IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA
Anno XXX Fasc. 1 - 2014

Marco Grotto

LA RILEVANZA PENALE DEL CONTROLLO DATORIALE ATTRAVERSO GLI STRUMENTI INFORMATICI

Estratto

Milano • Giuffrè Editore

MARCO GROTTO

LA RILEVANZA PENALE DEL CONTROLLO DATORIALE ATTRAVERSO GLI STRUMENTI INFORMATICI

SOMMARIO: 1. Le nuove forme del controllo datoriale. — 2. La normativa di riferimento. — 3. Il controllo datoriale della corrispondenza elettronica indirizzata al lavoratore. L'orientamento giurisprudenziale. — 4. Critica. — 5. L'assenza di antigiuridicità quale soluzione alternativa. — 5.1. Applicabilità della scriminante del consenso dell'avente diritto. — 5.2. Applicabilità della scriminante dell'esercizio del diritto. — 6. I limiti applicativi dell'art. 616 c.p. Il problema della lettura di e-mail archiviate su *server*. — 7. Il problema del concorso apparente di norme. — 8. Il regime sanzionatorio delle altre forme di controllo datoriale illegittimo. — 9. (*Segue*). Le applicazioni giurisprudenziali.

1. Le nuove forme del controllo datoriale.

Nella società moderna il controllo datoriale ha assunto nuova veste rispetto alle ipotesi "classiche", cui pensava il legislatore dello Statuto dei Lavoratori, di installazione di strumenti di videoripresa o di controllo del traffico telefonico. La tecnologica, infatti, mette a disposizione modalità e strumenti molto più *efficaci*, *invasivi* e *subdoli* di quelli conosciuti in passato. Ciò anche perché, come segnalato dal c.d. "Gruppo dell'articolo 29", la preferenza per modalità di lavoro "da remoto" o l'impiego di *device* sempre connessi alla rete rendono difficoltoso scindere tra attività professionale e vita privata [1].

L'attività di controllo è declinabile in una pressoché infinita serie di varianti operative. Oggetto del monitoraggio possono

* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

[1] Si veda il *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, adottato dal c.d. Gruppo dell'art. 29, costituito in applicazione della direttiva n. 95/46 CE, il 29 maggio 2002. Illustra A. Mantelero, *Riforma della Direttiva comunitaria sulla* data protection *e* privacy impact assessment, *verso una maggiore responsabilità dell'autore del trattamento?*, in questa *Rivista*, 2012, 145 ss. come le bozze di nuovo regolamento comunitario e della nuova direttiva comunitaria in tema di *data protection* sposino un'idea "evoluta" di protezione dei dati personali, privilegiando un'analisi *ex ante* sull'impatto che lo strumento o il servizio può avere sulla tutela dei dati trat-

essere, ad esempio, la navigazione *web*, la connessione a sistemi protetti, l'accesso a luoghi fisici tramite *badge*, gli spostamenti esterni all'area aziendale [2] oppure ancora lo scambio di corrispondenza telematica.

Lo scopo del presente contributo è quello di riflettere sulla normativa nazionale, ed in specie sanzionatoria, applicabile alle situazioni ora descritte e sui profili di maggiore criticità emersi in sede applicativa [3].

2. La normativa di riferimento.

Le potenzialità offerte dal mondo tecnologico ed informatizzato rendono il fenomeno del controllo datoriale poliedrico ed in continua, rapida evoluzione. A fronte di ciò, le fonti giuridiche atte a regolarlo sono disperse in numerosi testi legislativi, nessuno particolarmente recente. Vengono in rilievo, infatti, le norme del

tati (c.d. valutazione in termini di *privacy impact assessmet*). Un interessante confronto tra le tendenze continentali e quelle d'oltreoceano è contenuto in A. Mantelero, Data protection *ed attività di impresa. Verso dove guardano gli USA?*, in questa *Rivista*, 2011, 457 ss. L'A. mette in luce come il tema del trattamento dei dati personali sia affrontato in maniera sistematica e pervasiva dalle istituzioni comunitarie, sebbene l'implementazione di tali scelte sia rimessa alle singole autorità nazionali, e come, per converso, il panorama americano dimostri minore sensibilità (ed anche un certo anacronismo) rispetto alle diverse sfumature che caratterizzano la materia. Per una comparazione Canada-Stati Uniti si veda F. Giovannella, *Immagini pedopornografiche, privacy del lavoratore e protezione costituzionale: il punto della Corte Suprema Canadese*, in questa *Rivista*, 2013, 38 ss. Traccia il quadro delle tendenze comunitarie e della Corte EDU G. Tiberi, *Il diritto alla protezione dei dati personali nelle Carte e nelle Corti sovranazionali*, in *Cass. pen.*, 2009, 4467 ss. (prima parte) ed in *Cass. pen.*, 2010, 355 ss. (seconda parte), mentre danno conto dei rapporti tra Europa e USA M. Botta-M. Viola De Azevedo Cunha, *La protezione dei dati personali nelle relazioni tra UE e USA. La negoziazione sul trasferimento dei PNR*, in questa *Rivista*, 2010, 315 ss.

[2] Sulla possibilità di sfruttare i segnali emessi dai sistemi di localizzazione satellitare (GPS) ai fini di indagine si registra, di recente, un vasto dibattito: D. Gentile, Tracking *satellitare mediante GPS: attività atipica di indagine o intercettazione di dati?* (nota a Cass., sez. V, 15 gennaio 2010-10 marzo 2010, n. 9667), in *Dir. pen. proc.*, 1465 ss.; F. Iovene, *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen.*, 2012, 3556 ss.; S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, 580 ss.; M. Stramaglia, *Il pedinamento satellitare: ricerca ed uso di una prova "atipica"*, in *Dir. pen. proc.*, 2011, 213 ss. Con riferimento al panorama statunitense, in generale G. Di Paolo, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare e altre forme di localizzazione tecnologicamente assistita. Riflessioni a margine dell'esperienza statunitense*, in *Cass. pen.*, 2008, 1219 ss. Commentano, invece, la recente presa di posizione della Corte Suprema americana V. Fanchiotti, *U.S. v. Jones: una soluzione tradizionalista per il futuro della* privacy, in *Dir. pen. proc.*, 2012, 381 ss. e M. Cerase, *Il GPS innanzi alla Corte Suprema degli Stati Uniti tra originalismo interpretativo e progresso tecnologico*, in *Cass. pen.*, 2012, 1936 ss. Il tema del "pedinamento tramite GPS" è stato affrontato anche dalla Corte EDU nella sentenza resa dalla sezione V il 2 settembre 2010, Uzun c/ Germania, ric. n. 35623/2006, annotata, in chiave problematica, da S. Signorato, *La localizzazione satellitare nel sistema degli atti investigativi*, cit., 605 s.

[3] Esula dalla presente indagine il problema dell'acquisizione di informazioni attraverso i c.d. *social network*. In argomento si vedano M. Colonnello, *Facebook e controllo del lavoratore*, in *Dir. e pratica lav.*, 2011, 103 ss. e L. Picotti, *Diritti fondamentali nell'uso ed abuso dei* social network*: aspetti penali*, in *Giur. Merito*, 2012, 2522 ss.

codice civile sul potere di controllo della prestazione lavorativa (artt. 2086 e 2104); alcune disposizioni della Carta Costituzionale (1948), prima tra tutte l'art. 15 Cost. a tutela della libertà e della segretezza della corrispondenza; le previsioni contenute nell'art. 8 della Carta Europea dei Diritti dell'Uomo (1950) [4] ed ora anche negli artt. 7 ed 8 della Carta dei Diritti Fondamentali dell'Unione Europea (c.d. Carta di Nizza); il disposto degli artt. 3 e 4 dello Statuto dei Lavoratori (1970) [5]; gli articoli del codice penale in materia di segretezza della corrispondenza (artt. 616 e segg.) e di tutela della riservatezza informatica (art. 615-*ter* c.p.), frutto della novella del 1993; le disposizioni in materia di trattamento dei dati personali contenute nel D.Lgs. n. 196/2003 così come interpretate dai numerosi provvedimenti del Garante.

Sebbene il legislatore non si sia quindi mai espressamente occupato delle nuove forme di controllo datoriale, l'impiego, sin dallo Statuto dei Lavoratori, di formule normative particolarmente ampie ha permesso al sistema di mantenere la propria capacità regolativa anche rispetto ai fenomeni più recentemente emersi.

Ai fini di una più chiara disamina del panorama normativo è opportuno distinguere le attività di monitoraggio della corrispondenza telematica rispetto a tutti gli altri casi di controllo datoriale. La segretezza della corrispondenza gode, infatti, di un'espressa copertura costituzionale e di un presidio sanzionatorio autonomo, mentre per tutte le altre ipotesi devono applicarsi norme teleologicamente meno selettive [6].

3. Il controllo datoriale della corrispondenza elettronica indirizzata al lavoratore. L'orientamento giurisprudenziale.

In più di un'occasione la giurisprudenza si è occupata di valutare la rilevanza penale del comportamento del datore di lavoro

[4] Costituisce un'interessante applicazione dell'art. 8 CEDU il caso Halford c/ Regno Unito, in cui la Corte Europea dei Diritti dell'Uomo con sentenza del 25 giugno 1997 ha statuito che « *risulta chiaro… che le chiamate telefoniche effettuate da sedi commerciali possano, alla pari di quelle effettuate da casa, rientrare nell'ambito delle nozioni di "vita privata" e "corrispondenza" a termini dell'articolo 8, paragrafo 1* ». Il caso è stato citato quale precedente nella successiva pronuncia, sempre della Corte EDU, del 3 luglio 2007, Copland c/ Regno Unito, pubblicata in questa *Rivista*, 2008, 201 ss. con nota redazionale. Più recentemente si veda la sentenza della Corte EDU, sez. V, 5 ottobre 2010, Köpke c/ Germania (ric. n. 420/2007), pubblicata per estratto in *Cass. pen.*, 2011, 1972, nella quale si è affrontato il caso del controllo a mezzo di videoriprese di una dipendente di un supermercato sospettata di furto.

[5] Sostiene la perdurante attualità dell'impostazione della L. n. 300/1970 M. Napoli, *Lo Statuto dei Lavoratori ha quarant'anni e li porta bene*, in *Studi in onore di Mario Romano*, Vol. IV, Napoli, Jovene, 2857 ss.

[6] L'art. 15 della Costituzione qualifica come « inviolabili » la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, mentre le disposizioni sanzionatorie sono contenute negli articoli da 616 a 623-*bis* del codice penale.

che controlli le e-mail ricevute o spedite dal lavoratore a mezzo di un indirizzo di posta elettronica aziendale.

In tutti i casi noti il procedimento penale è stato attivato su impulso del lavoratore congiuntamente all'impugnazione civile del licenziamento irrogato per ragioni disciplinari. È accaduto, infatti, che il datore di lavoro abbia rinvenuto nella corrispondenza telematica la prova ora dell'infedeltà del lavoratore ora del suo inadempimento alle obbligazioni contrattuali.

Il problema consiste quindi nello stabilire quale sia il regime di utilizzabilità di una prova così raccolta, derivando da quello tanto la legittimità o illegittimità del licenziamento quanto la configurabilità di un reato [7].

A supporto della liceità del controllo sta il fatto che esso venga esercitato su un *account* attivato dal datore di lavoro (e non dal lavoratore) e da questi messo a disposizione del dipendente. Depone in senso contrario un'aspettativa di riservatezza fondata sulla considerazione che l'e-mail sia stata data in uso esclusivo ad un singolo lavoratore anziché abbinata ad una mansione (ad es.: mario.rossino@meazienda.it invece che ufficiocommerciale@nomeazienda.it) nonché la circostanza che, in presenza di una già accennata difficile separazione tra vita professionale e vita privata, della stessa possa essere fatto un uso promiscuo per finalità sia lavorative che extralavorative.

Le sentenze note che si sono occupate dell'applicabilità o meno al caso di specie dell'art. 616 c.p. sono tutte favorevoli al datore di lavoro [8].

La prima pronuncia in materia appartiene al Giudice per le Indagini Preliminari presso il Tribunale di Milano [9], il quale, decidendo su una richiesta di archiviazione, ha dettato una sorta di *vademecum* in tema di uso di posta elettronica sui luoghi di lavoro. Questi, in sintesi, i principi evidenziati: "personalità" dell'indirizzo di posta elettronica non significa "privatezza"; l'indirizzo e-mail costituisce uno strumento aziendale a disposizione

[7] È evidente che il licenziamento non può fondarsi su prove illegittimamente acquisite dal datore di lavoro. Uno speciale regime di inutilizzabilità è previsto dall'art. 11, comma 2 del D.Lgs. n. 196/2003, secondo il quale « i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati ».

[8] L'art. 616 c.p. sanziona al primo comma la "presa di cognizione" di corrispondenza "chiusa" ovvero la "sottrazione", "distrazione", "distruzione", "soppressione" della corrispondenza "chiusa" o "aperta"; mentre al secondo comma punisce la "rivelazione" del relativo contenuto "senza giusta causa". Già C. Pedrazzi, nella voce *Consenso dell'avente diritto*, cit., par. 13, si era posto il problema della rilevanza penale del comportamento di colui che apre « una lettera espresso a lui non indirizzata, per vedere se occorra prendere qualche urgente misura nell'interesse del destinatario assente ». L'A. riconduceva siffatta situazione alla categoria del "consenso presunto". Un tale inquadramento non sembra tuttavia praticabile con riferimento ai casi *de quibus*, in cui tutto lascia presumere che i lavoratori, se interpellati, avrebbero negato il consenso alla presa di cognizione della corrispondenza.

[9] G.I.P. presso il Tribunale di Milano, 10 maggio 2002.

del lavoratore e quindi il datore di lavoro ne ha la completa e totale disponibilità; non può configurarsi un diritto del lavoratore ad accedere in via esclusiva né al computer aziendale né all'e-mail aziendale; il lavoratore che utilizza, per qualunque fine, la casella di posta elettronica aziendale si espone al rischio che anche altri lavoratori della medesima azienda possano lecitamente entrare nella sua casella di posta elettronica e detto rischio non è necessario sia "ricordato" al lavoratore, perché esso è consequenziale alle doverose ed imprescindibili conoscenze informatiche del lavoratore stesso che, proprio perché utilizzatore dello strumento informatico, non può ignorare tale evidente implicazione [10].

In sostanza, secondo il giudice meneghino, la finalità della *password* necessaria per leggere le e-mail non è certo quella di proteggere la riservatezza del singolo lavoratore bensì solo quella di impedire che ai predetti strumenti possano accedere soggetti estranei alla società. Giammai da un uso illecito dello strumento di lavoro (*id est*: l'impiego dell'e-mail aziendale per finalità private) possono nascere diritti di sorta in capo al lavoratore [11].

Analoghe cadenze, anche se in una motivazione più sintetica, si ritrovano in una pronuncia del Tribunale di Torino resa nel 2006 [12]: la personalità dell'indirizzo di posta elettronica attribuito ad un dipendente non comporta la segretezza dei messaggi dallo stesso inviati e non configura, pertanto, il reato di violazione di corrispondenza la condotta del datore di lavoro che li legga accedendo alla relativa casella e ciò in quanto i beni aziendali sono affidati ai dipendenti esclusivamente per ragioni di servizio.

Sulla medesima vicenda torinese arriva a pronunciarsi, nel 2007, anche la sezione quinta della Cassazione [13], la quale, con una sentenza che ha immediatamente guadagnato popolarità, afferma che è la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite. Sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti e quando, in particolare, il sistema telematico sia pro-

[10] Al contrario, nel *Documento di lavoro* adottato il 29 maggio 2002 dal c.d. Gruppo dell'art. 29 si legge che « in ogni caso l'ubicazione e la proprietà del mezzo elettronico utilizzato non escludono la segretezza delle comunicazioni e della corrispondenza, quale sancita da principi giuridici fondamentali e costituzionali ».

[11] Adesivamente L. C. Natali-A. I. Natali, *Cessione d'azienda: uso della casella di posta dell'ex dipendente*, in *Dir. e pratica lav.*, 2010, 2005 e A. I. Natali, *Controllo del datore di lavoro sulle cartelle personali del lavoratore*, in *Dir. e pratica lav.*, 2011, 1273 ss.

[12] Tribunale di Torino — Sezione distaccata di Chivasso, 20 giugno 2006-15 settembre 2006, n. 143, in *Dir. internet*, 2007, 275 ss. con nota di M. Violante, *E-mail aziendale? Solo per lavoro*.

[13] Cass., sez. V, 11 dicembre 2007-19 dicembre 2007, n. 47096, in *Dir. pen. proc.*, 2008, 1425 ss. con commento di G. Andreazza, *Posta elettronica sul* computer *del lavoratore e limiti di conoscibilità del datore di lavoro*; in *Guida dir.*, 2008, 3, 77 ss. con nota di C. Petrucci-S. Taddei, *Solo un'adeguata* policy *aziendale può tutelare imprenditore e lavoratori*; in *Cass. pen.*, 2008, 4669 ss. con nota di S. Aterno.

tetto da una *password*, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che dispongano della chiave informatica di accesso [14].

La Corte di Cassazione, innovando rispetto ai precedenti di merito, che non si erano curati di dare "copertura giuridica" alle conclusioni raggiunte, fonda dunque il verdetto assolutorio sulla mancanza di tipicità del contegno datoriale: la corrispondenza elettronica non può considerarsi "chiusa" nei confronti del datore di lavoro che, attraverso un regolamento aziendale, si sia riservato il diritto di accedervi.

4. Critica.

La via prescelta dalla Corte di Cassazione, apprezzata da alcuni [15], si espone — a nostro avviso — ad alcune considerazioni critiche.

I dubbi maggiori s'appuntano sulla qualificazione del fatto come "non tipico". Secondo la Corte, la presenza di un regolamento interno, sufficientemente diffuso tra i lavoratori, che preveda il deposito delle *password* presso il superiore e ribadisca la destinazione aziendalistica dell'*account*, priverebbe la comunicazione elettronica spedita al lavoratore della qualità di corrispondenza "chiusa".

Il limite di una tale conclusione è evidente. In questo modo la qualificazione della corrispondenza come "chiusa" o "aperta" viene a dipendere da un comportamento (eventualmente) tenuto dal superiore gerarchico del destinatario. È rimesso, in sostanza, all'impresa titolare dell'*account* il potere di decidere, attraverso un regolamento interno, se l'e-mail possa essere letta da soggetti diversi dalla persona cui la stessa è indirizzata. Situazione, questa, esattamente opposta a quella che si registra in ambito cartolare, in cui è invece pacifico che debba considerarsi "chiusa" la corrispondenza che *il mittente* abbia deciso di inviare ad un *numerus clausus* di destinatari.

Stante il tenore letterale dell'art. 616 c.p., spetta *al mittente* decidere la natura "aperta" o "chiusa" della corrispondenza. È in ragione dalle scelte di questi che assume rilevanza penale la condotta di chi legga il messaggio. Un soggetto *terzo rispetto alla*

[14] Nel caso specifico il datore di lavoro, ottemperando alle prescrizioni del provvedimento del Garante per la protezione dei dati personali del 1° marzo 2007, aveva richiesto che i dipendenti comunicassero in busta chiusa ai propri superiori gerarchici la *password* utilizzata per accedere al *computer* dato loro in dotazione.

[15] E. Barraco-A. Sitzia, *Il problema dei "controlli difensivi" del datore di lavoro:* estne saepe ius summum malitia*?*, in *Il lavoro nella giurisprudenza*, 1005 ss.

comunicazione non può decidere di qualificarsi come destinatario *implicito* di un messaggio *a lui non diretto* [16].

Non è questione di "aspettativa di riservatezza" o di "proprietà del mezzo", ma di ricostruzione del fatto tipico. La modalità (elettronica) della comunicazione o il contesto (lavorativo) nella quale essa avviene non sono fattori tali da permettere di superare il chiaro dato normativo.

Affermare il contrario, ovvero ipotizzare che un soggetto *diverso dal destinatario* (benché suo superiore) possa decidere della segretezza di un messaggio *a lui non diretto*, travalica il limite dell'inviolabilità della corrispondenza e quindi contraddice l'art. 15 della Costituzione [17].

5. L'assenza di antigiuridicità quale soluzione alternativa.

5.1. *Applicabilità della scriminante del consenso dell'avente diritto.*

Il ragionamento sul piano della tipicità rende incerta l'argomentazione assolutoria. Trattandosi di una questione di bilanciamento di interessi, approdi sistematicamente più convincenti possono essere raggiunti sul piano dell'antigiuridicità.

Va esplorata la possibilità che, nel caso di specie, possano trovare applicazione la scriminante del consenso dell'avente diritto oppure, in alternativa, quella dell'esercizio di un diritto.

Poiché la segretezza delle comunicazioni deve ritenersi un diritto disponibile, come anche testimoniato dal regime di procedibilità a querela, potrà essere invocato l'art. 50 c.p. in presenza di una liberatoria sottoscritta dal dipendente nella quale sia chiara-

[16] Rileva questo aspetto anche G. Andreazza, *Posta elettronica sul* computer *del lavoratore e limiti di conoscibilità del datore di lavoro*, cit., 1428.

[17] Fanno eccezione i casi in cui l'indirizzo di posta elettronica del destinatario sia del tutto generico (ad esempio: *info@nomeazienda.it*) — in tal caso il destinatario è a conoscenza del fatto che il messaggio potrà essere letto da tutti coloro che, secondo l'organizzazione aziendale del titolare dell'*account* (che egli può anche sconoscere), abbiano accesso a quell'indirizzo — ovvero l'ipotesi — peraltro espressamente considerata dal Garante nella propria *Deliberazione* dell'1 marzo 2007 — in cui i messaggi di posta elettronica contengano un avvertimento in cui si precisi che le risposte potranno essere conosciute dall'organizzazione di appartenenza del mittente. In quest'ultima situazione chi *risponde* ad una e-mail recante un tale *disclaimer*, sa che si renderà mittente rispetto ad una comunicazione diretta sia all'interlocutore cui dà riscontro, sia ad altre persone legittimate a visionare quel messaggio. In detti contesti il datore di lavoro sarà dunque legittimato alla lettura dei messaggi di posta elettronica. Tale rappresenta, però, non una deroga, bensì una corretta applicazione dell'art. 616 c.p.: in queste ipotesi, infatti, la corrispondenza è indirizzata pur sempre ad un *numerus clausus* di destinatari (nel quale è compreso, questa volta, anche il datore di lavoro) e la sua qualificazione come "chiusa" dipende sempre dal mittente (che, edotto della *policy* aziendale, sa che ogni e-mail inviata al dipendente suo corrispondente potrà essere letta anche dal superiore).

mente specificato che il datore di lavoro è legittimato a prendere cognizione della corrispondenza inviata al lavoratore [18].

Quanto alle modalità di espressione del consenso, va chiarito che alla lettura della corrispondenza non è applicabile il disposto dell'art. 4, comma 2 dello Statuto dei Lavoratori. La mera presa di cognizione di una o più e-mail si sostanzia, infatti, in un comportamento che, per essere realizzato, non abbisogna di alcun "impianto" o "apparecchiatura" di controllo [19]. Né la rappresentanza sindacale aziendale o la Direzione Territoriale del Lavoro sono soggetti legittimati ad esprimere un consenso scriminante, non essendo titolari (nemmeno per rappresentazione) del diritto rinunciato [20].

Ammessa la disponibilità del bene giuridico tutelato ed esclusa la necessità di ricorrere alle forme previste dalla L. n. 300/1970, si può quindi fondatamente sostenere che sia tipica ma scriminata la condotta del datore di lavoro che acceda ad un *account* dato in uso al lavoratore forte del previo libero ed informato consenso di questi.

I limiti di operatività di questa scriminante non sono giuridici ma fattuali, poiché dovrà essere attentamente verificata, caso per caso, la completezza dalla previa informativa datoriale e l'effettiva libertà del lavoratore. In sostanza, ha efficacia scriminante solo il consenso prestato dal lavoratore che è libero di rifiutarlo; il che — è verosimile pensare — accade di rado [21].

5.2. *Applicabilità della scriminante dell'esercizio del diritto.*

L'altra causa di giustificazione che può assumere rilievo nel caso che ci occupa è quella dell'esercizio del diritto. Con riferimento a tale scriminante le coperture normative sono ben individuabili, mentre piuttosto selettivi sono i presupposti fattuali in presenza dei quali essa può operare. Riteniamo, infatti, che, non ostante la natura comunemente definita "non penale" delle cause di giustificazione, l'operatività della scriminante dell'esercizio del diritto

---

[18] L'applicabilità dell'art. 50 c.p. è ammessa da C. Pecorella-R. De Poti, *Impiego dell'elaboratore sul luogo di lavoro e tutela penale della* privacy, in *www.penalecontemporaneo.it*, 2011, 14 s. e, nella dottrina giuslavoristica, da E. Barraco-A. Sitzia, *Il problema dei "controlli difensivi" del datore di lavoro*, cit., 1006, note 53 e 54.

[19] Un *server mail* è un impianto informatico che, di per sé, non permette il controllo del lavoratore: tale controllo è conseguenza di un'attività specificamente posta in essere dal datore di lavoro. Il controllo sull'uso degli strumenti informatici e la lettura dell'e-mail del dipendente sono invece posti sullo stesso piano da Cass. civ., sez. lavoro, 23 febbraio 2010, n. 4375.

[20] *Contra* C. Pecorella-R. De Poti, *Impiego dell'elaboratore sul luogo di lavoro e tutela penale della* privacy, cit., 15 s.

[21] Nel Parere n. 8/2011 reso dal Gruppo dell'art. 29 si ritiene "debole" la tutela del consenso tutte le volte in cui il lavoratore non sia effettivamente libero di prestarlo o negarlo. Anche nel provvedimento del Garante n. 13 dell'1 marzo 2007 si dedica ampio spazio al profilo della compiuta informazione da fornire al dipendente ai sensi dell'art. 13 del D.Lgs. n. 196/2003.

vada circoscritta entro i limiti tracciati dalla norma che quel medesimo diritto prevede e disciplina; il che — come subito si vedrà — comporta, nel caso di specie, alcune ristrettezze applicative.

Tre le situazioni in cui si può invocare l'esercizio di un diritto: l'adozione di un disciplinare interno conforme a quello suggerito dal Garante per i dati personali nel provvedimento del 1º marzo 2007 [22]; l'implementazione di un sistema di trattamento informatico dei dati personali conforme all'Allegato B del T.U. *privacy* in materia di misure minime di sicurezza; il ricorso ai controlli difensivi.

Nel primo caso il diritto nasce dell'art. 24, comma 1, lett. *g*) del D.Lgs. n. 196/2003, ma ha limiti ben precisi. Prescrive l'*Authority* che per le assenze programmate il lavoratore debba attivare messaggi di *reply* automatico con l'indicazione di un altro soggetto cui rivolgersi o di modalità alternative di contatto dell'azienda; per le assenze non programmate, qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), vi potrà provvedere il titolare del trattamento (sempre che ciò sia necessario, mediante personale appositamente incaricato ed avvertendo gli interessati) oppure i messaggi di posta elettronica indirizzati al dipendente potranno essere letti da un suo collega, previamente individuato ed al quale sia stato affidato il compito di inoltrare al titolare del trattamento le comunicazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa.

La scriminante ha dunque una marcata connotazione procedurale, che, a rigore, ne limita l'ambito applicativo.

La seconda possibilità consiste nell'invocare il punto 10 dell'Allegato B al T.U. *privacy*. Significative, però, anche in questo caso, le incombenze formali da rispettare: le disposizioni per l'accesso devono essere scritte, preventive, idonee, volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici. Del pari l'accesso ai dati può avvenire in caso di prolungata assenza o impedimento dell'incaricato e quando sia indispensabile e indifferibile intervenire per necessità operative e di sicurezza del sistema. In ogni caso, l'incaricato deve essere tempestivamente informato dell'intervento effettuato.

---

[22] La *Delibera* n. 13 dell'1 marzo 2007 — *Linee guida per posta elettronica e Internet* (doc. web n. 1387522), è pubblicata nella Gazzetta Ufficiale del 10 marzo 2007, n. 58 ed in *Foro it.*, 2007, III, 214 ss. Nel settore pubblico le indicazioni del Garante sono state riprese all'interno della Direttiva n. 2 del 16 maggio 2009 adottata dalla Presidenza del Consiglio dei Ministri. In dottrina si registra un generale apprezzamento per il provvedimento generale del Garante, ma la maggioranza degli Autori non sembra porsi il problema dell'inquadramento giuridico del disciplinare interno che in quello si suggerisce di adottare. Questo problema non sfugge, invece, a P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *Riv. it. dir. lav.*, 2009, 340.

Circa, infine, il ricorso ai controlli difensivi, intendendosi per tali quelli posti in essere dal datore di lavoro che abbia già sentore della illegittima condotta del dipendente, qui il diritto nasce dal combinato disposto degli artt. 2086 e 2104 c.c., ma, stante l'inevitabile fluidità della lettura giurisprudenziale in argomento, è veramente complesso capire quando si sia in presenza di controlli legittimi (e quindi scriminanti) o quando, invece, si sia in presenza di controlli vietati [23].

Ciò a tacere del fatto che la connotazione della scriminante dell'esercizio del diritto è tipicamente oggettiva, mentre l'elemento di legittimità del controllo difensivo è tutto ancorato alla finalità per la quale viene eseguito.

Il quadro globale è quindi molto più complesso di quello che la giurisprudenza lascia intendere. Da un lato l'argomentazione in chiave di tipicità non è priva di profili critici; dall'altro, invocare le cause di giustificazione di cui agli artt. 50 e 51 c.p. garantisce un approdo ermeneutico dogmaticamente più saldo, ma impone anche di confrontarsi con notevoli ristrettezze applicative (giuridiche o fattuali).

A nostro avviso il problema, *de lege lata*, va risolto facendo una puntuale applicazione tanto della norma sanzionatoria, senza ingiustificate restrizioni dei limiti del fatto tipico, quanto delle scriminanti astrattamente applicabili, avendo anche qui l'accortezza di rispettare i purtroppo angusti confini del dato normativo.

De lege ferenda non pare inopportuno un intervento chiarificatore del legislatore, eventualmente anche con un avallo della soluzione già offerta dalla giurisprudenza quando non ci si voglia impegnare in una più compiuta regolamentazione delle nuove forme di controllo datoriale.

---

[23] Una ricostruzione del quadro giurisprudenziale in materia di "controlli difensivi" si ritrova in Cass. civ., sez. lavoro, 1 ottobre 2012, n. 16622. Nella giurisprudenza recente Cass. civ., sez. lavoro, 23 febbraio 2012, n. 2722 ha ritenuto legittimo il controllo effettuato *ex post* sugli strumenti informatici; Cass. civ., sez. lavoro, 18 gennaio 2011, n. 2117 ha ammesso come prova le videoriprese effettuate da un soggetto diverso dal datore di lavoro; Cass. civ., sez. lavoro, 18 novembre 2010, n. 23303 non vede ostacoli nell'impiego di agenzie di investigazione per effettuare controlli sui lavoratori (analogamente: Cass. civ., sez. lavoro, 12 giugno 2002, n. 8388); Cass. civ., sez. lavoro, 23 febbraio 2010, n. 4375 e Cass. civ., sez. lavoro, 17 luglio 2007, n. 15892 ritengono, invece, violato l'art. 4 St. Lav. nel caso di installazione di un *software* di monitoraggio (denominato *Super Scout*) e nell'impiego di *badge* per l'accesso al parcheggio aziendale. Sulla qualificazione dei controlli difensivi inzialmente quale *tertium genus*, intermedio tra i controlli vietati (art. 4, comma 1 St. Lav.) ed i controlli c.d. preterintenzionali (art. 4, comma 2 St. Lav.) e più recentemente quale *species* di questi ultimi, v. P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, cit., 327 ss., la quale pure parla di un indirizzo giurisprudenziale che lascia « margini di ambiguità ». In argomento anche R. Imperiali-R. Imperiali, *Controlli sul lavoratore e tecnologie*, Milano, Giuffrè, 2012, 173 ss.; M. Miscione, *I controlli intenzionali, preterintenzionali e difensivi sui lavoratori in contenzioso continuo*, in *Il lavoro nella giurisprudenza*, 2013, 761 ss.

6. I limiti applicativi dell'art. 616 c.p. Il problema della lettura di e-mail archiviate su *server*.

L'art. 616 c.p. — si è visto — è la norma più invocata dalla giurisprudenza penale che si è occupata del problema del controllo datoriale. Il riferirsi a tale norma pone però un problema, che finora pare passato sotto silenzio.

In tema di corrispondenza epistolare, un certo orientamento ritiene che la tutela della segretezza venga meno nel momento in cui il destinatario apra la missiva a lui indirizzata [24]. Se tanto dovesse valere anche per la corrispondenza telematica — e così potrebbe sostenersi in virtù dell'equivalenza di cui al comma 4 dell'art. 616 c.p. —, si dovrebbe concludere che non costituisca "presa di cognizione" la lettura, da parte del datore di lavoro, di messaggi di posta elettronica già aperti dal dipendente ed archiviati sul *server* aziendale. Situazione, questa, comune a tutti i casi sopra citati.

Due, ed antitetiche, le soluzioni possibili.

La prima consiste nel ritenere che l'orientamento riferito possa essere superato in virtù del fatto che una tale soluzione ermeneutica non è, in realtà, univocamente imposta dal dato normativo. Il concetto di "corrispondenza chiusa, a lui non diretta" si presta, infatti, ad essere interpretato in maniera estensiva fino a ricomprendere nell'ambito della tutela giuridica della norma non solo il privilegio ad "aprire per primi la busta", ma pure il successivo diritto a mantenere riservato il contenuto della comunicazione. Così l'aggettivo "chiusa" si adatterebbe a descrivere tanto la corrispondenza inserita in una busta ancora sigillata (interpretazione minima e fattuale) quanto la corrispondenza che, indipendentemente dalla sua lettura, il mittente abbia voluto riservare ad un numero determinato di destinatari (interpretazione estensiva e teleologica). In favore di questa soluzione depone il fatto che il codice Rocco, a differenza del codice Zanardelli, sanzioni la "presa di cognizione" anziché l'"apertura" della corrispondenza chiusa.

Se — come pensiamo — va escluso che chiunque possa visionare una lettera che il destinatario abbia già letto ma poi anche risposto all'interno della busta che la conteneva, dobbiamo allora ritenere che possa qualificarsi come tipica la condotta di chi prenda cognizione di un messaggio e-mail a lui non diretto pur dopo che il destinatario di quello ne abbia avuto contezza.

La soluzione alternativa — secondo la quale « una lettera

[24] P. Dubolino-P. L. Vigna, voce *Segreto (reati in materia di)*, in *Enc. Dir.*, vol. XLI, 1989, par. 39. Analogamente giurisprudenza risalente: Cass., sez. II, 30 giugno 1950, Dorigatti, in *Giust. pen.*, 1951, II, 74. Sul punto, v. G. Amato, *Art. 616*, in T. Padovani (a cura di), *Codice penale. Tomo II*, Milano, Giuffrè, 2007, 3787.

dissuggellata e aperta dal destinatario diventa per ciò stesso un "documento" cessando nel contempo di essere "corrispondenza" » [25] — induce ad escludere la condotta ora descritta dall'area di operatività della disposizione sanzionatoria in commento. Pertanto, ad essere fedeli alla tradizione interpretativa, dovrà farsi applicazione della norma residuale di cui all'art. 167 del D.Lgs. n. 196/2003 anziché dell'art. 616 c.p. [26].

7. Il problema del concorso apparente di norme.

Un altro aspetto tendenzialmente trascurato dai commentatori riguarda il rapporto tra il reato di violazione, sottrazione e soppressione di corrispondenza ed altri reati che, in virtù della clausola di sussidiarietà espressa contenuta nell'art. 616 c.p. (« se il fatto non è preveduto come reato da altra disposizione di legge »), devono invece trovare applicazione.

Vengono innanzi tutto in rilievo le fattispecie di cui agli artt. 617-*quater* e 617-*quinquies* c.p. [27]. La prima sanziona chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa, mentre la seconda si occupa di chi, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Il regime sanzionatorio — rispettivamente da sei mesi a quattro anni e da uno a quattro anni — è estremamente più gravoso di quello previsto dall'art. 616 c.p. (reclusione fino ad un anno o multa da 30 a 516 euro) e coinvolge sia la persona fisica che, eventualmente, l'ente alla quale essa afferisca (v. art. 24-*bis* del D.Lgs. n. 231/2001).

I problemi di coordinamento sistematico sono evidenti: che differenza c'è tra la condotta di "intercettare", "impedire", "interrompere", prevista dall'art. 617-*quater* c.p., e la condotta di

---

[25] P. Dubolino-P. L. Vigna, voce *Segreto (reati in materia di)*, cit., *ibidem*.

[26] La lettura di un'e-mail implica sicuramente un "trattamento" di "dati personali" (per le definizioni di tali termini si veda l'art. 4, comma 1, lett. *a*) e lett. *b*) del D.Lgs. n. 196/2003) che, se posto in essere senza il consenso previsto dall'art. 23 ovvero al di fuori dei casi di esenzione dal consenso di cui all'art. 24, può integrare il reato di trattamento illecito di dati (ammesso che si verifichi un nocumento e che la condotta sia sorretta dal dolo specifico di profitto o danno).

[27] In argomento: D. Fondaroli, *La tutela penale dei "beni informatici"*, in questa *Rivista*, 1996, 315 ss.; C. Pecorella, *Diritto penale dell'informatica*, Padova, Cedam, 2006, 302 ss.; V. Plantamura, *La tutela penale delle comunicazioni informatiche e telematiche*, in questa *Rivista*, 2006, 847 ss. La giurisprudenza sul punto è piuttosto scarsa: sull'art. 617-*quater* c.p., v. Cass., sez. V, 6 luglio 2007-31 luglio 2007, n. 31135, in *Dir. e pratica lav.*, 2007, 2508 ss. e Cass., sez. V, 19 maggio 2005-1 febbraio 2006, n. 4011, annotata da F. Cajani, in *Dir. Internet*, 2006, 250 ss.; sull'art. 617 *quinquies* c.p., v. Cass., sez. V, 9 luglio 2010-13 ottobre 2010, n. 36601 e Cass., sez. V, 12 gennaio 2011-18 febbraio 2011, n. 6239.

"sottrarre" o "distrarre", contemplata dall'art. 616 c.p.? L'istallazione di un semplice *foward* automatico che permetta al datore di lavoro di leggere la corrispondenza indirizzata al lavoratore è inquadrabile come un'"intercettazione di comunicazione", punita con la reclusione da sei mesi a quattro anni, oppure come "distrazione di corrispondenza", punita con la reclusione fino ad un anno oppure solo con la multa?

È vero che questo problema si pone esclusivamente nel caso in cui la condotta abbia ad oggetto una comunicazione *in fieri* — quando la comunicazione è giunta al *server* del destinatario non è, infatti, più "intercettabile" — ma, almeno in questo caso, la specialità degli artt. 617-*quater* e 617-*quinquies* c.p. ed il maggior carico sanzionatorio inducono a ritenere applicabili solo tali disposizioni.

In secondo luogo, la "lettura" di un messaggio di posta elettronica ovvero il suo salvataggio quale futura base, ad esempio, per una contestazione disciplinare costituiscono un "trattamento dei dati personali". Di qui l'applicabilità dell'art. 167 del D.Lgs. n. 196/2003 sia quando manchi una *policy* aziendale e difetti il consenso del lavoratore alla lettura dell'e-mail, sia quando, pur in presenza di un disciplinare interno conforme alle indicazioni del Garante, non sia stato rispettato l'obbligo di sufficiente informazione di cui all'art. 13 del T.U.: in entrambi i casi, infatti, il trattamento deve considerarsi eseguito "in violazione di quanto disposto dall'art. 23" [28] ed, anche in questa situazione, la clausola di sussidiarietà dell'art. 616 c.p. ha la "prevalenza" su quella dell'art. 167 T.U. *privacy* (« salvo che il fatto costituisca più grave reato »).

Infine, nel caso in cui non esista alcun regolamento aziendale interno e l'indirizzo e-mail sia concesso in uso esclusivo al dipendente, il datore di lavoro che vi acceda commetterà, con tutta probabilità, un reato di accesso abusivo a sistema informatico, punito, quanto alla persona fisica, con la reclusione fino a tre anni (art. 615-*ter* c.p.) e, quanto all'ente, con la sanzione da cento a cinquecento quote (art. 24-*bis*, comma 1 del D.Lgs. n. 231/2001) [29].

---

[28] L'art. 23 del D.Lgs. n. 196/2003 prevede che « il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato ». Il provvedimento generale adottato dal Garante l'1 marzo 2007 introduce una deroga a tale principio, rilevante ai sensi dell'art. 24, comma 1, lett. *g*) del Testo Unico. Le prescrizioni ivi contenute — compresa quella della sufficiente e chiara informazione *ex* art. 13 T.U. — diventano perciò elementi negativi del fatto tipico del reato previsto all'art. 167.

[29] La presenza di un regolamento interno ai fini della configurabilità del reato di accesso abusivo è stata ritenuta rilevante da Cass. pen., Sezioni Unite, 27 ottobre 2011-7 febbraio 2012, n. 4694. La pronuncia è stata commentata da R. Bartoli, *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Dir. pen. cont. (riv. trim.)*, 2012, 123 ss., R. Flor, *L'introdu-*

8. Il regime sanzionatorio delle altre forme di controllo datoriale illegittimo.

Le altre forme di controllo datoriale a mezzo di strumenti informatici, diverse dalla lettura della corrispondenza, trovano disciplina, *in primis*, nell'art. 4 della L. n. 300/1970.

Ai sensi di tale disposizione è vietata l'installazione di apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (comma 1) mentre le apparecchiature di controllo che siano richieste da esigenze organizzative o produttive ovvero dalla sicurezza del lavoro possono essere installate, ma solo previo accordo con le Rappresentanze Sindacali Aziendali oppure con la Direzione Territoriale del Lavoro (comma 2).

Quanto ai profili squisitamente sanzionatori, fino al 2003 l'art. 38 dello Statuto dei Lavoratori prevedeva la sanzione dell'ammenda da 300.000 lire a 3.000.000 o l'arresto da 15 giorni ad un anno per la violazione degli artt. 2, 4, 5, 6, 8 e 15. Con l'adozione del D.Lgs. n. 196/2003 il richiamo agli artt. 4 ed 8 è stato soppresso cosicché la disciplina sanzionatoria si trova oggi nell'art. 171 del T.U. La norma prevede che *« la violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della Legge 20 maggio 1970, n. 300 »*; l'art. 113, che, per inciso, ha un solo comma, recita *« resta fermo quanto disposto dall'articolo 8 della Legge 20 maggio 1970, n. 300 »*, mentre l'art. 114 ribadisce che *« resta fermo quanto disposto dall'articolo 4 della Legge 20 maggio 1970, n. 300 »*.

Sul piano della successione di leggi penali nel tempo, non si sono posti particolari problemi: si tratta, evidentemente, di un'ipotesi di continuità normativa, disciplinata dal comma 4 dell'art. 2 c.p. in quanto le condotte tipiche sono esattamente le stesse e medesimo è anche il regime sanzionatorio. Quel che viene meno è solo

---

zione abusiva ed il mantenimento non autorizzato in un sistema informatico nella recente sentenza delle Sezioni Unite: "abuso" dei profili autorizzativi, "abuso" dei poteri del pubblico ufficiale e violazione dello jus excludendi alios, in *Ciberspazio e diritto*, 2012, 93 ss.; I. Salvadori, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite delimitano l'ambito di applicazione dell'art. 615* ter *c.p.*, in *Riv. trim. dir. pen. econ.*, 2012, 369 ss. Per il dibattito sviluppatosi in precedenza, si confrontino le note a Cass. pen., sez. V, 29 maggio 2008-3 luglio 2008, n. 26797 di S. Civardi, *La distinzione fra accesso abusivo a sistema informatico ed abuso dei dati acquisiti*, in questa *Rivista.*, 2009, 58 ss. e R. Flor, *L'accesso per finalità illecite ad un sistema informatico o telematico da parte di soggetto autorizzato*, in *Cass. pen.*, 2009, 1502 ss. e le note a Cass. pen., sez. V, 16 febbraio 2010-21 maggio 2010, n. 19463 di E. Mengoni, *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo* round *alla configurabilità del reato*, in *Cass. pen.*, 2011, 2200 ss. e di S. De Flammineis, *Art. 615-*ter *c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico*, in *Cass. pen.*, 2011, 2209 ss. Sui profili più strettamente connessi alla responsabilità degli enti, si veda G. Corrias Lucente, *Introduzione dell'art. 24* bis *del decreto legislativo 8 giugno 2001, n. 231*, in G. Corasaniti-G. Corrias Lucente (a cura di), *Cybercrime, responsabilità degli enti, prova digitale*, Padova, Cedam, 2009, 151 ss.

la clausola di sussidiarietà espressa: prevista dall'art. 38 St. Lav., ma non replicata dall'art. 171 T.U. *privacy*. Non si è trattato, quindi, di un'*abolitio criminis*, bensì di un'*abrogatio sine abolitio* [30].

Sul piano del bene giuridico, la nuova collocazione non sembra avere ricadute particolari: le fattispecie sanzionatorie in materia di trattamento dei dati personali tutelano diversi interessi, connessi ora in maniera più forte ora in maniera più labile con il bene giuridico della riservatezza [31]. Anche l'art. 171 non fa eccezione: la condotta tipica consiste nella violazione dell'art. 4 St. Lav., cosicché, si può fondatamente sostenere che il bene giuridico tutelato vada ravvisato, anche dopo il 2003, nella dignità del lavoratore. Il senso dell'art. 4, infatti, è che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, non vada esasperata dall'uso delle tecnologie, ma mantenuta in una dimensione "umana" e tollerabile.

La novità della scelta operata dal legislatore del 2003 va allora ravvisata sul piano sistematico. La nuova collocazione sia della normativa prescrittiva (art. 114 T.U.) che di quella sanzionatoria (art. 171 T.U.) ha concrete ricadute di ordine pratico: ai fini del legittimo esercizio del controllo datoriale non è oggi più sufficiente rispettare il disposto dell'art. 4 St. Lav., ma si deve prestare attenzione anche all'intera normativa di cui al D.Lgs. n. 196/2003. D'altronde, è pressoché inevitabile che un monitoraggio tecnologico si traduca anche in un "trattamento" di "dati personali" [32].

Dal che deriva, innanzi tutto, che anche ai fini giuslavoristici assumono rilevanza i pronunciamenti dell'*Authority* ed, in particolare, per quel che qui interessa, i provvedimenti generali sull'uso dei sistemi informatici (1º marzo 2007), sui sistemi di videosorveglianza (8 aprile 2010) e sui sistemi di localizzazione dei veicoli (4 ottobre 2011 [33]).

Tali provvedimenti, oltre ad introdurre delle deroghe espresse

---

[30] In proposito, Cass., sez. III, 24 settembre 2009-16 ottobre 2009, n. 40199, in *Dir. e pratica lav.*, 2009, 2664 ss.

[31] Lo stesso art. 167, norma cardine del sistema sanzionatorio previsto dal D.Lgs. n. 196/2003, si ritiene tuteli non la riservatezza in sé, bensì la correttezza del trattamento dei dati: *id est* il rispetto delle norme civili dettate a tal fine. Su questo aspetto specificamente P. Veneziani, *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in L. Picotti (a cura di), *Il diritto penale nell'epoca di internet*, Padova, Cedam, 2004, 183 ss. e S. Cagli, *La rilevanza del consenso nella disciplina penale del trattamento dei dati personali*, *ibidem*, 277 ss.

[32] Raggiunge conclusioni analoghe P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, cit., 332: « il potere datoriale deve superare un appropriato *test* di legittimità non solo riguardo alle condizioni ed alle modalità di esercizio stabilite all'art. 4 St. Lav., ma anche sotto il profilo della raccolta delle informazioni relative al lavoratore ».

[33] Anche tale provvedimento è stato preceduto da uno studio del "Gruppo dell'art. 29": v. *Parere n. 13/2011 — WP 185 sui servizi di geolocalizzazione su disposi-*

al principio del consenso nel trattamento dei dati personali (artt. 23 e 24, comma 1, lett. *g*) del T.U. *privacy*), hanno l'effetto di integrare l'art. 4 St. Lav. Quest'ultima disposizione ammette in generale l'installazione di "impianti ed apparecchiature di controllo richiesti da esigenze produttive o organizzative", ma sono poi i regolamenti del Garante che, nel dettaglio, specificano quali "impianti" (informatici, di geolocalizzazione, di videocontrollo) e quali "esigenze" (funzionali, operative, di sicurezza) vengono concretamente in rilievo e provvedono quindi al bilanciamento tra opposti interessi. Gli interventi dell'autorità amministrativa « seguono [cioè] una direzione incrementale che rafforza il quadro regolativo, integrando i presupposti di legittimità fissati dallo Statuto con i principi cogenti in materia di trattamento dei dati » [34].

Riconoscere che il controllo datoriale integri un'ipotesi di trattamento di dati personali rende infine applicabili, anche in tale contesto, le disposizioni amministrative e penali pensate per la repressione di trattamenti illegittimi. Di conseguenza il datore di lavoro che effettui un controllo occulto sui lavoratori contravvenendo allo Statuto dei Lavoratori ed al T.U. *privacy* potrà essere sanzionato sia ai sensi dell'art. 171 T.U., che — come detto — è norma posta a tutela della dignità del lavoratore, sia in virtù dell'art. 167 T.U., che presidia il regolare trattamento dei dati personali, sia, infine, ai sensi delle norme del T.U. che prevedono sanzioni amministrative per l'omessa informativa (art. 161) ovvero, « in ogni caso », per le condotte di illecito trattamento (art. 162, comma 2-*bis*). Per contro, qualora i *vademecum* del Garante siano scrupolosamente osservati, nessuna di tali fattispecie sanzionatorie potrà ritenersi configurata, divenendo quelli elementi negativi del fatto tipico previsto da queste.

---

tivi mobili intelligenti, adottato il 16 maggio 2011.

[34] Così P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, cit., 332. Non solo il Garante, nei propri provvedimenti generali o specifici (tra i secondi si vedano, ad esempio, il provvedimento del 26 febbraio 2009 in tema di videosorveglianza; il provvedimento del 2 aprile 2009 in tema di monitoraggio degli accessi ad internet da parte del dipendente — caso *Squid* —; il provvedimento del 15 ottobre 2009 in tema di uso di rilevazioni biometriche; i provvedimenti del 10 giugno 2010 e del 17 novembre 2011, ancora in tema di videosorveglianza), fa salva la procedura "negoziata" con le RSA o le DTL, ma accade anche il contrario. Nel nota prot. n. 37/0007162/MA008.A002 emanata il 16 aprile 2012 dal Direttore Generale per l'Attività Ispettiva del Ministero del Lavoro e delle Politiche Sociali viene espressamente previsto che l'autorizzazione all'installazione di videocamere deve intendersi subordinata al rispetto della disciplina dettata dal D.Lgs. n. 196/2003 e dal provvedimento del Garante dell'8 aprile 2010 in tema di videosorveglianza. Il provvedimento autorizzativo — continua la nota — dovrà prescrivere il rispetto tanto delle disposizioni contenute nello Stattuo dei Lavoratori quanto della normativa sul trattamento dei dati personali.

9. (*Segue*). Le applicazioni giurisprudenziali.

La giurisprudenza penale in punto di art. 38 dello Statuto dei Lavoratori non è molta.

Ciò probabilmente è dovuto al fatto che si tratta di una contravvenzione punita — almeno nella sua forma base — con l'arresto "o" l'ammenda. Si può, quindi, applicare l'istituto dell'oblazione discrezionale o facoltativa di cui all'art. 162-*bis* c.p., anche se per beneficiarne è necessario che le conseguenze dannose o pericolose del reato siano state eliminate: ovvero che lo strumento di controllo sia stato rimosso o che il suo mantenimento sia stato concordato con le RSA o la DTL.

Le tematiche sopra descritte sono state così affrontate soprattutto in chiave processuale. In particolare, nel 2006 [35], nel 2010 [36] e ancora nel 2011 [37] la Corte di Cassazione si è trovata ad affrontare il problema dell'utilizzabilità, ai fini decisori, delle immagini raccolte mediante un sistema di videocontrollo installato per accertare sottrazioni di denaro dalla cassa di un negozio. La questione è stata risolta in senso affermativo richiamando espressamente l'orientamento giuslavoristico, secondo cui gli artt. 4 e 8 St. Lav. non vietano i c.d. controlli difensivi tesi alla difesa del patrimonio aziendale da azioni delittuose [38].

Merita invece specifica menzione una recente sentenza della terza sezione della Suprema Corte [39] secondo la quale l'installazione di un sistema di videosorveglianza può essere scriminato dal consenso prestato dai lavoratori.

Nel caso specifico tutti i dipendenti avevano assentito all'installazione delle videocamere attraverso la sottoscrizione di un documento esplicito. Ritiene allora il Supremo Collegio che « se è vero — come è innegabile — che la disposizione di cui all'art. 4 St.

[35] Cass., sez. III, 15 dicembre 2006-27 febbraio 2007, n. 8042, in *Dir. e pratica lav.*, 2007, 816 ss.: « devono ritenersi certamente fuori dall'ambito di applicazione della norma [di cui all'art. 4 St. Lav.] i controlli diretti ad accertare condotte illecite del lavoratore (i c.d. controlli difensivi) ».

[36] Cass., sez. V, 18 marzo 2010-1 giugno 2010, n. 20722, in *Dir. e pratica lav.*, 2010, 1775 ss.

[37] Cass., sez. V, 12 luglio 2011-16 settembre 2011, n. 34842, in *Dir. e pratica lav.*, 2011, 2416 ss. ed in *Cass. pen.*, 2012, 1432 con osservazioni di A. Mari, il quale dà conto del difficile inquadramento (come prova atipica, prova documentale o intercettazione) delle videoriprese effettuate dal privato. Sul tema delle videoriprese di atti non aventi contenuto comunicativo: A. Spinelli, *Videoregistrazioni: tra prove atipiche e deficit di tutela della Cassazione* (nota a Cass., sez. III, 7 luglio 2010-19 ottobre 2010, n. 37197), in *Dir. pen. proc.*, 2011, 1129 ss. oppure G. Tabasco, *Corte Costituzionale e videoriprese di condotte non comunicative: ancora dubbi e perplessità*, in *Dir. pen. proc.*, 2010, 234 ss.

[38] Per un quadro aggiornato e più generale sulle problematiche processuali accennate, si vedano R. Casiraghi, *Prove vietate e processo penale*, in *Riv. it. dir. proc. pen.*, 2009, 1768 ss. e G. Illuminati, *L'inutilizzabilità della prova nel processo penale italiano*, in *Riv. it. dir. proc. pen.*, 2010, 521 ss. In chiave monografica C. Conti, *Accertamento del fatto ed inutilizzabilità nel processo penale*, Padova, Cedam, 2007 e M. Daniele, *Regole di esclusione e regole di valutazione della prova*, Torino, Giappichelli, 2009.

[39] Cass., sez. III, 17 aprile 2012-11 giugno 2012, n. 22611.

Lav. intende tutelare i lavoratori contro forme subdole di controllo della loro attività da parte del datore di lavoro e che tale rischio viene escluso in presenza di un consenso di organismi di categoria rappresentativi (RSU o commissione interna), *a fortiori*, tale consenso deve essere considerato validamente prestato quando promani proprio da tutti i dipendenti ».

L'arresto è difficilmente condivisibile.

A differenza di quanto accade con la corrispondenza elettronica, l'attività di monitoraggio attraverso le telecamere avviene per il tramite di "impianti" o "apparecchiature". Non è quindi corretto — come si legge in motivazione — che « non [risultano] esservi disposizioni di alcun tipo che disciplinino l'acquisizione del consenso ». È anzi vero proprio il contrario: il singolo lavoratore non può decidere se farsi o meno controllare, perché tale compito, *ex* art. 4 L. n. 300/1970, spetta alle RSA o alle DTL.

La norma statutaria rende quindi indisponibile il diritto soggettivo, limitando così l'applicabilità al caso di specie della scriminante di cui all'art. 50 c.p. Né — per le ragioni già esposte — può ritenersi che la facoltà di esprimere il consenso spetti alla rappresentanza sindacale interna ovvero alla diramazione territoriale del Ministero del Lavoro.

Il recente arresto, d'altronde, pare contraddire non solo la chiara lettera della legge, ma l'intero assetto di una normativa, quella giuslavoristica, tutta costruita intorno allo squilibrio contrattuale e alla conseguente incapacità del lavoratore di esprimere incondizionatamente la propria volontà.

Abstract

The article investigates employer's power to control workers' personal email exchanges. In particular, the article sheds light on the extent of such power within the limits by the Italian Constitution, by the European Convention on Human Rights and by the legislation on personal data protection. In doing so, the paper argues that the employer's right to check on personal email exchanges needs to be balanced with the workers' right to privacy regarding the content of the messages received through the personal email account.