Federico Fusco

La *privacy* del lavoratore tra riforma dell'art. 4 St. lav. e regolamento generale sulla protezione dei dati personali

Sommario: **1.** Introduzione. **2.** La normativa sulla protezione dei dati personali letta in relazione al nuovo art. 4 St. lav. **3.** … *continua*: sull'idoneità della normativa sulla protezione dei dati personali a garantire il lavoratore contro un controllo eccessivamente pervasivo. **4.** Il sistema sanzionatorio: inutilizzabilità (relativa) dei dati raccolti e repressione penale. **5.** Conclusioni.

1. *Introduzione*

Come noto l'art. 23, co. 1, del d.lgs. 151/15 ha modificato l'art. 4 dello Statuto dei lavoratori e ha disegnato un assetto di interessi che, se da un lato mira indubbiamente ad ammodernare un testo normativo che, risalendo al 1970, stentava ad adattarsi agli attuali modelli produttivi (e, più in generale, di vita) oramai pervasi dall'uso di internet e di tecnologie digitali[1], dall'altro

[1] La bibliografia in tema di controlli a distanza è sterminata. Senza pretesa di esaustività v. Aimo, *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, 2003; Bellavista, *Il controllo sui lavoratori*, Giappichelli, 1995; Bellavista, *Controlli elettronici e art. 4 Statuto dei lavoratori*, in *RGL,* 2005, II, p. 772 ss.; Calcaterra, *Controllo sul lavoratore e agenzie investigative: compatibilità con lo Statuto dei lavoratori e tutela della privacy*, in *MGL*, 1999, p. 404 ss.; Carinci F., *Rivoluzione tecnologica e diritto del lavoro*, in *DLRI*, 1985, p. 224 ss.; Dell'Olio, *Art. 4 St. lav. ed elaboratori elettronici*, in *DL*, 1986, I, p. 487 ss.; Dessì, *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, Edizioni Scientifiche Italiane, 2017; Ghezzi, Liso, *Computer e controllo dei lavoratori*, in *DLRI*, 1986, 30, p. 353 ss.; Ingrao, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, 2018; Nuzzo, *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, 2018; Pera, *Innovazioni tecnologiche e Statuto dei lavoratori*, in *QDLRI*, 1, 1989; Santoro Passarelli G., *Osservazioni in tema di artt. 3 e 4 St. lav.*, in *DL*, 1986, I, p. 460 ss.; Troisi, *Il diritto del lavoratore alla protezione dei dati* personali, Giappichelli, 2013; Tullini, *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, nt. Cass. pen. 1 giugno 2010 n. 20722,

modifica gli equilibri in tema di controlli a distanza a vantaggio dei datori di lavoro.

Se, dunque, appare chiaro il fine perseguito dal legislatore, una simile conclusione non può essere raggiunta in ordine alla concreta portata della riforma. La novella, infatti, assoggetta il potere di controllo a distanza a un duplice ordine di limiti, i primi di natura procedurale, i secondi di natura sostanziale. Mentre quelli di matrice procedurale sono analiticamente specificati dall'art. 4 (che ai commi 1 e 3 individua in modo puntuale gli adempimenti necessari all'installazione degli strumenti dai quali possa discendere un controllo, nonché quelli per l'utilizzo, in relazione al rapporto di lavoro, delle informazioni raccolte), lo stesso non può dirsi per i limiti di natura sostanziale. Almeno per il più importante di essi, infatti, la norma, al comma 3, si limita a rinviare al Codice in materia di protezione dei dati personali (come, ovviamente, modificato, *ratione temporis*, dal Reg. UE2016/679 – o *GDPR* – cui nel prosieguo appare più opportuno fare riferimento)[2].

in *RIDL*, 2011, II, p. 86 ss.; Veneziani, *L'art. 4 legge 20 maggio 1970 n. 300: una norma da riformare?*, in *RGL*, 1991, I, p. 79 ss.; Zoli, *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in *RIDL*, 2009, I, p. 485 ss. Circa gli ostacoli che il vecchio art. 4 poneva all'introduzione di nuovi schemi organizzativi dell'attività di impresa v., per tutti, De Luca Tamajo, *Presentazione della ricerca*, in De Luca Tamajo, Imperiali D'Afflitto, Pisani, Romei, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, FrancoAngeli, 1988, p. 9 ss. *adde* Fusco, *Il pomo della discordia: il* badge *come strumento di controllo a distanza?*, in *RIDL*, 2011, II, p. 31 ss. Per un'analisi comparata v. Fusco, *Employee privacy in the context of EU Regulation n.2016/679: some comparative remarks*, in Aa.Vv., *Performance Appraisal in Modern Employment Relations. An Interdisciplinary Approach*, Palgrave Macmillan, 2019.

[2] Detta circostanza ha spinto parte della dottrina a parlare di "inediti livelli di penetrazione del diritto della *privacy* nell'ambito del rapporto di lavoro" (Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *WP C.S.D.L.E. "Massimo D'Antona". IT - 300/2016*, p. 5). Tale affermazione non pare, tuttavia, condivisibile in quanto, come dimostrato dai numerosi interventi del Garante per la protezione dei dati personali che si sono avuti già prima della novella *de qua*, la normativa sulla *privacy* pervade fin dalle sue origini la materia oggetto del presente studio. Al riguardo basti ricordare la deliberazione del 23 novembre 2006 n. 53 che detta linee guida in materia di trattamento dei dati personali del dipendente; il provvedimento dell'8 aprile 2010 in materia di videosorveglianza; la deliberazione del 1 marzo 2007 n. 13 che detta linee guida sull'uso della posta elettronica e internet; l'interpello del 28 novembre 2006 n. 6585 in tema di controllo a distanza dell'attività dei lavoratori attraverso sistema informatico; la *newsletter* del 2 marzo 2009 n. 320 in tema di controllo delle impronte digitali per l'accesso ai luoghi di lavoro e la *newsletter* del 22 settembre 2009 n. 328 in tema di controllo datoriale sulla navigazione in internet del dipendente. La riforma dell'art. 4, dunque, piuttosto che rendere più pervasiva l'influenza della normativa sulla protezione dei dati in seno al rapporto di lavoro si limita a esplicitare un obbligo preesistente, ossia quello del datore di

Tale rinvio appare, *prima facie*, rassicurante e ciò sia perché la normativa sulla *privacy* costituisce un *corpus* altamente pervasivo e dotato di un alto grado di specificità, sia perché, proprio a causa di queste sue caratteristiche, essa rassomiglia a una mitica chimera la cui fama è nota a tutti, ma la cui portata rimane ai più misteriosa. Lungi dal poter ritenere sufficiente il richiamo in esame occorre, dunque, procedere a un'analisi della cennata normativa, onde accertare quale ne sia l'effettiva portata e quali effetti produca sul nuovo sistema di controlli a distanza.

Il punto di partenza di tale studio risiede nella constatazione che pure il *GDPR* detta essenzialmente obblighi *lato sensu* procedurali e, quando, invece, pone limiti sostanziali al trattamento dei dati in molti casi rinvia per l'individuazione della loro esatta portata alla finalità del trattamento stesso[3]. I confini di liceità posti dalla normativa in tema di *data protection* sono, dunque, costituiti da barriere mobili il cui esatto posizionamento dipende dalla finalità perseguita. Ciò comporta che l'ampliamento delle tipologie di trattamento ammesse, nelle quali oggi si annovera anche quello teso (a talune condizioni) a controllare a distanza il prestatore di lavoro[4], produce l'effetto di spostare in avanti tali barriere, rendendo probabilmente leciti comportamenti che fino a ieri inevitabilmente cadevano sotto la scure del vaglio giurisdizionale.

Per tali motivi oggi ancor più che in passato si rende necessaria un'indagine sulle tutele apprestate dal Codice della *privacy*, nella consapevolezza che esse integrano il principale baluardo a difesa del lavoratore contro un eccessivo controllo datoriale.

trattare le informazioni personali del dipendente nel rispetto del *GDPR*. Proprio detta circostanza costituisce, come si vedrà nei paragrafi che seguono, uno dei limiti della riforma in quanto dall'imperfetto coordinamento tra normativa statutaria e quella in materia di *privacy* paiono residuare margini per un eccessivo controllo datoriale.

[3] In tal senso si è affermato che: "il nocciolo duro dei diritti della persona si coagula non sul sé, ma sul come va operato il trattamento dei propri dati personali, segnando così uno stacco estremamente rilevante rispetto a una concezione "proprietaria" degli stessi" CHIECO, *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*, Cacucci, 2000, p. 26.

[4] In tal senso v. MARAZZA, *Dei poteri*, cit., p. 26.

2. *La normativa sulla protezione dei dati personali letta in relazione al nuovo art. 4 St. lav.*

Nonostante il legislatore della riforma si limiti a richiamare il rispetto della normativa sulla *privacy* unicamente al terzo comma del nuovo art. 4 St. lav. non pare a chi scrive revocabile in dubbio che detta normativa vada rispettata in tutte le ipotesi in cui il datore abbia a trattare dati personali dei dipendenti e, dunque, non solamente qualora egli intenda utilizzarli per "tutti i fini connessi al rapporto di lavoro"; sicché il rispetto della normativa a tutela della riservatezza dovrà essere comunque assicurato indipendentemente da tale eventuale e futuro utilizzo del dato[5].

Ciò premesso, tralasciando gli obblighi *lato sensu* procedurali (quali informativa e consenso)[6] e prescindendo dagli specifici divieti posti per alcune categorie di dati (quali ad esempio quelli riguardanti lo stato di salute del

[5] In tal senso v. il combinato disposto dagli artt. 2, co. 1, e 4, co. 1, nn. 1 e 2, Reg. Ue 27 aprile 2016 n. 679 i quali dispongono che la citata normativa trova applicazione per qualunque operazione che coinvolga una qualsivoglia informazione relativa a una persona fisica, anche se solo potenzialmente identificabile. Peraltro anche in costanza del vecchio testo dell'art. 4 St. lav., il quale non rinviava alle norme a tutela dei dati personali, detta normativa era ritenuta pacificamente applicabile. Sul punto v. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, in *RIDL*, 2016, I, p. 90 ss.; Salimbeni, *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *RIDL*, 2015, I, p. 597, ss.; Tebano, *Ragionevolezza e potere di controllo del datore di lavoro*, in questa rivista, 2011, p. 440 ss.

[6] Nonostante a stretto rigor di termini il consenso sia un requisito sostanziale e non procedurale pare a chi scrive che esso ricopra un ruolo secondario in seno al rapporto di lavoro in quanto molte sono le ipotesi in cui il datore può procedere al trattamento anche in assenza dello stesso: ai sensi dell'art. 6, co. 1, lett. b) e c) *GDPR*, infatti, esso non è necessario ogniqualvolta il trattamento è finalizzato a eseguire obblighi derivanti dal contratto o imposti dalla legge. Si potrebbe, ovviamente, obiettare che detta norma vada letta in senso restrittivo, sicché il consenso sarebbe, invece, necessario allorquando il datore intendesse far valere un suo diritto scaturente dal contratto di lavoro. Tuttavia tale tesi non pare convincente in quanto è pacifico che il datore che intenda contestare un illecito disciplinare al dipendente o, ancora, voglia controllarne lo stato di malattia può trattare il dato personale inerente alla sua residenza – ai fini dell'invio di una lettera di contestazione o della visita fiscale – senza alcun consenso al trattamento da parte del lavoratore. In ogni caso si può prescindere dal consenso pure in tutte le ipotesi in cui (come avviene per la videosorveglianza) possa invocarsi il bilanciamento di interessi (art. 6, co. 1, lett. f) del Regolamento), ipotesi nella quale va ricompresa peraltro la necessità di far valere o difendere un diritto in sede giudiziaria. Inoltre un'analisi assistita da una giusta dose di realismo non può obliterare il rilievo che il lavoratore a cui venga richiesto di rilasciare il consenso al trattamento dei dati non è sovente posto in condizione di operare una libera scelta. Per tale motivo, anche in ossequio agli orientamenti formatisi nella vigenza della pregressa norma-

dipendente o le sue opinioni politiche e sindacali)[7], dalla veloce lettura dell'art. 5 Reg. UE n. 2016/679 (in precedenza artt. 3 e 11 d.lgs. 196/03) si evince che qualsiasi trattamento dei dati personali (dunque anche quello effettuato dal datore) è retto dai seguenti principi: finalità, necessità, proporzionalità, pertinenza, non eccedenza, liceità e correttezza.

Nonostante la norma ponga questi principi sul medesimo piano è facile rilevare che l'unico dotato di una propria autonomia, tale da farlo assurgere a chiave di volta dell'intero sistema, è quello di finalità, cui gli altri rimandano per la determinazione della loro esatta portata. Esso, infatti, stabilisce che ogni operazione riguardante i dati personali può avvenire unicamente se inerente al perseguimento della finalità in relazione alla quale è stato ottenuto il consenso (o altra forma di autorizzazione al trattamento). Com'è stato acutamente osservato, dunque, "il perno della *facultas agendi* del titolare (…) risiede nella scelta iniziale delle finalità da perseguire. È da tale scelta iniziale (…) che scaturisce e viene definito l'ambito del legittimo svolgimento dell'attività di trattamento (…)"[8].

I rimanenti principi, per contro, si riempiono di contenuti unicamente in rapporto a quello di finalità: il principio di necessità impone di raccogliere e utilizzare unicamente i dati indispensabili al perseguimento della finalità cui l'operazione mira; quello di proporzionalità statuisce che il trattamento dei dati già raccolti deve essere commisurato alla concreta finalità da perseguire con quel determinato atto (ed esempio preferendo, ove possibile, dati aggregati); quelli di pertinenza e non eccedenza, infine, vietano tutte le operazioni che non attengano alle finalità del trattamento[9].

tiva, l'art. 7 del Regolamento, letto alla luce del considerando n. 43, dovrebbe far dubitare della genuinità del consenso rilasciato dal lavoratore. La materia è peraltro affrontata dal considerando n. 155 il quale autorizza le normative nazionali a prevedere le condizioni in base alle quali i dati dei dipendenti possono essere trattati sulla base del consenso. Ciononostante né l'art. 88 del Regolamento, che pure disciplina il trattamento dei dati nell'ambito dei rapporti di lavoro, né la sua norma "attuativa" interna, ossia il nuovo art. 111 Cod. *Privacy*, non ricomprendono espressamente la materia del consenso tra quelle devolute al potere di specificazione dell'autonomia collettiva.

[7] Dati che, peraltro, godono di una specifica protezione da parte della normativa lavoristica, attesi i divieti di cui agli artt. 5 e 8 l. 300/70, nonché art. 10 d.lgs. 276/03, ambo richiamati dall'art. 113 d.lgs. 196/03.

[8] Barraco, Sitzia, *La tutela della* privacy *nei rapporti di lavoro*, Ipsoa, 2012, p. 119.

[9] Discorso a parte può essere fatto per i principi di liceità e correttezza i quali, costituendo forse una superflua ripetizione di principi generali del nostro ordinamento, non apportano, ad

È dunque chiaro che è la finalità del trattamento a determinare i tratti fondamentali dello stesso, ampliando o comprimendo le facoltà del titolare, sicché un'attenta iniziale calibrazione della finalità da perseguire consente di penetrare in modo anche molto invadente nella sfera di riservatezza del soggetto interessato.

Alla luce di questa considerazione si impone, dunque, una riflessione sui mutamenti che la novella dell'art. 4 dello Statuto ha introdotto nella materia in esame, precisando che la riforma esplica i propri effetti non sulla normativa in tema di *privacy* in sé, quanto, piuttosto, sui limiti entro i quali deve rimanere confinata la facoltà del datore di lavoro di trattare i dati personali dei dipendenti in tutte le ipotesi correlate all'esercizio del potere di controllo a distanza.

Come si è già ricordato nell'introduzione del presente lavoro, infatti, il controllo a distanza dell'attività dei lavoratori, che fino a ieri era rigidamente vietato (salvo essere, entro certi limiti, ammesso dalla giurisprudenza)[10], viene oggi, come si vedrà, in una certa misura sdoganato, dimodoché il trattamento di dati personali finalizzato a tale tipologia di controllo diviene una forma di trattamento lecita. In altri termini, dunque, in tutti i casi in cui la normativa statutaria consente al datore di controllare a distanza il dipendente, il trattamento dei dati personali finalizzato a tale controllo dovrebbe considerarsi ammesso.

L'assunto appena enunciato, pur semplice e coerente nella sua formulazione astratta, rischia, tuttavia, di scontrarsi con il precetto di cui all'art. 4 St. lav. La norma restituita dalla riforma, infatti, contiene un'indubbia antinomia laddove al comma 1 pare consentire il ricorso agli strumenti da cui possa discendere un controllo a distanza unicamente per perseguire finalità produttive, organizzative, di sicurezza del lavoro e tutela del patrimonio aziendale, mentre al comma 3 dichiara che le informazioni raccolte sono, invece, "utilizzabili a tutti i fini connessi al rapporto di lavoro"[11].

avviso di chi scrive, alcun significativo incremento agli standard di tutela, concretizzandosi nel divieto di trattare i dati personali in violazione delle norme di legge o con modalità occulte e/o ingannevoli (e, dunque, in violazione dell'obbligo all'informativa di cui agli artt. 12 ss. del Regolamento).

[10] Sul punto v., da ultimo, in senso critico, SALIMBENI, *La riforma*, cit., p. 593 ss.

[11] Tale antinomia viene, poi, acuita dal diritto vivente che, in costanza della vecchia normativa, aveva enucleato le categorie del controllo difensivo e di quello preterintenzionale le quali stentano a trovare una precisa collocazione in seno al nuovo disposto statutario.

Nonostante parte minoritaria della dottrina tenda ad arginare la portata della riforma, subordinando l'utilizzabilità del dato ai sensi del terzo comma al perseguimento anche mediante detto utilizzo delle esigenze di cui al primo comma[12], l'opinione maggioritaria pare orientata nel senso di consentire un impiego più ampio delle informazioni raccolte.

Nessun dubbio al riguardo è, infatti, avanzato da chi si limita a precisare che l'utilizzabilità in esame è subordinata a un triplice condizione, ossia non solo al rispetto delle norme del codice della *privacy* e alla preventiva esaustiva informativa data al lavoratore, ma anche al rispetto delle prescrizioni di cui ai commi 1 e 2 del nuovo articolo 4 (e, dunque, alla precipua osservanza delle prescrizioni sostanziali e procedurali di cui al comma 1)[13]. Le medesime conclusioni sono condivise da chi, pur critico verso la formulazione letterale della novella, osserva che il terzo comma del nuovo art. 4 neutralizza e smentisce il limite posto dal primo comma, sicché i dati acquisiti con strumenti che dovrebbero essere impiegati unicamente per perseguire le note esigenze organizzative, produttive etc. finiscono per essere, invece, utilizzabili anche per altri fini, quali quelli disciplinari[14]. Favorevole alla piena utilizzabilità delle

[12] In tal senso Dagnino, *Tecnologie e controlli a distanza*, in *DRI*, 2015, p. 1000 ss. ove l'A. afferma che le uniche finalità perseguibili mediante il trattamento dei dati previsto dal terzo comma restano sempre e comunque quelle tassativamente indicate dal comma I (esigenze organizzative e produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale), sicché le informazioni raccolte sarebbero utilizzabili per tutti i fini connessi al rapporto di lavoro solo qualora ciò risponda a dette citate esigenze. Ad avviso di chi scrive tale impostazione omette di considerare che il comma 3 dell'art. 4 St. lav. introduce, in realtà, una nuova e invero ampia finalità di trattamento, ossia quella relativa a "tutti i fini connessi al rapporto di lavoro", sicché il rispetto dell'art. 5, co. 1, let. b) del Regolamento è assicurato proprio da detto terzo comma. In ogni caso si rileva che anche abbracciando la tesi ora criticata si dovrebbe comunque concludere per l'utilizzabilità del dato per quella che sembra essere l'ipotesi principe della norma, ossia il fine disciplinare. La repressione dell'illecito disciplinare, specie se di particolare gravità, pare, infatti, legittimamente ascriversi alle categorie delle esigenze organizzative o produttive, se non addirittura in quella, finora assente dall'articolo 4, della tutela del patrimonio aziendale (in tal senso v. Marazza, *Dei poteri*, cit., p. 17, nt. 40 e ove l'A. afferma "non v'è ragione di non ricomprendere nelle esigenze di tutela del patrimonio aziendale anche l'esigenza di accertare il corretto adempimento della prestazione di lavoro" la quale "concorre alla valorizzazione del patrimonio aziendale" p. 16).

[13] In tal senso v. Del Punta, *op. ult. cit.*, pp. 104 e 105.

[14] V. Salimbeni, *La riforma*, cit., p. 611 ss. ove l'A. acutamente sottolinea che la formulazione letterale del testo *ante* riforma, vietando "l'uso" delle apparecchiature se finalizzate al controllo a distanza, ma consentendone, invece, "l'installazione" quando essa fosse richiesta per esigenze produttive etc., generava un certa qual ambiguità tale da permettere alla giurisprudenza, anche

informazioni è, infine, chi osserva che la novella è forse addirittura troppo restrittiva laddove, in relazione alla vecchia categoria dei controlli difensivi, rischia oggi di richiedere per la loro legittimità adempimenti prima non necessari, quali il rispetto della procedura sindacale o amministrativa per l'installazione delle apparecchiature a essi deputate[15].

A chi scrive pare che le opinioni da ultimo riportate siano da condividere e ciò sia in quanto il terzo comma dell'art. 4, facendo espresso riferimento alle "informazioni raccolte ai sensi dei commi 1 e 2", si pone in rapporto di specialità rispetto a quest'ultimi, sia poiché, come si è già fatto cenno, esso introduce una nuova finalità di trattamento dei dati personali dei dipendenti, ossia quella relativa all'utilizzo per "tutti i fini connessi al rapporto di lavoro".

3. …continua*: sull'idoneità della normativa sulla protezione dei dati personali a garantire il lavoratore contro un controllo eccessivamente pervasivo*

Un quesito importante che sorge alla luce delle nuove possibilità di controllo offerte dalla riforma è quello inerente all'idoneità dell'attuale normativa a tutelare il lavoratore contro un controllo a distanza eccesivo da parte del datore. Tale problema non pare tanto porsi con riguardo ai controlli effettuati ai sensi del comma 1 in quanto i vincoli imposti dal legislatore in relazione all'utilizzo degli strumenti in esame e alla loro installazione paiono idonei a scongiurare un rischio siffatto: all'obbligo di finalizzare lo strumento di controllo al perseguimento degli scopi tassativamente indicati consegue, infatti, che un qualsivoglia controllo del dipendente sia, per utilizzare una fortunata terminologia, di tipo "preterintenzionale" sicché difficilmente potrà raggiungere una pervasività tale da renderlo eccessivamente invasivo. Inoltre la procedura sindacale-amministrativa necessaria all'installazione dettando, come insegna la prassi, specifici requisiti sia in ordine alle caratteristiche degli strumenti da installare, sia alla loro ubicazione e modalità di funzionamento, sia infine alla possibilità di accesso alle informazioni raccolte (accesso che non

se in maniera forse non condivisibile, di "far "rientrare dalla finestra" un controllo che era stato "cacciato dalla porta". La nuova formulazione dell'articolo, per contro, distinguendo nettamente tra installazione e impiego, non pare dare adito a tale possibilità, rendendo ancora più stridente il contrasto tra primo e terzo comma.

[15] In tal senso v. MARAZZA, *op. ult. cit.*, pp. 16 e 18.

viene mai lasciato alla discrezionalità del datore, ma deve di norma essere effettuato in accordo con un rappresentante dei lavoratori) costituisce un altro importante baluardo a difesa del dipendente[16].

Maggiori dubbi sorgono, invece, in relazione a quanto previsto dal secondo comma dell'art. 4 il quale sottrae ai limiti ora velocemente ricordati sia gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", sia gli "strumenti di registrazione degli accessi e delle presenze".

Vista la natura eccezionale della norma la dottrina si è subito adoperata per specificare, in maniera restrittiva, tanto la nozione di "strumento di lavoro", quanto quella di "strumento di registrazione di accessi e presenze", chiarendo che il primo consiste in un mezzo necessario al lavoratore per rendere la prestazione lavorativa e che viene, dunque, volontariamente attivato da quest'ultimo, mentre i secondi sono quelli che consentono al datore di controllare il rispetto dell'orario di lavoro[17].

[16] Si rileva, peraltro, che a seguito della novella dell'art. 4 St. lav. il Ministero del Lavoro e delle Politiche Sociali ha provveduto a standardizzare su tutto il territorio nazionale la procedura e la documentazione necessarie al rilascio del nulla osta amministrativo che, in passato, erano rimesse alla discrezionalità delle singole DTL, presentando, dunque, rilevanti differenze tra loro.

[17] Sul punto v. SALIMBENI, *La riforma*, cit., pp. 605 e 609; DEL PUNTA, *op. ult. cit.*, pp. 100 e 101, ove l'A. specifica, in relazione a computer e altre apparecchiature elettroniche che rientrano nella nozione di strumento di lavoro unicamente gli applicativi necessari a rendere la prestazione di lavoro, con conseguente esclusione di *software* ulteriori e, magari, specificamente finalizzati al controllo; *adde* MARAZZA, *op. cit.*, p. 11 ss. Più controversa appare, invece, la nozione di "strumento di registrazione di accessi e presenze" in relazione alla possibilità di controllare anche gli spostamenti effettuati dal dipendente all'interno dell'azienda. Al riguardo, fermo restando il divieto di introdurre una sorta di "braccialetto elettronico" che consenta di monitorare in maniera costante la posizione del lavoratore all'interno dello stabilimento (MARAZZA, *op. cit.*, p. 24), mentre parte della dottrina ritiene tale tipo di controllo pacificamente consentito dalla norma in esame (sul punto MARAZZA, *op. ult. cit.*; *adde* DEL PUNTA, *op. ult. cit.*, p. 103), di particolare interesse appare la posizione di chi, invece, ipotizza una disapplicazione solo parziale del comma 1 dell'art. 4: il controllo degli spostamenti intraziendali sarebbe, infatti, lecito solo se motivato da specifiche esigenze, coincidenti con quelle elencate al comma 1, sicché l'effetto pratico della riforma sarebbe quello di escludere per tale tipo di controllo la procedura di autorizzazione preventiva (in tal senso v. SALIMBENI, *op. cit.*, p. 605). A parere di chi scrive tale ultima interpretazione appare particolarmente condivisibile in quanto consente di conciliare il diritto del lavoratore a non essere sottoposto a un controllo eccessivamente pervasivo con le legittime esigenze organizzative dell'azienda. Un esempio potrebbe, infatti, essere dato dall'esigenza datoriale di controllare che i lavoratori addetti ai videoterminali osservino la pausa di 15 minuti ogni 2 ore di lavoro prescritta dal d.lgs. 81/08 o, ancora, dall'introduzione di un nuovo regime di orario di lavoro che faccia coincidere l'inizio della giornata lavorativa non con l'ingresso del lavoratore all'interno dei locali aziendali, bensì con il momento in cui il dipendente

Nonostante queste importanti precisazioni, però, a chi scrive non pare del tutto escluso il rischio che il dipendente possa essere sottoposto a un controllo eccessivamente pervasivo e ciò soprattutto in relazione all'utilizzo degli strumenti di lavoro. Il riferimento è, come è intuitivo, alle apparecchiature, oramai onnipresenti, di tipo elettronico o informatico le quali, anche prescindendo dall'uso di specifici *software* "spia" finalizzati a rilevare momento per momento il comportamento dell'utente, consentono comunque di tenere traccia delle operazioni effettuate. Al riguardo, senza nemmeno aver bisogno di scomodare il vasto universo di *smartphone*, *tablet* e *app* varie, basti pensare a una comune stampante che permetta di tenere il conto delle stampe eseguite o, ancora, ad un qualsivoglia programma di scrittura elettronica che consente di tenere traccia delle singole battute effettuate[18]. In queste ipotesi, non certo fantascientifiche, ma, anzi, di comune esperienza nell'ordinaria vita lavorativa, la deroga al generale divieto di controllo a distanza introdotta dal comma 2 dell'art. 4 consente al datore di lavoro di verificare in modo invero pregnante e puntuale l'attività posta in essere dal dipendente, permettendogli finanche di rilevare quanti e quali tasti ha digitato sulla tastiera del computer e con quale cadenza! Il tutto, è bene precisarlo, senza ricorrere a nessun tipo di *software* esterno, ma utilizzando unicamente i dati raccolti da uno strumento, quale un comunissimo programma di scrittura elettronica, la cui riconducibilità alla categoria degli strumenti di lavoro non pare a chi scrive possa essere revocata in dubbio[19].

In un'ipotesi siffatta, quindi, mentre in passato si poteva ragionevolmente ancorare la tutela del dipendente al vecchio disposto dell'articolo 4 che, in assenza delle note causali e della prescritta procedura autorizzativa, bollava (salvo la famosa deroga giurisprudenziale dei controlli difensivi che,

si trova al suo posto di lavoro e pronto a cominciare l'attività (in tal senso v. il titolo II, art. 1 comma 2 del contratto collettivo specifico di lavoro del Gruppo Fiat del 7 luglio 2015). Infine altra accezione puntualmente analizzata dalla dottrina (Marazza, *op. ult. cit.*) e che può in parte trovare applicazione anche agli esempi pratici ora portati riguarda la nozione di "accesso digitale", ossia quello a banche dati e reti informatiche dell'azienda e che secondo l'Autore deve essere fatto rientrare nell'esenzione di cui al comma 2 dell'art. 4.

[18] Si pensi al riguardo al diffusissimo *Microsoft Word* che con la funzione "revisioni" permette di tracciare minuto per minuto i tasti digitati dall'utente. Peraltro dalla versione 2013 è possibile impedire la disattivazione del tracciamento delle revisioni mediante l'uso di una *password*.

[19] Per una puntuale analisi circa la natura degli strumenti in esame v. Nuzzo, *La protezione del lavoratore*, cit., p. 142 ss.

però, non pare rivestire alcun rilievo nel caso qui in esame) il controllo come illecito, viene, oggi, da chiedersi, essendo venuti meno i due importanti baluardi di tutela ora richiamati, dove risieda la disciplina a tutela del lavoratore.

Come si è già accennato essa è racchiusa nell'ultimo comma dell'art. 4 il quale, però, a una più attenta analisi appare inidoneo a proteggere il dipendente dal rischio di un'eccessiva aggressione da parte del potere di controllo datoriale. Nel nostro caso, infatti, l'utilizzabilità delle informazioni per qualsivoglia fine riconnesso al rapporto di lavoro è subordinata alla preventiva informativa in ordine alla "modalità d'uso degli strumenti e di effettuazione dei controlli" (requisito procedimentale idoneo a rendere edotto il dipendente circa l'*an* del controllo, ma non certo funzionale a metterlo al riparo dalle potenzialità lesive dello stesso), nonché al rispetto delle norme a tutela dei dati personali. L'analisi condotta al paragrafo che precede ha, però, evidenziato come gran parte delle garanzie ivi previste siano di natura procedimentale e che gli unici limiti di tipo sostanziale provengano dai principi enunciati all'art. 5 del Regolamento i quali, a loro volta, sono riconducibili al principio di finalità[20].

Posto ora che, stando alla lettera del terzo comma dell'art. 4, una finalità fino a ieri vietata, ossia quella di utilizzare le informazioni raccolte con gli strumenti di controllo a distanza per verificare l'attività dei dipendenti e farne derivare conseguenze relative al rapporto di lavoro, è oggi in una certa misura sdoganata dal legislatore (qualora l'informazione sia "involontariamente" acquisita tramite uno strumento legittimamente installato)[21], ne discende che il principio di finalità e i suoi diversi corollari saranno inidonei a impedire che il datore utilizzi le informazioni raccolte in relazione a detto rapporto di lavoro. Infatti se l'unico limite alla facoltà del datore di utilizzare

[20] Sottolinea la natura "procedimentale" delle tutele approntate dal Codice della *privacy* anche Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *RIDL*, 2016, I, p. 363.

[21] In tal senso Trib. Roma 13 luglio 2018: "Il controllo a distanza sui dipendenti non è più vietato in assoluto, ma qualora esercitato tramite strumenti di lavoro deve sempre essere oggetto di adeguata informativa pena l'inutilizzabilità delle risultanze" (in *GC*, 23 novembre 2018, nt. Ogriseg). *Adde* Trib. Roma 24 marzo 2017: "I dati raccolti nel rispetto di quanto prescritto dalla norma possono, quindi, essere utilizzati dal datore di lavoro a tutti i fini connessi al rapporto di lavoro, ivi compreso quello diretto al controllo sull'esatto adempimento della prestazione lavorativa così come quello disciplinare". In dottrina v. Proia, *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza*, in *RIDL*, 2016, I, p. 563.

il dato raccolto tramite lo strumento di lavoro deriva dalla normativa sulla *privacy*, la quale rimanda al fine perseguito dal trattamento per individuare i confini delle operazioni legittimamente eseguibili, ne consegue che un trattamento mirante all'esercizio del potere disciplinare rinverrà la linea di demarcazione tra lecito e illecito unicamente in relazione a quanto necessario per l'esercizio di detto potere. Pertanto, considerato che l'art. 7 dello Statuto dei lavoratori impone che la contestazione dell'addebito sia chiara e precisa, apparirà giustificato alla luce del principio di proporzionalità di cui all'art. 5 *GDPR* (da riempire di contenuto in relazione al fine perseguito) un trattamento del dato personale del dipendente che vada a indagare in modo molto minuzioso la condotta dallo stesso posta in essere. Inoltre, atteso che altro requisito indispensabile dell'azione disciplinare è la sua tempestività, il datore potrà agevolmente giustificare frequenti accessi alle informazioni raccolte dagli strumenti di lavoro con l'esigenza di non decadere dal potere sanzionatorio[22].

Quanto fin qui esposto in relazione ai principi di cui all'art. 5 del Regolamento vale a maggior ragione per le prescrizioni contenute nelle varie linee guida emanate dal Garante per disciplinare diverse ipotesi di trattamento di dati personali del lavoratore e che di tali principi costituiscono applicazione pratica. Così, ad esempio, in relazione alle linee guida in materia di trattamento dei dati personali dei lavoratori[23], posto che i principi di liceità,

[22] In tale ottica va, peraltro, considerata la recente giurisprudenza della Corte EDU che, nello specificare la portata dell'art. 8 della Convenzione (rispetto della vita privata e familiare) in relazione ai controlli datoriali, ha ancorato la tutela del lavoratore a limiti di natura essenzialmente procedimentale. In tal senso si vedano le decisioni B rbulescu v. Romania del 5 settembre 2017 (ove si censura la natura occulta del controllo e, dunque, il difetto di informativa), López Ribalda v. Spagna del 9 gennaio 2018 (che ritiene illegittima per difetto di informativa una telecamera nascosta installata al seguito del ripetuto verificarsi di ammanchi di cassa in un supermercato. Il caso è, tuttavia, ora pendente innanzi alla Grande Camera) e Libert v. Francia del 22 febbraio 2018 (che ripercorre il percorso argomentativo del caso B rbulescu). È, tuttavia, interessante notare che qui si ritiene esente da vizi la condotta datoriale consistita nell'accesso, in assenza e all'insaputa del dipendente, a dati sensibili dallo stesso archiviati nel computer aziendale (nella specie materiale pornografico). Difatti, da un lato il datore aveva fornito un'esaustiva informativa in merito all'uso delle apparecchiature informatiche ed alla possibilità di controlli, mentre dall'altro il dipendente aveva omesso di indicare il carattere personale dei documenti incriminati, avendoli generalmente archiviati in una cartella denominata "*fun*".

[23] Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati, deliberazione del Ga-

pertinenza e trasparenza vengono declinati nel senso di imporre che "le informazioni di carattere personale possono essere trattate dal datore di lavoro nella misura in cui siano necessarie per dare corretta esecuzione al rapporto di lavoro[24] – "e che "in ogni caso, deve trattarsi di informazioni pertinenti e non eccedenti[25] – " risulta evidente che nel momento in cui il fine legittimamente perseguito dal datore è quello di utilizzare per fini disciplinari le informazioni raccolte l'unico limite desumibile dalle norme in esame è quello che impedisce al datore di sviare il potere stesso per perseguire una diversa finalità. Ciò, tuttavia, non mette assolutamente al riparo il dipendente dal rischio di un controllo invero pregnante e continuativo[26].

Obblighi apparentemente più stringenti si rinvengono, invece, nelle Linee guida sull'utilizzo della posta elettronica e internet[27] ove il Garante solennemente "vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, co. 1, let. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (…)"[28]. A una più attenta lettura, tuttavia, tale divieto deve essere ritenuto almeno parzialmente stemperato in quanto il Garante lo ha formulato muovendo dal rilievo che l'articolo 4 St. lav. all'epoca vietava di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"[29], con la conseguenza che "il trattamento dei dati che ne consegue è illecito…"[30].

Come si è visto, però, la novella dell'art. 4 non solo ha calmierato il di-

rante per la protezione dei dati personali n. 53 del 23 novembre 2006, *www.garanteprivacy.it*, doc. web. n. 1364939.

[24] *Ibidem*, p. 4, punto 2.1.

[25] *Ibidem*.

[26] A risultato non dissimile si perviene dall'analisi della declinazione del principio di finalità contenuta in dette linee guida che recitano "il trattamento di dati personali riferibili a singoli lavoratori, anche sensibili, è lecito, se finalizzato ad assolvere obblighi derivanti dal contratto individuale (ad esempio per verificare l'esatto adempimento della prestazione…)". Pertanto, lungi dal porre limiti al potere datoriale di utilizzare i dati personali per sanzionare il dipendente (funzione, questa, che in passato era svolta, almeno in relazione ai controlli a distanza, dal vecchio testo dell'art. 4 dello Statuto) la norma in tema di *data protection* prevede espressamente tale tipo di trattamento. Sul punto v. linee guida, cit., p. 4, punto 2.2.

[27] Linee guida del Garante per posta elettronica e internet, deliberazione del Garante per la protezione dei dati personali n. 13 del 1 marzo 2007, *www.garanteprivacy.it*, doc. web. n. 1387522.

[28] *Ibidem*, p. 8.

[29] In tal senso v. linee guida cit., punto 4.

[30] *Ibidem*.

vieto in esame, ma al terzo comma ha addirittura tipizzato "una specifica finalità di trattamento dei dati personali dei lavoratori"[31]. È dunque evidente che il provvedimento del Garante, affondando le sue radici in una norma oggi novellata, dovrà necessariamente essere riletto alla luce del nuovo precetto, sicché laddove le informazioni provenienti da varie tipologie di *hardware* e *software* sono acquisite dal datore in modo lecito (perché, ad esempio, provenienti da strumenti di lavoro) esso datore potrà legittimamente trattare tali dati per tutti i fini relativi al rapporto di lavoro, anche disciplinare. È ora evidente che, al di là del dato puramente letterario, un uso siffatto legittima o comunque presuppone in un certo qual modo una forma di controllo (a distanza) dei dipendenti[32].

4. *Il sistema sanzionatorio: inutilizzabilità (relativa) dei dati raccolti e repressione penale*

Analizzate le tipologie di controllo lecite resta da studiare quale sia la norma di chiusura del sistema, ossia la sanzione applicabile in caso di violazione delle prescrizioni di legge. Come noto in caso di illecito controllo del dipendente gli esiti dello stesso sono inutilizzabili, sicché saranno inidonei a far discendere qualsivoglia conseguenza sul rapporto di lavoro. Tale approccio non è stato modificato a seguito della riforma, ma purtuttavia l'attuale formulazione del terzo comma dell'art. 4 St. lav. impone qualche riflessione. Il testo normativo, infatti, stabilisce che le informazioni raccolte sono utilizzabili se si soddisfano tre condizioni ossia l'osservanza delle prescrizioni dei primi due commi dell'articolo stesso, la preventiva informazione al dipendente circa modalità d'uso degli strumenti ed effettuazione dei controlli e il rispetto della normativa sulla *privacy*[33].

[31] Marazza, *op. ult. cit.*, p. 8 ove detta finalità viene identificata con l'utilizzo per "tutti i fini connessi al rapporto di lavoro".

[32] Si tralascia in questa sede l'analisi di un altro importante provvedimento del Garante, ossia quello in materia di videosorveglianza del 29 aprile 2004 (*www.garanteprivacy.it*, doc. web. n. 1003482), in quanto, essendo difficile ipotizzare (differentemente da quanto avviene per le caselle di posta elettronica o i programmi per la navigazione in internet) che un'apparecchiatura di videosorveglianza possa essere qualificata come strumento di lavoro, la tutela del lavoratore appare garantita (oggi come ieri) dai vincoli imposti dal primo comma dell'art. 4 dello Statuto.

[33] La classificazione riportata è di Del Punta, *op. ult. cit.*, pp. 104 e 105, cui si rinvia per

Visto, però, che la normativa a tutela dei dati personali viene richiamata nella sua interezza ciò comporta che, trattandosi di un *corpus* normativo completo e dotato delle sue norme di chiusura, per stabilire se essa sia rispettata la si deve necessariamente considerare nel suo complesso, senza limitarsi all'analisi di singole porzioni[34]. Detta considerazione forse banale assume fondamentale rilievo in relazione all'art. 160-*bis* del d.lgs. 196/03 (e dall'art. 2-*decies*) il quale, derogando al generale principio di inutilizzabilità dei dati trattati in violazione del Codice, dispone che è sempre ammesso l'utilizzo degli stessi in sede processuale se consentito dalle conferenti norme del codice di rito[35]. Dal combinato disposto dall'art. 4 St. lav. e dall'art. 160-*bis* del codice discende, dunque, che il primo subordina l'utilizzabilità delle informazioni al rispetto delle norme sulla *privacy*, ma tali norme, mediante l'art. 160-*bis*, sanciscono che eventuali violazioni di tale normativa sulla *privacy* non sono idonee a impedire l'uso delle informazioni in sede processuale, qualora tale uso sia consentito dal codice di rito[36].

Orbene, considerato che la materia che ci occupa vede nel momento processuale la chiave di volta dell'intero sistema in quanto il ricorso al giudice

un maggiore approfondimento. Sul punto v. anche MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *RIDL*, 2016, I, p. 538 il quale acutamente osserva che la norma oggi nettamente distingue due diversi momenti: quello del "controllo", che per essere lecito deve informarsi alle prescrizioni dei primi due commi e quello "dell'utilizzo" delle informazioni raccolte al quale solo si applicano le prescrizioni del terzo comma.

[34] Sembra propendere in tal senso anche MARESCA, *op. ult. cit.*, p. 542 secondo il quale il legislatore ha inteso individuare il confine tra il dominio dell'art. 4 e quello del Codice, al fine di ottenere l'integrazione delle due discipline, senza sovrapposizioni.

[35] Art. 160-*bis* d.lgs. 196/03 (inserito dall'art. 14, co 1, let. m) del d.lgs. 10 agosto 2018 n. 101): "La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale". Anteriormente alla riforma un'identica formulazione era contenuta al co. 6 dell'art. 160 del Codice della *privacy*. La natura cedevole della normativa a tutela dei dati personali nei confronti di quella processuale è peraltro chiaramente affermata dalle Sezioni Unite per le quali "deve ritenersi che la disciplina generale in tema di trattamento dei dati personali subisca deroghe ed eccezioni quando si tratti di far valere in giudizio il diritto di difesa, le cui modalità di attuazione risultano disciplinate dal codice di rito" (Cass. Sez. Un. 8 febbraio 2011 n. 3034).

[36] In tal senso v. PINORI, *Privacy e processo civile. I limiti di utilizzabilità nel giudizio civile di prove illecite: il difficile bilanciamento tra diritto alla protezione dei dati personali e il diritto alla difesa*, in *CI*, 2014, 1, p. 61; *adde* RESTA, *Privacy e processo civile: il problema della litigation "anonima"*, in *DII*, 2005, 4-5, p. 690 per il quale la norma *de qua* ha carattere di specialità rispetto all'art. 11; PECORA, STAGLIANÒ, *Commento all'art. 47*, in *Codice della privacy*, diretto da ITALIA, Giuffrè, 2004, p. 724.

è il principale strumento di difesa del lavoratore che abbia subito un pregiudizio (tipicamente un provvedimento disciplinare) a seguito di una forma di controllo illecita, da quanto ora esposto deriva una grave falla del sistema: la normativa sulla *privacy* cui il legislatore rinvia al fine di assicurare la tutela del dipendente contro forme illecite di controllo (almeno per la parte attinente alla violazione delle norme a tutela dei dati personali) consente, infatti, l'utilizzo in processo dei dati illecitamente raccolti[37].

L'onere della tutela del lavoratore contro forme illegittime di controllo viene, dunque, ulteriormente traslato sulle disposizioni del codice di rito il quale, tuttavia, non pare del tutto idoneo a tale scopo. Infatti, differentemente dal codice di procedura penale, che all'art. 191 statuisce che la prova non è utilizzabile se acquisita in violazione dei divieti di legge, le norme sul processo civile tacciono sul punto, ponendo la delicata questione della prova illecita[38]. Senza che in questa sede sia possibile anche solo accennare a un'indagine circa la dimensione epistemica del processo[39], sia sufficiente rilevare come la dottrina maggioritaria abbia affrontato la problematica rilevando che nel processo civile le prove precostituite fanno il loro ingresso

[37] L'utilizzabilità in sede giudiziaria dei dati trattati in violazione delle norme sulla *privacy* costituisce, peraltro, un tema ricorrente nella prassi giudiziale del Garante in quale, nel dichiarare illecite talune forme di trattamento e, di conseguenza, inutilizzabili i relativi dati, fa, però, espressamente salva la facoltà del loro futuro utilizzo processuale. In tal senso v. parere del 30/07/2015, n. 4298277, *www.deiure.it*; provvedimento 07/06/2006, *www.garanteprivacy.it*, doc. web. n. 1322812. Identica previsione è, contenuta, poi, nel recente regolamento UE 2016/679 che novella la normativa in tema di *data protection* e ove l'esigenza di consentire la difesa di un diritto in sede giudiziaria costituisce un vero e proprio *fil rouge* che legittima l'utilizzo dei dati illecitamente raccolti in una pluralità di ipotesi (v. in tal senso, artt. 17, 18, co. 1, let. c) e co. 2, 21 e 49, co. 1, let. e). In dottrina v. Vozza, *Privacy e difesa: una questione di bilanciamento di interessi*, nt. Cass. 3 aprile 2014 n. 7783, in *DR*, 2014, 10, p. 907 ss. la quale ricostruisce il rapporto tra diritto alla difesa e diritto alla riservatezza a tutto vantaggio del primo. In senso parzialmente difforme Ferrari, *La sanzione dell'inutilizzabilità nel codice della privacy e nel processo civile*, in *RDP*, 2013, 2, p. 348 ss., spec. p. 369 ove l'A., pur riconoscendo che la tutela della riservatezza trova ridimensionamento innanzi alle esigenze processuali, auspica però che il giudice, accanto a un criterio prettamente giuridico, ricorra anche a uno etico che tenga conto delle modalità con cui la prova è stata acquisita.

[38] Sul punto, in relazione alla specifica ipotesi di prova precostituita acquisita in violazione dei divieti dei cui al d.lgs. 196/03, v. Messina, Sub *artt. 46-57*, in Sica, Stanzione (a cura di), *La nuova disciplina della privacy*, Zanichelli, 2004, p. 232. Nega l'esistenza in seno al processo civile del divieto probatorio sancito per la materia penale Cass. 25 marzo 2013 n. 7466.

[39] Sul punto, anche per ulteriori approfondimenti, v. Taruffo, *La semplice verità. Il giudice e la costruzione dei fatti*, Laterza, 2009.

per il semplice fatto della loro tempestiva produzione, senza che vi sia alcun potere autorizzatorio da parte del giudice il quale, al contrario, deve fondare la decisione sulle prove proposte dalle parti (art. 115 c.p.c.)[40]. Per tale motivo esse possono avvalersi anche di prove illecitamente acquisite[41].

La normativa cui si è ora accennato ha trovato tradizionalmente applicazione in riferimento all'art. 4 St. lav. mediante le due note categorie giurisprudenziali dei controlli difensivi e di quelli preterintenzionali, col risultato di ritenere i primi sempre utilizzabili (in quanto sottratti alla – vecchia – norma statutaria), mentre i secondi legittimi solo in caso di previo esperimento della procedura autorizzativa[42].

A seguito della riforma, però, la questione si pone in termini diversi, non tanto in ordine all'effettiva sopravvivenza della categoria dei controlli difensivi[43], quanto, piuttosto, in relazione al circolo vizioso che si è venuto a

[40] V. Consolo, *Spiegazioni di diritto processuale civile: Volume III. Il processo di primo grado e le impugnazioni delle sentenze*, Giappichelli, 2010, p. 141. *Adde* Cass. 7 dicembre 2004 n. 22923.

[41] In tal senso v. Villecco, Bettelli, *Il trattamento dei dati in ambito giudiziario*, in Monducci, Sartor (a cura di), *Il Codice in materia di protezione dei dati personali. Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Cedam, 2004, p. 193 ss.; Pecora, Staglianò, *Commento all'art. 47*, cit., p. 724. *Adde* Gramano, *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi*, in *DLRI*, 2018, 1, par. 4. Quanto alla scarna giurisprudenza sul punto si veda Trib. Roma 24 marzo 2017; Trib. Bari 16 febbraio 2007, in *Il Merito*, 2007, 4, p. 22, nt. Antezza, secondo cui la violazione di divieti extraprocessuali non influenza in nessun modo l'efficacia probatoria, salva comunque l'applicabilità delle sanzioni di legge avverso l'illecito sostanziale perpetrato. *Adde* Trib. Torino ord. 8 maggio 2013, in *www.ilcaso.it*, che ammette la produzione in giudizio di *e-mail* e sms illecitamente acquisiti. In senso contrario, anche se in via solamente incidentale, Trib. Santa Maria Capua Vetere 13 giugno 2013, in *www.ilcaso.it*, che nel sancire l'utilizzabilità delle fotografie pubblicate su un *social network*, afferma che sarebbe stato applicabile un regime diverso qualora si fosse trattato di messaggi inviati tramite *chat* privata. Per una pronunzia più risalente v. Pret. Trapani 20 marzo 1193 in *FI*, 1994, I, p. 2575 che ammette la produzione in giudizio di un diario. Dopo una analitica ricostruzione della materia, conclude per l'utilizzabilità della prova illecitamente acquisita anche Trib. Milano 27 luglio 2016 n. 9431, salva la proponibilità di un'autonoma azione civile o penale volta alla repressione dell'illecito mediante il quale il documento è stato acquisito.

[42] Per la ricostruzione del dibattito sul punto v. Salimbeni, *op. ult. cit.*, p. 593 ss., nonché Dossi, *Controlli a distanza e legalità della prova: tra esigenze difensive del datore di lavoro e tutela della dignità del lavoratore*, in *DRI*, 2010, 4, p. 1153 ss., spec. p. 1160.

[43] Categoria che parrebbe aver perso la propria autonomia a seguito dell'inserimento della "tutela del patrimonio aziendale" tra le esigenze di cui al comma 1 dell'art. 4. In tal senso v. Del Punta, *op. ult. cit.*, p. 105. *Contra* Marazza, *op. ult. cit.*, pp. 18 e 19 il quale invoca la codificazione di una nuova tipologia di "controlli a distanza difensivi che – facendo leva sulla peculiare rilevanza (penale) antigiuridica del comportamento controllato (…), esulano dal campo

creare. Posto, infatti, che oggi è espressamente lecito utilizzare le informazioni raccolte per tutti i fini connessi al rapporto di lavoro, ne consegue che gli esiti di un controllo (magari effettuato con gli strumenti di lavoro) rispettoso dei primi due commi del nuovo art. 4, ma, purtuttavia, contrastante con una qualche norma in tema di trattamento dei dati personali, saranno legittimamente utilizzabili per tutti fini di cui al terzo comma. Quella stessa normativa sulla *privacy* contenente i precetti violati dispone, infatti, che dette violazioni non ostano all'utilizzo in giudizio del dato illegittimamente trattato, rimettendo alle norme processuali l'individuazione di eventuali limiti che, però, in seno al rito civile paiono essere assenti[44].

Siffatte conclusioni paiono confermate anche dal ragionamento *a contrario*: nel silenzio della normativa processuale il legislatore, laddove ha inteso limitare la possibilità di un soggetto di avvalersi di determinate modalità di conoscenza (e prova) della realtà empirica, lo ha sempre fatto mediante specifiche disposizioni[45], sicché, in assenza di un apposito divieto, il mezzo di prova deve ritenersi pienamente utilizzabile.

di applicazione dell'art. 4 della legge n. 300/1970". In tal senso v. anche MARESCA, *Controlli tecnologici*, cit., p. 525 il quale però non pare delimitare la categoria alla sola repressione delle condotte penalmente illecite. Sul punto v. anche MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità* post *panottica*, in *ADL*, 2015, 6, p. 1186 ss.; SANTONI, *Controlli difensivi e tutela della privacy dei lavoratori*, nt. a Trib. Roma 23 maggio 2015 n. 4009, in *GI*, 2016, 1, p. 145 ss. In senso critico avverso il perdurante utilizzo giurisprudenziale della categoria in esame v. GRAMANO, *La rinnovata (e ingiustificata)*, *cit*. Sul punto sia solo dato notare come qualsivoglia dibattito inerente questa forma di controllo rischi di dover essere almeno in parte rimeditato qualora la Grande Camera della Corte EDU dovesse confermare la sentenza emessa dalla terza sezione nel caso López Ribalda v. Spagna.

[44] Sembra propendere per la piena utilizzabilità del dato trattato in violazione delle norme del Codice anche MARESCA, *Controlli tecnologici*, cit., p. 543 il quale, però, fonda siffatta conclusione sul rilievo che il comma 3 del nuovo art. 4 St. lav. (che autorizza tale uso) costituisce norma speciale rispetto all'allora art. 11, co. 2 d.lgs. 196/03 (il quale sanziona con l'inutilizzabilità i trattamenti non conformi al dettame del Codice).

[45] Tra queste si può menzionare l'art. 9 d.l. 132/14 (convertito con modificazioni dalla l. 162/14) che nel disciplinare la c.d. "negoziazione assistita" sancisce che "le dichiarazioni rese e le informazioni acquisite nel corso del procedimento non possono essere utilizzate nel giudizio avente in tutto o in parte il medesimo oggetto" (comma 2) e che "i difensori delle parti e coloro che partecipano al procedimento non possono essere tenuti a deporre sul contenuto delle dichiarazioni rese e delle informazioni acquisite (comma 3)" e anzi estende a tutti costoro le tutele previste per il segreto professionale (art. 200 c.p.p.) e per la libertà del difensore (art. 103 c.p.p.). Altri esempi sono costituiti dall'art. 38 commi 2 e 3 del Codice deontologico forense che fa divieto all'avvocato di registrare conversazioni telefoniche con i colleghi e di al-

In sintesi a chi scrive pare dunque doversi concludere che le informazioni raccolte nel rispetto dei primi due commi dell'art. 4 St. lav., ma in violazione di una qualche norma sulla *privacy*, possono validamente essere utilizzate in giudizio in quanto in un'ottica complessiva sono assunte senza contravvenire a nessun divieto inderogabile di legge. Gli unici precetti violati sono, infatti, quelli sulla tutela dei dati personali i quali, però, espressamente decretano che la loro mancata osservanza non osta all'utilizzabilità processuale delle informazioni raccolte[46].

Sotto questo aspetto, dunque, l'apparato sanzionatorio restituito all'indomani della riforma deve dirsi senza dubbio insoddisfacente in quanto prima si rinvia (come visto nei paragrafi che precedono) al Codice della *privacy* (e al *GDPR*) per l'individuazione di importanti limiti al potere di con-

legare comunque in giudizio il contenuto dei colloqui riservati intercorsi con essi, nonché dall'art. 48 che estende lo stesso divieto alla corrispondenza riservata tra difensori. In ambito lavoristico possono, invece, richiamarsi gli artt. 2 e 3 St. lav. che, come noto, vietano al datore di accertare l'esatto adempimento della prestazione lavorativa mediante guardie giurate o personale occulto. In particolare proprio il divieto di ricorrere alle guardie particolari giurate, stante la fede privilegiata dei verbali da esse redatti (art. 255 r.d. n. 635/40), palesa la volontà del legislatore di escludere un particolare tipo di prova nella materia *de qua*. É giusto il caso di sottolineare che prima della novella del 2015 uno specifico divieto probatorio era previsto anche per gli strumenti di controllo a distanza; divieto oggi chiaramente eliminato dal 3° comma del testo novellato. É infine interessante evidenziare che l'art. 1, co. 912, l. 205/17 (legge di bilancio 2018) all'ultimo periodo statuisce che "la firma apposta dal lavoratore sulla busta paga non costituisce prova dell'avvenuto pagamento della retribuzione", avvalorando ulteriormente la tesi dell'utilizzabilità probatoria delle fonti documentali qualora manchi uno specifico divieto. Va, infine, sottolineato che le recenti "regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria" del 19 dicembre 2018 non proibiscono l'utilizzo da parte dell'avvocato di prove illecite ove ciò sia concesso dall'ordinamento processuale. Inoltre in riferimento ai dati di cui non è certo l'impiego lecito (dovendo, invece, essere ritenuto tale l'utilizzo ammesso dalle norme processuali) l'art. 2, co. 4, let. d) ne vieta il trattamento solo ove appaia "ingiustificato".

[46] Siffatto disposto della normativa sulla protezione dei dati personali costituisce uno degli elementi che induce a ritenere utilizzabili le prove illecite nella già menzionata sentenza del Trib. Bari 16 febbraio 2007. *Contra* MARAZZA, *op. cit.*, 7 ove, però, l'A. non spiega quale sia il fondamento giuridico della sostenuta inutilizzabilità del dato. Peraltro già prima della novella si pronunzia favorevolmente all'utilizzo processuale di dati acquisiti in violazione del d.lgs. 196/03, disattendendo sul punto lo specifico provvedimento del Garante, Trib. Torino 8 gennaio 2008 che argomenta anche in base all'assenza nel codice di procedura civile di uno specifico divieto in tal senso e alla espressa previsione contenuta nel citato art. 160, co. 6, d.lgs. 196/03 (ora art. 160-*bis*).

trollo a distanza, ma poi si esclude che la violazione degli stessi comporti l'inutilizzabilità delle informazioni acquisite[47].

[47] Le criticità ora analizzate appaiono, poi, accresciute da un approccio della giurisprudenza che denota una certa qual "'insofferenza" (…) verso il sistema della *privacy*" (così IMPERIALI, *Privacy e controllo sull'utilizzo di cellulare e computer aziendali a fini personali: un difficile equilibrio*, in *RIDL,* 2008, II, p. 862); insofferenza che, in una fattispecie di licenziamento fondato su illeciti disciplinari scoperti dal datore mediante controlli condotti in violazione del d.lgs. 196/2003, porta il giudice a bollare come "illegittimo" e "da disapplicare" il provvedimento del Garante che, accertando l'illiceità del trattamento, disponeva l'inutilizzabilità dei relativi dati (così T. Torino 8 gennaio 2008 in *RIDL,* 2008, II, p. 845, nt. IMPERIALI). Pongono l'accento sulla tendenza da parte della magistratura lavoristica a dare un minor peso alle doglianze relative alle violazioni datoriali della normativa a tutela dei dati personali commesse nell'esercizio del potere di controllo anche DEL PUNTA, *op. ult. cit.*, pp. 91 e 92 e TEBANO, *op. cit.*, p. 440. In senso critico avverso il vaglio giurisdizionale circa il rispetto della normativa *de* qua v. anche NUZZO, *I software che registrano la durata delle telefonate nei call center sono strumenti di lavoro?*, nt. Trib. Pescara 25 ottobre 2017 in *RIDL*, 2018, II, p. 307 ss. Va, infine, segnalato il rischio di un radicale contrasto "giurisprudenziale" tra gli arresti della magistratura e le decisioni rese dal Garante in sede di definizione dei ricorsi amministrativi (artt. 77 ss. *GDPR*). Infatti, in relazione alla qualità dei dati cui il datore può accedere per controllare il corretto utilizzo del computer aziendale in uso al dipendente, il Garante ha più volte adottato un'interpretazione alquanto restrittiva. Così, riguardo alla (vietata) memorizzazione sul pc di *file* di natura personale si è affermato che ci si deve limitare a constatare la presenza sul computer di documenti che per loro natura, nome e dimensioni appaiano difformi da quelli propri dell'attività lavorativa del dipendente (compiendo, quindi, un controllo unicamente sui metadati), senza che sia, invece, possibile accedere ai relativi contenuti (così provvedimento del Garante del 18 maggio 2006, *www.garanteprivacy.it*, doc. web n. 1299082). Analogamente in relazione a un abusivo utilizzo della connessione a internet aziendale per finalità personali l'*Autority* ha sancito l'illiceità del comportamento datoriale che, invece di limitarsi a contestare la collocazione temporale e la durata delle connessioni, si era concretizzato altresì nel controllo del contenuto dei diversi siti web visitati (v. provvedimento del Garante del 2 febbraio 2006, *www.garanteprivacy.it*, doc. web n. 1229854). Queste decisioni, però, si pongono in radicale contrasto con quella giurisprudenza che, attenendosi a un'interpretazione rigorosa dell'art. 7 St. lav., esige, pena l'insufficiente specificità dell'addebito e la conseguente illegittimità del provvedimento disciplinare, che il datore contesti altresì il tipo di sito internet illecitamente visitato (così Trib. Milano 30 settembre 2005 in *RCDL*, 2006, 3, 899, nt. CHIUSOLO). In un contesto siffatto è facile immaginare che il datore troverà più conveniente tenere un comportamento illegittimo secondo i crismi del Garante, ma poi giovarsi dell'utilizzabilità processuale dei dati illecitamente trattati, piuttosto che rischiare di vedere stigmatizzato il provvedimento disciplinare da parte del giudice del lavoro, con tutti i costi che da ciò derivano. Ulteriori e più stringenti limiti al potere datoriale non paiono di fatto potersi rinvenire nemmeno nella autorevole sentenza resa dalla Gran Camera della Corte Europea dei Diritti dell'Uomo (B rbulescu contro Romania, pubblicata il 5 settembre 2017). Nella fattispecie i giudici di Strasburgo hanno accertato la violazione dell'art. 8 della Convenzione (che garantisce il rispetto della vita privata e familiare) a carico dello Stato rumeno per non aver predisposto rimedi interni atti a impedire al datore di lavoro di monitorare le comunicazioni elettroniche, acce-

Altro aspetto che lascia perplessi è, infine, l'apparato sanzionatorio penale a tutela dell'art. 4 l. 300/70. Senza voler qui analizzare gli inutili barocchismi del legislatore[48], basti ricordare che il comma 2 dell'art. 23 d.lgs. 151/15 aveva novellato l'art. 171 del Codice della *privacy* limitando la sanzione penale alla sola violazione dei primi due commi del neonato art. 4 l. 300/70. L'inutile richiamo al comma 2, norma unicamente permissiva e dunque non suscettibile di violazione, è stato eliminato dall'art. 15, co. 1 let. f) del d.lgs. 10 agosto 2018 n. 101, sicché il presidio penale avverso illeciti controlli a distanza

dendo anche al relativo contenuto a carattere intimo, intrattenute dal dipendente (poi licenziato) utilizzando il computer aziendale, ma un *account* di messaggistica personale. La decisione, pur elencando una serie di requisiti ai quali si deve informare il potere di controllo datoriale e che costituiscono corollari del principio di proporzionalità già conosciuto dal nostro ordinamento, si fonda essenzialmente sulla circostanza che il lavoratore, pur essendo stato informato del divieto di utilizzo personale delle apparecchiature aziendali, non era stato tempestivamente reso edotto della possibilità del datore di compiere controlli in merito e sulla loro effettiva portata. Considerato, quindi, che sono questi requisiti di tipo procedimentale già previsti dal nostro art. 4 e, come si è visto, inidonei a porsi come saldo baluardo a tutela del lavoratore, non pare a chi scrive che efficaci limiti a un troppo pervasivo ricorso al potere di controllo possano essere rinvenuti nemmeno nella pur autorevole giurisprudenza della Corte Edu. Ciò, peraltro, è a maggior ragione valido se si considera che è ben più utile al datore creare un clima di controllo costante al fine di "spronare" la produttività dei dipendenti, piuttosto che "ficcanasare" nei loro affari privati una volta che sia palese l'inadempimento dell'obbligo lavorativo (in tal senso v. MARESCA, *Controlli tecnologici*, cit., p. 542, nonché NUZZO, *La protezione del lavoratore*, cit., p. 100). Anche un assiduo controllo limitato ai soli metadati e che non indaghi il preciso contenuto delle comunicazioni vietate, pur essendo rispettoso della vita privata del soggetto, può però rivelarsi eccessivamente pervasivo. Infine pure sotto il profilo dell'effettività della tutela la sentenza ora accennata pare inidonea a ristorare il pregiudizio subito dal lavoratore. Pur accertando l'illiceità del controllo datoriale in quanto contrario a un fondamentale diritto dell'uomo (e, come logica conseguenza, l'illegittimità del licenziamento scaturitone) la Corte nulla liquida a titolo di danno patrimoniale (che il ricorrente calcolava in base a parte delle retribuzioni perse) e, quanto ai pregiudizi non patrimoniali, afferma che l'avvenuto accertamento dell'illecito costituisce di per sé un adeguato ristoro. Per tali motivi il lavoratore, all'esito di una vicenda giudiziaria durata circa 10 anni, ottiene la sola (misera) somma di € 1.365,00 a titolo di rimborso delle spese di lite! Per l'analisi della decisione della Corte nel precedente grado del medesimo giudizio v. CRISCUOLO, *Il controllo sugli* account *di posta elettronica e di messaging aziendale*, nt. C. Eur. Dir. Uomo 12 gennaio 2016, in *RIDL*, 2016, II, p. 284 ss. ove l'A. sottolinea come per la Corte elemento dirimente per la liceità del controllo è la preventiva informazione al lavoratore.

[48] Con l'introduzione del Codice della *privacy* il legislatore da un lato ha abrogato l'inciso dell'art. 38 dello Statuto dei lavoratori che sanzionava penalmente la violazione dell'art. 4, ma dall'altro ha disposto all'art. 171 del Codice che la violazione dell'art. 4 in esame è punita con le sanzioni dell'art. 38 dello Statuto…il tutto con buona pace dell'esigenza di semplicità e chiarezza (e, quindi, di effettiva conoscibilità) della normativa penale!

permane unicamente in riferimento al comma 1[49]. Nessun reato si avrà, quindi, in caso di violazione del terzo comma dell'art. 4, sicché rimane nell'area del penalmente lecito un uso delle informazioni raccolte ai sensi dei commi 1 e 2 che avvenga senza la preventiva adeguata informazione al lavoratore o, ancora, in violazione delle norme sulla *privacy* (salvo, ovviamente, altre specifiche figure di reato da esse previste).

Ancora una volta, quindi, la norma che pone i maggiori vincoli contro un eccessivo controllo da parte del datore (soprattutto se attuato mediante gli strumenti di lavoro i quali sfuggono ai limiti di cui al primo comma) è sprovvista di un idoneo apparato sanzionatorio[50].

5. *Conclusioni*

Con l'analisi fin qui condotta si è tentato di dimostrare che la riforma dell'art. 4 St. lav. ha restituito una norma connotata da rilevanti criticità per lo meno sotto due importanti profili, ossia la definizione di precisi limiti al potere datoriale di controllo e la predisposizione di sanzioni contro la violazione degli stessi.

Quanto ai limiti, soprattutto a fronte di controlli effettuati attraverso strumenti di lavoro, da un lato essi si risolvono in obblighi in massima parte procedurali, mentre dall'altro il rinvio alla normativa sulla *privacy*, vista dal legislatore come norma di chiusura del sistema, si rileva inadeguato in quanto la stessa affida la demarcazione tra lecito e illecito alla finalità perseguita dal trattamento e, pertanto, la tutela da essa offerta risulta pesantemente influenzata dalla legalizzazione (entro i confini specificati) della finalità di controllo a distanza del dipendente.

[49] In tal senso v. DAGNINO, *op. cit.*, p. 1004.

[50] Altra problematica cui si può qui solo accennare riguarda, poi, la non chiara tipizzazione della condotta vietata dovuta alla già cennata antinomia tra i commi 1 e 3 dell'art. 4. Un'interpretazione restrittiva del terzo comma volta a consentire l'uso delle informazioni raccolte con gli strumenti di cui al primo comma solo se funzionale al perseguimento degli scopi dallo stesso tipizzati (sul punto DAGNINO, *op. cit.*, p. 1000) farebbe discendere, infatti, che ogni altra forma di impiego, non essendo giustificabile ai sensi dell'ultimo comma dell'art. 4, si risolverebbe in un utilizzo difforme rispetto a quello permesso dal comma 1 e andrebbe, dunque, penalmente sanzionata. Ciò comporterebbe, però, un'inammissibile dilatazione della fattispecie penale, resa ancor più insidiosa dal fatto di essere fondata sull'ambiguità del testo normativo.

Quanto, infine, all'apparato sanzionatorio, anche volendo tralasciare la, forse non opportuna, delimitazione delle condotte penalmente rilevanti, esso rischia di rivelarsi ineffettivo a causa del possibile utilizzo processuale dei dati raccolti in spregio dei vincoli sopra analizzati.

Muovendo da tali rilievi a chi scrive pare, dunque, necessario un forte richiamo ai precetti costituzionali in un'ottica di contenimento di forme di controllo a distanza eccessivamente pervasive, ma che purtuttavia paiono poter sfuggire alle maglie della rete di tutele prevista dall'art. 4 St. lav. Ricordando, dunque, la *ratio* del titolo I dello Statuto dei lavoratori (significativamente rubricato "della libertà e dignità del lavoratore"), quella dello stesso art. 4[51], nonché i fini definiti dal legislatore delegante[52], devono assurgere quali criteri ermeneutici fondamentali della norma in esame i principi di cui agli artt. 2 e 41, co. 2 della Costituzione.

Senza voler far professione di passatismo, ma anzi riconoscendo l'opportunità di un intervento che ha l'indubbio merito di aver adeguato al mutato contesto tecnologico e sociale una norma per certi versi non più attuale, va, quindi, fermamente sottolineato che qualsivoglia forma di controllo, che pure possa apparire lecita rispetto alla lettera del solo articolo 4, deve essere improntata alla (e limitata dalla) tutela della dignità del lavoratore, anche, com'è stato lucidamente scritto, mediante la riduzione dell'"impegno di lavoro nei limiti di una certa tollerabilità o lassismo, senza esasperazioni di tipo stakanovistico"[53].

[51] La cui relazione ministeriale di accompagnamento del 1970 chiarisce che il controllo deve rimanere in una "dimensione umana cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro".

[52] Art. 1, co. 7, let. f), l. 183/14 che impone di contemperare esigenze dell'impresa e tutela della dignità e riservatezza del lavoratore.

[53] PERA, *Sub art. 4*, in ASSANTI, PERA, *Commento allo Statuto dei lavoratori*, Cedam, 1972, p. 25.

Abstract

Il saggio analizza la riforma dell'art. 4 St. lav. e della normativa sulla tutela dei dati personali, indagandone i reciproci rinvii e legami. L'A. procede, poi, con lo studio delle sanzioni applicabili in caso di violazione di detta normativa e ne vaglia l'idoneità in relazione al bene giuridico tutelato, con particolare attenzione all'utilizzabilità processuale dei dati personali raccolti mediante forme di controllo a distanza che integrino una violazione della normativa sulla privacy.

The essay focuses on the workers' privacy, as regulated in art. 4 of the Italian labour protection act (St. lav.) and in the new EU *GDPR*. The A. analyses the links between the two sets of rules and their combined effect. A specific attention is dedicated to the sanctions against the infringement of the provisions of the abovementioned art. 4. This topic is especially studied with regard to the possibility to use in a trial documents based on an illegal processing of personal data.

Key words

Controlli a distanza, art. 4 St. lav., privacy, prove illecite, sanzioni.

Remote control, art. 4 St. lav., privacy, unlawful evidences, sanctions.