Il pensiero della CEDU sul controllo delle email

1.Controlli sulle email aziendali. Il caso Bărbulescu.

Quando i controlli del datore di lavoro sulla posta elettronica aziendale del dipendente sono legittimi?

È questo, in sintesi, il grande dubbio che attanaglia i datori di lavoro e che impegna, in un vorticoso ondeggiamento giurisprudenziale, le Corti italiane ed europee nella ricerca del delicato equilibrio tra diritto del datore di lavoro di tutelare il patrimonio aziendale e diritto alla riservatezza dei lavoratori.

Emblematico, a tal riguardo, è il caso *Bărbulescu.*

La vicenda trae origine da un ricorso contro il governo rumeno depositato presso la Corte Europea dei Diritti dell'Uomo-CEDU, nel 2008, da un cittadino rumeno, il signor *Bogdan Mihai Bărbulescu*, il quale ha lamentato che la decisione del datore di lavoro di risolvere il suo contratto era basata su una violazione del suo diritto al rispetto della vita privata e della corrispondenza sanciti dall'articolo 8 della Convenzione europea dei diritti dell'uomo[1] (la sua domanda era stata rigettata sia in primo che in secondo grado in Romania). Bărbulescu era stato impiegato da un'impresa privata come ingegnere incaricato delle vendite e, su richiesta del datore di lavoro, aveva creato un *account Yahoo Messenger* per rispondere alle richieste dei clienti. Il 3 luglio del 2007, l'impresa aveva fatto circolare un avviso tra gli impiegati comunicando che l'uso di internet, telefono e fotocopiatrice per ragioni private poteva costituire una causa di licenziamento per ragioni disciplinari.

Dieci giorni dopo il signor Bărbulescu, accusato di aver usato *Yahoo Messenger* per ragioni personali - comunicazioni con il fratello e la fidanzata – veniva licenziato. Il licenziamento era stato quindi comminato a valle della contestazione circa l'utilizzo di strumenti di lavoro – l'*account* di messaggistica istantanea, Internet e telefono - per finalità non lavorative.

2. Le vicende processuali dinanzi alla CEDU

Due i gradi del giudizio dinanzi alla Corte Europea dei diritti dell'uomo (CEDU), diversi gli esiti, fondamentale la differenza tra i due provvedimenti che, essenzialmente, si attesta sulla modalità - *id est* pervasività - del controllo eseguito dal datore di lavoro.

1) Sentenza *Bărbulescu* – 2016: la Camera semplice della CEDU, con la sentenza del 12 gennaio 2016, n. 61496/08 ha ritenuto che sì vi fosse stata una violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo (diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza), ma che il controllo del datore di lavoro delle sue comunicazioni nell'ambito di un procedimento disciplinare risultava legittimo. Ciò in quanto la giustizia romena aveva raggiunto un buon equilibrio tra il diritto alla privacy del dipendente e gli interessi del suo datore di lavoro, ritenendo che «*non è irragionevole che un datore di lavoro voglia verificare che i dipendenti portino a termine i propri incarichi durante l'orario di lavoro*».

A gennaio del 2016, il Garante per la Protezione dei dati personali italiano[2], alla domanda se la sentenza della Corte europea dei diritti umani sancisse la fine della privacy in ambito lavorativo, aveva risposto "*assolutamente no*", affermando che: "*…la Corte si è limitata a ritenere non irragionevole il bilanciamento tra privacy dei dipendenti ed esigenze datoriali, affermato dalla giurisdizione romena. E questo perché:*

a) *l'azienda **aveva informato i dipendenti** delle condizioni d'uso della mail aziendale, che non ne consentivano l'utilizzo per fini personali. Ragione, questa, che avrebbe quindi ridotto l'aspettativa di riservatezza riposta dai lavoratori rispetto alle loro comunicazioni via e-mail;*
b) *il monitoraggio delle mail **è stato limitato nel tempo e nell'oggetto**, nonché strettamente proporzionato allo scopo di provare l'inadempimento contrattuale del lavoratore (desunto da altri elementi), la cui scarsa produttività aveva determinato e legittimato il licenziamento;*
c) ***l'accesso alle e-mail del lavoratore da parte datoriale è stato legittimo** proprio perché fondato sul presupposto della natura professionale del contenuto delle comunicazioni (come da contratto avrebbe dovuto essere)…».*

---

[1] Art. 8 Diritto al rispetto della vita privata e familiare.

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

[2] Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali ("L'Huffington Post", 13 gennaio 2016).

In sostanza, posta l'esistenza di adeguata informazione al dipendente sulla modalità d'uso degli strumenti aziendali, il controllo sulle email e le sue modalità era stato ritenuto correttamente eseguito (si legge che l'accesso alla messaggeria *Yahoo* aziendale da parte del datore di lavoro era stato effettuato nella convinzione che contenesse solo comunicazioni professionali e che il contenuto delle comunicazioni private non è stato utilizzato dai tribunali per legittimare il licenziamento).

Di più, si era ritenuto all'epoca che la valutazione dei giudici di Strasburgo fosse in linea con la giurisprudenza italiana e con gli stessi principi affermati dal Garante privacy, in particolare con le *Linee Guida per posta elettronica ed Internet* del 1 marzo 2007, principi che restano validi anche dopo la riforma dei controlli datoriali operata dal Jobs Act[3].

Poi il cambio di rotta.

2) **Sentenza *Bărbulescu* – 2017**: detta modalità di controllo è stata totalmente "riletta" dalla **Grande Camera della CEDU, decisione 5 settembre 2017**, la quale, riformando la precedente sentenza, ha riaffermato la violazione del citato articolo 8, ovvero il diritto al rispetto della vita privata e familiare, perché il dipendente non era stato avvertito in anticipo della possibilità che le proprie comunicazioni potessero essere sorvegliate, né della durata di tale controllo, posto che il datore di lavoro avrebbe "*registrato tutte le comunicazioni del richiedente [ndr. del sig. Bărbulescu] durante il periodo di monitoraggio in tempo reale, accedendo e stampando il loro contenuto*[4]".

La sentenza di secondo grado non solo ritiene essenziale la predisposizione di una policy aziendale – come già aveva deciso quella di primo grado - indicando analiticamente quale debba essere il contenuto della stessa, ma sottolinea l'importanza della modalità con cui viene eseguita la verifica, affermando in particolare l'importanza dell'**estensione del** controllo da parte del datore di lavoro e il grado di intrusione nella privacy del dipendente e quindi il *"monitoraggio del flusso delle comunicazioni e 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".* In tal senso, degno di nota è il punto 121 della sentenza, ove appunto si elencano i requisiti che la policy aziendale dovrebbe contenere a tutela del lavoratore, le cui garanzie devono necessariamente essere protette dalle autorità nazionali, pena l'illegittimità del controllo datoriale[5].

Il punto essenziale è ora, secondo la Grande Camera, che il datore di lavoro deve descrivere preventivamente la portata e la natura delle attività di monitoraggio e la possibilità che possa avere accesso al contenuto effettivo dei messaggi personali del dipendente.

Ci si concentra quindi sulla modalità del controllo e la "profondità" dello stesso.

Ciò potrebbe ritenersi in linea con l'ordinamento italiano, ove il Garante privacy ha in più occasioni (nelle Linee Guida per posta elettronica ed Internet del 1 marzo 2007 e poi in vari provvedimenti dal 2006 ad oggi) ribadito la necessità, da parte del datore di lavoro, di predisporre una policy che disciplini modalità di utilizzo,

---

[3] "*...Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196*».

[4] Paragrafo 134 della sentenza della Grande Camera della CEDU

[5] Punto 121 della sentenza: «*La Corte è consapevole dei rapidi sviluppi in questo settore. Tuttavia, essa ritiene che la proporzionalità e procedurali garanzie contro l'arbitrarietà sono essenziali. In questo contesto, le autorità nazionali dovrebbero trattare i seguenti fattori come rilevanti: (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 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 natura un metodo chiaramente più invasivo, 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 l'uso da parte del 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*».

divieti e controlli degli strumenti di lavoro[6]. Quanto detto anche in accordo con quanto prescritto al comma 3 della nuova formulazione dell'art. 4 dello Statuto dei Lavoratori, a proposito dell'utilizzabilità a tutti i fini connessi al rapporto di lavoro delle informazioni raccolte dal datore mediante i controlli[7].

Su tale aspetto si potrebbe quindi dire che le Linee guida del Garante privacy italiano del lontano 2007 sono quanto mai attuali, atteso che già prevedevano all'art. 6.1 che "…*deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale. Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati".*

3.Regolamento Europeo in materia di protezione dei dati personali 2016/679 - GDPR

In questo contesto, l'evoluzione tecnologica abbinata al costante cambiamento del mercato del lavoro ha imposto una costante "corsa" del legislatore e della giurisprudenza al fine di garantire il delicatissimo equilibrio tra privacy del lavoratore e controlli datoriali. Il tutto, tenendo a mente che il nuovo Regolamento Europeo 2016/679 – *General Data Protection Regulation – GDPR*, è ispirato ad una maggiore trasparenza nella gestione dei dati e finalizzato a dare un maggiore controllo ai cittadini sull'utilizzo dei propri dati personali.

Se il GDPR lascia un ampio margine di apprezzamento agli Stati Membri consentendo agli ordinamenti nazionali di prevedere forme di tutela diverse[8], dall'altro lato il *Working Party ex art. 29*[9] ha emesso l'*Opinion 2/2017 ,* nella quale è stato evidenziato che, nei controlli da parte del datore di lavoro, il principio da rispettare è quello per cui ogni dipendente, indipendentemente dal tipo di contratto a lui applicato, ha diritto al rispetto della vita privata, della sua libertà e dignità. In sintesi:

- ogni lavoratore deve essere adeguatamente informato sulle modalità di trattamento dei dati personali in maniera chiara, semplice ed esaustiva, soprattutto qualora siano previste forme di controllo del lavoratore, che comunque dovranno essere rispettose anche delle norme nazionali;
- ogni trattamento deve essere proporzionato alla finalità perseguita e deve essere limitato quanto più possibile l'uso dei dati personali;

---

[6] Il datore di lavoro deve indicare in modo chiaro quali sono le corrette modalità di utilizzo degli strumenti messi a disposizione del lavoratore (posta elettronica e internet) e se ed in che misura e con quali modalità vengono effettuati dei controlli (punto 3.1. del provvedimento). Ciò tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

[7] "*Dunque, anche dopo il Jobs Act, i controlli datoriali devono comunque essere improntati a gradualità nell'ampiezza e nella tipologia con assoluta residualità dei controlli più invasivi, legittimati solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori.*

E così, ad esempio, 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. E non sono comunque 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 « (Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali ("L'Huffington Post", 13 gennaio 2016).

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

[9] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

- devono essere adottate appropriate misure tecniche ed organizzative per garantire la sicurezza del trattamento dei dati.

Con riferimento all'interesse legittimo del datore di lavoro, il *Working Party ex art. 29* ricorda di valutare preventivamente se il trattamento da porre in essere sia necessario e proporzionato per il perseguimento di una finalità legittima, redigendo in caso una valutazione d'impatto, ossia un *Data Protection Impact Assessment-DPIA* ai sensi dell'art. 35 del GDPR.

In particolare, l'*Opinion* ammette che il trattamento dei dati dei lavoratori, relativo all'utilizzo della loro strumentazione informatica (mail, cronologia delle ricerche, telefonate ecc.), rappresenti la più grande minaccia alla loro sicurezza, incoraggiando perciò l'adozione di soluzioni che limitino l'accesso indiscriminato ai dati, sia per tipologia sia per orizzonte temporale.

Conclusioni

Dopo la sentenza *Bărbulescu* della Grande Camera della CEDU e alla luce degli orientamenti del *Working Party ex art. 29*, non sembra potersi dubitare che i limiti ivi evidenziati siano sostanziali 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, norme contrattuali possono assumere rilievo solo entro i suddetti limiti. Il diritto del lavoratore alla riservatezza permane ma va contemperato con il diritto del datore di lavoro di tutelare il patrimonio aziendale. Il controllo sarà possibile ma solo quando: l'accertamento venga effettuato *a posteriori* (ossia quando siano emersi elementi tali da giustificare un'indagine retrospettiva e non preventiva), il lavoratore abbia preventivamente ottenuto un'adeguata informazione sulle modalità d'uso degli strumenti tecnologici e quando i controlli, le cui modalità vanno chiaramente esplicitiate nella policy, siano avvenuti rispettando i principi di pertinenza, non eccedenza e minimizzazione dei dati.

Avv. Francesca Gravili – Avv. Imma Ciarletta

Studio Associato Servizi Professionali Integrati
Fieldfisher Global