatti penalmente indifferenti e rilevanti solo sul piano disciplinare, o in relazione alla mera difesa dell'immagine aziendale o, addirittura, al corretto adempimento della prestazione lavorativa.

Sotto il secondo profilo, si è ammesso il potere datoriale unilaterale di disciplina dell'uso delle risorse elettroniche in azienda, e si è subordinata la legittimità dei controlli al mero avviso preventivo al lavoratore circa il potere datoriale relativo.

Le obiezioni di chi richiamava le esigenze di protezione della *privacy* del lavoratore nel luogo di lavoro venivano, in sostanza, superate attraverso la valorizzazione della *policy* aziendale quale strumento da rendere noto preventivamente al lavoratore e con il quale si poteva legittimamente prevedere il controllo datoriale, senza che il lavoratore potesse poi invocare alcuna "aspettativa di *privacy*".

È questa la linea seguita dallo stesso legislatore italiano, nell'ambito del *Jobs Act*, nel d.lgs n. 151/2015, che ha novellato secondo i principi ora richiamati l'art. 4 dello Statuto dei lavoratori.

A tale quadro si è, poi, aggiunta la sentenza della Corte Edu *Barbulescu c. Romania* (ric. n. 61496/08), del 12 gennaio 2016: nel caso, caratterizzato da un divieto espresso di uso dei *computer* aziendali per scopi personali, contenuto in un regolamento interno reso noto ai dipendenti, la Corte aveva ritenuto legittimo il monitoraggio fatto dal datore sulle comunicazioni elettroniche (nella specie, tramite il programma «Messenger») del lavoratore, e legittimo altresì il successivo licenziamento del lavoratore per il solo fatto della violazione della *policy* aziendale.

In quell'occasione, la decisione ha suscitato le critiche veementi di un giudice dissenziente che, configurato l'accesso a *internet* quale diritto umano, ha sottolineato la protezione delle comunicazioni *internet* del lavoratore in varie fonti del diritto internazionale e ha evidenziato che la *policy* aziendale non può rilevare se «*poorly drafted*», ossia se non prevede e salvaguarda una serie di tutele in favore del lavoratore, ferma restando in ogni caso la necessità della verifica della proporzionalità della sanzione irrogata dal datore – all'esito del controllo delle comunicazioni del lavoratore – rispetto al fatto ascritto.

2. Il nuovo indirizzo: la sentenza *Barbulescu c. Romania* della Grande Chambre

Il 5 settembre 2017, la Grande Camera della Corte Edu, a seguito di *referral* del ricorrente, è tornata sul tema, pervenendo a maggioranza a una soluzione del

tutto diversa dal proprio specifico precedente.

La sentenza ha riscritto le linee fondamentali di protezione del lavoratore dal controllo elettronico datoriale, stabilendo alcuni principi fondamentali:

- l'applicabilità della protezione della *privacy* anche nel caso in cui il datore di lavoro abbia approvato una specifica *policy* recante espresso divieto di uso delle *e-mail* aziendali per scopi personali;
- l'affermazione dell'obbligo dello Stato, pur in presenza di un ampio margine di apprezzamento, di assicurare che siano predisposte misure protettive contro eventuali abusi da parte del datore di lavoro;
- l'affermazione che la *compliance* degli Stati con l'obbligazione positiva di protezione della *privacy* dei lavoratori è assicurata da vari fattori, tra i quali rilevano, in particolare, la previa informativa datoriale circa la facoltà di monitoraggio delle *e-mail*, la portata e l'estensione del controllo, la giustificazione dello stesso, la configurabilità di misure alternative meno invasive, la gravità delle conseguenze del controllo, la previsione di garanzie in favore del dipendente. Tutti questi fattori, infatti, incidono sull'equo contemperamento degli interessi confliggenti, che gli Stati devono assicurare a garanzia della protezione del diritto di cui all'art. 8 della Convenzione.

La sentenza è importante non solo per il cambio di rotta rispetto al precedente specifico, non solo in quanto si ritiene essenziale la predisposizione di una *policy* aziendale in difetto della quale nessun controllo datoriale appare legittimo (il relativo principio era già stato affermato dalla stessa Corte nella sentenza *Copland c. Regno Unito* del 2007, su ricorso n. 62617/2000), ma perché si indica analiticamente quale debba essere il contenuto della *policy* e quali tutele spettino, in ogni caso, al lavoratore.

In tal senso, degni di nota sono, in particolare, i parr. 121 e 122 della sentenza, ove si elenca una sorta di decalogo che la *policy* aziendale deve rispettare a tutela del lavoratore, le cui garanzie devono necessariamente essere protette dalle autorità nazionali, pena l'illegittimità del controllo datoriale; si deve così verificare:

«(i) se il dipendente sia stato preventivamente informato della possibilità che il datore di lavoro controlli la corrispondenza e altre comunicazioni e dell'attuazione di tali misure;

(ii) quale sia l'estensione del controllo da parte del datore di lavoro e il grado di intrusione nella *privacy* del dipendente, distinguendo in proposito tra il monitoraggio del flusso delle comunicazioni e quello del loro contenuto, nonché il carattere totale o parziale dei dati monitorati, la durata nel tempo del monitoraggio, il numero di persone che hanno avuto accesso ai risultati, l'esistenza o l'assenza di limiti spaziali del monitoraggio;

(iii) se il datore di lavoro abbia fornito motivazioni legittime per giustificare il monitoraggio delle comunicazioni e l'accesso ai loro contenuti effettivi; posto che il monitoraggio del contenuto delle comunicazioni è, per sua natura, un metodo decisamente più invasivo, esso richiede una giustificazione più ampia;

(iv) se fosse stato possibile istituire un sistema di monitoraggio basato su metodi e misure meno intrusivi che non accedere direttamente al contenuto delle comunicazioni del dipendente, e se dunque l'obiettivo perseguito dal datore di lavoro avesse potuto essere raggiunto senza accedere direttamente all'intero contenuto delle comunicazioni del dipendente;

(v) quali siano le conseguenze del monitoraggio per il lavoratore subordinato e quale sia l'uso fatto dal datore di lavoro dei risultati dell'operazione di monitoraggio; in particolare, se tale uso sia conforme con lo scopo perseguito e dichiarato, e se sia necessario in relazione allo stesso;

(vi) se siano state predisposte adeguate misure di salvaguardia in favore del lavoratore, in particolare quando le attività di controllo del datore di lavoro siano di natura intrusiva, prevedendosi ad esempio che il datore di lavoro non possa accedere al contenuto effettivo delle comunicazioni, a meno che il lavoratore non sia stato avvisato in anticipo di tale eventualità».

Infine, si prevede il dovere, per le autorità nazionali, di assicurare che un dipendente la cui comunicazione sia stata monitorata abbia accesso a un rimedio davanti a un organo giudiziario competente a determinare, almeno in sostanza, come siano stati osservati i criteri predetti e la legittimità delle misure contestate.

Non si tratta, perciò, solo – bisogna sottolinearlo con forza – di prevedere una *policy* dal contenuto ampia, con l'indicazione delle garanzie del lavoro sopra indicate, ma di assicurare concretamente strumenti operativi con i quali rendere effettive quelle garanzie.

La sentenza *Barbulescu* 2 (che, sebbene resa verso altro Paese, reca i consueti effetti delle sentenze di Strasburgo nei confronti degli ordinamenti degli altri Paesi) rende dunque operanti direttamente all'interno del rapporto di lavoro tutte le garanzie che la disciplina della *privacy*, in genere, prevede nel trattamento dei dati personali e ha dunque un contenuto fortemente progressivo per le tutele del lavoro che vengono in tal modo a essere consacrate: infatti, a seguito della sentenza ora citata, forme di tutela necessariamente laburistiche si impongono, e in via aggiuntiva rispetto alle classiche tutele di matrice penalistica, di tutela della *privacy* o civilistica nell'ambito della *tort law*.

Dopo la *Barbulescu* 2, non sembra allora potersi più dubitare che i detti limiti oggi valgano non solo ai fini del trattamento lecito dei dati personali (e dell'eventuale risarcimento danni che compete all'interessato in caso di violazione, sulla base della legge sulla *privacy*), ma anche ai fini della legittimità del controllo datoriale per ogni aspetto rilevante nell'ambito del rapporto di lavoro (ad esempio, a fini di valutazione del lavoratore o a fini disciplinari), sicché le previsioni di *policy* aziendali, codici disciplinari e norme contrattuali possono assumere rilievo solo nei limiti evidenziati, dovendo invece, in ogni caso, essere assicurati in favore del lavoratore strumenti di tutela (e quell'ampia gamma di strumenti sopra indicati) verso i controlli a distanza, pur preterintenzionali, posti in essere dal datore di lavoro.

3. Altre sentenze della Corte Edu in materia di controllo e di videosorveglianza

Qualche mese dopo, la sezione V della Corte Edu è tornata sull'argomento nella sentenza *Libert c. Francia*, ric. n. 588/13, 22 febbraio 2018, in un caso di licenziamento per l'utilizzo di *computer* da lavoro per immagazzinare grandi volumi di materiale pornografico. I giudici avevano rigettato l'impugnativa del licenziamento in ragione dell'assenza di una chiara demarcazione dei *file* in questione come documenti privati.

Adita *ex* art. 8 Cedu, la Corte ha ravvisato nella specie una «interferenza da parte di un'autorità pubblica»: a differenza del caso *Barbulescu* - in cui l'interferenza è stata effettuata da un datore di lavoro strettamente privato -, il ricorso è stato analizzato dall'angolo non degli obblighi positivi dello Stato, ma dei suoi obblighi negativi, come dovere di non ingerirsi nella vita privata del dipendente. In tale ambito, la questione se i *file* fossero stati chiaramente identificati come personali è stata esaminata nel quadro della verifica della proporzionalità dell'ingerenza, ravvisandosi la legittimità della misura.

In materia di videosorveglianza, la V sezione della Corte si era pronunciata nel caso *Köpke c. Germany*, ric. n. 420/07, 5 ottobre 2010, caratterizzato dalla videoregistrazione senza preavviso della condotta del lavoratore sul posto di lavoro al fine di controllo avverso furti in un supermercato.

Come osservato dai tribunali tedeschi, la videosorveglianza del ricorrente era stata effettuata solo dopo che le perdite erano state rilevate durante l'inventario e le irregolarità scoperte nei conti del dipartimento in cui lavorava, sollevando un discutibile sospetto di furto commesso dal richiedente e da un altro dipendente, che sono stati gli unici dipendenti a essere presi di mira dalla misura di sorveglianza. La misura era stata limitata nel tempo (due settimane) e riguardava solo l'area circostante la cassa e accessibile al pubblico. I dati visivi ottenuti, elaborati da un numero limitato di persone che lavoravano per l'agenzia investigativa e dai membri del personale del datore di lavoro, erano stati usati solo in connessione con la cessazione del rapporto di lavoro e il procedimento dinanzi ai tribunali del lavoro. L'interferenza con la vita privata del richiedente si era, quindi, limitata a ciò che era stato necessario per raggiungere gli scopi perseguiti dalla videosorveglianza. I tribunali nazionali hanno, inoltre, ritenuto che l'interesse del datore di lavoro nella protezione dei suoi diritti di proprietà potesse essere efficacemente salvaguardato solo raccogliendo prove al fine di provare la condotta criminale del ricorrente nei procedimenti giudiziari.

La Corte aveva ritenuto che non c'era nulla che indicasse che le autorità nazionali non avevano raggiunto un giusto equilibrio, nel loro margine di apprezzamento, tra il diritto del richiedente al rispetto della sua vita privata e l'interesse del suo datore di lavoro alla tutela dei suoi diritti di proprietà.

La materia della videosorveglianza è stata, poi, rielaborata con le sentenze *Antović e Mirković c. Montenegro* e *López Ribalda c. Spagna*.

Con la sentenza *Antović e Mirković c. Montenegro*, ric. n. 70838/13, 18 novembre 2017, la Corte aveva già chiarito che la mera circostanza che la prestazione lavorativa (l'insegnamento) avesse svolgimento in luogo pubblico non valeva ad escludere l'ambito applicativo dell'art. 8 della Convenzione.

Nella specie, due professori universitari lamentavano che costituisse un'indebita violazione del loro diritto alla *privacy* la decisione assunta dall'Università del Montenegro di installare videocamere di sorveglianza nelle aule d'insegnamento, all'asserito scopo di proteggere l'incolumità delle persone e il patrimonio dell'Università. Le corti domestiche rigettavano le domande risarcitorie, affermato il principio che non può porsi un problema di tutela della vita privata in relazione a condotte poste in essere in luogo pubblico.

La Corte Edu, pronunciandosi sul ricorso, ha ampliato i limiti dell'ambito applicativo dell'art. 8 Cedu: a giudizio dalla Corte, infatti, anche quando il luogo di lavoro è pubblico o aperto/esposto al pubblico, l'aspettativa di protezione del diritto alla *privacy* del lavoratore non svanisce per ciò solo.

La decisione, nel ritenere l'ingerenza statale sproporzionata, ha ritenuto che le dichiarate finalità protettive dell'incolumità pubblica e del patrimonio dell'ente non fossero di rilevanza tale da poter bilanciare le misure restrittive adottate dall'Università, in quanto quest'ultima avrebbe ben potuto impiegare ulteriori differenti mezzi a disposizione, meno invasivi, ma ugualmente idonei ad assicurare il perseguimento di detti scopi.

4. I limiti della videosorveglianza secondo la sentenza *López Ribalda c. Spagna*

Con la sentenza *López Ribalda c. Spagna*, ricc. nn. 1874/13 e 8567/13, 9 gennaio 2018, la Corte è poi tornata sul tema della protezione del diritto alla *privacy* nel contesto dei controlli a distanza del lavoratore (anche qui, un caso di videosorveglianza segreta da parte del datore di lavoro sui cassieri di un supermercato, dopo che erano sorti sospetti di furto).

Nella vicenda, alla registrazione dei filmati era seguito il licenziamento delle lavoratrici accusate degli illeciti, il quale era stato basato principalmente sul materiale video raccolto. I tribunali interni avevano ritenuto giustificato il controllo difensivo.

La Corte europea, adita *ex* art. 8 Cedu, ha dapprima osservato che il Governo spagnolo aveva sostenuto che lo Stato non era responsabile in quanto, nel caso di specie, gli atti controversi erano stati eseguiti da una società privata. Tuttavia, la Corte ha ribadito l'obbligo positivo, per i Paesi, di adottare misure per garantire il rispetto della vita privata; di conseguenza, ha dovuto esaminare se lo Stato avesse raggiunto un giusto equilibrio tra i diritti dei ricorrenti e quelli del datore di lavoro: l'art. 8 Cedu, infatti, impone allo Stato non solo l'obbligazione negativa di impedire ogni arbitraria intromissione nella vita privata da parte della pubblica autorità, bensì anche l'obbligazione positiva di adottare ogni misura necessaria a garantire il rispetto della vita privata nelle relazioni intersoggettive orizzontali. Secondo la legge spagnola, le persone dovevano essere chiaramente informate sul trattamento dei dati personali e inoltre il monitoraggio aveva coinvolto tutti i dipendenti per diverse settimane, durante tutte le ore di lavoro. La Corte Edu ha rilevato quindi che, nel caso di specie, l'attività di "sorveglianza occulta" si è risolta in una misura di controllo diretta a colpire indistintamente l'intero *staff* impiegato presso il punto vendita, da ritenersi per questo sproporzionata rispetto al fine (in sé legittimo) di tutelare l'interesse organizzativo-patrimoniale del datore di lavoro. Pertanto, la Corte ha ritenuto che lo Stato convenuto, omettendo di sanzionare tale sproporzione tra strumento restrittivo e scopo perseguito, abbia fallito il giudizio di bilanciamento imposto dall'art. 8, par. 2, Cedu.

Con la sentenza *López Ribalda*, la Corte ha così ulteriormente chiarito i confini del perimetro applicativo dell'art. 8 Cedu, precisando che il concetto di «vita privata» ben può includere anche attività di natura professionale, che abbiano svolgimento sul luogo di lavoro.

Viene, in tal modo, affermato in modo chiaro (sebbene allo stato non definitivo, posto che la questione è stata oggetto di *referral* alla Grande Camera, che si pronuncerà nell'anno in corso), anche nella materia della videosorveglianza nei posti di lavoro, che il lavoratore, per il solo fatto di trovarsi all'interno dei locali aziendali o impegnato nell'utilizzazione di beni strumentali aziendali, non è privato del diritto a una sfera di protezione della sua vita privata.