ASSOCIAZIONE ITALIANA
DEI COSTITUZIONALISTI

OSSERVATORIO COSTITUZIONALE
Fasc. 3/2016
22 novembre 2016

Il "*cyberslacking*" e i diritti del lavoratore "catturato nella rete informatica". Note critiche a margine della sentenza della Corte Europea dei diritti dell'uomo, sez. IV, 12 gennaio 2016, n. 61496, *Bărbulescu* vs. Romania, in attesa della pronuncia della Grande Camera•

di **Alessandra Ingrao** – *Assegnista di ricerca in Diritto del Lavoro, Università degli Studi di Milano*

ABSTRACT: In the Barbulescu vs. Romania case, the European Court of Human Rights stated that the employee shall not oppose against the employer his/her right to confidentiality with respect to electronic communications when the latter, in the company's internal policy, prohibited the use of electronic devices for personal purposes. The author censures the judgment because it did not give enough weight to transparency as a value, on which the modern privacy right is based. For this reason the court distanced itself from all acts adopted by the European Union and by the Council of Europe.

1. *Introduzione.*

La sentenza in commento affronta un tema di grande attualità che riguarda il bilanciamento tra il diritto del lavoratore a mantenere riservate le comunicazioni elettroniche, inviate dal proprio *account* aziendale, e il potere del datore di lavoro a controllare che il prestatore non si renda inadempiente utilizzando le risorse elettroniche dell'azienda. Sin dalla sua pubblicazione la pronuncia ha sollevato un grande clamore nel dibattito giuridico[1] ed in quello istituzionale[2], culminato con la recente rimessione della decisione alla Grande Camera[3].

• Lavoro sottoposto a referaggio in base alle Linee guida della Rivista.

[1] A. SITZIA, D. PIZZONIA, *Il controllo del datore di lavoro su internet e posta elettronica: quale riservatezza sul luogo di lavoro?,*in *Nuova giur. civ.*, 2016, 6, 899 ss.; A. LOMBARDI, *Il potere di controllo del datore di lavoro alla luce della giurisprudenza CEDU. Riflessioni a margine della sentenza Bărbulescu*, in *L'effettività dei diritti alla luce della giurisprudenza della Corte europea dei diritti dell'uomo di Strasburgo*, Ricerca del Dipartimento di Diritto pubblico dell'Università di Perugia.

[2] Cfr. A. SORO, Presidente del Garante per la Protezione dei dati personali, *I lavoratori devono essere informati. Il datore di lavoro non può spiare le mail*, pubblicato su l'*Huffington Post*, 13 gennaio 2016.

[3] La Grande Camera della Corte Edu ha dichiarato ammissibile l'istanza di rinvio e ha fissato l'udienza di discussione alla data dell'11 novembre 2016. Il fatto che il Collegio dei cinque giudici abbia sporadicamente dichiarato ammissibili le domande di rinvio, sul punto v. B. RANDAZZO, *Giustizia costituzionale sovranazionale, La Corte europea dei diritti dell'uomo,* Giuffrè, Milano, 2012, 74, fa ritenere con probabilità che la decisione verrà ribaltata dalla Grande Camera.

Non si può negare che l'avvento delle tecnologie sui luoghi di lavoro abbia generato nuove forme di minaccia alla produttività. L'utilizzo improprio, in orario di lavoro, del computer collegato in rete è un fenomeno sempre più diffuso presso quella classe di lavoratori che svolge mansioni d'ufficio. L'uso per fini non lavorativi delle risorse telematiche aziendali nella scienza economica dell'organizzazione è denominato *cyberslacking* o *cyberloafing*[4] e annovera al suo interno una gamma di attività *online*, che spaziano dall'utilizzo della connessione per socializzare, per svolgere commissioni personali e, talvolta, anche per realizzare comportamenti indecenti. I lavoratori "catturati nella rete informatica" attuano condotte che oltre a costituire forme di devianza produttiva, perché distraggono tempo ed efficienza al lavoro, comportano dei costi per l'impresa, imputabili all'attività illecita svolta in rete, che può compromettere la sicurezza dei sistemi informatici e la funzionalità della banda.

Per contrastare questi comportamenti, la maggior parte dei datori di lavoro adotta regolamenti interni per disciplinare l'uso degli strumenti informatici e della rete internet, talvolta vietandone l'utilizzo, talvolta consentendone un limitato uso per finalità non lavorative.

Nonostante la diffusione di norme proprie dell'organizzazione, il datore di lavoro, proprietario delle risorse informatiche, conserva un interesse a verificare che tipo di utilizzo facciano i lavoratori dei *devices* tecnologici loro assegnati, anche al fine di suffragare, con prove,una eventuale contestazione disciplinare.

L'ordinamento italiano soddisfa questa esigenza attribuendo al datore di lavoro un vero e proprio potere di controllare a distanza l'attività del dipendente (art. 4 St. lav.), che non è, tuttavia, privo di limiti. Il principale è rappresentato dal diritto alla *privacy* del lavoratore, tutelato a livello nazionale, europeo ed internazionale, oggetto della sentenza in commento.

2. *Il fatto, i giudizi della magistratura rumena e la decisione della Corte EDU.*

Il caso riguarda la vicenda di un ingegnere rumeno, responsabile delle vendite presso una società privata. Il dipendente aveva creato, su richiesta del datore di lavoro, un account Yahoo Messenger[5], per gestire i contatti per le vendite. A seguito di controlli sulla cronologia delle *chat*, effettuati dal datore in un limitato lasso temporale (dal 5 al 13 luglio 2007), era emerso che il ricorrente aveva utilizzato, durante l'orario di lavoro, l'account aziendale per *chattare* con la fidanzata ed il fratello, su questioni relative alla sua vita sessuale ed al suo stato di salute.

La contestazione disciplinare, supportata da copioso materiale istruttorio (ben 44 pagine di trascrizioni di *chat* personali) censurava la condotta del lavoratore perché contraria al regolamento aziendale, che proibiva di utilizzare sistemi informatici aziendali a scopi personali. L'ingegnere veniva, così, licenziato.

Il lavoratore, quindi, impugnava il licenziamento alla Bucarest County Court, perché irrogato all'esito di un procedimento disciplinare istruito soltanto grazie ad un'intrusione del datore nella sua corrispondenza privata, la cui inviolabilità era sancita sia dalla Costituzione che dalla legge penale rumena.

---

[4] I termini sono considerati sinonimi dalla scienza economica dell'organizzazione del lavoro: cfr. W. H. FRIEDMAN, *Is the answer to Internet addiction, Internet interdiction?*, in M. CHUNG (edited by), *Proceedings of the 2000 Americas Conference on Information System*, 2000; V.K.G. LIM, *The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice*, in *Journal of Organizational Behavior*, 2002, 23, 675 ss. Recenti indagini hanno rilevato che il 90% dei lavoratori intervistati afferma di dedicare alla navigazione per scopi personali almeno un terzo del tempo trascorso *online* dal luogo di lavoro, cfr. G. BLAU, Y. YANG, *Testing a measure of cyberloafing*, in *Journal of Allied Health*, 2006, 35, 9 ss.

[5] Si tratta di un *software* di messaggistica istantanea che permette all'utente di comunicare, scambiando messaggi, in tempo reale, grazie alla rete internet. Il caso offre lo spunto per affermare che *chat* e posta elettronica sono assimilabili quanto a funzionamento. La *chat* sta a una chiacchierata, realizzata in modo istantaneo ed in forma scritta, come la *email* sta alla corrispondenza, atteso che non c'è forma di interattività di testo, immagini, messaggi vocali. La *chat* quindi è assimilabile ad una conversazione e la mail allo scambio di corrispondenza.

Il ricorso veniva respinto dalla Bucarest County Court ed il licenziamento dichiarato legittimo. I giudici di primo grado evidenziavano che il lavoratore agiva con la piena consapevolezza di violare il regolamento aziendale. Inoltre, affermavano che la violazione della corrispondenza privata era "scriminata" dal diritto del datore a vigilare sull'utilizzo della tecnologia, affinché di essa venga fatto un uso conforme agli obiettivi aziendali. L'intromissione del datore di lavoro costituiva, secondo la Corte, l'unico modo per verificare l'adempimento del lavoratore agli obblighi contenuti nel disciplinare interno.

Il dott. Bărbulescu proponeva appello alla Bucarest Court of Appeal la quale rigettava il gravame, confermando le statuizioni di primo grado e aggiungendo una parte motiva, ripresa, poi, dalla Corte EDU, relativa alle modalità con cui il controllo sull'*account Messenger* era stato effettuato. Secondo i giudici d'appello il controllo datoriale risultava proporzionato e ragionevole secondo i principi contenuti nella Direttiva 95/46/EC in materia di raccolta e trattamento di dati personali.

Esperite le vie di ricorso interne presso cui era risultato soccombente, il lavoratore ricorreva alla Corte di Strasburgo. Lamentava che la Magistratura rumena aveva emesso decisioni in violazione al «diritto al rispetto della vita privata e familiare, del proprio domicilio e della corrispondenza» di cui all'art. 8 CEDU.

Le decisioni delle Corti, secondo il ricorrente (§ 29-33), avevano violato il suo diritto a mantenere riservata la corrispondenza, sia professionale sia personale[6], perché il monitoraggio era stato svolto in assenza di un'informativa diretta al sorvegliato (§ 33) e con modalità scorrette.

La Corte Edu ritiene che non vi sia stata alcuna violazione dell'art. 8. Preliminarmente, la Corte dichiara ammissibile il ricorso dell'ingegnere rumeno, riconoscendo che il fatto sottoposto alla sua attenzione è sussumibile nel disposto dell'art. 8 CEDU. In linea rispetto alle pronunce precedentemente emesse[7], ribadisce che il «il diritto al rispetto della vita privata e familiare» è suscettibile di essere interpretato in maniera estensiva[8]e ricomprende tutti gli ambiti nei quali si sviluppa la personalità umana. La Convenzione, infatti, ad avviso dei Giudici di Strasburgo, non si limita a proteggere la vita intima e familiare dell'individuo, ma estende la tutela alle relazioni che l'individuo intesse per motivi professionali. Di conseguenza anche le *email* inviate dal luogo di lavoro devono essere meritevoli di tutela da parte della Convenzione.

Nondimeno, la Corte, anticipando il giudizio di merito, esclude che il dott. Bărbulescu potesse vantare alla luce delle circostanze specifiche del caso concreto «una ragionevole aspettativa di *privacy*». Chiariscono, infatti i Giudici di Strasburgo che il caso in esame si differenzia dai precedenti decisi perché il regolamento aziendale conteneva una chiara proibizione di utilizzo per scopi personali delle tecnologie aziendali, laddove in *Halford, Copland* e *Peev* l'uso personale dei dispositivi era pacificamente ammesso. Al lavoratore, secondo la Corte, poteva sorgere, quindi, quantomeno il dubbio di essere controllato a distanza dal datore di lavoro.

Peraltro, nonostante si trattasse di un punto fondamentale della controversia, l'effettiva conoscenza del regolamento aziendale da parte del lavoratore non risultava provata dal Governo Rumeno, il quale si era limitato a produrre in giudizio il regolamento generale della società e alcuni

[6] Nel § 31 il lavoratore sostiene di avere due differenti *user ID*, uno utilizzato per scopi professionali e l'altro per scopi personali e che quindi il datore di lavoro avrebbe avuto accesso anche al suo profilo personale protetto da una password.

[7] Niemietz c. Germania, sentenza del 16 dicembre 1992, n. 13710/88; Halford c. Regno Unito, sentenza del 25 giugno 1997, n. 20605/92; Copland c. Regno Unito, sentenza del 3 aprile 2007, n. 62617/00; Peev c. Bulgaria, sentenza del 26 luglio 2007, n.64209/01; E.B. c. Francia, sentenza del 22 febbraio 2008, n.4354/02; Pay c. Regno Unito, sentenza del 16 settembre 2008, n. 32792/05; Kopke c. Germany, sentenza del 5 ottobre 2010, n. 420/07; Bohlen c. Germania, sentenza del 19 febbraio 2015, n. 53495/09.

[8] Il primo comma prevede quattro ambiti su cui si basa l'autonomia della persona: la vita privata, la vita familiare, la corrispondenza e il domicilio. Quanto al concetto di «vita privata» da uno studio dei ricorsi dichiarati ammissibili dalla Corte emerge che le cause che riguardano questo diritto possono essere suddivise in tre categorie principali: i) l'integrità fisica, psicologica e morale della persona, ii) la sua *privacy* e iii) la sua identità. Per una esemplificazione, cfr. *Guida pratica sulle condizioni di ricevibilità*, 2014, reperibile sul sito *www.echr.coe.int*.

documenti riguardanti un precedente licenziamento di un dipendente della stessa azienda che aveva utilizzato internet e la fotocopiatrice per scopi personali. La Corte considera, dunque, erroneamente raggiunta la prova dell'effettiva conoscenza da parte del lavoratore in assenza della prova dell'informativa individuale sull'esistenza dei controlli sugli account aziendali.

Quanto all'esame del merito la Corte valuta il giudizio di bilanciamento effettuato dalle Corti rumene tra diritto alla *privacy* del lavoratore e potere del datore di lavoro di verificare l'adempimento del dipendente attraverso la sorveglianza sugli strumenti di lavoro tecnologici.

I Giudici di Strasburgo ritengono che le decisioni interne abbiano correttamente bilanciato le posizioni in conflitto, replicando la giurisprudenza precedente[9], secondo cui il potere di controllo è esercitato legittimamente nella misura in cui non travalichi lo scopo di verifica dell'adempimento contrattuale del prestatore di lavoro e risulti proporzionato e ragionevole nelle modalità di esercizio.

Nel caso di specie, avevano rilevato le Corti Rumene, che il controllo sull'*account Yahoo messenger* era stato svolto in buona fede da parte del datore il quale vi aveva avuto accesso nella convinzione di reperire esclusivamente corrispondenza professionale; solo dopo essersi, per casualità, imbattuto nelle numerose *chat* personali del lavoratore, era riuscito a procurarsi le prove dell'inadempimento del Bărbulescu e, quindi, aveva stampato legittimamente la cronologia delle *chat* per utilizzarle nel procedimento disciplinare prodromico al licenziamento.

Quanto alle modalità con cui la sorveglianza era stata esercitata secondo i giudici di Strasburgo esse erano state ritenute a ragione dalle Corti rumene proporzionate e ragionevoli.

La Corte, infatti, rileva che il datore di lavoro si fosse limitato ad apprendere che i destinatari delle conversazioni erano familiari del lavoratore e non clienti della società, senza, quindi, attingere al contenuto specifico dei messaggi per utilizzarlo come elemento di prova rilevante per giustificare il licenziamento disciplinare.

3. *L'interpretazione restrittiva adottata dalla Sentenza* Bărbulescu *del diritto alla privatezza delle comunicazioni elettroniche del lavoratore.*

Per vagliare in modo critico il contenuto del ragionamento della sentenza occorre mettere in luce che la Corte EDU si pronuncia su un tema "caldo" nel dibattito politico e giuridico delle Istituzioni internazionali, ma risulta completamente "sconnessa" rispetto alle indicazioni che provengono da queste ultime[10].

La Corte, infatti, nella sezione II della pronuncia, «*Relevant International Law*», riporta il testo di alcuni estratti della Convenzione del 1981 del Consiglio d'Europa e dei provvedimenti dell'Unione Europea, in particolare del *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, adottato il 29 maggio 2002 dal Gruppo art. 29[11],senza, tuttavia, tenerne in alcuna considerazione i contenuti nel ragionamento prospettato.

[9] V., in particolare, Copland c. Regno Unito, cit., in cui la Corte, nove anni prima, aveva sostenuto che «the monitoring of an employee's use of telephone, e-mail or internet at the place of work may be considered "necessary in a democracy society" in certain situation in pursuit of a legitimate aim».

[10] Vale la pena di notare che la sentenza in commento si colloca temporalmente tra l'emanazione della Raccomandazione R(2015)5 del Consiglio d'Europa e la pubblicazione dell'allora emanando Regolamento europeo in materia di protezione dei dati personali delle persone fisiche.

[11] Si tratta in particolare della Direttiva 96/45/CE e dei lavori del Gruppo art. 29 – un organo consultivo indipendente dell'UE per la protezione dei dati personali e della sfera privata, istituito in virtù dell'articolo 29, dir. 95/46/CE – in materia di sorveglianza elettronica sui luoghi di lavoro. I lavori del Gruppo art. 29 suggeriscono al datore di lavoro una serie di misure da adottare per garantire il rispetto dei principi di legittimità, trasparenza, proporzionalità e finalità del trattamento.

Ed infatti, il moderno diritto alla *privacy* del lavoratore[12], corollario del diritto alla vita privata di cui all'art. 8 CEDU, è la risultante di un'evoluzione normativa tributaria soprattutto dell'elaborazione avvenuta in sede europea[13] ed internazionale[14].

Proprio in attuazione dell'art. 8 CEDU, a proposito di sorveglianza elettronica sui luoghi di lavoro, il Consiglio d'Europa[15] – il medesimo organo in seno al quale è istituita la Corte EDU – ha emanato la Raccomandazione R(2015)5, 1 aprile 2015, in sostituzione della precedente R(1989)2[16], considerata oramai obsoleta a causa dell'ingente ricorso alle tecnologie dell'informazione e della comunicazione che viene fatto sui luoghi di lavoro.

Si tratta d'indicazioni di *soft law*[17], cui le legislazioni dei 47 Stati aderenti, caratterizzati da tradizioni storiche e giuridiche eterogenee, dovrebbero, nell'ottica dell'adozione di una politica comune, allinearsi e adeguarsi.

La Corte EDU, dal canto suo, non è vincolata alla loro applicazione in sede di decisione delle controversie, essendo tenuta a garantire esclusivamente l'applicazione uniforme delle norme della Convenzione con autonomia di giudizio[18]. Per tale ragione, essa può fornire, legittimamente, un'interpretazione restrittiva e riduttiva del nucleo di alcuni diritti fondamentali, come del resto accade nel caso che ci occupa. Ed infatti, la Corte EDU fornisce un'interpretazione "riduttiva" del diritto al rispetto della vita privata di cui all'art. 8 CEDU nella sua accezione di diritto alla *privacy* del lavoratore[19], che verosimilmente sarà ribaltata dalla Grande Camera.

Emblematica al riguardo la qualificazione della posizione giuridica vantata dal lavoratore, di «reasonable expectation of privacy» e non, invece, di *diritto* alla privacy. I giudici di Strasburgo, infatti, utilizzano il concetto di aspettativa, che è una forma di protezione degli interessi privati

---

[12] V., se vuoi, F. IAQUINTA, A. INGRAO, *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks: quando prevenire è meglio che curare*, in *Dir. rel. ind.*, 2014, n. 4, XXIV, 1027 ss.

[13] Gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea tutelano, a livello di principio il diritto alla *privacy*. Il fulcro centrale attorno al quale ruota l'intera legislazione europea è la direttiva 96/45/CE in materia di trattamento dei dati personali, attuata in Italia con il d.lgs. 196/2003, che contiene una specifica disciplina applicabile alle informazioni trattate nell'ambito dei rapporti di lavoro. La Direttiva è destinata ad essere abrogata dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[14] In particolare il Consiglio d'Europa (CEDU), da tenere concettualmente distinto dall'ordinamento dell'Unione Europea (UE) perché possiede su un proprio sistema di fonti ed un proprio sistema di Corti, ha svolto un ruolo fondamentale nella concretizzazione dei principi della Convenzione in materia di *privacy*. Ed infatti, soprattutto in tema di protezione dei dati personali sui luoghi di lavoro, i due ordinamenti sono intrecciati negli effetti che determinano, con l'obiettivo condiviso di creare una fitta trama di regole che il datore deve rispettare, nell'esercizio del suo potere di controllo, per preservare la sfera privata del lavoratore.

[15] Sul sistema del Consiglio d'Europa v. B. RANDAZZO, *Giustizia costituzionale sovranazionale*, cit.

[16] Nell'ambito del presente lavoro, ci si riferirà alle indicazioni contenute nella R(2015)5, che tuttavia non era ancora in vigore al tempo della emanazione della sentenza. Corre l'obbligo di puntualizzare, tuttavia, che anche la R(2989)2 già conteneva indicazioni specifiche volte a limitare i poteri datoriali di controllo e indagine sui lavoratori.

[17] Le Raccomandazioni non costituiscono fonti di diritto direttamente applicabili all'interno degli ordinamenti interni, né possono essere invocate davanti alla Corte EDU come parametro di legittimità per valutare i provvedimenti nazionali, legislativi e giudiziari.

[18] Autonomia interpretativa vale a dire che essa giudica secondo la giurisprudenza da lei stessa creata ed a prescindere dal diritto interno dello Stato di volta in volta interessato. L'autonomia di giudizio della Corte, anche dal punto di vista degli usi linguistici nazionali, è riconducibile all'art. 32 §1 CEDU.

[19] Di contrario avviso Antonello Soro, Presidente del Garante per la Protezione dei dati personali, il quale in un intervento, *I lavoratori devono essere informati. Il datore di lavoro non può spiare le mail*, pubblicato su l'*Huffington Post*, 13 gennaio 2016, ha dichiarato che la Corte EDU ha «riaffermato il principio secondo cui i controlli datoriali sull'attività lavorativa sono ammissibili soltanto nella misura in cui siano strettamente proporzionati e non eccedenti lo scopo di verifica dell'adempimento (…) Infine, devono essere già previsti dalla policy aziendale, di cui il dipendente deve essere adeguatamente edotto».

meno intensa rispetto al diritto soggettivo[20], esautorando il lavoratore delle facoltà che avrebbe potuto vantare laddove fosse stato riconosciuto titolare di un vero e proprio diritto[21].

La prima lacuna che si rinviene nella motivazione riguarda l'obbligo informativo che ricade sul datore di lavoro circa l'esistenza di un monitoraggio informatico sugli strumenti di lavoro.

La Corte, nel caso di specie, desume e presume la conoscenza dell'esistenza del controllo informatico da parte del lavoratore esclusivamente dal fatto che il datore avesse inserito nel regolamento aziendale una generale proibizione di utilizzo a fini personali dei *devices* aziendali[22].

Tuttavia, in virtù dell'applicazione del principio di trasparenza, principio cardine della disciplina della protezione dei dati personali del prestatore, elaborato sia in sede europea[23]che dal Consiglio d'Europa[24], il lavoratore ha diritto di essere preventivamente ed adeguatamente informato sull'esistenza di un controllo informatico della corrispondenza, sulle sue tempistiche e sulle finalità che spingono il datore di lavoro a sorvegliare l'attività lavorativa e sugli strumenti che saranno utilizzati per eseguire il monitoraggio[25].

La presenza di un regolamento aziendale non può, come velatamente sostiene la Corte, sostituire la funzione dell'informativa sulla *privacy*, che costituisce un adempimento aggiuntivo rispetto alla policy aziendale e che, quindi, dovrebbe essere consegnata a tutti i lavoratori[26].

In secondo luogo, con riferimento alle modalità con cui il potere di controllo dovrebbe essere esercitato, che si traducono in limiti d'azione per il datore, la pronuncia tralascia di considerare il principio generale secondo cui il datore, nel trattamento dei dati personali dei lavoratori, si dovrebbe astenere da «ingerenze ingiustificabili e irragionevoli nella vita privata del dipendente»[27].

La Corte, nel caso di specie, considera l'intrusione nelle *chat* – peraltro posta in essere in modo occulto – rispettosa dei principi di proporzionalità e ragionevolezza in quanto il datore di lavoro si era limitato a prendere atto della circostanza che i destinatari della "posta in uscita" erano familiari del lavoratore. La Corte EDU, quindi, scrimina la condotta del datore di lavoro perché costui non si

---

[20] Perché si tratta di una situazione giuridica strumentale, in potenza di consolidarsi in diritto soggettivo, a condizione che non si verifichino fatti ostativi che ne impediscano la nascita. F. GAZZONI, *Manuale di diritto privato*, Esi, Napoli, 2010, 65.

[21] Non solo per l'ordinamento dell'Unione europea, ma anche secondo le Raccomandazioni del Consiglio d'Europa dal diritto alla *privacy* conseguono per il lavoratore le facoltà di essere informato e di prestare il consenso al trattamento, di accedere ai suoi dati personali e di opporsi al trattamento stesso.

[22] Peraltro l'effettiva conoscenza del regolamento aziendale non veniva provata dal Governo rumeno (cfr. nota 9).

[23] Cfr. par. 3.1.3, *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, adottato il 29 maggio 2002 dal Gruppo art. 29.

[24] Cfr. Principio n. 10 R(2015)5 in base al quale il lavoratore ha diritto di essere reso edotto e consapevole non solo della tipologia di informazioni di cui è in possesso il datore e delle finalità per le quali sono state acquisite (cfr. 10.1 e 10.2), ma anche delle tecnologie di cui si serve per raccogliere e memorizzare i dati, nonché dell'utilizzo che il datore ne voglia fare (cfr. 10.3 e 10.4).

La piena consapevolezza delle operazioni di trattamento, oltre ad avere una funzione di *moral suasion* sul lavoratore, il quale sapendo di essere controllato è portato ad "auto-controllarsi", è propedeutica e preliminare all'esercizio dei suoi diritti (Principio n. 11), in particolare il diritto di accedere ai dati trattati, di esaminare e ottenere copia del proprio fascicolo personale e di esigere che le informazioni errate, incomplete o raccolte e trattate in violazione della *policy* aziendale siano cancellate o rettificate.

[25] Peraltro, il datore di lavoro dovrebbe dare la prova della conoscenza effettiva e diretta di tale informativa, non potendosi, invece, limitare ad assicurare la sua conoscibilità.

[26] Tanto è vero che non è necessario che l'informativa contenga anche la descrizione delle condotte configurate come inadempimento disciplinare e delle relative sanzioni che normalmente sono contenute nel disciplinare interno.

[27] Cfr. Principio n. 14 della R(2015)5 che regola l'utilizzo di internet e delle comunicazioni elettroniche sui luoghi di lavoro. In particolare, il datore è tenuto a fornire ai controllati informazioni periodiche e su base regolare, che chiariscano anche le ragioni legittime per le quali il trattamento viene effettuato (14.1). Quando il datore di lavoro controlla la navigazione internet dovrebbe adottare un approccio "scalare" e preferire controlli generalizzati su dati anonimi piuttosto che su base individuale. Ad esempio, qualora i sistemi di filtro per impedire determinate operazioni non fossero sufficienti a evitare il *cyberslacking*, il datore dovrebbe realizzare verifiche con gradualità, che riguardino *in primis* i reparti, poi gli uffici, e solo successivamente i gruppi di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo in caso di reiterazione delle anomalie il datore potrebbe eseguire controlli su base individuale.

è spinto a leggere il contenuto delle comunicazioni per utilizzarlo a fini disciplinari contro il lavoratore.

Non si dubita tuttavia, che anche i nomi dei destinatari delle comunicazioni elettroniche, ottenuti dal datore a seguito di controllo, costituiscano dati personali del lavoratore e come tali debbano soggiacere alla disciplina specifica in materia. Quindi, occorre distinguere il caso in cui tali dati vengano reperiti dal datore di lavoro attraverso controlli sulle comunicazioni personali dall'ipotesi in cui siano stati reperiti a seguito di sorveglianza sugli indirizzo elettronico aziendale.

Nella prima ipotesi, il Principio 14.4 prevede che «In nessun caso dovrebbero essere oggetto di sorveglianza il contenuto, l'invio e la ricezione di comunicazioni elettroniche di natura privata sul luogo di lavoro», anche quando essi siano memorizzati nella casella di posta aziendale del lavoratore. Con riferimento al caso esaminato dalla pronuncia, quindi, il datore che nel procedimento disciplinare utilizzi i dati e le informazioni, estrapolati dalla corrispondenza personale del dipendente, anche quando non si spinga a leggere il contenuto dei messaggi, viola l'art. 8 Cedu, come specificato dalle Raccomandazioni del Consiglio d'Europa.

Anche a volere controbattere che nel caso del dipendente rumeno, oggetto di controllo era stato l'account di posta aziendale, occorre evidenziare che il datore di lavoro non è completamente libero di controllare a distanza le conversazioni elettroniche del lavoratore.

Ed infatti, il controllo sulla corrispondenza elettronica di tipo aziendale[28] dei lavoratori soggiace a regole diverse: può essere svolto per finalità legittime (come ad esempio per garantire la sicurezza dei sistemi informatici) e sempre previa e specifica informazione sulla esistenza del controllo[29].

Peraltro, la sorveglianza elettronica sulla corrispondenza di un lavoratore, per tutelare il suo diritto alla *privacy* e alla riservatezza dovrebbe essere posta in essere nel rispetto del principio di necessità[30]. Da cui deriva che il datore di lavoro può monitorare le comunicazioni elettroniche dei propri dipendenti in casi eccezionali, ovvero ad esempio per rilevare la presenza di virus informatici o per garantire la sicurezza dei sistemi, oppure per acquisire prove da utilizzare in giudizio per difendere i propri interessi nei confronti di azioni criminose del lavoratore di cui esista perlomeno un sospetto in atto.

Di tutto questo non vi è traccia nella sentenza in commento. La Corte nella sentenza non esplicita la portata applicativa dei principi giuridici che presiedono al trattamento dei dati personali, desumendo piuttosto la proporzionalità e la ragionevolezza del controllo esclusivamente dalla circostanza che il datore aveva costatato un inadempimento senza spingersi a valutare il contenuto della corrispondenza privata del lavoratore.

4. *Il* cyberslacking *e l'ordinamento italiano.*

Anche in Italia, a seguito della riforma dell'art. 4 St. lav.[31], il dibattito giuridico si è focalizzato sul potere datoriale di controllo a distanza e sui suoi limiti.

---

[28] Il Principio n. 14 prevede l'ipotesi del controllo della corrispondenza elettronica quando il lavoratore è assente e nell'ipotesi in cui il rapporto di lavoro è cessato. Nel primo caso la Raccomandazione caldeggia l'adozione di idonee procedure che, in caso di necessità lavorative, consentano l'accesso alla casella di posta, nel secondo misure tecniche che consentano di disattivare l'account automaticamente senza accedere alla corrispondenza del lavoratore. Ad esempio, l'impresa dovrebbe prevedere messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi o consentire di delegare un altro lavoratore a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio.

[29] In verità il Principio n. 27, lett. c), rubricato «*additional safeguards*» prevede che ogni tipologia di monitoraggio dovrebbe essere comunque preceduta da una procedura di consultazione sindacale. Nel nostro ordinamento, a seguito della Riforma del 2015, quest'obbligo per il datore è venuto meno nell'ipotesi in cui il monitoraggio sia condotto sugli strumenti che servono al lavoratore a rendere la prestazione (ma v. *infra*).

[30] Cfr. l'art. 3.1.1-2 del *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, adottato il 29 maggio 2002 dal Gruppo art. 29.

[31] Intervenuta con l'art. 23, d.lgs. 81/2015, attuativo di una più estesa riforma che ha riguardato più istituti centrali del diritto del lavoro.

La norma – che rappresenta la chiave di volta del sistema giuslavoristico del controllo realizzato grazie all'utilizzo di strumenti tecnologici – è stata riformata perché si era rivelata progressivamente inadeguata a regolare il fenomeno per il quale era stata dettata[32].

Tra le innumerevoli innovazioni apportate dal legislatore del 2015, per quanto interessa ai fini della presente analisi, nel testo della norma emerge, oggi, il legame di correlazione e dipendenza sussistente tra potere di controllo e *privacy*. La Riforma ha, infatti, raccordato[33] la tutela giuslavoristica di cui all'art. 4 St. lav. con la normativa speciale di tutela dei dati personali, di cui al d.lgs. 196/2003 (Codice della *privacy*).

In particolare, ai sensi della nuova disciplina contenuta nel comma 3 dell'art. 4 st. lav. il datore di lavoro che intenda utilizzare i dati «a tutti i fini connessi al rapporto di lavoro» tra cui anche quello disciplinare, acquisiti interrogando strumenti tecnologici e informatici, dovrà dimostrare di avere rispettato sia le prescrizioni contenute nel Codice della privacy sia di avere reso consapevole il lavoratore, attraverso la consegna di un documento informativo circa l'esistenza dei controlli e delle modalità con cui sono svolti. Il datore di lavoro, contestualmente avrà l'onere di redigere una *policy* aziendale nella quale specifichi quali siano gli usi consentiti delle risorse elettroniche aziendali, come la mail e internet. Il rinvio espresso al Codice della *privacy*, peraltro, deve intendersi comprensivo delle Linee Guida emanate dal Garante per la protezione dei dati personali, il quale ha avuto, nel vigore del testo precedente della norma, un ruolo chiave nella produzione di regole specifiche con riferimento agli strumenti più utilizzati dalle imprese per il controllo a distanza[34].

---

[32] La disposizione era stata emanata nel 1970 per disciplinare l'installazione di telecamere a circuito chiuso e microfoni sui luoghi di lavoro. Nel sistema dello Statuto dei lavoratori la tutela della riservatezza sui luoghi di lavoro era radicata in un controllo affidato al sindacato. Successivamente, l'informatizzazione dei metodi produttivi, che implicava un controllo maggiormente penetrante sulla prestazione lavorativa fece sorgere il problema dell'applicabilità della disciplina di cui all'art. 4 anche all'installazione di apparecchi tecnologici come i computer. Il filtro dell'accordo sindacale non fu in grado di assicurare la tutela del lavoratore. Gli accordi furono pochi, perché le imprese non volevano attivare la procedura ed i sindacati accettavano la situazione. I controlli, quindi, venivano effettuati al di fuori dell'accordo sindacale. La tutela del lavoratore avrebbe potuto realizzarsi solo in giudizio, quando il datore intendeva utilizzare il dato a fine disciplinare e il lavoratore poteva paralizzare la pretesa sostenendo che il potere di controllo non era stato esercitato legittimamente. Si trattava quindi di una tutela del caso concreto e non di tipo collettivo. Peraltro, a privare di effettività l'art. 4 St. lav. contribuì quella parte della giurisprudenza (a partire da Cass. 3 aprile 2002, n. 4746, *Riv. giur. lav.*, 2002, 642 ss.) che disapplicava integralmente la disposizione normativa nell'ipotesi in cui il datore fosse mosso dalla finalità di accertare comportamenti illeciti del lavoratore. Cfr. A. BELLAVISTA, *Il controllo sui lavoratori*, Giappichelli, Torino, 1995; R. DE LUCA TAMAJO, *Presentazione della ricerca*, in R. DE LUCA TAMAJO, R. IMPERIALI D'AFFLITTO, C. PISANI, R. ROMEI (a cura di), *Nuove tecnologie e tutela della riservatezza dei lavoratori*, Franco Angeli,Milano, 1988; sulla nuova disposizione cfr. R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151/2015)*, in *Riv.it. dir. lav.*, 2016, 77 ss.; I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour and Law Issues*, vol. 2, 1, 2016.

[33] Già prima della riforma il Codice della *privacy* era applicabile nelle ipotesi in cui il datore di lavoro acquisiva dati personali dei lavoratori per il tramite di controlli a distanza. Questo perché le definizioni di «dato personale» e «trattamento» contenute nel d.lgs. 196/2003 erano molto ampie e si prestavano, pertanto, ad includere nell'ambito applicativo del Codice ogni operazione effettuata dal datore di lavoro su informazioni appartenenti al lavoratore ed in grado di renderlo identificabile. La giurisprudenza, tuttavia, solo sporadicamente aveva ritenuto applicabile il Codice della *privacy* all'istituto del potere di controllo a distanza. Oggi, quindi, il legislatore riscrivendo il comma terzo dell'art. 4 st. lav. ha previsto che il rispetto del Codice della *privacy* costituisca una condizione di legittimità per utilizzare i dati raccolti a fini disciplinari. M.P. AIMO, *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, Napoli, 2003; P. CHIECO, *Privacy e lavoro. La disciplina del trattamento di dati personali del lavoratore*, Cacucci, Bari, 2000.

[34] Con particolare riferimento all'utilizzo di Internet e posta elettronica fondamentale è la delibera n. 13 del 2007, nella quale il Garante della *privacy*, concretizzando i principi legali contenuti nel Codice (di liceità, necessità, correttezza, trasparenza, pertinenza e finalità) ha stabilito quali regole deve seguire il datore per controllare internet e mail dei dipendenti, nel rispetto del diritto alla *privacy* di questi ultimi. Cfr. M. PAISSAN, *E-mail e navigazione in internet: le linee del Garante*, in TULLINI (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, in *Trattato di diritto commerciale*

La violazione dei precetti rivolti alla tutela della *privacy* del lavoratore, contenuti nel Codice della *privacy*, che si risolve nell'inutilizzabilità delle informazioni acquisite a carico del lavoratore comporta conseguenze rilevanti sulla validità degli atti datoriali posti in essere dal datore di lavoro nel procedimento disciplinare[35]. Affiora, così, il rapporto di funzionalità del potere di controllo rispetto all'esercizio del potere disciplinare.

I precetti del Codice della *privacy*, tuttavia non sono i soli a dover essere rispettati dal datore di lavoro, che si voglia servire di strumenti tecnologici per monitorare il comportamento dei dipendenti. Infatti, la norma, nei primi due commi, distingue due fattispecie cui corrispondono discipline differenti.

Il primo comma replica parzialmente quanto già previsto nella precedente versione testuale e assoggetta l'installazione degli impianti audiovisivi e degli altri strumenti da cui possa derivare la possibilità di controllo a distanza dei lavoratori alla previa autorizzazione sindacale (o in mancanza, all'ottenimento di un provvedimento amministrativo) e alla sussistenza di causali tipiche che giustifichino le esigenze imprenditoriali che rendono necessario il controllo: motivi organizzativi, produttivi e di sicurezza sul lavoro. A queste esigenze il legislatore del 2015 ha aggiunto «la tutela del patrimonio aziendale», intendendo approvare l'installazione di sistemi di controllo allo scopo di preservare i beni materiali e immateriali dell'impresa, a fronte di condotte potenzialmente lesive dei lavoratori[36].

Nel comma secondo della disposizione, poi, è previsto che quando il datore intenda consegnare al lavoratore strumenti che servano a rendere la prestazione e strumenti di rilevazione degli accessi e delle presenze (*badge*) non debba espletare alcuna procedura sindacale, né addurre alcuna ragione causale che ne giustifichi l'installazione.

A causa dell'innovativa semplificazione contenuta nella diposizione, il dibattito giuridico si è immediatamente concentrato sulla delimitazione della categoria "strumento di lavoro", al fine di stabilire se rientrino nella disciplina del comma 1 o del comma 2, quelle apparecchiature che contestualmente consentano la resa della prestazione lavorativa e il controllo da parte dell'azienda. Il Ministero del Lavoro con una Circolare del 18 giugno 2015 ha chiarito che quando allo strumento di lavoro vengano aggiunte funzioni di controllo dell'attività dei lavoratori (mediante ad esempio il *download* di software appositi) si dovrà espletare la procedura sindacale per accertare l'effettiva sussistenza delle causali di legge. Nonostante il chiarimento del Ministero restano molti dubbi su alcuni casi *borderline*, di strumenti di lavoro che incorporano funzioni native di controllo[37].

In tutti questi casi, si può concludere che il legislatore nell'era della digitalizzazione abbia preferito affidare la tutela alla sua consapevolezza individuale piuttosto che al vaglio collettivo sindacale.

In conclusione, l'unico vero limite che costringe il potere datoriale di controllo a distanza è quello rappresentato dalle norme del Codice della *privacy*, alle quali è affidato il compito di garantire la riservatezza dei lavoratori nei confronti delle svariate modalità tecniche che ha il datore a sua disposizione per monitorare il comportamento di questi ultimi.

---

e di diritto pubblico dell'economia, Cedam, Padova, 2010, 11 ss.; P. TULLINI, *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *Riv. it. dir. lav*., 2009, II, 324 ss.

[35] La sanzione prevista in caso di violazione dell'art. 4 St. lav. è la inutilizzabilità delle informazioni. Tali informazioni, però, servono nella maggior parte dei casi al datore di lavoro come prove dell'infrazione contestata al lavoratore nel procedimento disciplinare.

[36] Questa ipotesi non era prevista nella versione della norma antecedente la riforma. La giurisprudenza, per far fronte all'esigenze imprenditoriali di verificare i comportamenti scorretti dei lavoratori, aveva creato la categoria dei controlli difensivi, ovvero quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, a cui non dovevano applicarsi i limiti di cui all'art. 4.

[37] Si pensi agli applicativi, installati in *tablet* o *smartphone*, che permettono di geolocalizzare il lavoratore, al *telepass*, al cronotachigrafo. In tutti questi casi, si pone il delicato problema di stabilire, attraverso una valutazione caso per caso, se l'applicativo risulti indispensabile al lavoratore per eseguire le mansioni assegnategli, tenuto anche conto del tipo di organizzazione dell'impresa. Solo in quest'ultimo caso la consegna dello strumento di lavoro potrà avvenire in assenza dell'accordo sindacale che comprovi le esigenze aziendali che rendono necessaria l'installazione, ai sensi del comma 2 dell'art. 4 St. lav. Cfr. R. DEL PUNTA, *La nuova disciplina,* cit., 102 s.